Easy PSK

Feature History for Easy PSK

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 Easy PSK

Release	Feature	Feature Information
Cisco IOS XE Bengaluru, 17.5.1	Easy PSK	The Easy PSK feature provides a simple and easy way to implement security mechanism for large-scale deployments. The Easy PSK feature is released as an Early Field Trial feature in this release and has been tested against third-party AAA servers and gateways.

Information About Easy PSK

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.

Note A RADIUS server is required for the Easy PSK feature to work, because the RADIUS takes care of matching the PSK and informing the controller.

Use Cases

The following are the use cases and functionalities supported by the Easy PSK feature:

- WPA2
- APs in connected mode
- Multiple PSKs per SSID
- Installation of policy per PSK
- Local mode
- Central traffic switching
- Multiple unit SSIDs per AP (maxium 16)
- Unicast traffic segregation
- Multicast traffic segregation
- Central client association
- Central client authentication
- Management through CLI, web UI, NETCONF, and SNMP
- Roaming between APs
- Interoperability with third-party RADIUS server

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

- This feature is not supported in Cisco Embedded Wireless Controller (EWC).
- This feature is not supported in fabric mode.
- Maximum APs per named site-tag:
  - Cisco Catalyst 9800-CL Cloud Wireless Controller: 800
  - Cisco Catalyst 9800-L Wireless Controller: 500
  - Cisco Catalyst 9800-40 Wireless Controller: 800
  - Cisco Catalyst 9800-80 Wireless Controller: 800
- Maximum available VLANs: 4090
- Traffic segregation per PSK: Unicast and Multicast
- Traffic segregation method: VLAN and iPSK tag
- Common areas: All users can connect
- Throughput limit per controller:
  - Cisco Catalyst 9800-CL Cloud Wireless Controller: 2.1 Gbps
  - Cisco Catalyst 9800-L Wireless Controller: 10 Gbps
  - Cisco Catalyst 9800-40 Wireless Controller: 40 Gbps
  - Cisco Catalyst 9800-80 Wireless Controller: 80 Gbps

Configuration Workflow

1. Configuring RADIUS Server, RADIUS Server Groups, and Mac-Filtering List
2. Configuring Easy PSK (CLI)
3. Configure a Policy Profile
4. Configure a Policy Tag
5. Attach Policy to AP

Configuring RADIUS Server, RADIUS Server Groups, and Mac-Filtering List

Note For information about GUI configuration for the RADIUS and Mac filtering, see AAA Wizard section.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA new model configuration.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server easy_psk_server`	Creates a RADIUS server and enters RADIUS server configuration mode.
Step 4	**address ipv4** *ip-address* **auth-port** *auth-port-num* **acct-port** *acct-port-num* **Example:** `Device(config-radius-server)# address ipv4 21.0.0.3 auth-port 1812 acct-port 1813`	Specifies the RADIUS server IP address and the port used for authentication and accounting requests, as well as the port used for such requests.
Step 5	**aaa group server radius** *server-group-name* **Example:** `Device(config-radius-server)# aaa group server radius easy_psk_servers_group`	Configures a RADIUS server group.
Step 6	**server name** *server-name* **Example:** `Device(config-sg-radius)# server name easy_psk_server`	Adds the RADIUS server as a member of the RADIUS server group.
Step 7	**throttle access** *outstanding-requests* **access-timeout** *timeout* **Example:** `Device(config-sg-radius)# throttle access 100 access-timeout 10`	(Optional) Adds throttling of AAA requests sent to RADIUS servers, making it a part of the RADIUS server group.
Step 8	**exit** **Example:** `Device(config-sg-radius)# exit`	Returns to global configuration mode.
Step 9	**aaa authorization network** *server-list* **group** *server-group-name* **Example:**	Configures a named authorization list for the servers that are a part of the RADIUS server group.

