



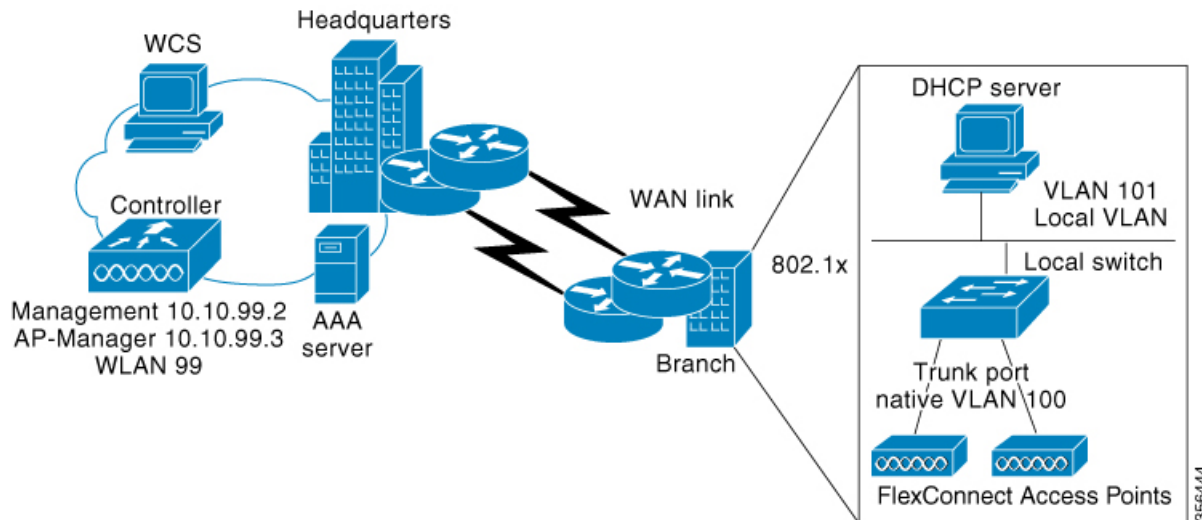
FlexConnect

- [Information About FlexConnect, on page 1](#)
- [Guidelines and Restrictions for FlexConnect, on page 5](#)
- [Configuring a Site Tag, on page 8](#)
- [Configuring a Policy Tag \(CLI\), on page 9](#)
- [Attaching a Policy Tag and a Site Tag to an Access Point \(GUI\), on page 10](#)
- [Attaching Policy Tag and Site Tag to an AP \(CLI\), on page 11](#)
- [Linking an ACL Policy to the Defined ACL \(GUI\), on page 12](#)
- [Applying ACLs on FlexConnect, on page 12](#)
- [Configuring FlexConnect, on page 13](#)
- [Flex AP Local Authentication \(GUI\), on page 19](#)
- [Flex AP Local Authentication \(CLI\), on page 20](#)
- [Flex AP Local Authentication with External Radius Server, on page 22](#)
- [Configuration Example: FlexConnect with Central and Local Authentication , on page 25](#)
- [NAT-PAT for FlexConnect, on page 25](#)
- [Split Tunneling for FlexConnect, on page 29](#)
- [VLAN-based Central Switching for FlexConnect, on page 36](#)
- [OfficeExtend Access Points for FlexConnect, on page 38](#)
- [Proxy ARP, on page 41](#)

Information About FlexConnect

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) 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 FlexConnect access points can also 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. FlexConnect access points support multiple SSIDs. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 1: FlexConnect Deployment



The controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all the clients are disconnected and are authenticated again. This functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. When both the access point and the controller have the same configuration, the connection between the clients and APs is maintained.

After the client connection is established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default or new configured values only after the session timer expires.

The controller can send multicast packets in the form of unicast or multicast packets to an access point. In FlexConnect mode, an access point can receive only multicast packets.

In Cisco Catalyst 9800 Series Wireless Controller, you can define a flex connect site. A flex connect site can have a flex connect profile associate with it. You can have a maximum of 100 access points for each flex connect site.

FlexConnect 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. FlexConnect access points also support a many-to-one NAT or PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

Workgroup bridges and Universal Workgroup bridges are supported on FlexConnect access points for locally switched clients.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to an IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

An access point does not have to reboot when moving from local mode to FlexConnect mode and vice-versa.

FlexConnect Authentication

When an 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 nonvolatile memory for use in standalone mode.



Note Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode.



Note 802.1X is not supported on the AUX port for Cisco Aironet 2700 series APs.

A FlexConnect 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.



Note OTAP is not supported.

- 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, we recommend 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.

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



Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect 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:



Note For the FlexConnect local switching, central authentication deployments, whenever passive client is enabled, the IP Learn timeout is disabled by default.

- 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 FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect 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 FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

- Policy type
- Access VLAN
- VLAN name
- Supported rates
- Encryption cipher

Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 576 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

- Notes about local authentication are as follows:
 - Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
 - Local RADIUS on the controller is not supported.
 - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected 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 FlexConnect 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. This configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or Cisco Centralized Key Management, but these authentication types require that an external RADIUS server be configured.

You can also configure a local RADIUS server on a FlexConnect access point to support 802.1X in a standalone mode or with local authentication.

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 FlexConnect 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, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.



Note A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect 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 FlexConnect.

When web-authentication is used on FlexConnect access points at a remote site, the clients get the IP address from the remote local subnet. To resolve the initial URL request, the DNS is accessible through the subnet's default gateway. In order for the controller to intercept and redirect the DNS query return packets, these packets must reach the controller at the data center through a CAPWAP connection. During the web-authentication process, the FlexConnect access points allows only DNS and DHCP messages; the access points forward the DNS reply messages to the controller before web-authentication for the client is complete. After web-authentication for the client is complete, all the traffic is switched locally.

When a FlexConnect access point enters into a standalone mode, the following occurs:

- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:

- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and allows client connectivity again.

Guidelines and Restrictions for FlexConnect

- When you apply a configuration change to a locally switched WLAN, the access point resets the radio, causing associated client devices to disassociate (including the clients that are not associated with the modified WLAN). However, this behavior does not occur if the modified WLAN is centrally switched.

