



8.5 Identity PSK Feature Deployment Guide

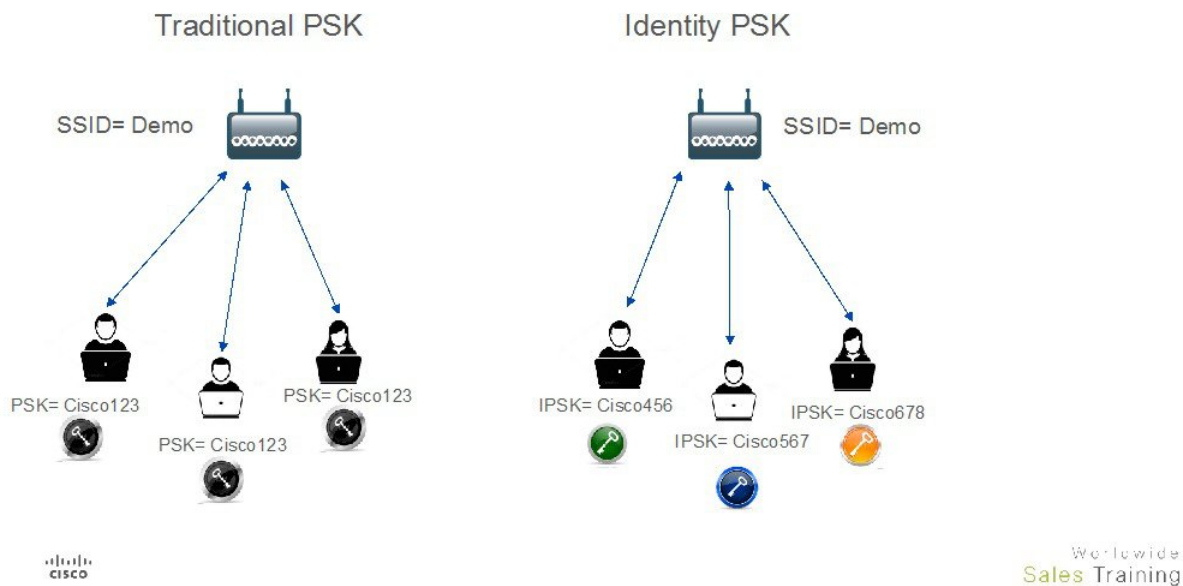
Product or Feature Overview	2
IPSK solution	2
Configurations Steps for IPSK in 8.5 release	3
Controller Configuration Steps	6
WLC Local Policies Combined with IPSK	10
Introduction to Profiling and Policy Engine on the WLC	11
Scope and Objectives	12
Profiling and Policy Configuration	12
Mapping Policy on WLAN	17
Interface Group Override	20
End User Device Setup	21
Conclusion	22
IPSK Configuration through CLI commands	23

Product or Feature Overview

With the advent of internet of things, the number of devices that connect to the internet is increased multifold. Not all of these devices support 802.1x supplicant and need an alternate mechanism to connect to the internet. One of the security mechanisms, WPA-PSK could be considered as an alternative. With the current configuration, the pre-shared-key is the same for all clients that connect to the same WLAN. In certain deployments such as Educational Institutions, this results in the key being shared to unauthorized users resulting in security breach. Therefore, above mentioned and other requirements lead to the need for provisioning unique pre-shared keys for different clients on a large scale.

- Identity PSKs are unique pre-shared keys created for individuals or groups of users on the same SSID.
- No complex configuration required for clients. The same simplicity of PSK, making it ideal for IoT, BYOD, and guest deployments.
- Supported on most devices, where 802.1X may not, enabling stronger security for IoT.
- Easily revoke access, for a single device or individual, without affecting everyone else.
- Thousands of keys can easily be managed and distributed via the AAA server.

Traditional Vs Identity PSK



As depicted in the above diagram, in the Traditional PSK, for all the clients that connect to a particular SSID, the key would remain same leading to security issues. With Identity PSK, every client connecting to the same SSID can have potentially a different key.

IPSK solution

During client authentication, the AAA server would authorize the client mac address and send the passphrase (if configured) as part of the Cisco-AVPair list. The WLC would receive this as part of the radius response and would process this further for the computation of PSK.

