cisco.



8.5 Identity PSK Feature Deployment Guide

Product or Feature Overview 2 IPSK solution 3 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 12 Scope and Objectives 12 Profiling and Policy Configuration 13 Mapping Policy on WLAN 18 End User Device Setup 21 Conclusion 22 IPSK Configuration through CLI commands 23 Revised: September 14, 2017,

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.



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 serer 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.

dentity Services Engine	Home	► Contex	t Visibility	Operations	▶ Policy	- Administration	→ Wo	rk Centers	
System Identity Management	- Network	Resources	Device Po	ortal Manageme	ent pxGrid	Services + Feed	Service	Threat Centric N/	AC
Network Devices Network Device	Groups 1	Network Dev	ice Profiles	External RADIL	JS Servers	RADIUS Server Se	equences	NAC Managers	Đ
	3								
Network devices	Netw	ork Devic	es						
Default Device									
Device Security Settings	/ Ed	it 🕂 Add	Duplicate	Import	Export 👻	Generate PAC	X Delete	*	
, ,	N	lame	▲ IP/M	ask P	rofile Name		Location	I.	
		NAD_10.10.1	0.2 10.10	0.10.2/32	cisco 🕀		All Locat	tions	

dentity 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 C	Sroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	Network Devices List > New Network Device
Network devices	Network Devices
Default Device	* Name NAD
Device Security Settings	Description Wireless Controller
	* IP Address: 10.10.10.2 / 32
	Device Profile ## Cisco
	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.

dentity Services Engine H	ome	ns Policy Administration Work Centers	License Warning 🔺 🔍 🥥
Authentication Authorization Profiling	Posture Client Provisioning Bailey	Elements	Click here to do wireless setup and visibility setup Do not show this
Authentication Authorization	Standard Authorization Profiles For Policy Export go to Administration > 8	; System > Backup & Restore > Policy Export Page	Selected 0 Total 8
Authorization Profiles	/ Edit 🕂 Add 🖓 Duplicate 🗙 D	leiete	Show All
Downloadable ACLs	Name	Profile	Description
Downloadable ACLS	Blackhole_Wireless_Access	🗰 Cisco 🕀	Default profile used to blacklist wireless devices. Ensure that
Profiling	Cisco_IP_Phones	🗰 Cisco 🕀	Default profile used for Cisco Phones.
▶ Posture	Cisco_WebAuth	🗰 Cisco 🕀	Default Profile used to redirect users to the CWA portal.
	IPSK-device	🗱 Cisco 🕀	Identity PSK
Client Provisioning	NSP_Onboard	ditto Cisco 🕀	Onboard the device with Native Supplicant Provisioning

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.

dentity Services Engine	Home	Operations		► Administration	► Work Centers	
Authentication Authorization P	rofiling Posture Client Provisioni	ng Policy Eleme	ents			Click
Dictionaries Conditions Re	esults					
Authentication	Authorization Profiles > IPSK-o Authorization Profile	levice				
- Authorization	* Name	PSK-device]		
Authorization Profiles	Description I	dentity PSK				
Downloadable ACLs	* Access Type	CCESS_ACCEPT	*			
Profiling	Network Device Profile	the Cisco				
Authorization Profiles	▼ Advanced Attribu	ites Settings				
Downloadable ACLs						
Profiling	Cisco:cisco-av-pair		psk-mode	e=ascii	0 -	
Posture	Cisco:cisco-av-pair	0	= psk=abc1	12345	0	
Client Provisioning						
	▼ Attributes Detail	s				
	Access Type = ACCESS cisco-av-pair = psk-mo cisco-av-pair = psk=at	G_ACCEPT de=ascli pc12345				

- 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.

