FlexConnect

FlexConnect Overview

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 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. In the connected mode, the FlexConnect access point can also perform local authentication.

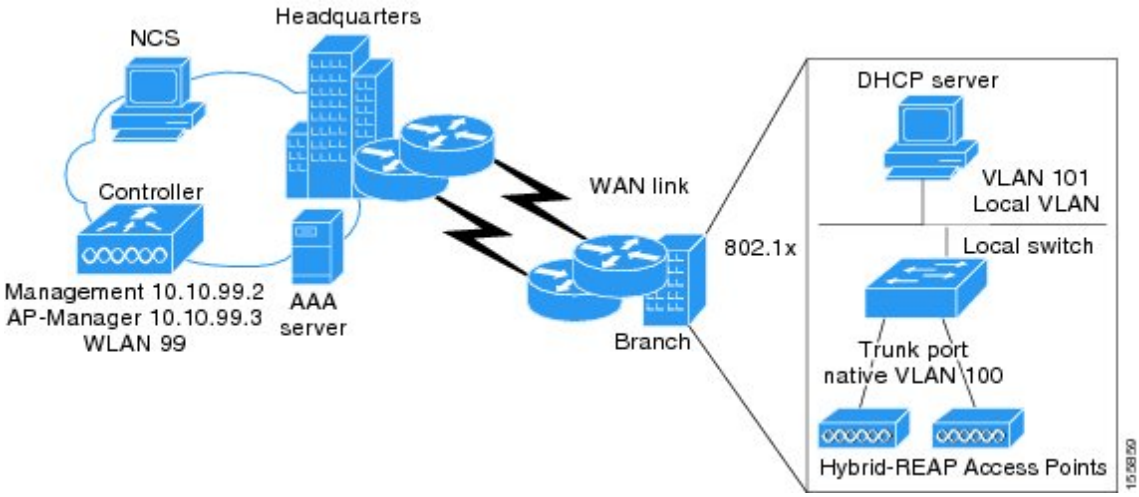
A FlexConnect AP can, on a per-WLAN basis, either tunnel client data in CAPWAP to the controller (called Central Switching), or have client data egress at the AP's LAN port (called Local Switching). With Locally Switched WLANs, the AP can tag client traffic in separate VLANs, to segregate the traffic from its management interface.

For a Locally Switched WLAN, the client authentication can either be handled by the controller (Central Authentication) or by the AP (Local Authentication).

If a FlexConnect AP should lose its CAPWAP connection to its controller, it goes into Standalone mode. In Standalone mode, any Centrally Switched WLANs are down, but Locally Switched WLANs remain operational. If the Locally Switched WLAN is configured for Central Authentication, the associated clients remain connected when the AP goes into Standalone mode, but will be unable to form new associations. A Locally Switched WLAN that uses Local Authentication remains operational whether the AP is in Standalone or Connected mode.

Figure 1: FlexConnect Deployment

The figure below shows a typical 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 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 has been 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 values only after the session timer expires.

There is no deployment restriction on the number of FlexConnect access points per location. Multiple FlexConnect groups can be defined in a single location.

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

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/PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

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

VPN and PPTP are supported for locally switched traffic if these security types are accessible locally at the access point.

FlexConnect access points support multiple SSIDs.

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 IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

When AP is changed from local mode to FlexConnect mode, the AP does not reboot. However, when the AP is changed from FlexConnect mode to local mode, the AP reboots and displays the following error message:

```
Warning: Changing AP Mode will reboot the AP and will rejoin the controller
after a few minutes. Are you sure you want to continue?
```

Note For the Cisco Flex 7510 WLC, auto convert mode is available on the CLI. The auto convert mode triggers the change on all the connected APs. The change of the mode from Local to FlexConnect and the reboot works in conjunction with the auto convert mode for the Cisco Flex 7510 WLC.

FlexConnect Authentication Process

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 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.

Note For more information about how access points find controllers, see the controller deployment guide at: http://www.cisco.com/c/en/us/td/docs/wireless/technology/controller/deployment/guide/dep.html.

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:

- 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.

  Note For the FlexConnect local switching, central authentication deployments, if there is a passive client with a static IP address, it is recommended to disable the Learn Client IP Address feature under the **WLAN** > **Advanced** tab.

- 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.

Note Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

- 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.
  - Local authentication in connected mode requires a WLAN configuration.

Note When locally switched clients that are connected to a FlexConnect access point renew the IP addresses, on joining back, the client continues to stay in the run state. These clients are not reauthenticated by the controller.

- 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. In controller software release 4.2 or later releases, 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.