We recommend that you modify the configuration only during a maintenance window. This is also applicable when a centrally switched WLAN is changed to a locally switched WLAN.

This guideline is specific to Cisco Wave 1 APs, and not for Cisco Wave 2 APs or 11AX APs.

- FlexConnect mode can support only 16 VLANs per AP.
- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the context of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to 4 fragmented packets, or a minimum 576-byte maximum transmission unit (MTU) WAN link.
- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In scenarios where you cannot achieve the 300-ms round-trip latency, configure the access point to perform local authentication.
- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode. After the access point moves, the access point's radio is also reset.
- When multiple APs come from standalone mode to connected mode on FlexConnect and all the APs send the client entry in hybrid-REAP payload to the controller. In this scenario, the controller sends disassociation messages to the WLAN client. However, the WLAN client comes back successfully and joins the controller.
- When APs are in standalone mode, if a client roams to another AP, the source AP cannot determine whether the client has roamed or is just idle. So, the client entry at source AP will not be deleted until idle timeout.
- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and the secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- 802.11r fast transition roaming is not supported on APs operating in local authentication.
- The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features, such as WLAN overrides, VLANs, static channel number, and so on, might not operate correctly. In addition, make sure you duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at the time of initialization, a few syslog packets from the access point are tagged with VLAN ID 1.
- MAC filtering is not supported on FlexConnect access points in standalone mode. However, MAC filtering is supported on FlexConnect access points in connected mode with local switching and central authentication. Also, Open SSID, MAC Filtering, and RADIUS NAC for a locally switched WLAN with FlexConnect access points is a valid configuration, where MAC is checked by Cisco ISE.
- FlexConnect does not display any IPv6 client addresses in the Client Detail window.

- FlexConnect access points with locally switched WLANs cannot perform IP source guard and prevent ARP spoofing. For centrally switched WLANs, the wireless controller performs IP source guard and ARP spoofing.
- To prevent ARP spoofing attacks in FlexConnect APs with local switching, we recommend that you use ARP inspection.
- Passive client feature is not supported on FlexConnect local switching mode.
- When you enable local switching on policy profile for FlexConnect APs, the APs perform local switching. However, for the APs in local mode, central switching is performed.

In a scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported, the client may not get the correct IP address due to VLAN difference after the move. Also, L2 and L3 roaming between FlexConnect mode AP and Local mode AP are not supported.

FlexConnect local switching is not supported on Cisco Aironet Cisco 1810T and 1815T (Teleworker) Access Points.

- Cisco Centralized Key Management (CCKM) is not supported in FlexConnect standalone mode. Hence, CCKM enabled client will not be able to connect when AP is in FlexConnect standalone mode.
- For Wi-Fi Protected Access Version 2 (WPA2) in FlexConnect standalone mode or local authentication in connected mode or Cisco Centralized Key Management fast roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or Cisco Centralized Key Management fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and Cisco Centralized Key Management fast-roaming in connected mode.
- Only 802.11r fast-transition roaming is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- AVC on locally switched WLANs is supported on second-generation APs.
- Local authentication fallback is not supported when a user is not available in the external RADIUS server.
- For WLANs configured for FlexConnect APs in local switching and local authentication, synchronization of dot11 client information is supported.
- DNS override is not supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- The Cisco Aironet 1830 Series and 1850 Series APs do not support IPv6. However, a wireless client can pass IPv6 traffic across these APs.
- VLAN group is not supported in Flex mode under flex-profile.
- Configuring maximum number of allowed media streams on individual client or radio is not supported in FlexConnect mode.
- The WLAN client association limit will not work when the AP is in FlexConnect mode (connected or standalone) and is performing local switching and local authentication.
- A local switching client on FlexConnect mode will not get IP address for RLAN profile on the Cisco Aironet 1810 Series AP.
- Standard ACL is not supported on FlexConnect AP mode.

- IPv6 RADIUS Server is not configurable for FlexConnect APs. Only IPv4 configuration is supported.
- Cisco Centralized Key Management (CCKM) is supported in wave 1 APs in FlexConnect when you use local association, but fails when you use central association.
- Using custom VLANs under the policy profile of the FlexConnect locally switched WLANs stops the SSID broadcast. In such scenarios, run the **shut** and **no shut** commands on the policy profile to start the SSID broadcast.

SSIDs are broadcasted when you:

- Perform VLAN name to id mapping under FlexConnect profile and map the custom VLAN name under the policy profile.
- Use VLAN id or standard VLAN name, for example, VLANxxxx.
- For Flex mode deployments, both local association and central association configured policy profiles are not supported at a given time on the WLAN. Only the local association command must be enabled. Ensure that central association is disabled by running the **no central association** command during configuration.
- In the FlexConnect mode, NetFlow has a performance degradation impact on the Cisco Internetwork Operating System (IOS) AP models, especially on 2700, 3700, and 1700.
- From Cisco IOS XE Amsterdam 17.1.1 release onwards, the police rate per client in the flex connect APs in the controller, is represented as **rate_out** for Ingress (input) and **rate_in** for Egress (output). To verify police rate on the flex AP, use the **show rate-limit client** command.
- Cisco Wave 2 and Catalyst Wi-Fi6 APs in FlexConnect local switching mode do not support Layer2(PSK, 802.1X) + Layer3(LWA, CWA, redirection-based posturing) + Dynamic AAA override + NAC.
- Network access control (NAC) is not supported in FlexConnect local authentication.
- Multicast traffic on an AAA overridden VLAN is not supported. Using this configuration may result in potential traffic leaks between VLANs.

Configuring a Site Tag

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless tag site <i>site-name</i> Example: Device(config)# wireless tag site default-site-tag	Configures site tag and enters site tag configuration mode.

