Configure Workgroup Bridges with PEAP Authentication

Contents

Introduction

This document describes how to configure a Work Group Bridge (WGB) to connect to an 802.1X Service Set Identifier (SSID) that uses Protected Extensible Authentication Protocol (PEAP) with a 9800 Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- C9800 WLC
- WGB
- 802.1X protocol

Components Used

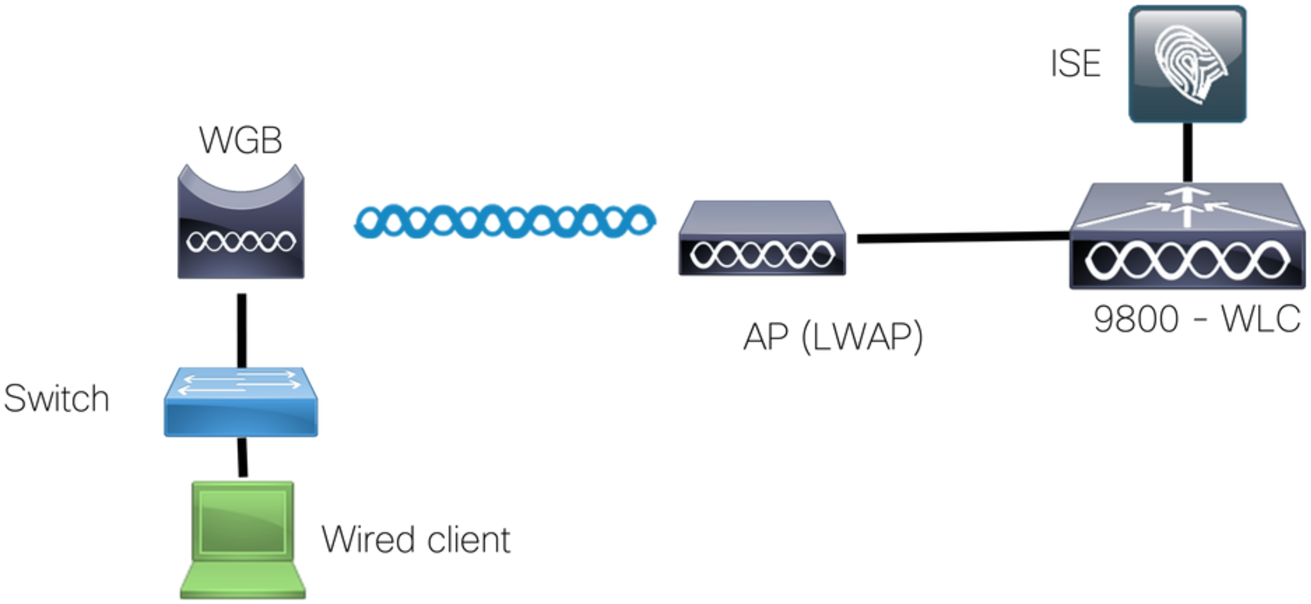
The information in this document is based on these software and hardware versions:

- Cisco IOS® Release 15.3(3)JPN1 for WGB
- Cisco IOS XE Release 17.9.2 for WLC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram

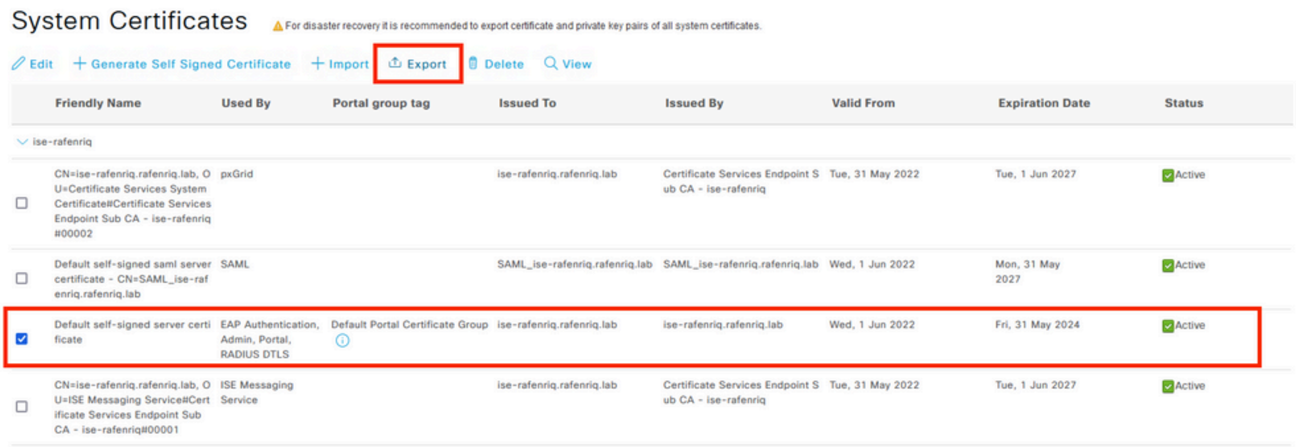


In this example, the IW3702 Autonomous Access Point (AP) is configured as a WGB and connects to the Lightweight Access Point network. Use this SSID, **dot1XSSID-R**, for the connection to the WLAN and use the PEAP for the authentication of the WGB to the network.