Jt	henticatio	Authorization Profiling	Positive Ctient Provisioning Policy Elements		Click here to do wireless se
h	orizati e the Aut olicy Exp	horization Policy by configuring a nort go to Administration > System	ules based on identity groups and/or other conditions. Drag and drop rules to change the orde > Backup & Restore > Policy Export Page	er.	
st	Matched	Rule Applies]		
SI	tandard	ons (U)			
	Status	s Rule Name	Conditions (identity groups and other conditions)	F	Permissions
		IdentityPSK	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS A0:38:E3:95:73:4E)	then	IPSK-device
I		IdentityPSK_copy	<pre>if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS f4:5c:89:8f:10:43)</pre>	then	IPSK-device
1	~	Wireless Black List Default	if Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access
1		Profiled Cisco IP Phones	if Cisco-IP-Phone	then	Cisco_IP_Phones
	Status	Rule Name	Conditions (identity aroups and other conditions) Permissions		
		IdentityPSK	if Any $rightarrow$ and Wireless_MAB AND Radius:Callin Characteristic formations	3	
		IdentityPSK_copy	Wireless_MAB_AND Radiu Condition Name Description f4:5c:98/8ft:10:43) Wireless_MAB Normalised Radius:RadiusFlowType EQUALS Wi	relessMAB	AND -
		Wireless Black List Default	If Blacklist AND Wireless_Ac	▼ A0:3B:E	3:95:73:4E 📀
			MAC address		

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.

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLL	ler w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagemen	NT
WLANs	WLANs > Edit 'Identity PS	SK'	
WLANS	General Security Qo	S Policy-Mapping Advanced	
Advanced	Profile Name	Identity PSK	
	Туре	WLAN	
	SSID	Pod1-IPSK	
	Status Security Policies	MAC Filtering[WPA2][Auth(PSK)]	
		(Modifications done under security tab will appe	ear a
	Radio Policy	All	
	Interface/Interface Group(G)	management 🔻	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	Cnabled	
	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.

.ılıılı. cısco	MONITOR WLANS CON	roller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c
WLANs	WLANs > Edit 'Identit	y PSK'
▼ WLANs WLANs	General Security	QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3	AAA Servers
	Layer 2 Security Fast Transition Fast Transition Over the DS Reassociation Timeout 20 Protected Management PMF	VPA+WPA2 AC Filtering2 Adaptive Seconds Frame Disabled V
	WPA+WPA2 Parameters	5
	WPA Policy	
	WPA2 Folicy WPA2 Encryption OSEN Policy	AES TKIP CCMP256 GCMP128

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

Advanced	Authentication Key Management 19
	802.1X Enable
	PSK 🕑 Enable
	FT 802.1X Enable FT PSK Enable PSK Format ASCII V

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 WLA	Ns <u>C</u> ONTROLLER	W <u>I</u> RELESS <u>S</u> EC	URITY M <u>a</u> nagement
WLANs	WLANs > Edit	'Identity-PSK'		
WLANS	General	ecurity QoS	Policy-Mapping	Advanced
▶ Advanced	Layer 2	Layer 3 AAA S	ervers	
	Select AAA se RADIUS Serve RADIUS Se Apply Cisco	ervers below to over ers rver Overwrite interfa) ISE Default Settings	rride use of default ace Enabled Enabled	servers on this WLAN
		Authentication Serv	ers Account	ing Servers
	Server 1	Enabled IP:10.91.104.106, P	€ Enabl ort:1812 ▼ IP:10.9	ed 1.104.106, Port:1813 ▼
	Server 2	None	▼ None	T

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

cisco	MONITOR WLANS CONTROL	ller w <u>i</u> reless <u>s</u> ecu	RITY M <u>a</u> nagemen	NT (
WLANs	WLANs > Edit 'Identity-F	PSK'		
WLANS	General Security Q	oS Policy-Mapping	Advanced	
Advanced	Allow AAA Override	🗹 Enabled		DHCP
	Coverage Hole Detection	Enabled		DHO
	Enable Session Timeout	Session Timeout (secs)		DHO
	Aironet IE	Enabled		OEAP
	Diagnostic Channel <u>18</u>	Enabled		
	Override Interface ACL	IPv4 None ▼	IPv6 None ▼	Spl
	Layer2 Acl	None 🔻	1	Manag
	URL ACL	None T	7	
	P2P Blocking Action	Disabled 🔹		MFP
	Client Exclusion 3	Enabled Timeout Value	(secs)	DTIM F