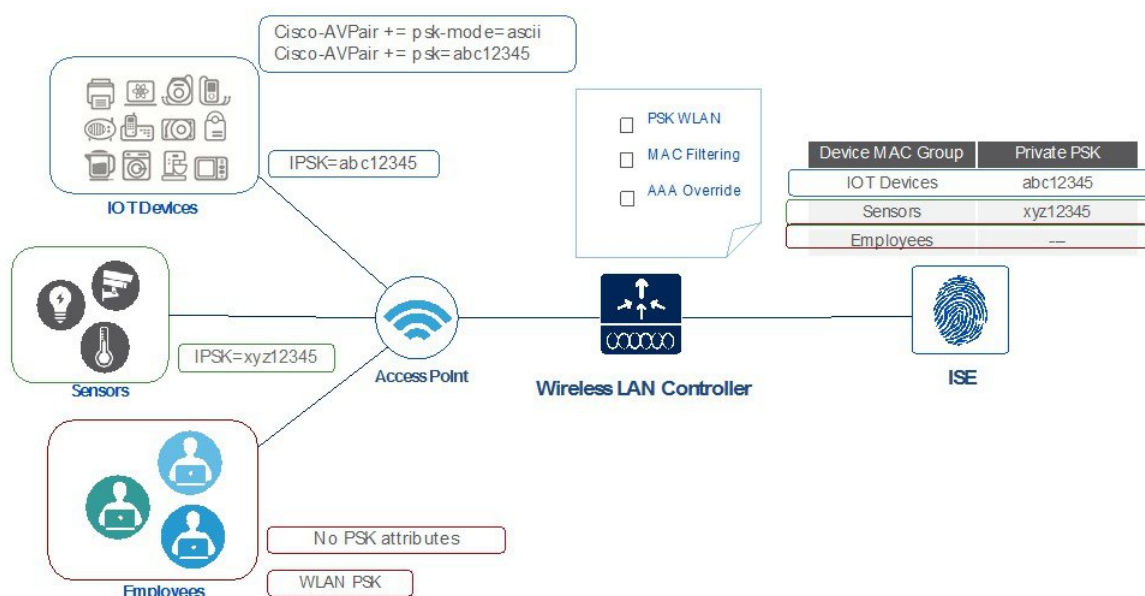
When the client sends association request to the SSID broadcasted by the access point, the Wireless LAN Controller forms the RADIUS request packet with the particular mac address of the client and relays to the RADIUS server.

The RADIUS server performs the authentication and checks whether the client is allowed or not and sends either ACCESS-ACCEPT or ACCESS-REJECT as response to the WLC.

To support Identity PSK, in addition to sending the authentication response, the authentication server would also provide the AV Pair passphrase for this specific client. This is used further for the computation of PSK.

The RADIUS server could also provide additional parameters such as username, VLAN, QoS, etc in the response, that is specific to this client. For multiple devices that is owned by a single user, the passphrase could remain the same.

Private PSK On The same WLAN



Configurations Steps for IPSK in 8.5 release

IPSK can be configured on any AAA server that supports Cisco av-pair. In this deployment guide we focus on the configuration on the Cisco Identity Service Engine. ISE 2.2 Configuration Steps

Procedure

Step 1 Add wireless controller under test on ISE as shown below with a secret password configured in "Radius Authentication Setting" and then Submit the configuration.

Identity Services Engine

Home > Context Visibility > Operations > Policy > **Administration** > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers

Network devices

Default Device

Device Security Settings

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location
<input type="checkbox"/> NAD_10.10.10.2	10.10.10.2/32	Cisco	All Locations

Network Devices List > [New Network Device](#)

Network Devices

* Name: NAD

Description: Wireless Controller

* IP Address: 10.10.10.2 / 32

* Device Profile: Cisco

Model Name: 3504

Software Version: 8.5

* Network Device Group

Device Type: All Device Types

IPSEC: Is IPSEC Device

Location: All Locations

☒ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit Cancel

Step 2

Create an Authorization Profile and verify it Under Policy>Results>Authorization> Authorization Profiles IPSK-Device as shown in example below.

Identity Services Engine

Home > Context Visibility > Operations > **Policy** > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Click here to do wireless setup and visibility setup Do not show this

Dictionary Conditions **Results**

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit Add Duplicate Delete

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/> IPSK-device	Cisco	Identity PSK
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Suppliment Provisioning

Selected 0 | Total 8

Show All

Step 3 Create Authorization profile With Access Type Access_Accept with cisco-av-pair(s) with psk-mode and psk password as shown in the example below is configured.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for an Authorization Profile. The breadcrumb trail is "Policy > Authorization Profiles > IPSK-device". The left sidebar shows the navigation menu with "Authorization Profiles" highlighted. The main content area is titled "Authorization Profile" and contains the following fields:

- * Name: IPSK-device
- Description: Identity PSK
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco

Below these fields is the "Advanced Attributes Settings" section, which contains two rows of attributes:

Attribute	Value
Cisco:cisco-av-pair	psk-mode=ascii
Cisco:cisco-av-pair	psk=abc12345

At the bottom is the "Attributes Details" section, which displays the configured attributes:

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=abc12345
```

At the bottom of the page are "Save" and "Reset" buttons.

Step 4 Under Policy> Authorization Configure Rule for every Device or User MAC address to be used with IPSK as shown in example below. Use as many Mac address entries as you wish.

Note Rule is linked to the Profile created in step 3.

Note Make sure Mac address of the device configured properly. We have configured Apple MacBook laptop Mac address for this Exercise.

Identity Services Engine Home Context Visibility Operations **Policy** Administration Work Centers

Authentication **Authorization** Profiling Posture Client Provisioning Policy Elements

Click here to do wireless s

Authorization Policy

Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	IdentityPSK	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS A0:3B:E3:95:73:4E)	then IPSK-device
✓	IdentityPSK_copy	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS f4:5c:89:8f:10:43)	then IPSK-device
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	IdentityPSK	if Any and Wireless_MAB AND Radius:Callin...	then IPSK-device
✓	IdentityPSK_copy	if Wireless_MAB AND Radius f4:5c:89:8f:10:43	then
✓	Wireless Black List Default	if Blacklist AND Wireless_Ac	then
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiling_Phones	then Non_Cisco_IP_Phones

Condition Name **Description**

Wireless_MAB Normalised Radius:RadiusFlowType EQUALS WirelessMAB


MAC address Radius:Calling-Sta... Equals A0:3B:E3:95:73:4E

Step 5 Verify every step performed above and make sure all configuration are applied and saved.

Controller Configuration Steps

Procedure

Step 1 Create WLAN on your controller as in the shown example Pod1-IPSK.

 **MONITOR** **WLANs** **CONTROLLER** **WIRELESS** **SECURITY** **MANAGEMENT**

WLANs

▼ **WLANs**
WLANs

► **Advanced**

WLANs > Edit 'Identity PSK'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name Identity PSK

Type **WLAN**

SSID Pod1-IPSK

Status ☒ Enabled

Security Policies **MAC Filtering[WPA2][Auth(PSK)]**
(Modifications done under security tab will appear)

Radio Policy All ▼

Interface/Interface Group(G) management ▼

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID none

Step 2 Configure WLAN with Security WPA2/PSK and enable **MAC filtering**. In the example below the PSK key used is **PSK=12345678**.

The image shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes links for MONITOR, **WLANs**, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. On the left, the 'WLANs' menu is expanded, showing 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Identity PSK''. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. In the 'Layer 2 Security' section, 'WPA+WPA2' is selected from the dropdown menu, and 'MAC Filtering' is checked. Below this, the 'Fast Transition' section shows 'Fast Transition Over the DS' checked and 'Reassociation Timeout' set to 20 seconds. The 'Protected Management Frame' section shows 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA2 Policy' checked, 'WPA2 Encryption' set to 'AES', and 'OSN Policy' unchecked. Other encryption options like TKIP, CCMP256, and GCMP128 are also visible but unchecked.

Step 3 Configure WLAN with Security WPA2/PSK and configure PSK. In the example below the PSK key used is **PSK=12345678**.

The image shows the 'Advanced' configuration page for the same WLAN. The 'Authentication Key Management' section is expanded. It lists several authentication methods: 802.1X, CCKM, **PSK**, FT 802.1X, and FT PSK. The 'PSK' option is selected and its 'Enable' checkbox is checked. Below this, the 'PSK Format' is set to 'ASCII'. A red arrow points to the PSK key field, which contains the value '12345678' (represented by dots in the image).