Configure WGB

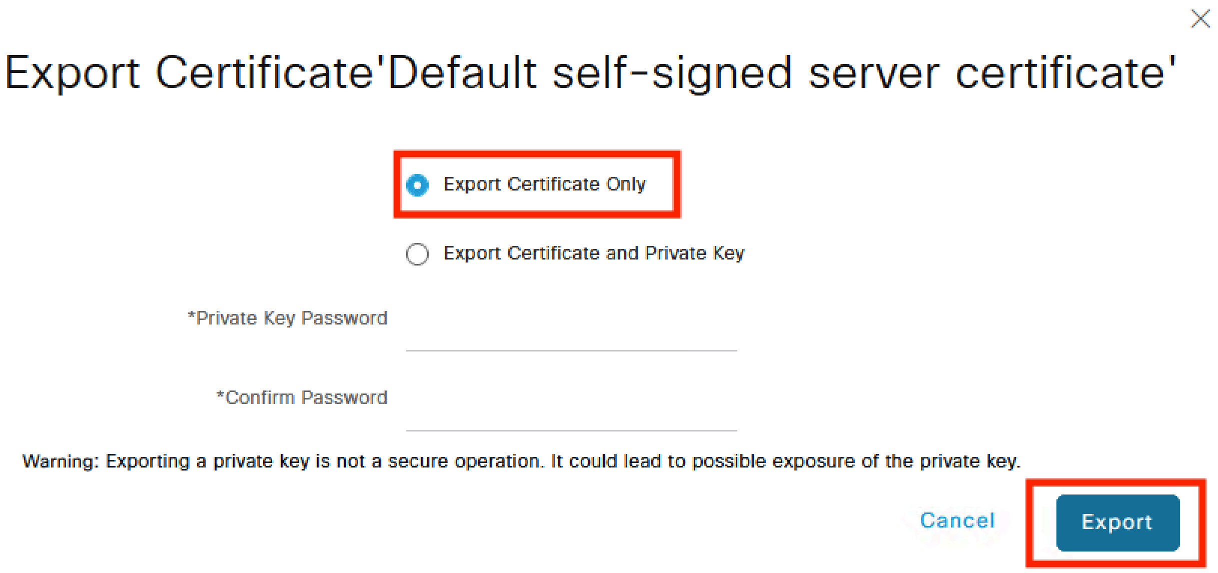
In order to configure the WGB, complete these steps:

1. Set the hostname.
```
configure terminal
hostname WGB-Client
```
2. Configure the time. The time must be correct so the certificate can be installed on the WGB.
```
clock set hh:mm:ss dd Month yyyy
example: clock set 15:33:00 15 February 2023
```
3. Configure the trustpoint for the Certificate Authority (CA): enrollment terminal - allows you to copy/paste the certificate from the authenticator. In this case, Identity Services Engine (ISE) to WGB.revocation - check none. We tell the WGB not to perform any further verification on the server certificate. This command is necessary to avoid the problem described in Cisco bug ID CSCsl07349 (registered customers only). WGB disassociates/reassociates often and takes a long time to reconnect.
```
crypto pki trustpoint isecert
enrollment terminal
revocation-check none
```
4. Download the authenticator certificate. Obtain a copy of the CA certificate. For this example, we used ISE as the Authenticator server. Navigate to **Administration > System > Certificates**.Identify the certificate that ISE uses for EAP authentication (the Use By column has EAP Authentication) and download it, as shown in the screenshots.The previous steps result in a .pem file. This is the certificate to be installed in the WGB so the tunnel can be established and within it credentials are exchanged.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-rafenriq								
□	CN=ise-rafenriq.rafenriq.lab, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise-rafenriq #00002	pxGrid		ise-rafenriq.rafenriq.lab	Certificate Services Endpoint Sub CA - ise-rafenriq	Tue, 31 May 2022	Tue, 1 Jun 2027	✓Active
□	Default self-signed saml server certificate - CN=SAML_ise-rafenriq.rafenriq.lab	SAML		SAML_ise-rafenriq.rafenriq.lab	SAML_ise-rafenriq.rafenriq.lab	Wed, 1 Jun 2022	Mon, 31 May 2027	✓Active
☑	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise-rafenriq.rafenriq.lab	ise-rafenriq.rafenriq.lab	Wed, 1 Jun 2022	Fri, 31 May 2024	✓Active
□	CN=ise-rafenriq.rafenriq.lab, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - ise-rafenriq#00001	ISE Messaging Service		ise-rafenriq.rafenriq.lab	Certificate Services Endpoint Sub CA - ise-rafenriq	Tue, 31 May 2022	Tue, 1 Jun 2027	✓Active



