Easy PSK Deployment Guide

Easy PSK Overview

With the number of devices connecting to the internet increasing rapidly, a simple and easy way to implement a security mechanism is recommended for large-scale deployments. One such solution is Easy PSK feature. This feature bundles several pre-shared keys (PSKs) onto an SSID and performs client group authentication and authorization on the PSKs. Easy PSK feature eliminates the need for client preregistration, and automatically adds a client to a group and applies the requisite policies. This feature also provides the means to limit peer-to-peer communication among the clients of a group.

PSK grouping on an SSID is useful for different deployment scenarios such as multidwelling units, university halls, hospitality centers, and hospitals where a single SSID offers efficient use of airtime and roaming capabilities across the access infrastructure while segregating clients as if they were on a private SSID.

Recommendations and Limitations

- This feature supports only Local Mode, Central Authentication, and Central Switching
- When used with iPSK peer-to-peer blocking, this feature blocks traffic between the clients sharing the same VLAN, but not the same passphrases
- This feature is supported only on the following controllers:
- Cisco Catalyst 9800-CL Cloud Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- CW 9800-M, H1, H2 Wireless Controllers
- This feature is not supported in Cisco Embedded Wireless Controller (EWC)
- This feature is not supported in fabric mode
- This feature is not supported with WPA3

Setup Options

The 9800 WLC can be setup in two distinct ways:

1. WLC integrated with AAA directly
2. WLC integrated with ISE as proxy

Note: In the example below, it is assumed that the PSK computation is handled by the radius server with all the AAA related configuration in place, and therefore only the WLC-related configurations are highlighted.

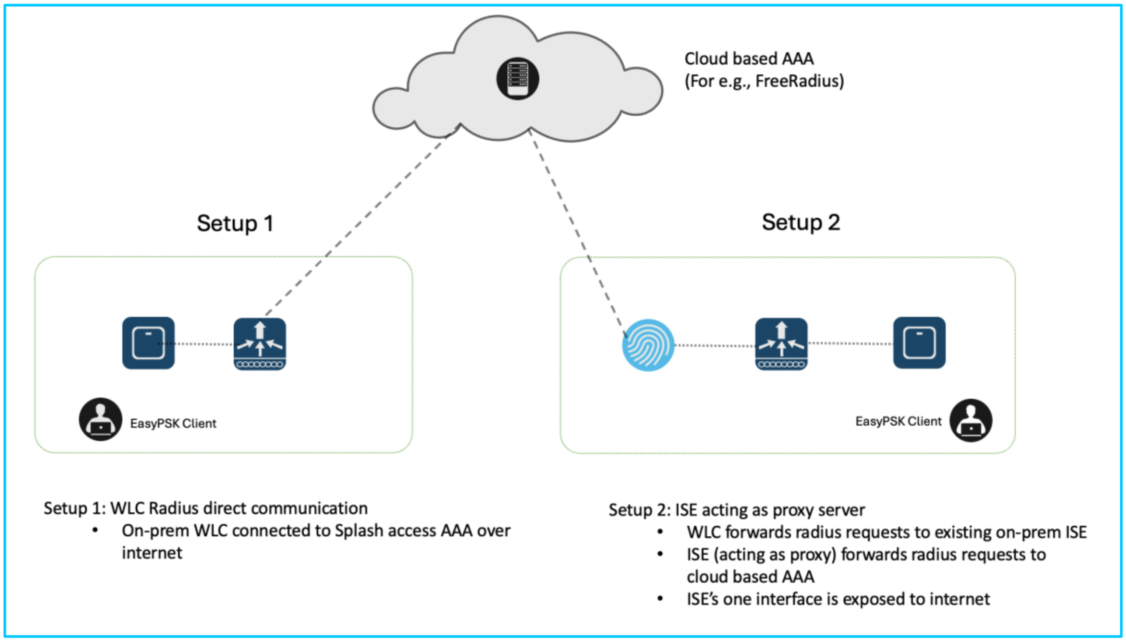

Cloud based AAA
(For e.g., FreeRadius)
Setup 1
Setup 2
EasyPSK Client
EasyPSK Client
Setup 1: WLC Radius direct communication
• On-prem WLC connected to Splash access AAA over internet
Setup 2: ISE acting as proxy server
• WLC forwards radius requests to existing on-prem ISE
• ISE (acting as proxy) forwards radius requests to cloud based AAA
• ISE's one interface is exposed to internet

Figure 1. 9800 WLC Setup with AAA Server

Configuration

Step 1: Configure AAA server details by entering the IP address and setting up a radius server group