Note If your controller is configured for NAC, clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the Configuring Dynamic Interfaces section for information about creating quarantined VLANs and the Configuring NAC Out-of-Band section for information about configuring NAC out-of-band support.

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 on FlexConnect

- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to four 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 cases where you cannot achieve the 300 milliseconds round-trip latency, you can 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.
- 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 secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- Cisco FlexConnect mode requires that the client send traffic before learning the client's IPv6 address. Compared to in local mode where the controller learns the IPv6 address by snooping the packets during Neighbor Discovery to update the IPv6 address of the client.
- To use CCKM fast roaming with FlexConnect access points, you must configure FlexConnect Groups.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- 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 to duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Do not connect access points in FlexConnect mode directly to a 2504 WLC.
- 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 time of initialization, few syslog packets from the access point are tagged with VLAN ID 1. This is a known issue.
- 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 ISE.

- FlexConnect does not support IPv6 ACLs, neighbor discovery caching, and DHCPv6 snooping of IPv6 NDP packets.
- FlexConnect does not display any IPv6 client addresses within the client detail page.
- FlexConnect Access Points with Locally Switched WLAN cannot perform IP Source Guard and prevent ARP spoofing. For Centrally Switched WLAN, the wireless controller performs the IP Source Guard and ARP Spoofing.
- To prevent ARP spoofing attacks in FlexConnect AP with Local Switching, we recommend that you use ARP Inspection.
- When you enable local switching on WLAN for the FlexConnect APs, then APs perform local switching. However, for the APs in local mode, central switching is performed.

  A scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported. The client may not get 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.
- For Wi-Fi Protected Access version 2 (WPA2) in FlexConnect standalone mode or local-auth in connected mode or CCKM 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 CCKM 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 CCKM fast-roaming in connected mode.
- AVC is not supported on APs in FlexConnect local switched mode.
- Flexconnect access points in WIPS mode can significantly increase the bandwidth utilization depending on the activity detected by the access points. If the rules have forensics enabled, the link utilization can go up by almost 100kbps.
- Local authentication fall back is not supported when user is not available in the external RADIUS server.
- For WLAN configured for the FlexConnect AP in the local switching and local authentication, synchronization of dot11 clients information is supported.
- It is not possible for the Cisco WLC to detect if an AP has dissociated and with that whether the radio is in operational state or non-operational state.

  When a FlexConnect AP dissociates from the Cisco WLC, the AP can still serve the clients with the radios being operational; however, with all other AP modes, the radios go into non-operational state.
- 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.
- ACL override is not supported in TKIP encrypted clients.
- IRCM is not supported in FlexConnect deployments.
- The Cisco Wave 2 APs in FlexConnect mode attempt discovery of the controller 18 times before renewing the DHCP on the Ethernet interface to get a new DHCP IP address. In a non-FlexConnect mode, the Cisco Wave 2 APs attempt discovery five times before renewing the IP address.

Configuring FlexConnect

Note The configuration tasks must be performed in the order in which they are listed.

Configuring the Switch at a Remote Site

Step 1 Attach the AP that will be enabled for FlexConnect to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect AP connected to a trunk port on the switch.

Step 2 See the sample configuration in this procedure to configure the switch to support the FlexConnect AP.

