# Wired Guest Access



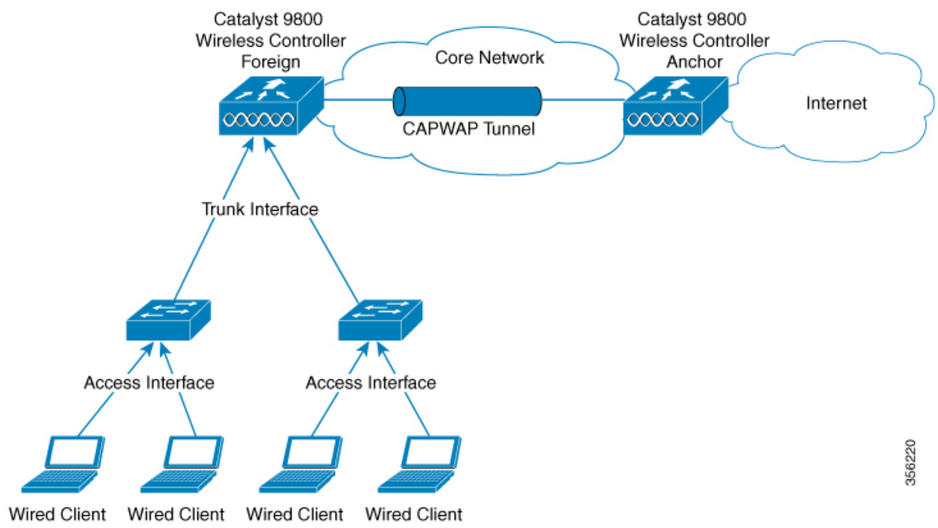
## Information About Wired Guest Access

The Wired Guest Access feature enables guest users of an enterprise network that supports both wired and wireless access to connect to the guest access network. The wired guest clients can connect from the designated and configured wired Ethernet ports for the guest access after they complete the configured authentication methods. Wired session guests are directed to a wireless guest controller in a demilitarized zone (DMZ) through a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel.

Wired guest access can be configured in a dual-controller configuration that uses both an anchor controller and a foreign controller. A dual-controller configuration isolates wired guest access traffic from the enterprise user traffic.

The wired session guests are provided open or web-authenticated access from the wireless controller.

*Figure 1: Guest Access Architecture*




## IPv6 Router Advertisement Forwarding for a Wired Guest

Wired clients get the IPv6 based connectivity when they receive the IPv6 Router Advertisement (RA) message. The IPv6 router sends these RA messages and it contains information such as IPv6 prefix and router link-local address.

These RA messages are sent as Unicast or Multicast messages. The Unicast RA messages are routed as same as the client directed traffic. The Multicast RA messages are forwarded to all the clients present in the intended VLAN. RA message forwarding is enabled by default and requires no specific configuration.

**Guest Anchor Controller**: Guest anchor controller forwards the RA packets, from the receiving VLAN, to all the foreign controllers using the mobility data tunnel. The RA packets are tagged with the anchor VLAN to ensure the message is forwarded to the correct clients using the foreign controller data path.

**Guest Foreign Controller**: Guest foreign controller forwards the received RAs from the guest anchor to the wired ports on which the wired guest clients are connected. To forward the RAs to the intended clients, the guest foreign controller keeps a track of the wired guest clients–per interface, access VLANs, and anchor VLANs.

## Supported Features

- Cisco Catalyst 9800 Series Wireless Controllers-Anchor
- Cisco AireOS Wireless Controllers-Anchor
- Cisco Catalyst 9800 Series Wireless Controllers-Foreign
- Cisco AireOS Wireless Controllers-Foreign
- Dual controller solution (foreign + anchor) and access switch
- Trunk Ports
- Open Authentication
- Local Web Authentication

To configure Web Authentication, see Web-based Authentication section of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

- Local Web Authentication (web consent).

**Note** In AireOS, this is referred to as **web pass-through**.

- Local Web Authentication + ISE (External Web Authentication).
- LWA (local web authentication), with a username and a password.
- Web consent (LWA + consent), that is with a username, a password and the check box of acceptance.