	Command or Action	Purpose
Step 3	flex-profile <i>flex-profile-name</i> Example: Device(config-site-tag)# flex-profile rr-xyz-flex-profile	Maps a flex profile to a site tag.
Step 4	ap-profile <i>ap-profile</i> Example: Device(config-site-tag)# ap-profile xyz-ap-profile	Assigns an AP profile to the wireless site.
Step 5	description <i>site-tag-name</i> Example: Device(config-site-tag)# description "default site tag"	Adds a description for the site tag.
Step 6	no local-site Example: Device(config-site-tag)# no local-site	Moves the access point to FlexConnect mode.
Step 7	end Example: Device(config-site-tag)# end	Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.
Step 8	show wireless tag site summary Example: Device# show wireless tag site summary	(Optional) Displays the summary of site tags.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	wireless tag policy <i>policy-tag-name</i> Example: <pre>Device(config-policy-tag)# wireless tag policy default-policy-tag</pre>	Configures policy tag and enters policy tag configuration mode. Note When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	description <i>description</i> Example: <pre>Device(config-policy-tag)# description "default-policy-tag"</pre>	Adds a description to a policy tag.
Step 5	remote-lan <i>name</i> policy profile-policy-name {ext-module port-id } Example: <pre>Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2</pre>	Maps a remote-LAN profile to a policy profile.
Step 6	wlan <i>wlan-name</i> policy profile-policy-name Example: <pre>Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1</pre>	Maps a policy profile to a WLAN profile.
Step 7	end Example: <pre>Device(config-policy-tag)# end</pre>	Exits policy tag configuration mode, and returns to privileged EXEC mode.
Step 8	show wireless tag policy summary Example: <pre>Device# show wireless tag policy summary</pre>	(Optional) Displays the configured policy tags. Note To view detailed information about a policy tag, use the show wireless tag policy detailed <i>policy-tag-name</i> command.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

-
- Step 1** Choose **Configuration > Wireless > Access Points**.
 - Step 2** Click the **Access Point** name.
 - Step 3** Go to the **Tags** section.
 - Step 4** Choose the **Policy Tag** from the **Policy** drop-down list.

- Step 5** Choose the **Site Tag** from the **Site** drop-down list.
- Step 6** Click **Update and Apply to Device**.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ap mac-address Example: Device(config)# ap F866.F267.7DFB	Configures a Cisco AP and enters AP profile configuration mode. Note The <i>mac-address</i> should be a wired mac address.
Step 3	policy-tag policy-tag-name Example: Device(config-ap-tag)# policy-tag rr-xyz-policy-tag	Maps a policy tag to the AP.
Step 4	site-tag site-tag-name Example: Device(config-ap-tag)# site-tag rr-xyz-site	Maps a site tag to the AP.
Step 5	rf-tag rf-tag-name Example: Device(config-ap-tag)# rf-tag rf-tag1	Associates the RF tag.
Step 6	end Example: Device(config-ap-tag)# end	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	show ap tag summary Example: Device# show ap tag summary	(Optional) Displays AP details and the tags associated to it.
Step 8	show ap name <ap-name> tag info Example: Device# show ap name ap-name tag info	(Optional) Displays the AP name with tag information.

	Command or Action	Purpose
Step 9	show ap name <ap-name> tag detail Example: Device# show ap name ap-name tag detail	(Optional) Displays the AP name with tag details.

Linking an ACL Policy to the Defined ACL (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Flex**.
 - Step 2** Click **Add**.
 - Step 3** In the **General** tab, enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
 - Step 4** In the **Policy ACL** tab, click **Add**.
 - Step 5** Select the ACL from the **ACL Name** drop-down list and click **Save**.
 - Step 6** Click **Apply to Device**.
-

Applying ACLs on FlexConnect

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile flex flex-profile-name Example: Device(config)# wireless profile flex Flex-profile-1	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	acl-policy acl-policy-name Example: Device(config-wireless-flex-profile)# acl-policy ACL1	Configures an ACL policy. Access control lists (ACLs) perform packet filtering to control the movement of packets through a network.
Step 4	exit Example:	Returns to wireless flex profile configuration mode.

	Command or Action	Purpose
	Device(config-wireless-flex-profile-acl)# exit	
Step 5	native-vlan-id Example: Device(config-wireless-flex-profile)# native-vlan-id 25	Configures native vlan-id information.
Step 6	vlan <i>vlan-name</i> Example: Device(config-wireless-flex-profile)# vlan-name VLAN0169	Configures a VLAN.
Step 7	acl <i>acl-name</i> Example: Device(config-wireless-flex-profile-vlan)# acl ACL1	Configures an ACL for the interface.
Step 8	vlan-id <i>vlan-id</i> Example: Device(config-wireless-flex-profile-vlan)# vlan-id 169	Configures VLAN information.

Configuring FlexConnect

Configuring a Switch at a Remote Site

Procedure

-
- Step 1** Attach the access point, which will be enabled for FlexConnect, to a trunk or access port on the switch.
- Note** The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.
- Step 2** The following example configuration shows you how to configure a switch to support a FlexConnect access point.
- In this sample configuration, the FlexConnect access point is connected to the 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 or resources on VLAN 101. A DHCP pool is created in the local switch for both the VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

·
·

```

.
ip dhcp pool NATIVE
  network 209.165.200.224 255.255.255.224
  default-router 209.165.200.225
  dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
  network 209.165.201.224 255.255.255.224
  default-router 209.165.201.225
  dns-server 192.168.100.167
!
interface Gig1/0/1
  description Uplink port
  no switchport
  ip address 209.165.202.225 255.255.255.224
!
interface Gig1/0/2
  description the Access Point port
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 100
  switchport trunk allowed vlan 101
  switchport mode trunk
!
interface Vlan100
  ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
  ip address 209.165.201.225 255.255.255.224
end
!
.
.
.

```

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN
- Locally switched WLAN

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. This table shows three WLAN scenarios.

Table 1: WLAN Scenarios

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Employee	WPA1+WPA2	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched GUEST VLAN)

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Guest-central	Web authentication	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Configuring Local Switching in FlexConnect Mode (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** On the **Policy Profile** page, click the name of a policy profile to edit it or click **Add** to create a new one.
- Step 3** In the **Add/Edit Policy Profile** window that is displayed, uncheck the **Central Switching** and the **Central Association** check boxes.
- Step 4** Click **Update & Apply to Device**.
-

Configuring Local Switching in FlexConnect Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example: Device(config)# wireless profile policy rr-xyz-policy-1	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	no central switching Example: Device(config-wireless-policy)# no central switching	Configures the WLAN for local switching.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Central Switching in FlexConnect Mode (GUI)

Before you begin

Ensure that the policy profile is configured. If the policy profile is not configured, see *Configuring a Policy Profile (GUI)* section.

