Guest Anchor with Centralized EoGRE

- Feature History for Guest Anchor with Centralized EoGRE , on page 1
- Information About Guest Anchor with Centralized EoGRE, on page 1
- Guidelines and Limitations for Guest Anchor with Centralized EoGRE, on page 2
- Enabling Guest Anchor with Centralized EoGRE, on page 2
- Verifying Centralized EoGRE Guest Clients, on page 5

Feature History for Guest Anchor with Centralized EoGRE

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Guest Anchor with Centralized EoGRE

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	Guest Anchor with Centralized EoGRE	The Guest Anchor with Centralized EoGRE feature for Cisco Embedded Wireless Controller (EWC) allows you to provide internet services to wireless guest clients.

Information About Guest Anchor with Centralized EoGRE

You can provide internet services to guest wireless clients and also safeguard your company's internal information and infrastructure assets by using the Guest Anchor with Centralized EoGRE feature on the Cisco Embedded Wireless Controller (EWC). The guest anchor feature on EWC uses EoGRE as the tunnel between the primary access point (AP) on the EWC platform and the gateway router. Client traffic flows from the subordinate APs to the primary AP and then to the EoGRE tunnel gateway.

Guidelines and Limitations for Guest Anchor with Centralized EoGRE

Cisco EWC does not support AP and client SSO. After the switchover, guest clients are cleaned up, causing interruption in the client traffic. Guest clients rejoin after switchover and traffic is then re-established.

Enabling Guest Anchor with Centralized EoGRE

To support guest anchoring using centralized EoGRE, complete the following configurations in the given order.

- Required Configuration
  1. Configuring Wireless Profile Tunnel Under Wireless Profile Policy (CLI), on page 2
  2. Configuring Central Forwarding (CLI), on page 4
  3. Configuring DHCP Required Under Policy Profile (CLI), on page 4
- Example of Recommended Configurations
  - Configuration Examples of ACLs for Guest Clients, on page 4

Configuring Wireless Profile Tunnel Under Wireless Profile Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy_profile_name* **Example:** `Device(config)# wireless profile policy open_policy`	Configures wireless policy profile and goes into wireless policy configuration mode.
Step 3	**no central dhcp** **Example:** `Device(config-wireless-policy)# no central dhcp`	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 4	**no central switching** **Example:**	Configures a WLAN for local switching.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no central switching`	
Step 5	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Enables the FlexConnect DHCP-Required feature.
Step 6	**tunnel-profile** *tunnel-profile-name* **Example:** `Device(config-wireless-policy)# tunnel-profile eogre_central`	Configures a tunnel profile.
Step 7	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 2121`	Configures the VLAN name or ID.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Configuring Central Forwarding (GUI)

Procedure

Step 1 From the Cisco Embedded Wireless Controller for Catalyst Access Points GUI, choose **Configuration** > **Tags & Profiles** > **EoGRE**.

Step 2 Click the **Tunnel Profiles** tab.

Step 3 Under the **Tunnel Profiles** tab, click **Add**.
The **Add Tunnel Profile** window is displayed.

Step 4 Click the **Central Forwarding** toggle button to enable the feature.

Step 5 Click **Apply to Device**.

Configuring Central Forwarding (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile tunnel** *tunnel-profile-name* **Example:** `Device(config)# wireless profile tunnel tunnel-profile-name`	Configures wireless tunnel profile and goes into tunnel profile configuration mode.
Step 3	**central-forwarding** **Example:** `Device(config-tunnel-profile)# central-forwarding`	Enables centralized forwarding.

Configuring DHCP Required Under Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile-name`	Configures a policy profile.
Step 3	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for a WLAN.

Configuration Examples of ACLs for Guest Clients

Guest clients and local clients use the same network resources. Therefore, to safeguard the local client traffic with respect to the guest traffic, default ACLs are pushed for guest clients.

If a WLAN has an EoGRE guest tunnel profile, you can push the default ACLs to block traffic to the local subnet and ACLs to block the multicast traffic for guest clients.

The following example shows you the recommended configuration of ACLs for guest clients:

IPv4 ACL

```
Device# configure terminal
Device(config)# ip access-list extended igmp
Device(config-ext-nacl)# 10 deny igmp any any
Device(config-ext-nacl)# 20 permit ip any any

Device(config)# wireless profile flex igmp-flex
Device(config-wireless-flex-profile)# acl-policy igmp

Device(config)# wireless tag site sp-flex-site
Device(config-site-tag)# flex-profile igmp-flex
Device(config-site-tag)# no local-site

Device# show ip access-lists
Extended IP access list igmp
    1 deny igmp any any
    2 permit ip any any
```

IPv6 ACL

```
Device(config)# wireless profile flex igmp-flex
Device(config-wireless-flex-profile)# acl-policy igmp
Device(config-wireless-flex-profile)# acl-policy mldv6

Device(config)# ipv6 access-list igmp
Device(config-ipv6-acl)# sequence 10 deny icmp any any mld-query
Device(config-ipv6-acl)# sequence 20 deny icmp any any mld-reduction
Device(config-ipv6-acl)# sequence 30 deny icmp any any mld-report
Device(config-ipv6-acl)# sequence 40 deny icmp any any mld-v2-report
Device(config-ipv6-acl)# sequence 50 permit ipv6 any any
Device(config-ipv6-acl)# acl-policy mldv6

Device# show ipv6 access-list
Extended IPv6 access list mldv6
    10 deny 58 any any
    20 deny 58 any any
    30 deny 58 any any
    40 deny 58 any any
    50 permit ipv6 any any

Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# ipv4 acl igmp
Device(config-wireless-policy)# ipv6 acl mldv6
```

Verifying Centralized EoGRE Guest Clients

To verify the centralized EoGRE guest clients, run the following command:

```
Device# show tunnel eogre client central-forwarding summary
Client MAC      AP MAC          Domain                          Tunnel        VLAN
-------------------------------------------------------------------------------------
74xx.38xx.88xx  0cxx.f8xx.9cxx  domain1                         N/A           2121
74xx.38xx.88xx  0cd0.f8xx.9cxx  domain1                         N/A           2121
74xx.38xx.88xx  0cd0.f8xx.9cxx  domain1                         N/A           2121
```