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.

cisco	MONITOR WLANS CON	TROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS
Security • AAA General • RADIUS Authentication Accounting Fallback DNS Downloaded AVP • TACACS+ LDAP Local Net Users MAC Filtering • Disabled Clients User Login Policies Password Policies Password Policies • Local EAP Advanced EAP • Priority Order • Certificate • Access Control Lists • Wireless Protection Policies • Web Auth • TrustSec Local Policies • OpenDNS • Advanced	MONITOR WLANS CON Policy > Edit Policy Name Policy Id Policy Id Match Criteria Match Role String Match Role String Match EAP Type Device List Device Type Action IPv4 ACL URL ACL VLAN ID Qos Policy Average Data Rate(kbps) Average Real time Data Rate(kbps) Burst Real time Data Rate(kbps) Session Timeout (seconds) Sleeping Client Timeout (min	(kbps) bps)	WIRELESS		MANAGEMENT IP5K-test 1	
	Session Timeout (seconds) Sleeping Client Timeout (min Flexconnect ACL AVC Profile mDNS Profile OpenDNS Profile Day Start Time End Time	1)	1800 720 none ▼ none none Mon ▼ Mon ▼ Hours Hours			
	Day	Start Tim	Add	E	ind 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.

ANS > Eait 'POD1-0	JOLIX.				< Back	Apply
Seneral Security	QoS Policy-Mapping	Advanced				
Allow AAA Override	Enabled		DHCP			
Coverage Hole Detection	S Enabled		DHCP Server	Override		
Enable Session Timeout	Session Timeout (secs)		DHCP V6 Server	Override		
Aironet IE Diagnostic Channel	Enabled		DHCP Addr. Assignment	🗹 Required 🗲		
Override Interface ACL	IPv4 None :	IPv6 None :	OEAP			
Layer2 Acl	None :		Split Tunnel	Enabled		
P2P Blocking Action	Disabled :		Management Frame Prote	ction (MEP)		
Client Exclusion 2	Enabled Timeout Value (secs)				
Maximum Allowed Clients	0		MFP Client Protection 4	Optional :		
-			DTIM Period (in beacon in	tervals)		

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**.

VLANs > Edit 'POD1-de	ot1x'					< Back	Apply
General Security	QoS Policy-Mapping	Advanced					
Mgmt Via Wireless	Enabled		Passive Client	0			
Off Channel Scanning Defer			Voice				
Scan Defer Priority	0 1 2 3 4 5 6 7		Media Session Snooping		Enabled		
			Re-anchor Roamed Voice Clients		Enabled		
Scan Defer Time(msecs)	100		KTS based CAC Policy		Enabled		
FlexConnect			Radius Client Profiling				
FlexConnect Local			DHCP Profiling				
Switching 2	Enabled		HTTP Profiling				
FlexConnect Local Auth 12	Enabled		Local Client Profiling				
Learn Client IP Address 5	Senabled		DHCP Profiling	۷			
Vian based Central	C Fashind		HTTP Profiling	ø			
Switching 13	Endbled		PMIP				
Central DHCP Processing	Enabled		PMIP Mobility Type				
Override DNS	Enabled		PMIP NAL Type	П	exadecimal :		
NAT-PAT	Enabled			-			0

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.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	General
AAA General PADIUS Authentication Accounting Falback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Maximum Local Database entries (on next reboot). 2048 (Current Maximum is 2048) Number of entries, already used 3
Local EAP	
Priority Order	
 Certificate Access Control Lists 	
Wireless Protection Policies	
 Web Auth TrustSec SXP Local Policies Advanced 	-

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.