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
 - Step 2** On the **Policy Profile** page, select a policy.
 - Step 3** In the **Edit Policy Profile** window, in General Tab, use the slider to enable or disable **Central Switching**.
 - Step 4** Click **Update & Apply to Device**.
-

Configuring Central Switching in FlexConnect Mode

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy profile-policy Example: Device(config)# wireless profile policy rr-xyz-policy-1	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	central switching Example: Device(config-wireless-policy)# central switching	Configures the WLAN for central switching.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring an Access Point for FlexConnect

For more information, see *Configuring a Site Tag (CLI)* topic in New Configuration Model chapter.

Configuring an Access Point for Local Authentication on a WLAN (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
 - Step 2** In the **Policy Profile** page, select a policy profile name. The **Edit Policy Profile** window is displayed.
 - Step 3** In the General tab, deselect **Central Authentication** check box.
 - Step 4** Click **Update & Apply to Device**.
-

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example: Device(config)# <code>wireless profile policy rr-xyz-policy-1</code>	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	no central authentication Example: Device(config-wireless-policy)# <code>no central authentication</code>	Configures the WLAN for local authentication.
Step 4	end Example: Device(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created, as specified in the [#unique_137](#).

In the example scenarios (see [#unique_137](#)), there are three profiles on the client:

1. To connect to the *employee* WLAN, create a client profile that uses WPA or WPA2 with PEAP-MSCHAPV2 authentication. After the client is authenticated, the client is allotted an IP address by the management VLAN of the controller.

2. To connect to the *local-employee* WLAN, create a client profile that uses WPA or WPA2 authentication. After the client is authenticated, the client is allotted an IP address by VLAN 101 on the local switch.
3. To connect to the *guest-central* WLAN, create a client profile that uses open authentication. After the client is authenticated, the client is allocated an IP address by VLAN 101 on the network local to the access point. After the client connects, a local user can enter 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 window appears, the user should enter the username and password.

Configuring FlexConnect Ethernet Fallback

Information About FlexConnect Ethernet Fallback

You can configure an AP to shut down its radio when the Ethernet link is not operational. When the Ethernet link comes back to operational state, you can configure the AP to set its radio back to operational state. This feature is independent of the AP being in connected or standalone mode. When the radios are shut down, the AP does not broadcast the WLANs, and therefore, the clients cannot connect to the AP, either through first association or through roaming.

Configuring FlexConnect Ethernet Fallback

Before you begin

This feature is not applicable to APs with multiple ports.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile flex flex-profile-name Example: Device(config)# wireless profile flex test	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	fallback-radio-shut Example: Device(config-wireless-flex-profile)# fallback-radio-shut	Enables radio interface shutdown.
Step 4	end Example: Device(config-wireless-flex-profile)# end	Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show wireless profile flex detailed <i>flex-profile-name</i> Example: Device# show wireless profile flex detailed test	(Optional) Displays detailed information about the selected profile.

Flex AP Local Authentication (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Flex**.

Step 2 In the **Flex** page, click the name of the **Flex Profile** or click **Add** to create a new one.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Local Authentication** tab.

When local authentication and association is enabled in Access Point with Flex mode, the following occurs:

- AP handles the authentication.
- AP handles the rejection of client joins (in Mobility).

Note The controller does not increment statistics when AP rejects client association.

Step 4 Choose the server group from the **RADIUS Server Group** drop-down list.

Step 5 Use the **Local Accounting RADIUS Server Group** drop down to select the RADIUS server group.

Step 6 Check the **Local Client Roaming** check box to enable client roaming.

Step 7 Choose the profile from the **EAP Fast Profile** drop-down list.

Step 8 Choose to enable or disable the following:

- LEAP: Lightweight Extensible Authentication Protocol (LEAP) is an 802.1X authentication type for wireless LANs and supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.
- PEAP: Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- TLS: Transport Layer Security (TLS) is a cryptographic protocol that provide communications security over a computer network.
- RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

Step 9 In the **Users** section, click **Add**.

Step 10 Enter username and password details and click **Save**.

Step 11 Click **Save & Apply to Device**.

Flex AP Local Authentication (CLI)



Note The Cisco Catalyst 9800 Series Wireless Controller + FlexConnect local authentication + AP acting as RADIUS are not supported on Cisco COS and IOS APs.

Procedure

	Command or Action	Purpose
Step 1	aaa new-model Example: Device (config) # aaa new-model	Creates a AAA authentication model.
Step 2	aaa session-id common Example: Device (config) # aaa session-id common	Ensures that all the session IDs information that is sent out from the RADIUS group for a given call are identical.
Step 3	dot1x system-auth-control Example: Device (config) # dot1x system-auth-control	Enables system authorization control for the RADIUS group.
Step 4	eap profile <i>name</i> Example: Device (config) # eap profile alocal-test	Creates an EAP profile.
Step 5	method fast Example: Device (config-eap-profile) # method fast	Configures the FAST method on the profile.
Step 6	exit Example: Device (config-radius-server) # exit	Returns to configuration mode.
Step 7	wireless profile flex <i>flex-profile</i> Example: Device (config) # wireless profile flex default-flex-profile	Configures the flex policy.
Step 8	local-auth ap eap-fast <i>name</i> Example:	Configures EAP-FAST profile details.

	Command or Action	Purpose
	Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test	
Step 9	local-auth ap leap Example: Device(config-wireless-flex-profile)# local-auth ap leap	Configures the LEAP method.
Step 10	local-auth ap peap Example: Device(config-wireless-flex-profile)# local-auth ap peap	Configures the PEAP method.
Step 11	local-auth ap username <i>username</i> Example: Device(config-wireless-flex-profile)# local-auth ap username test1 test1	Configures username and password.
Step 12	local-auth ap username <i>username password</i> Example: Device(config-wireless-flex-profile)# local-auth ap username test2 test2	Configures another username and password.
Step 13	exit Example: Device(config-wireless-flex-profile)# exit	Returns to configuration mode.
Step 14	wireless profile policy <i>policy-profile</i> Example: Device(config)# wireless profile policy default-policy-profile	Configures profile policy.
Step 15	shutdown Example: Device(config-wireless-policy)# shutdown	Disables the policy profile.
Step 16	no central authentication Example: Device(config)# no central authentication	Disables central (controller) authentication.
Step 17	vlan-id <i>vlan-id</i> Example: Device(config)# vlan-id 54	Configures VLAN name or VLAN ID.