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

A sample local switch configuration is as follows:

```
ip dhcp pool NATIVE
   network 192.168.200.224 255.255.255.224
   default-router 192.168.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 192.168.201.224 255.255.255.224
   default-router 192.168.201.225
   dns-server 192.168.100.167
!
interface GigabitEthernet1/0/2
 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 192.168.200.225 255.255.255.224
!
interface Vlan101
 ip address 192.168.201.226 255.255.255.229
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: WLANs Example

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

Configuring the Controller for FlexConnect for a Centrally Switched WLAN Used for Guest Access

Before you begin

You must have created guest user accounts. For more information about creating guest user accounts, see the *Cisco Wireless LAN Controller System Management Guide*.

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

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the **WLANs > New page** .

Step 3 From the **Type** drop-down list, choose **WLAN**.

Step 4 In the **Profile Name** text box, enter **guest-central**.

Step 5 In the **WLAN SSID** text box, enter **guest-central**.

Step 6 From the **WLAN ID** drop-down list, choose an ID for the WLAN.

Step 7 Click **Apply**. The **WLANs > Edit** page appears.

Step 8 In the **General** tab, select the **Status** check box to enable the WLAN.

Step 9 In the **Security > Layer 2** tab, choose **None** from the **Layer 2 Security** drop-down list.

Step 10 In the **Security > Layer 3** tab:

a) Choose **None** from the **Layer 3 Security** drop-down list.
b) Choose the **Web Policy** check box.
c) Choose **Authentication**.

If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL on the Layer 3 tab.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the Controller for FlexConnect (GUI)

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

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the **WLANs > New** page.

Step 3 From the **Type** drop-down list, choose **WLAN**.

Step 4 In the **Profile Name** field, enter a unique profile name for the WLAN.

Step 5 In the **WLAN SSID** field, enter a name for the WLAN.

Step 6 From the **WLAN ID** drop-down list, choose the ID number for this WLAN.

Step 7 Click **Apply**.
The **WLANs > Edit** page is displayed.

Step 8 You can configure the controller for FlexConnect in both centrally switched and locally switched WLANs:

Note Do not enable ip-learn on FlexConnect local switched WLAN. When several sites use similar local subnets or overlapping subnets that are terminated on the same WLC, you will see ip-theft false positives. If ip-theft exclusion is enabled on the WLC, the clients might be put in a blocked list or a similar message is displayed to convey the feature behavior.

To configure the controller for FlexConnect in a centrally switched WLAN:

a) In the **General** tab, check the **Status** check box to enable the WLAN.
b) If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the **General** tab.
c) In the **Security > Layer 2** tab, choose **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.

To configure the controller for FlexConnect in a locally switched WLAN:

a) In the **General** tab, check the **Status** check box to enable the WLAN.
b) If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
c) In the **Security** > **Layer2** tab, choose **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.
d) In the **Advanced** tab:

- Check or uncheck the **FlexConnect Local Switching** check box to enable or disable local switching of client data associated with the APs in FlexConnect mode.

  Note The guidelines and limitations for this feature are as follows:

  - When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).
  - For FlexConnect access points, the interface mapping at the controller for WLANs that is configured for FlexConnect Local Switching is inherited at the access point as the default VLAN tagging. This mapping can be changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is determined by each WLAN's interface mapping.

- Check or uncheck the **FlexConnect Local Auth** check box to enable or disable local authentication for the WLAN.
- Check or uncheck the **Learn Client IP Address** check box to enable or disable the IP address of the client to be learned.
- Check or uncheck the **VLAN based Central Switching** check box to enable or disable central switching on a locally switched WLAN based on AAA overridden VLAN. For more information see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/FlexConnect_DG.html#pgfId-43615.

  Note These are the guidelines and limitations for this feature:

  - VLAN based central switching is not supported by mac filter.
  - Multicast on overridden interfaces is not supported.
  - This feature is available only on a per-WLAN basis, where the WLAN is locally switched.
  - IPv6 ACLs, CAC, NAC, and IPv6 are not supported.
  - IPv4 ACLs are supported only with VLAN-based central switching enabled and applicable only to central switching clients on the WLAN.
  - This feature is applicable to APs in FlexConnect mode in locally switched WLANs.
  - This feature is not applicable to APs in Local mode.
  - This feature is not supported on APs in FlexConnect mode in centrally switched WLANs.
  - This feature is supported on central authentication only.
  - This features is not supported on web authentication security clients.
  - Layer 3 roaming for local switching clients is not supported.

- Check or uncheck the **Central DHCP Processing** check box to enable or disable the feature. When you enable this feature, the DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
- Check or uncheck the **Override DNS** check box to enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
- Check or uncheck the **NAT-PAT** check box to enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 9 Save the configuration.

Related Topics

Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (GUI)

Configuring the Controller for FlexConnect (CLI)

Step 1 **config wlan flexconnect local-switching** *wlan_id* **enable**—Configures the WLAN for local switching.

Note When a WLAN is locally switched (LS), you must use the **config wlan flexconnect learn-ipaddr** *wlan-id* {**enable** | **disable**} command. When the WLAN is centrally switched (CS), you must use the **config wlan learn-ipaddr-cswlan** *wlan-id* {**enable** | **disable**} command.