- Scale max 2k clients and 5 guest-LANs (5 VLANs max)
- Client IPv6 support
- Idle Timeout and Session Timeout
- Accounting on Foreign

**Note** Statistics computation not supported.

- Manageability (SNMP/Yang/WebUI)
- QoS Rate-Limiting and MQC Policies (Upstream at foreign, Upstream, and Downstream at the anchor)

**Note** QoS rate-limiting supports bps rate-limiting, pps rate-limiting is not supported.

- QoS support with AireOS Anchor setup
- Stateful Switch Over (SSO)
- Port Channel support on Anchor and Foreign with no restrictions to the controller's role.
- Access Port on Foreign
- Cisco Umbrella (not supported in AireOS Anchor)
- ACL support at anchor
- Fully Qualified Domain Name (FQDN) URL filtering is supported at Anchor controller.
- IP theft detection
- Sleeping Client

# Restrictions for Wired Guest Access

- A maximum of five guest LANs are supported on the foreign controller.
- A maximum of 2000 clients per foreign are supported.
- No Multicast or Broadcast support.
- You can map only one wired VLAN to a guest LAN.
- You can map only one guest LAN to one policy profile.
- Every guest LAN has a unique name and this name cannot be shared with RLAN or WLAN.
- Ensure that the Anchor VLAN ID and the wired VLAN ID configured on the Foreign controller is not the same.
- QoS is not supported on VLAN and on physical interfaces of the controller.

# Configuring Access Switch for Wired Guest Client

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)#vlan 200` | Creates the VLAN ID. |
| **Step 3** | **exit**<br>**Example:**<br>`Device(config)#exit` | Returns to configuration mode. |
| **Step 4** | **interface GigabitEthernet***interface number*<br>**Example:**<br>`Device(config)#interface GigabitEthernet1/0/1` | Enters the interface to be added to the VLAN. |
| **Step 5** | **switchport access vlan** *vlan-id*<br>**Example:**<br>`Device(config-if)#switchport access vlan 200` | Assigns the port to a VLAN. The valid VLAN IDs range is between 1 and 4094. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **switchport mode access**<br>**Example:**<br>`Device(config-if)#switchport mode access` | Defines the VLAN membership mode for the port. |
| **Step 7** | **no cdp enable**<br>**Example:**<br>`Device(config-if)#no cdp enable` | Disables CDP on the interface. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)#end` | Saves the configuration and exits configuration mode and returns to privileged EXEC mode. |

# Configuring Access Switch for Foreign Controller

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)#vlan 200` | Creates the VLAN ID. |
| **Step 3** | **exit**<br>**Example:**<br>`Device(config)#exit` | Returns to configuration mode. |
| **Step 4** | **interface GigabitEthernet***interface number*<br>**Example:**<br>`Device(config)#interface GigabitEthernet1/0/2` | Enters the interface to be added to the VLAN. |
| **Step 5** | **switchport trunk allowed vlan** *vlan-id*<br>**Example:**<br>`Device(config-if)#switchport trunk allowed vlan 200` | Assigns the allowed VLAN ID to the port when it is in trunking mode. |
| **Step 6** | **switchport mode trunk**<br>**Example:**<br>`Device(config-if)#switchport mode trunk` | Sets the trunking mode to trunk unconditionally. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **end**<br>**Example:**<br>`Device(config-if)#end` | Saves the configuration and exits configuration mode and returns to privileged EXEC mode. |