	Command or Action	Purpose
Step 18	no shutdown Example: Device(config)# no shutdown	Enables the configuration.

Flex AP Local Authentication with External Radius Server

In this mode, an access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

Procedure

	Command or Action	Purpose
Step 1	aaa new-model Example: Device(config)# aaa new-model	Creates a AAA authentication model.
Step 2	aaa session-id common Example: Device(config)# aaa session-id common	Ensures that all the session ID's information that is sent out, from the RADIUS group for a given call are identical.
Step 3	dot1x system-auth-control Example: Device(config)# dot1x system-auth-control	Enables the system authorization control for the RADIUS group.
Step 4	radius server <i>server-name</i> Example: Device(config)# radius server Test-SERVER1	Specifies the RADIUS server name. Note To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the crypto key generate rsa general-keys exportable label <i>name</i> command to achieve this. Do not configure key-wrap option under the radius server and radius server group, as it may lead to clients getting stuck in authentication state.
Step 5	address {ipv4 ipv6} ip address {auth-port port-number acct-port port-number } Example:	Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
	<pre>Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113 Device(config-radius-server)# address ipv6 2001:DB8:0:20::15 auth-port 1812 acct-port 1813</pre>	
Step 6	<p>key string</p> <p>Example:</p> <pre>Device(config-radius-server)# key test123</pre>	<p>Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.</p> <p>Note The maximum number of characters allowed for the shared secret is 63.</p>
Step 7	<p>radius server server-name</p> <p>Example:</p> <pre>Device(config)# radius server Test-SERVER2</pre>	Specifies the RADIUS server name.
Step 8	<p>address {ipv4 ipv6} ip address {auth-port port-number acct-port port-number }</p> <p>Example:</p> <pre>Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113 Device(config-radius-server)# address ipv6 2001:DB8:0:21::15 auth-port 1812 acct-port 1813</pre>	Specifies the secondary RADIUS server parameters.
Step 9	<p>key string</p> <p>Example:</p> <pre>Device(config-radius-server)# key test113</pre>	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.
Step 10	<p>exit</p> <p>Example:</p> <pre>Device(config-radius-server)# exit</pre>	Returns to configuration mode.
Step 11	<p>aaa group server radius server-group</p> <p>Example:</p> <pre>Device(config)# aaa group server radius aaa_group_name</pre>	<p>Creates a RADIUS server group identification.</p> <p>Note <i>server-group</i> refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.</p>
Step 12	<p>radius server server-name</p> <p>Example:</p> <pre>Device(config)# radius server Test-SERVER1</pre>	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 13	radius server <i>server-name</i> Example: Device(config-radius-server)# radius server Test-SERVER2	Specifies the RADIUS server name.
Step 14	exit Example: Device(config-radius-server)# exit	Exit from RADIUS server configuration mode.
Step 15	wireless profile flex <i>flex-profile</i> Example: Device(config)# wireless profile flex default-flex-profile	Creates a new flex policy.
Step 16	local-auth radius-server-group <i>server-group</i> Example: Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name	Configures the authentication server group name.
Step 17	exit Example: Device(config-wireless-flex-profile)# exit	Returns to configuration mode.
Step 18	wireless profile policy <i>policy-profile</i> Example: Device(config)# wireless profile policy default-policy-profile	Configures a WLAN policy profile.
Step 19	shutdown Example: Device(config-wireless-policy)# shutdown	Disables a policy profile.
Step 20	no central authentication Example: Device(config-wireless-policy)# no central authentication	Disables central (controller) authentication.
Step 21	vlan-id <i>vlan-id</i> Example: Device(config-wireless-policy)# vlan-id 54	Configures a VLAN name or VLAN Id.
Step 22	no shutdown Example:	Enables the configuration.

	Command or Action	Purpose
	Device(config-wireless-policy)# no shutdown	

Configuration Example: FlexConnect with Central and Local Authentication

To see configuration example on how to configure a controller for FlexConnect central and local authentication, see the [FlexConnect Configuration with Central and Local Authentication on Catalyst 9800 Wireless Controllers](#) document.

NAT-PAT for FlexConnect

If you want to use a central DHCP server to service clients across remote sites, NAT-PAT should be enabled. An AP translates the traffic coming from a client and replaces the client's IP address with its own IP address.



Note You must enable local switching, central DHCP, and DHCP required using the (**ipv4 dhcp required**) command to enable NAT and PAT.

Configuring NAT-PAT for a WLAN or a Remote LAN

Creating a WLAN

Follow the steps given here to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wlan wlan-name wlan-id SSID-name Example: Device(config)# wlan wlan-demo 1 ssid-demo	Enters the WLAN configuration sub-mode. <ul style="list-style-type: none"> • <i>wlan-name</i>—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • <i>wlan-id</i>—Enter the WLAN ID. The range is from 1 to 512. • <i>SSID-name</i>—Enter the Service Set Identifier (SSID) for this WLAN. If the

	Command or Action	Purpose
		SSID is not specified, the WLAN profile name is set as the SSID. Note If you have already configured WLAN, enter <i>wlan wlan-name</i> command.
Step 3	no shutdown Example: Device(config-wlan)# no shutdown	Shut down the WLAN.
Step 4	end Example: Device(config-wlan)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring a Wireless Profile Policy and NAT-PAT (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
 - Step 2** Click **Add**.
 - Step 3** In the **General** tab, enter the **Name** of the policy.
 - Step 4** Disable the **Central Switching** toggle button.
 - Step 5** Enable the **Central DHCP** toggle button.
 - Step 6** Enable the **Flex NAT/PAT** toggle button.
 - Step 7** In the **Advanced** tab, under the **DHCP Settings**, check the **IPv4 DHCP Required** check box.
 - Step 8** Click **Apply to Device**.
-

Configuring a Wireless Profile Policy and NAT-PAT

Follow the procedure given below to configure a wireless profile policy and NAT-PAT:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example:	Configures the policy profile for NAT.