Step 2: Configure a named authorization list for the servers that are a part of the RADIUS server group

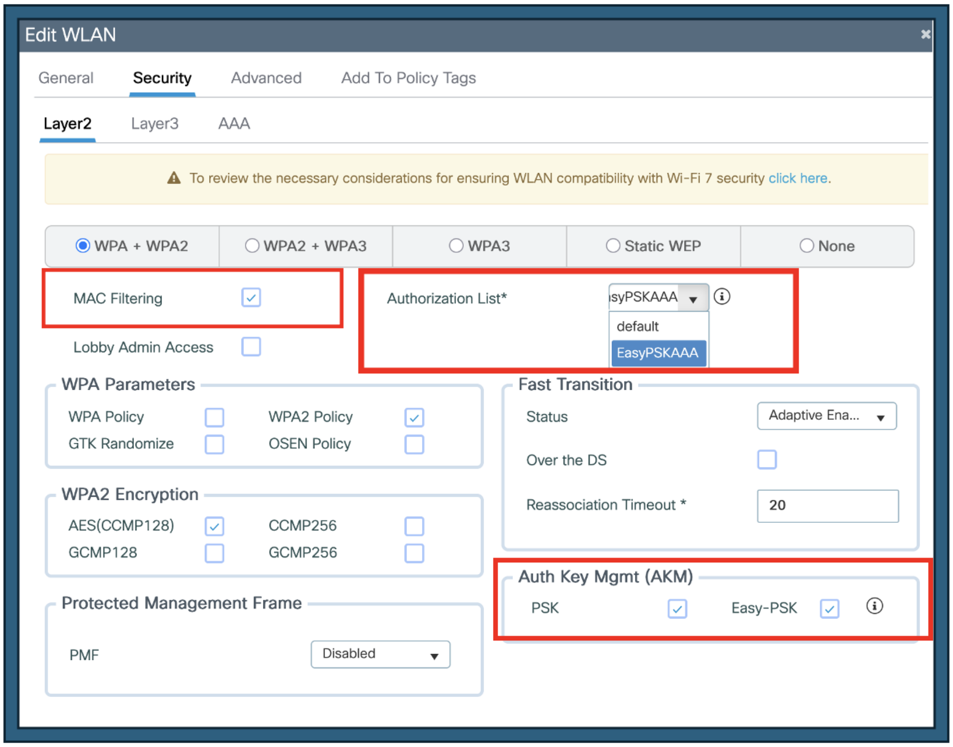
Step 3: Configure the SSID with Easy PSK enabled along with Mac-filtering.

Step 4: Set the authorization list to the named AAA server

Step 5: Check the PSK and Easy-PSK check box

Step 6: Click Update and Apply to Device

Step 7: Select 'Allow AAA Override' for the respective policy profile under Advanced option



Edit WLAN

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security click here.

● WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ○ None

MAC Filtering ☑

Authorization List* syPSKAAA (default / EasyPSKAAA)

Lobby Admin Access □

WPA Parameters

WPA Policy □ WPA2 Policy ☑
GTK Randomize □ OSEN Policy □

WPA2 Encryption

AES(CCMP128) ☑ CCMP256 □
GCMP128 □ GCMP256 □

Protected Management Frame

PMF Disabled

Fast Transition

Status Adaptive Ena...

Over the DS □

Reassociation Timeout * 20

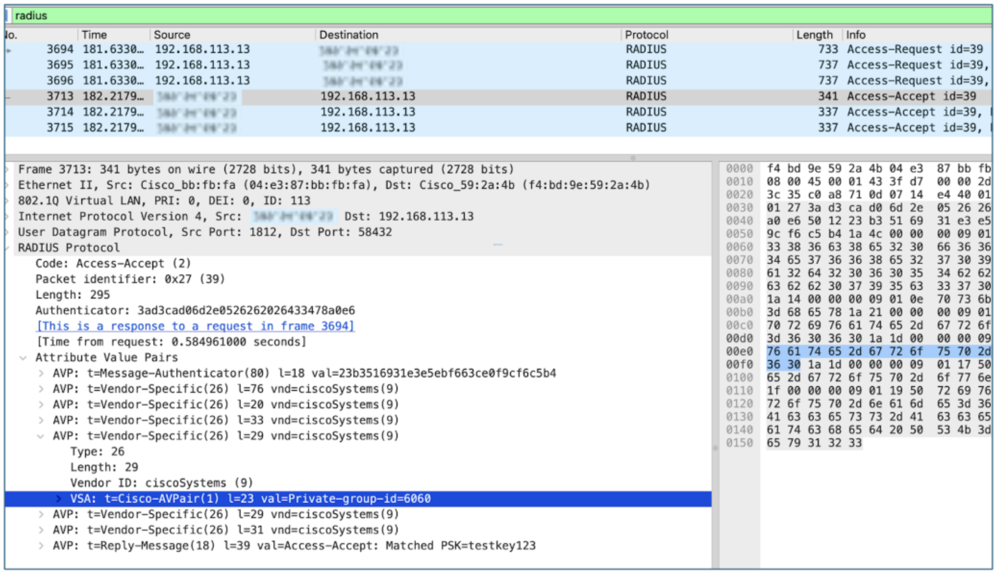
Auth Key Mgmt (AKM)