Step 4 Configure on the WLC the Authentication Server with ISE IP address and apply it to WLAN Pod1-IPSK created in the steps above. In our example, ISE IP address is 10.91.104.106.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs

▼ **WLANs**
WLANs

► **Advanced**

WLANs > Edit 'Identity-PSK'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

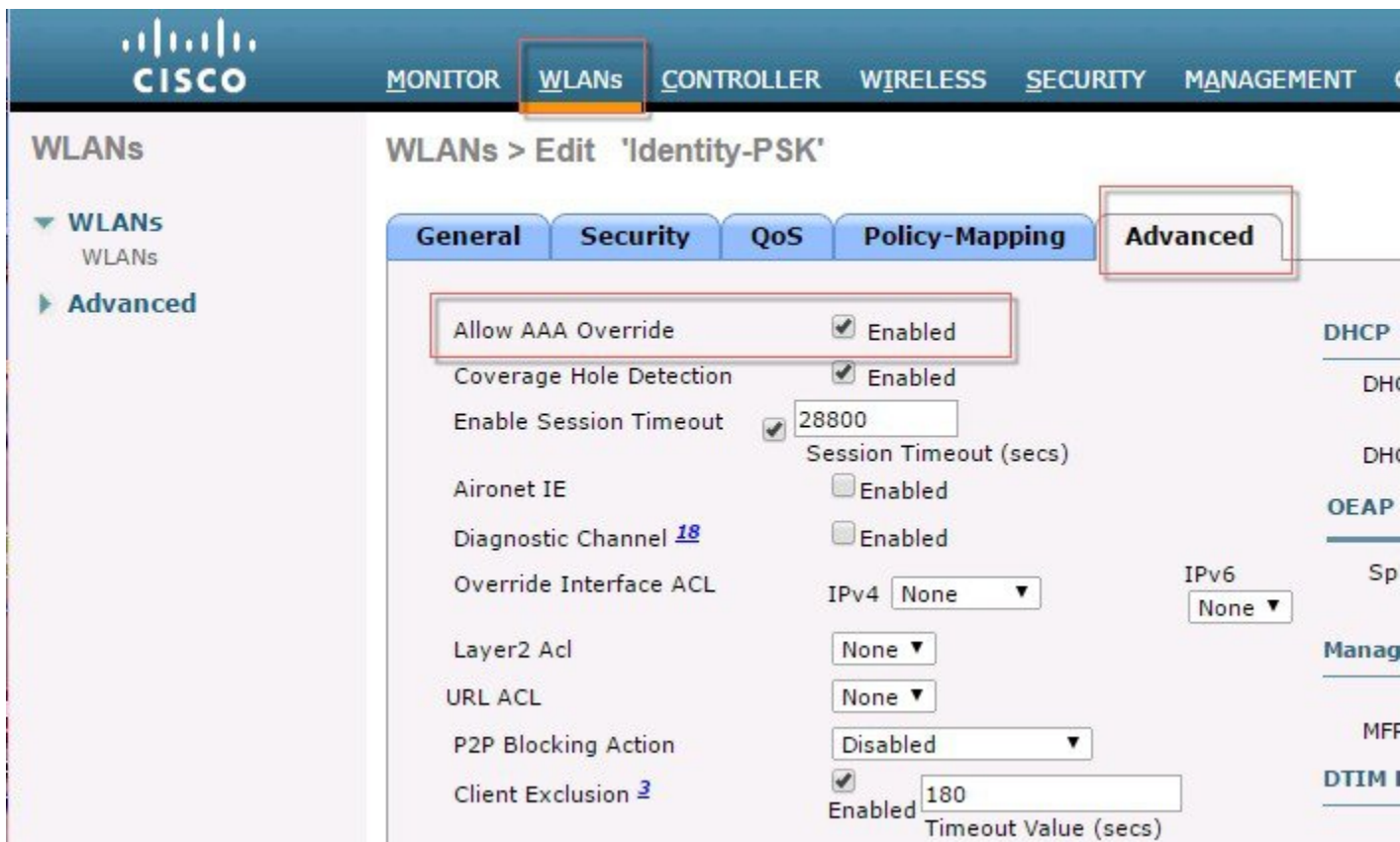
RADIUS Servers

RADIUS Server Overwrite interface ☐ Enabled

Apply Cisco ISE Default Settings ☐ Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.91.104.106, Port:1812 ▼	<input checked="" type="checkbox"/> Enabled IP:10.91.104.106, Port:1813 ▼
Server 2	None ▼	None ▼

Step 5 Lastly, under WLAN advanced settings enable AAA Override.



WLC Local Policies Combined with IPSK

Just like AVC, mDNS or Open DNS profile can be mapped to a local policy for a client with a particular device type. IPSK also can be combined with Local policies on the controller and mapped to a specific WLAN. When configuring the AV-pair=PSK-mode and PSK-password on the AAA server such as ISE, admin can easily add another AV-pair=role for example for a teacher or a student group and then configure a Local policy to that specific Role. Each local policy can be configured with a different profile name, ACL, Role, Device Type and even Active Hours based on the AAA override to restrict/permit the policy from being able to use/deny the services not allowed by the profile on the same WLAN.

When combining IPSK and Local Policies on the same WLAN the use cases can be unlimited and open to many different deployment scenarios.

For example on campus admin can configure a use case where students have to login with IPSK and then apply local policy that only those students belonging to the group Students can access specific applications at certain bandwidth on specific device and during specific time. There practically unlimited set of capabilities and tweaks available when combining the two.

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
 - Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec
 - Local Policies
- OpenDNS
- Advanced

Policy > Edit

Policy Name: IPSK-test
Policy Id: 1

Match Criteria

Match Role String:
Match EAP Type: none

Device List

Device Type	Add
<input type="text" value=""/>	<input type="button" value="Add"/>

Action

IPv4 ACL	none
URL ACL	none
VLAN ID	0
Qos Policy	none
Average Data Rate(kbps)	0
Average Real time Data Rate(kbps)	0
Burst Data Rate(kbps)	0
Burst Real time Data Rate(kbps)	0
Session Timeout (seconds)	1800
Sleeping Client Timeout (min)	720
Flexconnect ACL	none
AVC Profile	none
mDNS Profile	none
OpenDNS Profile	none

Active Hours

Day: Mon
Start Time: Hours Mins
End Time: Hours Mins

Day: Start Time: End Time:

Introduction to Profiling and Policy Engine on the WLC

Cisco currently offers a rich set of features which provide device identification, on boarding, posture, and policy, through ISE. This new feature on the WLC does the profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the end devices on the network. The user can configure the device-based policies and enforce per user or per device policy on the network. The WLC will also display statistics based on per user or per device end points and policies applicable per device.

With BYOD (Bring your own device), this feature has an impact on understanding the different devices on the network. With this, BYOD can be implemented on a small scale within the WLC itself.

Scope and Objectives

In this section, we will be configuring and implementing Profiling and Policy on a Cisco WLC running AireOS8.5 code.