	Command or Action	Purpose
	<code>Device(config)# wireless profile policy nat-enabled-policy</code>	
Step 3	no central switching Example: <code>Device(config-wireless-policy)# no central switching</code>	Configures the WLAN for local switching.
Step 4	ipv4 dhcp required Example: <code>Device(config-wireless-policy)# ipv4 dhcp required</code>	Configures the DHCP parameters for WLAN.
Step 5	central dhcp Example: <code>Device(config-wireless-policy)# central dhcp</code>	Configures the central DHCP for locally switched clients.
Step 6	flex nat-pat Example: <code>Device(config-wireless-policy)# flex nat-pat</code>	Enables NAT-PAT.
Step 7	no shutdown Example: <code>Device(config-wireless-policy)# no shutdown</code>	Enables policy profile.
Step 8	end Example: <code>Device(config-wireless-policy)# end</code>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Mapping a WLAN to a Policy Profile

Follow the procedure given below to map a WLAN to a policy profile:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>Device# configure terminal</code>	Enters global configuration mode.
Step 2	wireless tag policy <i>policy-tag-name</i> Example: <code>Device(config)# wireless tag policy demo-tag</code>	Configures a policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
Step 3	wlan <i>wlan-name</i> policy <i>profile-policy-name</i> Example: Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy	Maps a policy profile to a WLAN profile.
Step 4	end Example: Device(config-policy-tag)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless tag site <i>site-name</i> Example: Device(config)# wireless tag site flex-site	Configures a site tag and enters site tag configuration mode.
Step 3	no local-site Example: Device(config-site-tag)# no local-site	Moves an access point to FlexConnect mode.
Step 4	end Example: Device(config-site-tag)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

- Step 1** Choose **Configuration > Wireless > Access Points**.
- Step 2** Click the **Access Point** name.
- Step 3** Go to the **Tags** section.
- Step 4** Choose the **Policy Tag** from the **Policy** drop-down list.
- Step 5** Choose the **Site Tag** from the **Site** drop-down list.

Step 6 Click **Update and Apply to Device**.

Attaching a Policy Tag and a Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and a site tag to an access point:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ap mac-address Example: Device(config)# ap F866.F267.7DFB	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	policy-tag policy-tag-name Example: Device(config-ap-tag)# policy-tag demo-tag	Maps a policy tag to the AP.
Step 4	site-tag site-tag-name Example: Device(config-ap-tag)# site-tag flex-site	Maps a site tag to the AP.
Step 5	end Example: Device(config-ap-tag)# end	Returns to privileged EXEC mode.

Split Tunneling for FlexConnect

If a client that connects over a WAN link that is associated with a centrally switched WLAN has to send traffic to a device present in the local site, this traffic should be sent over CAPWAP to the controller, and the same traffic is sent back to the local site either over CAPWAP or with the help of some off-band connectivity.

This process consumes WAN link bandwidth unnecessarily. To avoid this, you can use the Split Tunneling feature, which allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic, and the rest of the traffic as centrally switched.

To configure local split tunneling on an AP, ensure that you have enabled DHCP Required on the policy profile using the (**ipv4 dhcp required**) command. This ensures that the client that is associating with the split WLAN does DHCP.



Note Apple iOS clients need option 6 (DNS) to be set in DHCP offer for split tunneling to work.



-
- Note**
- FlexConnect split tunneling (vlan-based central switching for FlexConnect) on auto-anchor deployment is not supported.
 - Split tunneling does not work on RLAN clients. When the **split-tunnel** option is enabled on RLAN, traffic denied by the split tunnel ACL is not translated based on the IP address, instead the traffic is sent back to the controller through CAPWAP.
 - URL filter must not be configured with wildcard URLs such as * and *.*.
-

Configuring Split Tunneling for a WLAN or Remote LAN

Defining an Access Control List for Split Tunneling (GUI)

Procedure

- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** Click **Add**.
- Step 3** In the **Add ACL Setup** dialog box, enter the **ACL Name**.
- Step 4** Choose the ACL type from the **ACL Type** drop-down list.
- Step 5** Under the **Rules** settings, enter the **Sequence** number and choose the **Action** as either **permit** or **deny**.
- Step 6** Choose the required source type from the **Source Type** drop-down list.
- If you choose the source type as **Host**, then you must enter the **Host Name/IP**.
 - If you choose the source type as **Network**, then you must specify the **Source IP** address and **Source Wildcard** mask.
- Step 7** Check the **Log** check box if you want the logs.
- Step 8** Click **Add**.
- Step 9** Add the rest of the rules and click **Apply to Device**.
-

Defining an Access Control List for Split Tunneling

Follow the procedure given below to define an Access Control List (ACL) for split tunneling:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ip access-list extended <i>name</i> Example: Device(config)# ip access-list extended split_mac_acl	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	deny ip any host <i>hostname</i> Example: Device(config-ext-nacl)# deny ip any host 9.9.2.21	Allows the traffic to switch centrally.
Step 4	permit ip any any Example: Device(config-ext-nacl)# permit ip any any	Allows the traffic to switch locally.
Step 5	end Example: Device(config-ext-nacl)# end	Exits configuration mode and returns to privileged EXEC mode.

Linking an ACL Policy to the Defined ACL

Follow the procedure given below to link an ACL policy to the defined ACL:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile flex <i>flex-profile</i> Example: Device(config)# wireless profile flex flex-profile	Configures the Flex profile and enters flex profile configuration mode.
Step 3	acl-policy <i>acl policy name</i> Example: Device(config-wireless-flex-profile)# acl-policy split_mac_acl	Configures an ACL policy for the defined ACL.

	Command or Action	Purpose
Step 4	end Example: Device(config-wireless-flex-profile)# end	Exits configuration mode and returns to privileged EXEC mode.

Creating a WLAN

Follow the procedure given below to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wlan wlan-name wlan-id SSID-name Example: Device(config)# wlan wlan-demo 1 ssid-demo	Specifies the WLAN name and ID: <ul style="list-style-type: none"> • <i>wlan-name</i>—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • <i>wlan-id</i>—Enter the WLAN ID. The range is from 1 to 512. • <i>SSID-name</i>—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 3	no shutdown Example: Device(config-wlan)# no shutdown	Enables the WLAN.
Step 4	end Example: Device(config-wlan)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI)

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** Click **Add**.
- Step 3** In the **General** tab, enter the **Name** of the policy.