MONITOR	WLAN		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Policy > I	New								< Back Apply
Policy Nar	me t	eacher-LP	-						

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.

cisco	MONITOR WLAN	s <u>c</u> ontroller	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Security	Policy > Edit					
 ★ AAA General ★ RADIUS Authentication Accounting Fallback 	Policy Name Policy Id				IPSK-test 1	
DNS Downloaded AVP TACAC5+ LDAP Local Net Users MAC Filtering Disabled Clients	Match Criteria Match Role String Match EAP Type Device List		teacher none T]		
User Login Policies AP Policies Password Policies Local EAP Advanced EAP	Device Type		T	1	Add	
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies OpenDNS Advanced 	IPv4 ACL URL ACL VLAN ID Qos Policy Average Data Ratel Average Real time Burst Data Rate(kt Burst Real time Da Session Timeout (s Sleeping Client Tim Flexconnect ACL AVC Profile mDNS Profile OpenDNS Profile Day	kbps) Data Rate(kbps) ps) ta Rate(kbps) seconds) eout (min)	none 0 none 0 0 0 0 1800 720 1800 720 AUTOQOS-AT default-mdns none ▼	VC-PROFILE V		
	Start Time End Time		10 Hours 22 Hours Add	15 Mins 30 Mins		
	Day	Start Ti	me	E	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

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 beable 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.

aluth											Saye Configuration Ping Logout Refrest				
cisco	MONI	TOR M	/LANs	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK					
Security	Acce	ss Cor	ntrol Li	sts > Edit						< Back	Add New R	ule			
▼ AAA General	Gene	ral													
Authentication	Access	s List Nam	пе	deny-all											
Fallback DNS Downloaded AVP TACACS+	Deny	Action	Source IP/M	0 ce E ask I	estination P/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits				
LDAP Local Net Users MAC Filtering Disabled Clients	1	Deny	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 thedeny allACL to it, do not choose any devices roles or profiles.

aludu							Sa <u>v</u> e (Configuration	Ping	Logout Refres
CISCO	MONITOR WLANS CO	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		
Security	Policy > Edit									< Back
AAA	·			-						
ADJUS Authentication Accounting Fallback	Policy Name Policy Id		block-all 3							
DNS Downloaded AVP	Match Criteria									
TACACS+ LDAP	Match Role String									
Local Net Users MAC Filtering	Match EAP Type	nor	e •							
Disabled Clients User Login Policies	Device List									
AP Policies Password Policies	Device Type	A	ndroid		•	Add				
Local EAP										
Advanced EAP	Action									
Priority Order	IPv4 ACL	de	eny-all 🔻							
Certificate	VLAN ID	0								
Access Control Lists	Qos Policy	n	one	•						
CPU Access Control Lists	Session Timeout (second	is) 18	00	1						
Layer2 ACLs	Sleeping Client Timeout	(min) 72	0							
Wireless Protection Policies	Flexconnect ACL	n	one 🔻							
Web Auth	AVC Profile	n	one 🔻]						
TrustSec SXP	mDNS Profile	n	one							
in the first										

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.

General	Security	QoS	Policy-Mapping	Advanced	
Priority In	ndex (1-16)		1		
Local Poli	су		teacher-LP ‡		
			Add		

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

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	nfiguration <u>Ping</u> COMMANDS) Logout <u>R</u> efresh HELP <u>F</u> EEDBACK
WLANs		WLANs	>Edit 'pod3	-dot1x'			< Back	Apply
WLANS		Genera	al Security	QoS	Policy-Mappin	g Advanced		
Advanced		Priorit Local	ty Index (1-16) Policy	[eacher-LP V			
		Priorit	y Index		Local Policy I	Name		
		1			teacher-LP			
		3			block-all	-		