# Configuring Foreign Controller with Open Authentication (GUI)

**Procedure**

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

**Step 2** Click on a **Policy Name**.

**Step 3** Go to the **Mobility** tab.

**Step 4** In the **Mobility Anchors** section, check the **Export Anchor** check box.

**Step 5** Click **Apply to Device**.

**Step 6** Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Configuration**

**Step 7** Click **Add**.

**Step 8** In the **General** tab, enter the **Profile Name**, **Guest LAN ID**, **Client Association Limit**.

**Step 9** Choose the desired mode from the **mDNS Mode** drop-down list.

**Step 10** Enable or disable the **Status** and **Wired VLAN Status** toggle button.

**Step 11** In the **Security** tab, disable the **Web Auth** toggle button.

**Step 12** Click **Apply to Device**.

**Step 13** Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Map Configuration**

**Step 14** Click **Add Map**.

**Step 15** In the Add Guest LAN Map window, enter the **Guest LAN Map**.

**Step 16** Click **Apply to Device**.

**Step 17** Click **Add**.

**Step 18** Choose the values from the **Profile Name** and **Policy Name** drop-down lists.

**Step 19** Click **Save**.

# Configuring Foreign Controller with Open Authentication

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **wireless profile policy** *wlan-policy-profile-name*<br>**Example:**<br>`Device(config)#wireless profile policy testpro-1` | Configures the WLAN policy profile. |
| **Step 3** | **mobility anchor** *non-local-mobility-cntlr-ip* **priority** *priority*<br>**Example:**<br>`Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1` | Configures the mobility anchor and sets its priority. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)#no shutdown` | Enables the configuration. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-wireless-policy)#exit` | Returns to configuration mode. |
| **Step 6** | **guest-lan profile-name** *guest-profile-name guest-lan-id* **wired-vlan** *wired-vlan-id*<br>**Example:**<br>`Device(config)#guest-lan profile-name gstpro-1 1 wired-vlan 25` | Configures guest LAN profile with a wired VLAN.<br>**Note** Configure the wired VLAN only for the Guest Foreign controller. |
| **Step 7** | **no security web-auth**<br>**Example:**<br>`Device(config-guest-lan)#no security web-auth` | Disables web-authentication. |
| **Step 8** | **no shutdown**<br>**Example:**<br>`Device(config-guest-lan)#no shutdown` | Enables the guest LAN. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-guest-lan)#exit` | Returns to configuration mode. |
| **Step 10** | **wireless guest LAN map** *gst-map-name*<br>**Example:**<br>`Device(config)#wireless guest LAN map gstmap-1` | Configures a guest LAN map. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **guest-lan** *guest-profile-name* **policy** *wlan-policy-profile-name*<br>**Example:**<br>`Device(config-guest-lan-map)#guest-lan gstpro-1 policy testpro-1` | Attaches a guest LAN map to the policy profile. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-guest-lan-map)#exit` | Returns to configuration mode. |

# Configuring Foreign Controller with Local Web Authentication (GUI)

### Procedure

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

**Step 2** Select a **Policy Name**.

**Step 3** Go to the **Mobility** tab.

**Step 4** In the **Mobility Anchors** section, check the **Export Anchor** check box.

**Step 5** Click **Update & Apply to Device**.

**Step 6** Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Configuration**

**Step 7** Click **Add**.

**Step 8** In the **General** tab, enter the **Profile Name**, **Guest LAN ID**, **Client Association Limit**.

**Step 9** Choose the desired mode from the **mDNS Mode** drop-down list.

**Step 10** Enable or disable the **Status** and **Wired VLAN Status** using toggle button.

**Step 11** Go to the **Security** tab.

**Step 12** Enable the **Web Auth** using toggle button.

**Step 13** Choose the values from the **Web Auth Parameter Map**, **Authentication List** and **Authorization List** drop-down lists.

**Step 14** Click **Apply to Device**.

**Step 15** Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Map Configuration**

**Step 16** Click **Add Map**.

**Step 17** In the Add Guest LAN Map window, enter the **Guest LAN Map**.

**Step 18** Click **Apply to Device**.

**Step 19** Click **Add**.

**Step 20** Choose the values from the **Profile Name** and **Policy Name** drop-down lists.

**Step 21** Click **Save**.

# Configuring Foreign Controller with Local WEB Authentication

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| Step 2 | **wireless profile policy** *wlan-policy-profile-name*<br>**Example:**<br>`Device(config)#wireless profile policy testpro-1` | Configures the WLAN policy profile. |
| Step 3 | **mobility anchor** *non-local-mobility-cntlr-ip* **priority** *priority*<br>**Example:**<br>`Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1` | Configures the mobility anchor and sets its priority. |
| Step 4 | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)#no shutdown` | Enables the configuration. |
| Step 5 | **exit**<br>**Example:**<br>`Device(config-wireless-policy)#exit` | Returns to configuration mode. |
| Step 6 | **guest-lan profile-name** *guest-profile-name guest-lan-id* **wired-vlan** *wired-vlan-id*<br>**Example:**<br>`Device(config)#guest-lan profile-name gstpro-2 3 wired-vlan 26` | Configures guest LAN profile with a wired VLAN. |
| Step 7 | **security web-auth**<br>**Example:**<br>`Device(config-guest-lan)#security web-auth` | Enables web-authentication. |
| Step 8 | **security web-auth authentication-list** *auth-list-name*<br>**Example:**<br>`Device(config-guest-lan)#security web-auth authentication-list default` | Configures the authentication list for a IEEE 802.1x network. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **security web-auth parameter-map** *parameter-map-name*<br><br>**Example:**<br>`Device(config-guest-lan)#security web-auth parameter-map global` | Configures the security web-auth parameter map. |
| **Step 10** | **no shutdown**<br><br>**Example:**<br>`Device(config-guest-lan)#no shutdown` | Enables the guest LAN. |
| **Step 11** | **exit**<br><br>**Example:**<br>`Device(config-guest-lan)#exit` | Returns to configuration mode. |
| **Step 12** | **wireless guest-lan map** *gst-map-name*<br><br>**Example:**<br>`Device(config)#wireless guest-lan map gstmap-2` | Configures a guest LAN map. |
| **Step 13** | **guest-lan** *guest-lan-profile-name* **policy** *policy-profile-name*<br><br>**Example:**<br>`Device(config-guest-lan-map)#guest-lan gstpro-2 policy testpro-1` | Attaches a guest LAN map to the policy profile. |
| **Step 14** | **exit**<br><br>**Example:**<br>`Device(config-guest-lan-map)#exit` | Returns to configuration mode. |