Step 2 **config wlan flexconnect local-switching** *wlan_id* {**enable** | **disable**}—Configures the WLAN for central switching.

Step 3 **config wlan flexconnect vlan-central-switching** *wlan_id* {**enable** | **disable**}—Configures central switching on a locally switched WLAN based on an AAA overridden VLAN.

The guidelines and limitations for this feature are as follows:

- VLAN based central switching is not supported by mac filter.
- Multicast on overridden interfaces is not supported.
- This feature is available only on a per-WLAN basis, where the WLAN is locally switched.
- IPv6 ACLs, CAC, NAC, and IPv6 are not supported.
- IPv4 ACLs are supported only with VLAN-based central switching enabled and applicable only to central switching clients on the WLAN.
- This feature is applicable to APs in FlexConnect mode in locally switched WLANs.
- This feature is not applicable to APs in Local mode.
- This feature is not supported on APs in FlexConnect mode in centrally switched WLANs.
- This feature is supported on central authentication only.
- This features is not supported on web authentication security clients.
- Layer 3 roaming for local switching clients is not supported.

Additional Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/FlexConnect_DG.html#pgfId-43615

Step 4 Use these commands to get FlexConnect information:

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

Step 5 Use these commands to obtain debug information:

- **debug flexconnect aaa** {**event** | **error**} {**enable** | **disable**}—Enables or disables debugging of FlexConnect backup RADIUS server events or errors.
- **debug flexconnect cckm** {**enable** | **disable**}—Enables or disables debugging of FlexConnect CCKM.
- **debug flexconnect** {**enable** | **disable**}—Enables or disables debugging of FlexConnect Groups.
- **debug pem state** {**enable** | **disable**}—Enables or disables debugging of the policy manager state machine.
- **debug pem events** {**enable** | **disable**}—Enables or disables debugging of policy manager events.

Configuring an Access Point for FlexConnect

Configuring an Access Point for FlexConnect (GUI)

Before you begin

Ensure that the access point has been physically added to your network.

Note The AP will reboot when you change the AP behavior from Flexconnect to Local.

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

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

Step 3 From the **AP Mode** drop-down list, choose **FlexConnect** to enable FlexConnect for this access point.

Note The last parameter in the **Inventory** tab indicates whether the access point can be configured for FlexConnect.

Step 4 Click **Apply** to commit your changes and to cause the access point to reboot.

Step 5 Choose the **FlexConnect** tab to open the **All APs > Details for (FlexConnect)** page.

If the access point belongs to a FlexConnect group, the name of the group appears in the **FlexConnect Name** text box.

Step 6 Select the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.

Note By default, a VLAN is not enabled on the FlexConnect access point. After FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller.

Note If PMIPv6 MAG on FlexConnect AP is configured, VLAN Support can be checked or unchecked on the FlexConnect AP. If you check the VLAN Support check box, enter the number of the native VLAN on the remote network in the Native VLAN ID text box.

Note To preserve the VLAN mappings in the access point after an upgrade or downgrade, it is necessary that the access point join is restricted to the controller for which it is primed. That is, no other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point may get mismatched.

Note For Cisco 1140 access point, when the native VLAN ID is set, it disconnects and joins back the Cisco 8510 WLC. And after resuming the admin mode for the AP, is disabled.

Step 7 Click **Apply**. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 8 Click the name of the same access point and then click the **FlexConnect** tab.

Step 9 Click **VLAN Mappings** to open the **All APs** > *Access Point Name* > **VLAN Mappings** page.

Step 10 Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the **VLAN ID** text box.

Step 11 To configure Web Authentication ACLs, do the following:

a) Click the **External WebAuthentication ACLs** link to open the ACL mappings page. The ACL Mappings page lists details of WLAN ACL mappings and web policy ACLs.

b) In the **WLAN Id** box, enter the WLAN ID.

c) From the **WebAuth ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

d) Click **Add**.

e) Click **Apply**.

Step 12 To configure Local Split ACLs:

a) Click the **Local Split ACLs** link to open the ACL Mappings page.

b) In the **WLAN Id** box, enter the WLAN ID.

c) From the **Local-Split ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

If a client that connects over a WAN link associated with a centrally switched WLAN has to send some traffic to a device present in the local site, the client has to send traffic over CAPWAP to the controller and then get the same traffic back to the local site either over CAPWAP or using some offband connectivity. This process unnecessarily consumes WAN link bandwidth. To avoid this issue, 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 DCHP Required on the WLAN, which ensures that the client associating with the split WLAN does DHCP.

Note Local split tunneling is not supported on Cisco 1500 Series, Cisco 1130, and Cisco 1240 access points, and does not work for clients with static IP address.

d) Click **Add**.

Step 13 To configure Central DHCP processing:

a) In the WLAN Id box, enter the WLAN ID with which you want to map Central DHCP.

b) Select or unselect the **Central DHCP** check box to enable or disable Central DHCP for the mapping.

c) Select or unselect the **Override DNS** check box to enable or disable overriding of DNS for the mapping.

d) Select or unselect the **NAT-PAT** check box to enable or disable network address translation and port address translation for the mapping.

e) Click **Add** to add the Central DHCP - WLAN mapping.

Step 14 To map a locally switched WLAN with a WebAuth ACL, follow these steps:

a) In the **WLAN Id** box, enter the WLAN ID.

b) From the **WebAuth ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

