Configuring WGB

This chapter contains these topics:

Configuring AP to WGB Mode

Cisco 802.11ac wave2 AP (IW6300 and ESW6300) and 802.11ax AP module (WP-WIFI6) are Cheetah OS (COS) based access points. The COS WGB function runs on the following image versions:

- **ap3g3-k9w8-tar.xxx.tar**
- **ap1g8-k9w8-tar.xxx.tar**

Make sure that you use the correct image version for WGB deployment.

- To configure a Cisco AP from Capwap mode to WGB mode, use the following command:

```
# ap-type workgroup-bridge

WGB is a wireless client that serve as nonroot ap for wired clients.
AP is the Master/CAPWAP AP, system will need a reboot when ap type is
changed to WGB. Do you want to proceed? (y/N):y
```

- To reverse the AP to Capwap mode, configure ap-type as Capwap by using the following command:

```
# ap-type capwap
```

Note Switching between EWC mode and WGB mode is not supported.

Configuring IP Address

Configuring IPv4 Address

Configure IPv4 address of the AP by entering the following command:

configure ap address ipv4 dhcp

For IPv4 static configuration, use the following command:

configure ap address ipv4 static *ipv4_addr netmask gateway*

Configuring IPv6 Address

Configure the IPv6 address of the AP by entering the following commands:

- **configure ap address ipv6 static** *ipv6addr prefixlen gateway*
- **configure ap address ipv6 auto-config** {**enable**|**disable**}

Note The **configure ap address ipv6 auto-config enable** command is designed to enable IPv6 SLAAC. However, SLAAC is not applicable for cos WGB. This CLI will config IPv6 address with DHCPv6 instead of SLAAC.

- **configure ap address ipv6 dhcp**

Configuring a Dot1X Credential

Configure a dot1x credential by entering this command:

# **configure dot1x credential** *profile-name* **username** *name* **password** *pwd*

View the WGB EAP dot1x profile summary by entering this command:

# show wgb eap dot1x credential profile

Deauthenticating WGB Wired Client

Deauthenticate WGB wired client by entering this command:

# **clear wgb client** {**all** |**single** *mac-addr*}

Configuring an EAP Profile

Follow these steps to configure the EAP profile:

1. Bind dot1x credential profile to EAP profile.
2. Bind EAP profile to SSID profile
3. Bind SSID profile to the radio.

Step 1 Configure the EAP profile method type by entering this command:

# configure eap-profile *profile-name* **method** {**fast** | **leap** | **peap** | **tls**}

Step 2 Attaching the CA Trustpoint for TLS by entering this command:

# configure eap-profile *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*}

Note With the default profile, WGB uses the internal MIC certificate for authentication.

Step 3 Bind dot1x-credential profile by entering this command:

# configure eap-profile *profile-name* **dot1x-credential** *profile-name*

Step 4 [Optional] Delete an EAP profile by entering this command:

# configure eap-profile *profile-name* **delete**

Step 5 View summary of EAP and dot1x profiles by entering this command:

# show wgb eap profile all

Configuring Manual Enrollment of a Trustpoint for Terminal and TFTP

Step 1 Create a Trustpoint in WGB by entering this command:

# configure crypto pki trustpoint *ca-server-name* **enrollment terminal**

Step 2 Authenticate a Trustpoint manually by entering this command:

# configure crypto pki trustpoint *ca-server-name* **authenticate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 3 Configure a private key size by entering this command:

# configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Generate a private key and Certificate Signing Request (CSR) by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **enroll**

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Import the signed certificate in WGB by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **import certificate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 7 [Optional] Delete a Trustpoint by entering this command:

# **configure crypto pki trustpoint** *trustpoint-name* **delete**

Step 8 View the Trustpoint summary by entering this command:

# **show crypto pki trustpoint**

Step 9 View the content of the certificates that are created for a Trustpoint by entering this command:

# **show crypto pki trustpoint** *trustpoint-name* **certificate**

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge

Step 1 Enroll a Trustpoint in WGB using the server URL by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url*

Step 2 Authenticate a Trustpoint by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **authenticate**

This command will fetch the CA certificate from CA server automatically.

Step 3 Configure a private key size by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Enroll the Trust point by entering this command:

# **configure crypto pki trustpoint** *ca-server-name* **enroll**

Request the digitally signed certificate from the CA server.

Step 6 Enable auto-enroll by entering this command:

# configure crypto pki trustpoint *ca-server-name* **auto-enroll enable** *renew-percentage*

You can disable auto-enrolling by using the disable syntax in the command.