### What to do next

For more information about Local Web Authentication, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/wireless-web-authentication.html

# Configuring Anchor Controller with Open Authentication (GUI)

### Procedure

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

**Step 2** Click **Add**.

**Step 3** In the **General** tab, enter the **Name**.

**Step 4** Go to the **Access Policies** tab.

**Step 5** Under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.

**Step 6** Go to the **Mobility** tab.

**Step 7** Under the **Mobility Anchors** settings, check the **Export Anchor** check box.

**Step 8** Click **Apply to Device**.

**Step 9** Choose **Configuration** > **Wireless** > **Guest LAN**.

**Step 10** Click **Add**.

**Step 11** In the **General** tab, enter the **Profile Name**, the **Guest LAN ID** and the **Client Association Limit**.

**Step 12** In the **Security** tab, under the **Layer3** settings, disable the **Web Auth** toggle button.

**Step 13** Click **Apply to Device**.

# Configuring Anchor Controller with Open Authentication

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile policy** *wlan-policy-profile-name*<br>**Example:**<br>`Device(config)#wireless profile policy testpro-2` | Configures the WLAN policy profile. |
| **Step 3** | **mobility anchor**<br>**Example:**<br>`Device(config-wireless-policy)#mobility anchor` | Configures the mobility anchor. |
| **Step 4** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config-wireless-policy)#vlan 29` | Configure a VLAN name or a VLAN ID. |
| **Step 5** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)#no shutdown` | Enables the configuration. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-wireless-policy)#exit` | Returns to configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **guest-lan profile-name** *guest-profile-name guest-lan-id*<br>**Example:**<br>`Device(config)#guest-lan profile-name testpro-2 1` | Configures the guest LAN profile with a wired VLAN. |
| **Step 8** | **client association limit** *guest-lan-client-limit*<br>**Example:**<br>`Device(config-guest-lan)#client association limit` | Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000. |
| **Step 9** | **no security web-auth**<br>**Example:**<br>`Device(config-guest-lan)#no security web-auth` | Disables web authentication. |
| **Step 10** | **no shutdown**<br>**Example:**<br>`Device(config-guest-lan)#no shutdown` | Enables the guest LAN. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-guest-lan)#exit` | Returns to configuration mode. |

# Configuring Anchor Controller with Local Web Authentication (GUI)

### Procedure

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Policy**.
**Step 2** Click **Add**.
**Step 3** In the **General** tab, enter the **Name**.
**Step 4** Go to the **Access Policies** tab.
**Step 5** Under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.
**Step 6** Go to the **Mobility** tab.
**Step 7** Under the **Mobility Anchors** settings, check the **Export Anchor** check box.
**Step 8** Click **Apply to Device**.
**Step 9** Choose **Configuration** > **Wireless** > **Guest LAN**.
**Step 10** Click **Add**.
**Step 11** In the **General** tab, enter the **Profile Name**, the **Guest LAN ID** and the **Client Association Limit**.

**Step 12** In the **Security** tab, under the **Layer3** settings, enable the **Web Auth** toggle button. Choose the Parameter map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.