The profiling and policy enforcement will be configured as two separate components. The configuration on the WLC is based on defined parameters specific to clients joining the network with IPSK security as configured in the previous sections. The policy attributes which are of interest are:

1. Role–Role defines the user type or the user group the user belongs to.
2. PSK-mode ASCII
PSK-password–match of the specific PSK password with the device MAC address
For example: Student or Employee
3. Device–Device defines the type of device.
For example: Windows machine, Smart phone, Apple device such as iPad, iPhone and so on.
4. Time of day–Allows configuration to be defined at what time of the day end-points are allowed on the network.

The above parameters are configurable as policy match attributes. Once the WLC has a match corresponding to the above parameters per end-point, the policy enforcement comes into picture. Policy enforcement will be based on session attributes such as:

- VLAN
- ACL
- Session Timeout
- QoS
- Sleeping Client
- Flexconnect ACL
- AVC profile
- mDNS profile
- Open DNS profile
- Security Group Tag

The user can configure these policies and enforce end-points with specified policies. The wireless clients will be profiled based on the MAC address, MAC OUI, DHCP, and HTTP user agent (valid Internet required for successful HTTP profiling). The WLC uses these attributes and predefined classification profiles to identify the device.

Profiling and Policy Configuration

Procedure

Step 1 To configure device profiling on a WLAN, go to the specific WLAN on which you want to implement Native profiling and policy and click **Advanced**. Disable **Allow AAA Override** if it is enabled. In the **DHCP** area, check the Required check box for **DHCP Addr. Assignment**.

WLANs > Edit 'POD1-dot1x' < Back Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Allow AAA Override ☐ Enabled
 Coverage Hole Detection ☒ Enabled
 Enable Session Timeout ☒ 1800
 Session Timeout (secs)
 Aironet IE ☒ Enabled
 Diagnostic Channel ☐ Enabled
 Override Interface ACL IPv4 IPv6
 Layer2 Acl
 P2P Blocking Action
 Client Exclusion ☒ Enabled 60
 Timeout Value (secs)
 Maximum Allowed Clients
 DTIM Period (in beacon intervals)

DHCP
 DHCP Server ☐ Override
 DHCP V6 Server ☐ Override
 DHCP Addr. Assignment ☒ Required
OEAP
 Split Tunnel ☐ Enabled
Management Frame Protection (MFP)
 MFP Client Protection
 DTIM Period (in beacon intervals)

Step 2 After enabling the DHCP required option, scroll down and in the **Local Client Profiling** area, enable DHCP Profiling and HTTP Profiling if they are not enabled and click **Apply**.

WLANs > Edit 'POD1-dot1x' < Back Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Mgmt Via Wireless ☐ Enabled
 Off Channel Scanning Defer
 Scan Defer Priority 0 1 2 3 4 5 6 7
☐ ☐ ☐ ☒ ☒ ☒ ☐ ☐
 Scan Defer Time(msecs)
FlexConnect
 FlexConnect Local Switching ☐ Enabled
 FlexConnect Local Auth ☐ Enabled
 Learn Client IP Address ☒ Enabled
 Vlan based Central Switching ☐ Enabled
 Central DHCP Processing ☐ Enabled
 Override DNS ☐ Enabled
 NAT-PAT ☐ Enabled

Local Client Profiling
 DHCP Profiling ☒
 HTTP Profiling ☒
PMIP
 PMIP Mobility Type
 PMIP NAI Type

Creating Policies on the WLAN from the WLC GUI

Step 3 Once Profiling is configured, we can move on to create Local policies and apply them on the WLAN. On the WLC menu bar, go to **Security > Local Policies**, which will take you to the Policy List.



Step 4 When in the Local Policy List, click **New** to create a Policy Name. In this example, **teacher-LP** is used as a policy name, but you can use any name to define your own policy.