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

eneral	Security	QoS	Policy-Mapping	Advanced			
Allow AA	AA Override		🕑 Enabled 4			DHCP	
Coverag	e Hole Detection	1	🗹 Enabled			DHCP Server	Override
Enable S	Session Timeout	✓ 180 Se	0 ssion Timeout (secs)			DHCP Addr. Assignment	Required
Aironet I	IE		Cnabled			OFAR	
Diagnost	tic Channel <u>18</u>		Enabled				
Override	e Interface ACL		IPv4 None ▼		IPv6 None ▼	Split Tunnel	Enabled
Layer2 A	Acl		None T			Management Frame Prote	ection (MFP)
URL ACL			None 🔻				
P2P Bloc	king Action		Disabled	T		MFP Client Protection 4	Optional T
Client Ex	clusion 3		Enabled 60			DTIM Period (in beacon i	ntervals)
			Tim	ieout Value (secs))		
Maximur	m Allowed Client	s <u>8</u>	0			802.11a/n (1 - 255)	1
Static IP	Tunneling 11		Enabled			802.11b/g/n (1 - 255)	1
Wi-Fi Dir	ect Clients Polic	y	Disabled	T		NAC	
Maximur	m Allowed Client	s Per AP	200			NAC State None	¥
Radio						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.

dentity Services Engine	Home → Context Visibility → Operations ▼Policy → Administration → Work Centers
Authentication Authorization Profili	ng Posture Client Provisioning - Policy Elements
Dictionaries Conditions Results	
0	
Authentication	
- Authorization	* Access Type Access Accept
Authorization Profiles	
Downloadable ACLs	Network Device Profile
▶ Profiling	Service Template
Posture	Track Movement ()
Client Provisioning	
	Common Tasks Web Authentication (Local Web Auth)
	Airespace ACL Name
	ASA VPN
	AVC Profile Name
	✓ Advanced Attributes Settings
	Cisco:cisco-av-pair 📀 = psk-mode=ascii 📀 —
	Cisco:cisco-av-pair
	🗄 Cisco:cisco-av-pair 📀 = role=teacher
	Access Type = ACCESS_ACCEPT cisco-av-pair = psk-mode=ascii cisco-av-pair = psk=abc12345 cisco-av-pair = role=teacher
	Save Reset

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**

?	password.			?	password		
	Password:	abc12345			Password:	12345678	
4		 Show password Remember this network 	vork			 Show password Remember this network 	

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

eneral AVC Statist	tics	
Encryption Cipher	CCMP (AES)	
EAP Type	PEAP	
SNMP NAC State	Access	
Radius NAC State	RUN	
CTS Security Group Tag	Not Applicable	
AAA Override ACL Name	none	
AAA Override ACL Applied Status	Unavailable	
AAA Override Flex ACL	none	
AAA Override Flex ACL Applied Status	Unavailable	
Redirect URL	none	
IPv4 ACL Name	none	
FlexConnect ACL Applied Status	Unavailable	
IPv4 ACL Applied Status	Unavailable	
IPv6 ACL Name	none	
IPv6 ACL Applied Status	Unavailable	
Layer2 ACL Name	none	
Layer2 ACL Applied Status	Unavailable	
mDNS Profile Name	default-mdns-profile	
mDNS Service Advertisement Count	0	
AAA Role Type	teacher	
Local Policy Applied	teacher-LP	-

Conclusion

• Controller that has Mac Filtering and AAA overide enabled with ISE configured, will allow IPSK configured devices connect to WLAN with MAC addresses configured on ISE.

- Devices with MAC addresses configured on ISE will not be able to connect to WLAN generic PSK but only with IPSK configured for that device.
- Devices with no-MAC addreses configured on ISE will be able to connect to WLAN with generic PSK only.
- IPSK is not supported on the Flex Connect locally switched mode. AAA server is required with AV-Pair support.
- IPSK is not supported on the Flex Connect Group.
- IPSK supports FSR and key caching is done fo 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>

© 2017 Cisco Systems, Inc. All rights reserved.



Americas Headquarters Cisco Systems, Inc. San Jose, CA 95134-1706 USA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore **Europe Headquarters** Cisco Systems International BV 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.