**Step 13** Click **Apply to Device**.

# Configuring Anchor Controller with Local Web Authentication

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile policy** *wlan-policy-profile-name*<br>**Example:**<br>`Device(config)#wireless profile policy testpro-2` | Configures the WLAN policy profile. |
| **Step 3** | **mobility anchor**<br>**Example:**<br>`Device(config-wireless-policy)#mobility anchor` | Configures the mobility anchor. |
| **Step 4** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config-wireless-policy)#vlan 30` | Configure a VLAN name or a VLAN ID. |
| **Step 5** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)#no shutdown` | Enables the configuration. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-wireless-policy)#exit` | Returns to configuration mode. |
| **Step 7** | **guest-lan profile-name** *guest-profile-name guest-lan-id*<br>**Example:**<br>`Device(config)#guest-lan profile-name testpro-2 1` | Configure a guest LAN profile with a wired VLAN. |

| | Command or Action | Purpose |
|---|---|---|
| Step 8 | **client association limit** *guest-lan-client-limit*<br>**Example:**<br>`Device(config-guest-lan)#client association limit` | Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000. |
| Step 9 | **security web-auth**<br>**Example:**<br>`Device(config-guest-lan)#security web-auth` | Configures web authentication. |
| Step 10 | **security web-auth parameter-map** *parameter-map-name*<br>**Example:**<br>`Device(config-guest-lan)#security web-auth parameter-map testmap-1` | Configures the security web-auth parameter map. |
| Step 11 | **security web-auth authentication-list** *authentication-list-name*<br>**Example:**<br>`Device(config-guest-lan)#security web-auth authentication-list testlwa-1` | Configures the authentication list for the IEEE 802.1x network. |
| Step 12 | **no shutdown**<br>**Example:**<br>`Device(config-guest-lan)#no shutdown` | Enables the guest-LAN. |
| Step 13 | **exit**<br>**Example:**<br>`Device(config-guest-lan)#exit` | Returns to configuration mode. |

# Configuring Session Timeout for a Profile Policy

Session Timeout for a wired guest is set to infinite by default. Perform the following procedure to configure the timeout values to the wired guest.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| Step 2 | **wireless profile policy** *wlan-policy-profile-name* | Configures the WLAN policy profile. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)#wireless profile policy testpol-1` | |
| **Step 3** | **guest-lan enable-session-timeout**<br>**Example:**<br>`Device(config-wireless-policy)#guest-lan enable-session-timeout` | Enables the client session timeout on the guest LAN. |
| **Step 4** | **session-timeout** *timeout-duration*<br>**Example:**<br>`Device(config-wireless-policy)#session-timeout 1000` | Configures the client session timeout in seconds. The valid range is between 0 and 86400 seconds. |

# Global Configuration (GUI)

### Procedure

**Step 1** Choose **Administration** > **User Administration**.

**Step 2** Click **Add**.

**Step 3** Enter the **Username**, **Password** and **Confirm Password**.

**Step 4** Choose the desired value from the **Policy** and **Privilege** drop-down lists.

**Step 5** Click **Apply to Device**.

**Step 6** Choose **Administration** > **Management** > **HTTP/HTTPS/Netconf**.

**Step 7** In the **HTTP/HTTPS Access Configuration** settings, enable or disable the **HTTP Access**, **HTTPS Access** and **Personal Identity Verification** toggle buttons.

**Step 8** Enter the **HTTP Port** and **HTTPS Port**.

**Step 9** Click **Apply**.

# Verifying Wired Guest Configurations

To validate the wireless configuration, use the following command:

```
Device# wireless config validate

Wireless Management Trustpoint Name: 'WLC-29c_WLC_TP'
        Trustpoint certificate type is WLC-SSC
    Wireless management trustpoint config is valid

Jan 22 07:49:15.371: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
Error in No record found for VLAN 9, needed by Guest-LAN open-wired
```

To display the summary of all Guest-LANs, use the following command:

```
Device# show guest-lan summary

Number of Guest LANs: 1

GLAN  GLAN Profile Name                 Status
----------------------------------------------
1     wired_guest_open                  UP
```

To view the detailed output of all Guest-LANs, use the following command:

```
Device# show guest-lan all

Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                    : 1
Wired-Vlan                                      : 200
Status                                          : Enabled
Number of Active Clients                        : 1
Max Associated Clients                          : 2000
Security
    WebAuth                                     : Enabled
    Webauth Parameter Map                       : global
    Webauth Authentication List                 : LWA-AUTHENTICATION
    Webauth Authorization List                  : LWA-AUTHENTICATION
```