Export Certificate'Default self-signed server certificate'

● Export Certificate Only

○ Export Certificate and Private Key

*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

5. Install the CA certificate: Enter the **crypto pki authenticate isecert** command.Open the .pem file in a text editor and copy the string. The format is as follows:

```
-----BEGIN CERTIFICATE-----
[ ... ]
-----END CERTIFICATE-----
```

   Copy/paste the CA certificate > blank line press **Enter** > enter **quit** on the last line by itself.Paste the text from the .cer file downloaded in the previous step.

```
   -----BEGIN CERTIFICATE-----
   [ ... ]
   -----END CERTIFICATE----
(hit enter)
   quit
(hit enter)
   Certificate has the following attributes:
   Fingerprint: 45EC6866 A66B4D8F 2E05960F BC5C1B76
   % Do you accept this certificate? [yes/no]: yes
   Trustpoint CA certificate accepted.
   % Certificate successfully imported
```

6. Define the authentication method on WGB, in this case **peap**.

```
conf terminal
eap profile peap
method peap
end
```

7. Configure credentials for WGB, in this case **cred**. Make sure to add the trustpoint we created, in this case **isecert**.

```
dot1x credentials CRED
```

```
username userWGB
password 7 13061E010803
pki-trustpoint isecert
```

8. Configure SSID on WGB, and make sure you use the correct string for the EAP profile and credentials, in this case **peap** and **cred**, respectively.

```
configure terminal
dot11 ssid dot1XSSID-R
authentication open eap PEAP
authentication key-management wpa
dot1x credentials cred
dot1x eap profile peap
infrastructure-ssid
```

At this point, the AP configuration looks like this example. Enter the **show run** command.

```
Building configuration...
version 15.3
!
hostname WGB-Client
!
.....
!
dot11 ssid dot1XSSID-R
  authentication open eap PEAP
  authentication key-management wpa
  dot1x credentials cred
  dot1x eap profile peap
  infrastructure-ssid
!
eap profile PEAP
 method peap
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint isecert
 enrollment terminal
 revocation-check none
!
crypto pki certificate chain isecert
 certificate ca 5CC74BD9508B78AF4AB5C5F84C32AC2A
 ...
 C3B7249C F75C4525 D02A40AB 50E19196 9D1C2853 8BAEFDFC 1CE1945E 1CABC51B AFF5
     quit
!
dot1x credentials PEAP
 username userWGB
 password 7 13061E010803
 pki-trustpoint isecert
!
....
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid dot1XSSID-R
 !
 antenna gain 0
 station-role workgroup-bridge
 bridge-group 1
 bridge-group 1 spanning-disabled
!
.....
```

Verify

Use this section to confirm that your configuration works properly.

In order to verify the association on WGB, show the dot11 associations.

The WGB association from the WLC looks like this example:

```
9800#show wireless client summary

Number of Clients: 3
MAC Address     AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------------
-------------------------
843d.c6e8.76e0 AP687D.B45C.46E8                               WLAN 3    RUN           11ac
Dot1x      Local

9800-rafenriq#show wireless wgb summary

Number of WGBs: 1
MAC Address     AP Name                          WLAN State              Clients

---------------------------------------------------------------------------------
843d.c6e8.76e0 AP687D.B45C.46E8                 3    RUN           2

9800-rafenriq#show wireless wgb mac-address 843d.c6e8.76e0 detail

Work Group Bridge
MAC Address        : 843d.c6e8.76e0
AP Name            : AP687D.B45C.46E8
WLAN ID            : 3
State              : RUN

Number of Clients: 2
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Debug the Workgroup Bridge

In order to debug the WGB, enter these commands:

```
debug aaa authentication
debug dot11 supp-sm-dot1
```

Debug WGB in the WLC

As WGB behaves as another wireless client, see Troubleshoot Catalyst 9800 Client Connectivity Issues Flow in order to collect traces and captures on the 9800 WLC.