PSK ☑ Easy-PSK ☑

Figure 2. **WLAN Configuration**

Verify

Try Connecting a client by entering the PSK:



```
radius
No.    Time       Source          Destination      Protocol   Length Info
  3694 181.6330…  192.168.113.13  [redacted]       RADIUS        733 Access-Request id=39
  3695 181.6330…  192.168.113.13  [redacted]       RADIUS        737 Access-Request id=39,
  3696 181.6330…  192.168.113.13  [redacted]       RADIUS        737 Access-Request id=39,
  3713 182.2179…  [redacted]      192.168.113.13   RADIUS        341 Access-Accept id=39
  3714 182.2179…  [redacted]      192.168.113.13   RADIUS        337 Access-Accept id=39,
  3715 182.2179…  [redacted]      192.168.113.13   RADIUS        337 Access-Accept id=39,
```

```
> Frame 3713: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits)
> Ethernet II, Src: Cisco_bb:fb:fa (04:e3:87:bb:fb:fa), Dst: Cisco_59:2a:4b (f4:bd:9e:59:2a:4b)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 113
> Internet Protocol Version 4, Src: [redacted] Dst: 192.168.113.13
> User Datagram Protocol, Src Port: 1812, Dst Port: 58432
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x27 (39)
    Length: 295
    Authenticator: 3ad3cad06d2e0526262026433478a0e6
    [This is a response to a request in frame 3694]
    [Time from request: 0.584961000 seconds]
  v Attribute Value Pairs
    > AVP: t=Message-Authenticator(80) l=18 val=23b3516931e3e5ebf663ce0f9cf6c5b4
    > AVP: t=Vendor-Specific(26) l=76 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
        Type: 26
        Length: 29
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=23 val=Private-group-id=6060
    > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Reply-Message(18) l=39 val=Access-Accept: Matched PSK=testkey123
```

```
0000  f4 bd 9e 59 2a 4b 04 e3  87 bb fb
0010  08 00 45 00 01 43 3f d7  00 00 2d
0020  3c 35 c0 a8 71 0d 07 14  e4 40 01
0030  01 27 3a d3 ca d0 6d 2e  05 26 26
0040  a0 e6 50 12 23 b3 51 69  31 e3 e5
0050  9c f6 c5 b4 1a 4c 00 00  00 09 01
0060  33 38 36 63 38 65 32 30  66 36 36
0070  34 65 37 36 36 38 65 32  37 30 39
0080  61 32 64 32 30 36 30 35  34 62 62
0090  63 62 62 30 37 39 35 63  33 37 30
00a0  1a 14 00 00 00 09 01 0e  70 73 6b
00b0  3d 68 65 78 1a 21 00 00  00 09 01
00c0  70 72 69 76 61 74 65 2d  67 72 6f
00d0  3d 36 30 36 30 1a 1d 00  00 00 09
00e0  76 61 74 65 2d 67 72 6f  75 70 2d
00f0  36 30 1a 1d 00 00 00 09  01 17 50
0100  65 2d 67 72 6f 75 70 2d  6f 77 6e
0110  1f 00 00 00 09 01 19 50  72 69 76
0120  72 6f 75 70 2d 6e 61 6d  65 3d 36
0130  41 63 63 65 73 73 2d 41  63 63 65
0140  61 74 63 68 65 64 20 50  53 4b 3d
0150  65 79 31 32 33
```

Figure 3. **Packet Capture on WLC Uplink**

Troubleshooting

The below commands may be used for troubleshooting:

- show wireless client upn
- show wireless client <mac> | sec Private
- show wireless client upn <group name>

The “Private Network” information will be made up of 3 new Radius Vendor Specific Attributes (VSA):

private-group-id

private-group-name

private-group-owner

References

1. UDN Plus Deployment Guide

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.