To view the guest-LAN configuration by ID, use the following command:

```
Device# show guest-lan id 1
Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                    : 1
Wired-Vlan                                      : 200
Status                                          : Enabled
Number of Active Clients                        : 1
Max Associated Clients                          : 2000
Security
    WebAuth                                     : Enabled
    Webauth Parameter Map                       : global
    Webauth Authentication List                 : LWA-AUTHENTICATION
    Webauth Authorization List                  : LWA-AUTHENTICATION
```

To view the guest-LAN configuration by profile name, use the following command:

```
Device# show guest-lan name open

Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                    : 1
Wired-Vlan                                      : 200
Status                                          : Enabled
Number of Active Clients                        : 1
Max Associated Clients                          : 2000
Security
    WebAuth                                     : Enabled
    Webauth Parameter Map                       : global
    Webauth Authentication List                 : LWA-AUTHENTICATION
    Webauth Authorization List                  : LWA-AUTHENTICATION
```

To view the guest-LAN map summary, use the following command:

```
Device# show wireless guest-lan-map summary

Number of Guest-Lan Maps: 2

WLAN Profile Name                  Policy Name
------------------------------------------------------------------------
open_wired_guest                   open_wired_guest
lwa_wired_guest                    lwa_wired_guest
```

To view the active clients, use the following command:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                                             Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
000a.bd15.0001 N/A                                                 GLAN 1    Run
802.3    Web Auth   Export Foreign
```

To view the detailed information about a client by MAC address, use the following command:

```
Device# show wireless client mac-address 3383.0000.0001 detail

Client MAC Address : 3383.0000.0001
Client IPv4 Address : 155.165.152.151
Client Username: N/A
AP MAC Address:  N/A
AP slot : N/A
Client State : Associated
Policy Profile : guestlan_lwa
Flex Profile : N/A
Guest Lan:
  GLAN Id: 2
  GLAN Name: guestlan_lwa
  Wired VLAN: 312
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 128 seconds
Protocol : 802.3
Channel : N/A
Client IIF-ID : 0xa0000002
Association Id : 0
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Timer not running)
Session Warning Time : Timer not running
Input Policy Name  : clsilver
Input Policy State : Installed
Input Policy Source : AAA Policy
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream              : 0 (kbps)
  QoS Realtime Average Data Rate Upstream     : 0 (kbps)
  QoS Burst Data Rate Upstream                : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream       : 0 (kbps)
  QoS Average Data Rate Downstream            : 0 (kbps)
```

```
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Anchor IP Address           : 101.0.0.1
  Point of Attachment         : 0x00000008
  Point of Presence           : 0xA0000001
  AuthC status                : Enabled
  Move Count                  : 0
  Mobility Role               : Export Foreign
  Mobility Roam Type          : L3 Requested
  Mobility Complete Timestamp : 05/07/2019 22:31:45 UTC
Client Join Time:
  Join Time Of Client : 05/07/2019 22:31:42 UTC
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 125 seconds
Policy Type : N/A
Encryption Cipher : N/A
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
Access VLAN : 153
Anchor VLAN : 155
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Point of Attachment : TenGigabitEthernet0/0/0
  IIF ID             : 0x00000008
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 00000000000000CB946C8BA3
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP :
  Auth Method Status List
   Method : Web Auth
    Webauth State    : Authz
    Webauth Method   : Webauth
  Local Policies:
   Service Template : wlan_svc_guestlan_lwa_local (priority 254)
    VLAN             : 153
    Absolute-Timer   : 1800
  Server Policies:
    QOS Level        : 0
  Resultant Policies:
    VLAN Name         : VLAN0153
    QOS Level        : 0
    VLAN             : 153
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
```

```
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 8
  Number of Packets Sent : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
  Idle time : 0 seconds
  Last idle time update : 05/07/2019 22:32:27
  Last statistics update : 05/07/2019 22:32:27
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
```

# Wired Guest Access—Use Cases

This feature while performing as a guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

### Scenario One–Equipment Software Update

This feature can be configured to allow the wired port to connect to the manufacture or vendor website for equipment maintenance, software, or firmware updates.

### Scenario Two–Video Streaming

This feature can be configured to allow devices that are connected to a wired port to stream video to visitor information screens.