Once policy name is configured, you can create policies to match a Role, EAP Type, and DeviceType. Also, you can define the required actions related to the Match criteria.

Here, in our setup we use **User Role** and **Device Type** to Match Criteria, but you can use any other type if required.

Note Make sure Match Role string is the same as AAA defined role name. In this example, it is configured as teacher.

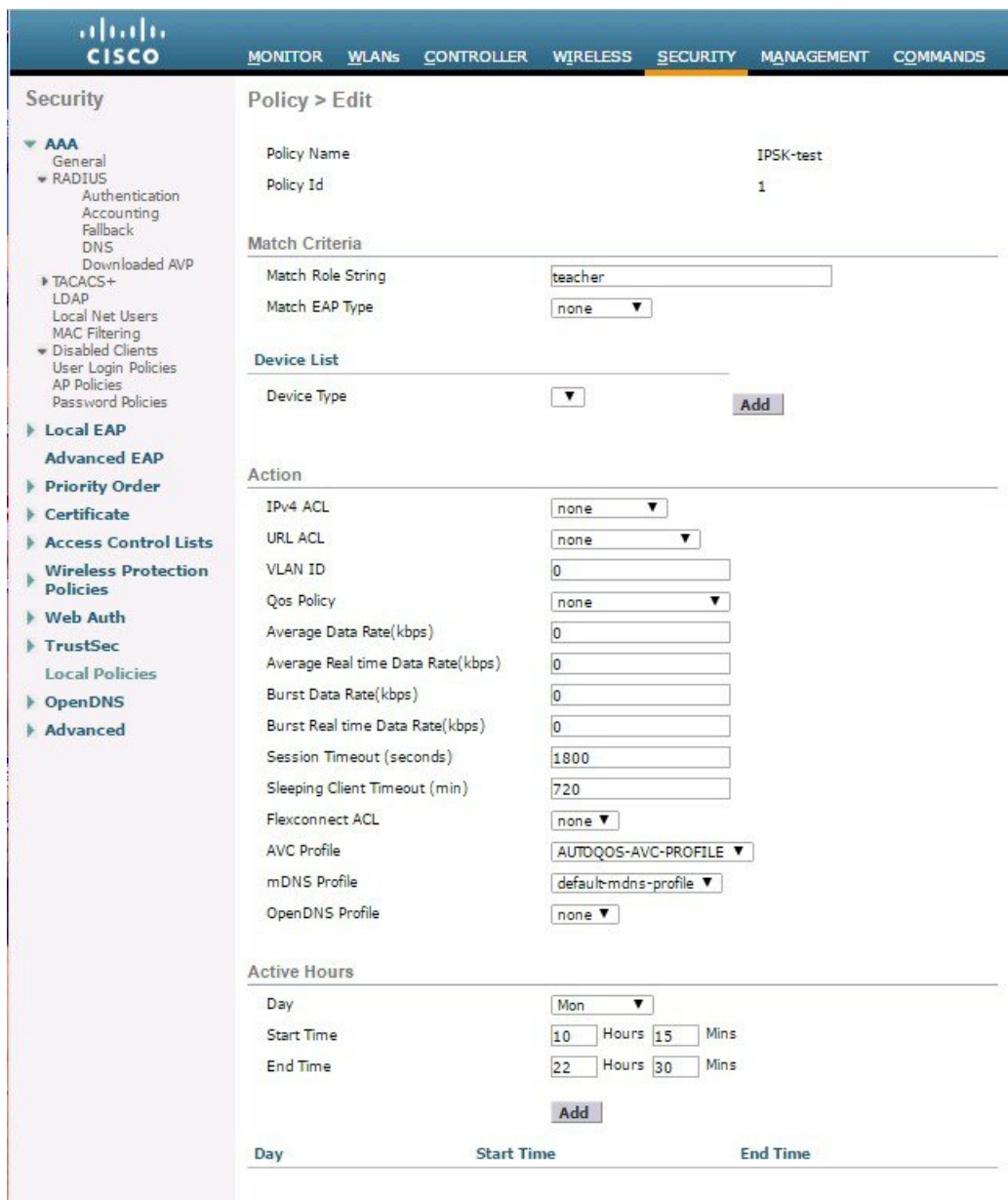
Step 5 Enter User Role and click **Apply**. Here the role name "teacher" is used as an example.

Step 6 To apply the policy based on a user device, in the **Device List** area, from the Device Type drop-down list, choose the **device type** on which you want to enforce the policy and then click **Add**.

Here, we used **Apple-iPad** as a device type for **Match Criteria**. You can add Apple-iPhone and other Apple devices as well from the **Device Type** drop-down list.

Note If you do not want to match any device type then do not configure the **Device Type** option.

Step 7 To apply the appropriate action, choose from the parameters under the **Action** area to enforce the policy. Select the AVC profile that should be defined in the last section.



The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface for a Security Policy. The left sidebar contains a tree view with categories like AAA, RADIUS, Local EAP, and Advanced EAP. The main area is titled 'Policy > Edit' and shows the configuration for a policy named 'IPSK-test' with ID '1'. The 'Match Criteria' section includes 'Match Role String' set to 'teacher' and 'Match EAP Type' set to 'none'. The 'Device List' section has a 'Device Type' dropdown and an 'Add' button. The 'Action' section lists various settings: IPv4 ACL (none), URL ACL (none), VLAN ID (0), Qos Policy (none), Average Data Rate (0), Average Real time Data Rate (0), Burst Data Rate (0), Burst Real time Data Rate (0), Session Timeout (1800), Sleeping Client Timeout (720), Flexconnect ACL (none), AVC Profile (AUTOQOS-AVC-PROFILE), mDNS Profile (default-mdns-profile), and OpenDNS Profile (none). The 'Active Hours' section shows 'Day' as 'Mon', 'Start Time' as 10:15, and 'End Time' as 22:30, with an 'Add' button. At the bottom, there are labels for 'Day', 'Start Time', and 'End Time'.

Note For additional details on configuring Local Policy please see the link http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_01110.html

Step 8 User can create more than one Local policy and apply it for student as “student-LP”.

Note Ensure that the Match Role String is the same as the defined role name on the AAA/Radius Server.

Policy > Edit

Policy Name

student-LP

Policy Id

6

Match Criteria

Match Role String

student

Match EAP Type

none

Device List

Device Type

Android

Add

Apple-iPad

☒

Action

IPv4 ACL

none

VLAN ID

0

Qos Policy

none

Session Timeout (seconds)

1800

Sleeping Client Timeout (min)

720

Flexconnect ACL

none

AVC Profile

student-AVC

mDNS Profile

none

Active Hours

Day

Mon

Start Time

Hours

Mins

End Time

Hours

Mins

Add

352901

Step 9 Create a default local policy for any other device.

If no other ACL is applied in the Local policy, then any other device, other than Apple-iPad, will be able to access the applications because the final filter function of all policies is **Allow all**.

In order to block all applications on all devices except Apple-iPad, create a **deny all** ACL and apply it on the Local Policy and then apply that policy on the WLAN as the last resort. See the configuration examples in the screenshots below.

Create an ACL to deny all IPv4 flow.

Security > Access Control Lists > Edit