	Command or Action	Purpose
	`Device(config)# aaa authorization network easypsk_list group easy_psk_servers_group`	
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Example

```
aaa new-model
 radius server easy_psk_server
 address ipv4 21.0.0.3 auth-port 1812 acct-port 1813
  aaa group server radius easy_psk_servers_group
  server name easy_psk_server
aaa authorization network easypsk_list group easy_psk_servers_group
```

Configuring Easy PSK (CLI)

Before you begin

Set **aaa-override** to the wireless profile policy associated with the WLAN used in the Easy PSK feature.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-epsk 3 ssid-epsk`	Configures a WLAN and enters WLAN configuration submode. **Note** If you have already configured a WLAN, run the **wlan** *profile-name* command.
Step 3	**mac-filtering** *mac-filter-name* **Example:** `Device(config-wlan)# mac-filtering easypsk_list`	Enables MAC filtering on the WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables dot1x security on the WLAN.

	Command or Action	Purpose
Step 5	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the security type as PSK on the WLAN.
Step 6	**security wpa wpa2 easy-psk** **Example:** `Device(config-wlan)# security wpa wpa2 easy-psk`	Configures the Easy PSK feature on the WLAN.
Step 7	**peer-blocking allow-private-group** **Example:** `Device(config-wlan)# peer-blocking allow-private-group`	(Optional) Enables peer-to-peer blocking between peers that are sharing the same VLAN, but use different passphrases.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Example

```
configure terminal
 wlan wlan-epsk 3 ssid-epsk
  mac-filtering easypsk_list
  no security wpa akm dot1x
  security wpa akm psk
  security wpa wpa2 easy-psk
  peer-blocking allow-private-group
  no shutdown
```

Configuring Easy PSK (GUI)

Procedure

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

Step 2 From the list of WLANs, choose a WLAN.

The **Edit WLAN** window is displayed.

Step 3 Click the **Security** tab.

Step 4 Click the **Layer2** tab.

Step 5 From the **Layer 2 Security Mode** drop-down list, choose the WPA + WPA2 security method.

Step 6 In the **Auth Key Mgmt** area, uncheck the **802.1x** check box.

Step 7 Check the **PSK** check box.

Step 8 Check the **Easy-PSK** check box.

Step 9 Check the **MAC Filtering** check box to enable MAC filtering.

Step 10 From the **Authorization List** drop-down list, choose an authorization list.

Step 11 Click **Update &Apply to Device**.

Verifying Easy PSK

To verify whether the Easy PSK feature is enabled on WLANs, use the following command:

```
Device# show wlan summary

Number of WLANs: 1

ID   Profile Name    SSID            Status Security
-------------------------------------------------------------------------------
9    easypsk         easypsk         UP     [WPA2][EASYPSK][AES],MAC Filtering
```

To verify whether the Easy PSK feature is enabled on a WLAN profile, use the following command:

```
Device# show wlan name easypsk

WLAN Profile Name     : easypsk
================================================
Identifier                                       : 19
Description                                      :
Network Name (SSID)                              : easypsk
Status                                           : Disabled
.
.
.
Security
    802.11 Authentication                        : Open System
    Static WEP Keys                              : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)       : Enabled
        WPA (SSN IE)                             : Disabled
        WPA2 (RSN IE)                            : Enabled
            MPSK                                 : Disabled
            EasyPSK                              : Enabled
            AES Cipher                           : Enabled
            CCMP256 Cipher                       : Disabled
            GCMP128 Cipher                       : Disabled
            GCMP256 Cipher                       : Disabled
            Randomized GTK                       : Disabled
        WPA3 (WPA3 IE)                           : Disabled
```

To verify the MAC filter authorization list used on a WLAN profile, use the following command:

```
Device# show wlan name easypsk

WLAN Profile Name     : easypsk
================================================
Identifier                                       : 19
```

```
Description                                     :
Network Name (SSID)                             : easypsk
Status                                          : Disabled
Broadcast SSID                                  : Enabled
.
.
.
DTIM period for 802.11b radio                   :
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : easypsk_list
Mac Filter Override Authorization list name     : Disabled
.
.
.
```