- Step 4** Enable the **Central Switching** toggle button.
- Step 5** Enable the **Central DHCP** toggle button.
- Step 6** In the **Advanced** tab, under the **DHCP** settings, check the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.
- Step 7** Under the **WLAN Flex Policy** settings, choose the split MAC ACL from the **Split MAC ACL** drop-down list.
- Step 8** Click **Apply to Device**.

Configuring a Wireless Profile Policy and a Split MAC ACL Name

Follow the procedure given below to configure a wireless profile policy and a split MAC ACL name:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example: Device(config)# wireless profile policy split-tunnel-enabled-policy	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	flex split-mac-acl <i>split-mac-acl-name</i> Example: Device(config-wireless-policy)# flex split-mac-acl split_mac_acl	Configures a split MAC ACL name. Note You should use the same ACL name for linking the flex and the policy profile.
Step 4	central switching Example: Device(config-wireless-policy)# central switching	Configures WLAN for central switching.
Step 5	central dhcp Example: Device(config-wireless-policy)# central dhcp	Enables central DHCP for centrally switched clients.
Step 6	ipv4 dhcp required Example: Device(config-wireless-policy)# ipv4 dhcp required	Configures the DHCP parameters for a WLAN.
Step 7	ipv4 dhcp server <i>ip_address</i> Example:	Configures the override IP address of the DHCP server.

	Command or Action	Purpose
	Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100	
Step 8	no shutdown Example: Device(config-wireless-policy)# no shutdown	Enables a policy profile.

Mapping a WLAN to a Policy Profile (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
 - Step 2** Click **Add**.
 - Step 3** Enter the **Name** of the Tag Policy.
 - Step 4** Under **WLAN-POLICY Maps** tab, click **Add**.
 - Step 5** Choose the WLAN Profile from the **WLAN Profile** drop-down list.
 - Step 6** Choose the Policy Profile from the **Policy Profile** drop-down list.
 - Step 7** Click the **Tick Icon**.
 - Step 8** Click **Apply to Device**.
-

Mapping WLAN to a Policy Profile

Follow the procedure given below to map WLAN to a policy profile.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless tag policy <i>policy-tag-name</i> Example: Device(config)# wireless tag policy split-tunnel-enabled-tag	Configures a policy tag and enters policy tag configuration mode.
Step 3	wlan <i>wlan-name</i> policy <i>profile-policy-name</i> Example: Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy	Maps a policy profile to a WLAN profile.

	Command or Action	Purpose
Step 4	end Example: Device(config-policy-tag) # end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless tag site <i>site-name</i> Example: Device(config) # wireless tag site flex-site	Configures a site tag and enters site tag configuration mode.
Step 3	no local-site Example: Device(config-site-tag) # no local-site	Local site is not configured on the site tag.
Step 4	flex-profile <i>flex-profile-name</i> Example: Device(config-site-tag) # flex-profile flex-profile	Configures a flex profile.
Step 5	end Example: Device(config-site-tag) # end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Attaching a Policy Tag and Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and site tag to an access point.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	ap <i>ethernet-mac-address</i> Example: Device(config)# ap 188b.9dbe.6eac	Configures an AP and enters ap tag configuration mode.
Step 3	policy-tag <i>policy-tag-name</i> Example: Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag	Maps a policy tag to an AP.
Step 4	site-tag <i>site-tag-name</i> Example: Device(config-ap-tag)# site-tag flex-site	Maps a site tag to an AP.
Step 5	end Example: Device(config-ap-tag)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

VLAN-based Central Switching for FlexConnect

In FlexConnect local switching, if the VLAN definition is not available in an access point, the corresponding client does not pass traffic. This scenario is applicable when the AAA server returns the VLAN as part of client authentication.

When a WLAN is locally switched in flex and a VLAN is configured on the AP side, the traffic is switched locally. When a VLAN is not defined in an AP, the VLAN drops the packet.

When VLAN-based central switching is enabled, the corresponding AP tunnels the traffic back to the controller. The controller then forwards the traffic to its corresponding VLAN.



Note

- For VLAN-based central switching, ensure that VLAN is defined on the controller.
- VLAN-based central switching is not supported by mac filter.
- For local switching, ensure that VLAN is defined on the policy profile and FlexConnect profile.
- VLAN-based central switching with central web authentication enabled in Flex profile is not supported.

Configuring VLAN-based Central Switching (GUI)

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Policy**.

- Step 2** Click the name of the policy profile.
- Step 3** In the **Edit Policy Profile** window, perform these tasks:
- Set **Central Switching** to **Disabled** state.
 - Set **Central DHCP** to **Disabled** state.
 - Set **Central Authentication** to **Enabled** state.
- Step 4** Click the **Advanced** tab.
- Step 5** Under **AAA Policy**, check the **Allow AAA Override** check box to enable AAA override.
- Step 6** Under **WLAN Flex Policy**, check the **VLAN Central Switching** check box, to enable VLAN-based central switching on the policy profile.
- Step 7** Click **Update & Apply to Device**.

Configuring VLAN-based Central Switching (CLI)

Follow the procedure given below to configure VLAN-based central switching.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example: Device(config)# wireless profile policy default-policy-profile	Configures a wireless policy profile.
Step 3	no central switching Example: Device(config-wireless-policy)# no central switching	Configures a WLAN for local switching.
Step 4	no central dhcp Example: Device(config-wireless-policy)# no central dhcp	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 5	central authentication Example: Device(config-wireless-policy)# central authentication	Configures a WLAN for central authentication.
Step 6	aaa-override Example:	Configures AAA policy override.

	Command or Action	Purpose
	Device(config-wireless-policy)# aaa-override	
Step 7	flex vlan-central-switching Example: Device(config-wireless-policy)# flex vlan-central-switching	Configures VLAN-based central switching.
Step 8	end Example: Device(config-wireless-policy)# end	Returns to privileged EXEC mode.
Step 9	show wireless profile policy detailed <i>default-policy-profile</i> Example: Device# show wireless profile policy detailed default-policy-profile	(Optional) Displays detailed information of the policy profile.