c) Click **Add**.

Note The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

Step 15 From the **WebPolicy ACL** drop-down list, choose a FlexConnect ACL and then click **Add** to configure the FlexConnect ACL as a web policy.

Note You can configure up to 16 Web Policy ACLs that are specific to an access point.

Step 16 Click **Apply**.

Step 17 Click **Save Configuration**.

Note Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

Configuring an Access Point for FlexConnect (CLI)

Note The AP will reboot when you change the AP behavior from Flexconnect to Local.

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

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

  Note To delete a RADIUS server that is configured for a FlexConnect access point, enter the **config ap flexconnect radius auth delete** {**primary | secondary**} *Cisco_AP* command.

- **config ap flexconnect vlan wlan** *wlan_id vlan-id Cisco_AP*—Enables you to assign a VLAN ID to this FlexConnect access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap flexconnect vlan** {**enable | disable**} *Cisco_AP*—Enables or disables VLAN tagging for this FlexConnect access point. By default, VLAN tagging is not enabled. After VLAN tagging is enabled on the FlexConnect access point, WLANs that are enabled for local switching inherit the VLAN assigned at the controller.
- **config ap flexconnect vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this FlexConnect access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per FlexConnect access point (when VLAN tagging is enabled). Make sure the switch port to which the access point is connected has a corresponding native VLAN configured as well. If the

FlexConnect access point's native VLAN setting and the upstream switch port native VLAN do not match, the access point cannot transmit packets to and from the controller.

Note To save the VLAN mappings in the access point after an upgrade or downgrade, you should restrict the access point to join the controller for which it is primed. No other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point might get mismatched.

- Configure the mapping of a Web-Auth or a Web Passthrough ACL to a WLAN for an access point in FlexConnect mode by entering this command:

  config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* {**enable** | **disable**}

Note The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

- Configure a Policy ACL on an AP in FlexConnect mode by entering this command:

  config ap flexconnect acl {**add** | **delete**} *acl_name cisco_ap*

Note You can configure up to 16 Policy ACLs that are specific to an access point.

- To configure local split tunneling on a per-AP basis, enter this command:

  config ap local-split {**enable** | **disable**} *wlan-id* **acl** *acl-name ap-name*

- Configure central DHCP on the AP per WLAN by entering this command:

  config ap flexconnect central-dhcp *wlan-id ap-name* {**enable override dns** | **disable** | **delete**}

Note The gratuitous ARP for the gateway is sent by the access point to the client, which obtained an IP address from the central site. This is performed to proxy the gateway by the access point.

Use these commands on the FlexConnect access point to get status information:

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

Use these commands on the FlexConnect access point to get debug information:

- **debug capwap reap**—Shows general FlexConnect activities.

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

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

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

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

Step 3 Clicked the **Advanced** tab to open the **WLANs** > **Edit (WLAN Name)** page.

Step 4 Select the **FlexConnect Local Switching** check box to enable FlexConnect local switching.

Step 5 Select the **FlexConnect Local Auth** check box to enable FlexConnect local authentication.

Caution Do not connect access points in FlexConnect mode directly to 2500 Series Controllers.

Step 6 Click **Apply** to commit your changes.

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

Before you begin

Before you begin, you must have enabled local switching on the WLAN where you want to enable local authentication for an access point. For instructions on how to enable local switching on the WLAN, see the Configuring the Controller for FlexConnect (CLI) section.

Procedure

- **config wlan flexconnect ap-auth** *wlan_id* {**enable** | **disable**}—Configures the access point to enable or disable local authentication on a WLAN.

⚠

Caution Do not connect the access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

- **show wlan** *wlan-id* —Displays the configuration for the WLAN. If local authentication is enabled, the following information appears:

```
. . .
. . .
Web Based Authentication..................... Disabled
```

```
    Web-Passthrough.............................. Disabled
    Conditional Web Redirect..................... Disabled
    Splash-Page Web Redirect..................... Disabled
    Auto Anchor.................................. Disabled
    FlexConnect Local Switching.................. Enabled
    FlexConnect Local Authentication............. Enabled
    FlexConnect Learn IP Address................. Enabled
    Client MFP................................... Optional
    Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
. . .
. . .
```

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the Configuring the Controller for FlexConnect section.

In the example scenarios (see the Configuring the Controller for FlexConnect section), there are three profiles on the client:

1. To connect to the “employee” WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. After the client becomes authenticated, the client gets an IP address from the management VLAN of the controller.
2. To connect to the “local-employee” WLAN, create a client profile that uses WPA/WPA2 authentication. After the client becomes authenticated, the client gets an IP address from 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 becomes authenticated, the client gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user can type any HTTP address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters the username and password.

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