General

Access List Name: deny-all

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Create a Local Policy **Block-all** and apply the **deny all** ACL to it, do not choose any devices roles or profiles.

Security > Policy > Edit

Policy Name: block-all

Policy Id: 3

Match Criteria

Match Role String:

Match EAP Type: none

Device List

Device Type: Android

Action

IPv4 ACL: deny-all

VLAN ID: 0

Qos Policy: none

Session Timeout (seconds): 1800

Sleeping Client Timeout (min): 720

Flexconnect ACL: none

AVC Profile: none

mDNS Profile: none

Mapping Policy on WLAN

Procedure

Step 1 Go to **WLANs** from the WLC menu bar and click the **WLAN ID** on which you want the policy to be implemented. From the WLAN edit menu, click the **Policy-Mapping** tab.

Set the Priority index to any value from 1-16. From the Local Policy drop-down list, choose the policy which you have already created. To apply the policy on the WLAN, click Add. The policy will be added.

WLANs > Edit 'POD1-dot1x'

< Back Apply

General Security QoS Policy-Mapping Advanced

Priority Index (1-16) 1

Local Policy teacher-LP

Add

Priority Index	Local Policy Name
1	teacher-LP

352904

Step 2 Add the appropriate policies to **Policy-Mapping** under WLAN.

WLANs > Edit 'pod3-dot1x'

< Back Apply

General Security QoS Policy-Mapping Advanced

Priority Index (1-16)

Local Policy teacher-LP

Add

Priority Index	Local Policy Name
1	teacher-LP
2	student-LP
3	block-all

352905

Step 3 In the **Advanced** tab, disable **Allow AAA Override** if it is enabled as was configured also for IPSK.

WLANs > Edit 'Pod1-IPSK'

General Security QoS Policy-Mapping Advanced

Allow AAA Override ☒ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☒ 1800 Session Timeout (secs)

Aironet IE ☒ Enabled

Diagnostic Channel [18](#) ☐ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion [2](#) ☒ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8](#) 0

Static IP Tunneling [11](#) ☐ Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☒ Required

OEAP

Split Tunnel ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4](#) Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Load Balancing and Band Select

Step 4

Check if the AAA role is configured properly, that is, role name on the AAA server should match the role string defined in the local policy. The example below is from the Cisco ISE server configured with cisco-av-pair role=teacher. Same configure for role=students.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is selected, and the 'Policy Elements' sub-tab is active. The left sidebar shows a tree view with 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Authorization' section is expanded, showing 'Authorization Profiles' and 'Downloadable ACLs'. The main content area is titled 'Authorization Profile' and contains the following fields:

- * Name: IPSK-device
- Description: Identity PSK
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: ☐
- Track Movement: ☐
- Passive Identity Tracking: ☐

Below these fields is the 'Common Tasks' section with the following options:

- ☐ Web Authentication (Local Web Auth)
- ☐ Airespace ACL Name
- ☐ ASA VPN
- ☐ AVC Profile Name

The 'Advanced Attributes Settings' section contains a table of attributes:

Attribute	Value
Cisco:cisco-av-pair	psk-mode=ascii
Cisco:cisco-av-pair	psk=abc12345
Cisco:cisco-av-pair	role=teacher

A red arrow points to the 'role=teacher' value in the third row. Below this table is the 'Attributes Details' section, which is highlighted with a red box. It contains the following text:

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=abc12345
cisco-av-pair = role=teacher
```