Step 7 [Optional] Delete a Trustpoint by entering this command:

# configure crypto pki trustpoint *trustpoint-name* **delete**

Step 8 View the Trustpoint summary by entering this command:

# show crypto pki trustpoint

Step 9 View the content of the certificates that are created for a Trustpoint by entering this command:

# show crypto pki trustpoint *trustpoint-name* **certificate**

Step 10 View the PKI timer information by entering this command:

# show crypto pki timers

Configuring Manual Certificate Enrollment Using TFTP Server

Step 1 Specify the enrollment method to retrieve the CA certificate and client certificate for a Trustpoint in WGB by entering this command:

# configure crypto pki trustpoint *ca-server-name* **enrollment tftp** *tftp-addr/file-name*

Step 2 Authenticate a Trustpoint manually by entering this command:

# configure crypto pki trustpoint *ca-server-name* **authenticate**

Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension “.ca” to the specified filename.

Step 3 Configure a private key size by entering this command:

# configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

# configure crypto pki trustpoint *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Generate a private key and Certificate Signing Request (CSR) by entering this command:

# configure crypto pki trustpoint *ca-server-name* **enroll**

Generates certificate request and writes the request out to the TFTP server. The filename to be written is appended with the extension “.req”.

Step 6 Import the signed certificate in WGB by entering this command:

# configure crypto pki trustpoint *ca-server-name* **import certificate**

Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The WGB will attempt to retrieve the granted certificate via TFTP using the same filename and the file name append with ".crt" extension.

Step 7 View the Trustpoint summary by entering this command:

# show crypto pki trustpoint

Step 8 View the content of the certificates that are created for a Trustpoint by entering this command:

# show crypto pki trustpoint *trustpoint-name* **certificate**

SSID configuration

SSID configuration consists of the following two parts:

1. Creating an SSID Profile
2. Configuring Radio Interface for Workgroup Bridges, on page 7

Creating an SSID Profile

Choose one of the following authentication protocols for the SSID profile.

- Configuring an SSID profile with Open Authentication
- Configuring an SSID profile with PSK Authentication
- Configuring an SSID Profile with Dot1x Authentication

Configuring an SSID profile with Open Authentication

Use the following command to configure an SSID profile with Open Authentication:

# **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication open**

Configuring an SSID profile with PSK Authentication

Use the following command to configure an SSID profile with PSK WPA2 Authentication:

# **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2**

Use the following command to configure an SSID profile with PSK Dot11r Authentication:

# **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r**

Use the following command to configure an SSID profile with PSK Dot11w Authentication:

# **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w**

Configuring an SSID Profile with Dot1x Authentication

Use the following commands to configure an SSID profile with Dot1x authentication:

# **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** { **dot11r** | **wpa2** | **dot11w** { **optional | required** } }

The following example configures an SSID profile with Dot1x EAP-PEAP authentication:

```
configure dot1x credential c1 username wgbusr password cisco123456
configure eap-profile p1 dot1x-credential c1
configure eap-profile p1 method peap
configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1 key-management
 wpa2
```

Configuring Radio Interface for Workgroup Bridges

- From the available two radio interfaces, before configuring WGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  # **configure dot11radio** *radio-interface* **mode root-ap**

  Example

  ```
  # configure dot11radio 0 mode root-ap
  ```

  Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

- Map a radio interface to a WGB SSID profile by entering this command:

  # **configure dot11radio** *radio-interface* **mode wgb ssid-profile** *ssid-profile-name*

  Example

  ```
  # configure dot11radio 1 mode wgb ssid-profile psk_ssid
  ```

- Configure a radio interface by entering this command:

  # **configure dot11radio** *radio-interface*{ **enable | disable** }

  Example

  ```
  # configure dot11radio 0 disable
  ```

  Note After configuring the uplink to the SSID profile, we recommend you to disable and enable the radio for the changes to be active.

Note Only one radio or slot is allowed to operate in WGB mode.

Configuring Workgroup Bridge Timeouts

The timer configuration CLIs are common for both WGB and uWGB. Use the following commands to configure timers:

- Configure the WGB association response timeout by entering this command:

  # **configure wgb association response timeout** *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.

- Configure the WGB authentication response timeout by entering this command:

  # **configure wgb authentication response timeout** *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.

- Configure the WGB EAP timeout by entering this command:

  # **configure wgb eap timeout** *timeout-secs*

  The default value is 3 seconds. The valid range is between 2 and 60 seconds.

- Configure the WGB bridge client response timeout by entering this command:

  # **configure wgb bridge client timeout** *timeout-secs*

  Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.

Flex Antenna Band Configuration

Flex antenna band configuration is supported on IW6300, ESW6300, and WP-WiFi6.

Use the following command to set antenna band to dual or single:

```
# configure wgb antenna band mode {dual|single}
```

Use the following command to check if WGB antenna band is set successfully:

```
# show configuration | inc Band
```

For WP- WiFi6, use the following command to check WGB antenna band set by GPIO values. For single band: GPIO_34 : 0, GPIO_35 : 1. For dual band: GPIO_34 : 1, GPIO_35 : 0.

```
# show capwap client config | inc GPIO
GPIO_34                            : 1
GPIO_35                            : 0
```

Note IW6300 and ESW6300 do not suppot to check GPIO values.