OfficeExtend Access Points for FlexConnect

A Cisco OfficeExtend access point (OEAP) provides secure communications from a controller to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. A 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 an access point and the controller ensures that all communications have the highest level of security.



Note Preconfigure the controller IP for a zero-touch deployment with OEAP. All other home users can use the same access point to connect for home use by configuring the local SSID from AP.



Note In releases prior to Cisco IOS XE Amsterdam 17.3.2, when an AP is converted to OEAP, the local DHCP server on the AP is enabled by default. If the DHCP server on home router has a similar configuration, a network conflict occurs and AP will not be able to join back to the controller. In such a scenario, we recommend that you change the default DHCP server on the Cisco AP using OEAP GUI.



Note In Cisco OfficeExtend access point (Cisco OEAP), if the OEAP local DHCP server is enabled and the user configures DNS IP from OEAP GUI, the wireless and wired clients connected to Cisco OEAP will receive that IP as DNS server IP in DHCP ACK.

Configuring OfficeExtend Access Points

Follow the procedure given below to configure OfficeExtend access points.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	wireless profile flex <i>flex-profile-name</i> Example: Device(config)# <code>wireless profile flex test</code>	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	office-extend Example: Device(config-wireless-flex-profile)# <code>office-extend</code>	Enables the OfficeExtend AP mode for a FlexConnect AP.
Step 4	end Example: Device(config-wireless-flex-profile)# <code>end</code>	Exits configuration mode and returns to privileged EXEC mode. Note After creating a flex profile, ensure that OEAP is in flex connect mode and mapped to its corresponding site tag. OfficeExtend is disabled by default. To clear the access point's configuration and return it to the factory-defaults, use the clear ap config cisco-ap command.

Disabling OfficeExtend Access Point

Follow the procedure given below to disable an OfficeExtend access point.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	wireless profile flex <i>flex-profile-name</i> Example: Device(config)# wireless profile flex test	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	no office-extend Example: Device(config-wireless-flex-profile)# no office-extend	Disables OfficeExtend AP mode for a FlexConnect AP.
Step 4	end Example: Device(config-wireless-flex-profile)# end	Exits configuration mode and returns to privileged EXEC mode.

Clearing Personal SSID from an OfficeExtend Access Point

To clear the personal SSID from an access point, run the following command:

```
ap name Cisco_AP clear-personal-ssid
```

Example: Viewing OfficeExtend Configuration

This example displays an OfficeExtend configuration:

```
Device# show ap config general

Cisco AP Name      : ap_name
=====

Cisco AP Identifier      : 70db.986d.a860
Country Code           : Multiple Countries : US,IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-ABDN
AP Country Code        : US - United States
AP Regulatory Domain
  Slot 0                : -A
  Slot 1                : -D
MAC Address            : 002c.c899.7b84
IP Address Configuration : DHCP
IP Address             : 9.9.48.51
IP Netmask             : 255.255.255.0
Gateway IP Address     : 9.9.48.1
CAPWAP Path MTU       : 1485
Telnet State          : Disabled
SSH State             : Disabled
Jumbo MTU Status      : Disabled
Cisco AP Location     : default location
Site Tag Name         : flex-site
RF Tag Name           : default-rf-tag
Policy Tag Name       : split-tunnel-enabled-tag
AP join Profile       : default-ap-profile
Primary Cisco Controller Name : uname-controller
Primary Cisco Controller IP Address : 9.9.48.34
```



```

Secondary Cisco Controller Name      : uname-controller1
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name       : uname-ewlc2
Tertiary Cisco Controller IP Address  : 0.0.0.0
Administrative State                 : Enabled
Operation State                      : Registered
AP Mode                              : FlexConnect
AP Submode                           : Not Configured
Office Extend Mode                   : Enabled
Remote AP Debug                      : Disabled
Logging Trap Severity Level          : information
Software Version                     : 16.8.1.1
Boot Version                         : 1.1.2.4
Mini IOS Version                     : 0.0.0.0
Stats Reporting Period               : 0
LED State                            : Enabled
PoE Pre-Standard Switch              : Disabled
PoE Power Injector MAC Address       : Disabled
Power Type/Mode                      : PoE/Full Power (normal mode)

```

Proxy ARP

Proxy address resolution protocol (ARP) is the most common method for learning about MAC address through a proxy device. Enabling Proxy ARP known as ARP caching in Cisco Catalyst 9800 Series Wireless Controller means that the AP owning client is the destination of the ARP request, replies on behalf of that client and therefore does not send the ARP request to the client over the air. Access points not owning the destination client and receiving an ARP request through their wired connection will drop the ARP request. When the ARP caching is disabled, the APs bridge the ARP requests from wired-to-wireless and vice-versa increasing the air time usage and broadcasts over wireless.

The AP acts as an ARP proxy to respond to ARP requests on behalf of the wireless clients.

Enabling Proxy ARP for FlexConnect APs (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > Flex**.
 - Step 2** Click **Add**.
 - Step 3** In the **General** tab, enter the **Name** of the Flex Profile and check the **ARP Caching** check box. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
 - Step 4** Click **Apply to Device**.
-

Enabling Proxy ARP for FlexConnect APs

Follow the procedure given below to configure proxy ARP for FlexConnect APs.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile flex <i>flex-policy</i> Example: Device(config)# wireless profile flex flex-test	Configures WLAN policy profile and enters wireless flex profile configuration mode.
Step 3	arp-caching Example: Device(config-wireless-flex-profile)# arp-caching	Enables ARP caching. Note Use the no arp-caching command to disable ARP caching.
Step 4	end Example: Device(config-wireless-flex-profile)# end	Returns to privileged EXEC mode.
Step 5	show running-config section wireless profile flex Example: Device# show running-config section wireless profile flex	Displays ARP configuration information.
Step 6	show wireless profile flex detailed <i>flex-profile-name</i> Example: Device# show wireless profile flex detailed flex-test	(Optional) Displays detailed information of the flex profile.
Step 7	show arp summary Example: Device# show arp summary	(Optional) Displays ARP summary.