At the bottom of the page are 'Save' and 'Reset' buttons.

Interface Group Override

Like VLAN, ACL and QoS returned from AAA to override the policy configuration mapped in WLAN, Interface Group (list of interfaces VLAN) can be overridden from the AAA for a particular client. iPSK combined with the Interface group can allow the iPSK wireless client to obtain IP address from any of the VLANs present in the interface group

Attribute **Airespace: Airespace-Interface-Name** can be used along with the iPSK attributes to override the WLC Interface group.

The screenshot shows the Cisco ISE Policy configuration interface. The 'Results' tab is selected, displaying the 'Advanced Attributes Settings' section. This section contains four rows of attributes, each with a dropdown menu for the attribute name, a text input for the value, and a status indicator. The attributes are: 'Airespace:Airespace-Interface' with value 'ifgroup', 'Cisco:cisco-av-pair' with value 'psk-mode=ascii', 'Cisco:cisco-av-pair' with value 'psk=cisco123', and a 'Select an item' dropdown. Below this, the 'Attributes Details' section shows the resulting values: 'Access Type = ACCESS_ACCEPT', 'Airespace-Interface-Name = ifgroup', 'cisco-av-pair = psk-mode=ascii', and 'cisco-av-pair = psk=cisco123'.

Sample FreeRadius Configuration for combining iPSK attributes and Interface Group

```
"6c96cff283d0" Cleartext-Password:= "6c96cff283d0"
293 Cisco-AVPair += "psk-mode=ascii",
294 Cisco-AVPair += "psk=cisco123",
295 Airespace-Interface-Name += "ifgroup"
```

Client Debug

Client debugs while returning interface groups along with iPSK and making use of one of the VLANs from the group.

```
*apfReceiveTask: Dec 14 13:25:17.264: [PA] 6c:96:cf:f2:83:d0 Inserting AAA Override struct for mobile
MAC: 6c:96:cf:f2:83:d0, source 2

*apfReceiveTask: Dec 14 13:25:17.264: [PA] 6c:96:cf:f2:83:d0 Inserting new RADIUS override into chain for
station 6c:96:cf:f2:83:d0
*apfReceiveTask: Dec 14 13:25:17.264: [PA] 6c:96:cf:f2:83:d0 Assigned interface 'vlan70' from interface group
'ifgroup' for the client
*apfReceiveTask: Dec 14 13:25:17.264: [PA] 6c:96:cf:f2:83:d0 Found an interface name:'vlan70' for interface
group name received: ifgroup
```

End User Device Setup

Procedure

Step 1 On the End User device with MAC address configured on ISE connect to the WLAN Pod1-IPSK and enter IPSK password **abc12345** for that device or as it was configured on ISE.

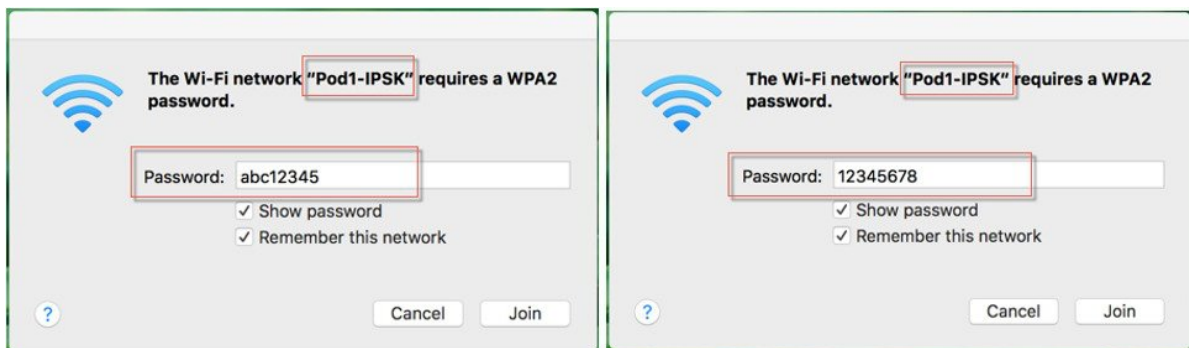
----- Connection **successful**

Step 2 Connect to the same WLAN with PSK **12345678**.

----- connection will be **un-successful**

Step 3 Connect to the same WLAN with device MAC address not configured on ISE with **PSK 12345678**.

----- connection **successful**



Step 4 To verify if the policy is applied from the WLCGUI, go to **Monitor > Clients**, and then click the **Client MAC address**.

Max Number of Records 10

352909

- Devices with no-MAC addresses configured on ISE will be able to connect to WLAN with generic PSK only.
- IPSK supports Local Mode and Flexconnect Mode (Central Authentication & Local Switching).
- IPSK supports FSR and key caching is done for faster roams to avoid RADIUS connect on every roam.
- To enable validity of the IPSK at certain scheduled times - the time schedule/validity can be exploited using radius session-timeout attribute in radius response.

IPSK Configuration through CLI commands

The following existing CLIs would be used for this feature:

```
config wlan mac-filtering enable <wlanId>
config wlan aaa-override enable <wlanId>
config wlan security wpa akm psk enable <wlanId>
config wlan security wpa akm psk set-key <ascii/hex> <key> <wlanId>
```

The existing show command would display the configuration of the WLAN and the client.

```
show wlan <wlanId>
show client detail <clientMac>
```




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.