

Wireless Device Profiling and Policy Classification Engine on WLC

Last Updated: November, 2013 Release: Wireless Device Profiling and Policy Classification Engine on WLC, Release 7.5



Table of Contents

- Overview
- Scope, Objectives, and Expectations
- Terminology
- Profiling and Policy Configuration
- Creating Policies on WLAN from WLC GUI
- Mapping a Policy on WLAN
- Mapping the Policy to an AP Group



Cisco Systems, Inc. www.cisco.com

- Example of Policy Enforcement on Other Device Types
- Limitations
- Summary
- Show Commands
- Debug Commands
- Commands to Configure Profiling through CLI
- Commands to Configure Policy through CLI
- Appendix-A
 - Sleeping Client Support
 - WLAN Configuration for Sleeping Client
 - Sleeping Client CLI commands

Overview

Cisco currently offers a rich set of features which provides device identification, onboarding, posture and policy, through ISE. WLC has been enhanced with some of these capabilities. This document deals with basic configuration of device profiling and policy implementation through Cisco WLC.

This new feature (Profiling and Policy) on WLC does the profiling of devices based on protocols like HTTP and DHCP to identify the end devices on the network. Users can configure 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.

Wireless device profiling and policy classification engine enables simple BYOD deployments with visibility and user/wireless device policy integrated into the wireless controller.

BYOD

Wireless Policy Engine and ISE positioning

	WLAN Controller + policy engine	ISE Wireless License	Full ISE License
Wireless Device profiling	v		
Wireless Device visibility and policy	Single WLAN Controller	Enterprise-wide wireless	Enterprise wide wired + wireless
Device onboarding	Basic*	Advanced**	Advanced**
MDM integration	3rd party	Partner ecosystem	Partner ecosystem
SGA		v	0
AAA		Wireless	Wireless, Wired & VPN
Reporting	Basic client visibility and troubleshooting	30 days+	30 days+
Device feed updates license	With Controller sw upgrades	3, 5 yr lic (1yr planned)	3, 5 yr lic (1yr planned)
* WLC basic onboarding allows vlan as ** ISE enables Advanced device onboa	ssignment, ACL application and arding with certificate based dev	application of QoS policies fo	r profiled devices

1

Wireless Device Profiling and Policy Classification Engine on WLC

Scope, Objectives, and Expectations

Profiling and policy enforcement allows profiling of mobile devices and basic onboarding of the profiled devices to a specific vlan, assigns ACL and QOS, or configures session timeout. It can be configured as two separate components. The configuration on the WLC is based on defined parameters specific to clients joining the network. The policy attributes which are of interest are:

- a. Role Defines the user type or the user group the user belongs to. Example: Student, Employee
- **b.** Device Defines the type of device. Example: Windows machine, Smart phone, Apple device like iPad, iPhone and so on.
- **c.** Location Defines where the end point is connected on the network. Location represents AP-group. APs can be divided or grouped according to the location and policy can be applied per AP group.
- **d.** Time of day Allows configuration to be defined at what time of the day end-points are allowed on the network.
- e. EAP Type Checks what EAP method the client is getting connected to.

The above parameters are configurable as policy match attributes. Once WLC has a match corresponding to the above parameters per end-point, the policy enforcement comes into picture. Policy enforcement allows basic device on-boarding of mobile devices based on session attributes like:

- a. Vlan Assignment
- **b**. ACL
- c. Session Timeout
- $\textbf{d.} \quad QoS$
- e. Sleeping Client-Timeout duration for a specific sleeping client (in hours)

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

Terminology

Term	Expansion
APM	AP Manager Interface
Dyn	Dynamic Interface
Mgmt	Management Interface
Port	Physical Gbps port
AP	Access Point
LAG	Link Aggregation
VSL	Virtual Switch Link
VLAN	Virtual LAN

Term	Expansion
SSO	Stateful Switchover
WiSM-2	Wireless Service Module-2

Profiling and Policy Configuration

In 7.5 release, only embedded or built-in profiles are available on the WLC through which it can identify devices.

In later releases, it should be possible to create user-defined profiles, which will take precedence over the embedded profiles. Currently there are 88 built-in profiles and can be viewed through WLC CLI prompt.

Go to WLC and run show profiling policy summary. For the purpose of this document we just displayed the first 6 profile.



To configure device profiling on a WLAN through GUI, go to the WLAN (here we created WLAN Demo-Employee) and click **Advance**, then enable DHCP by checking the **Required** check box. After enabling the DHCP required option, scroll down and under **Local Client Profiling** enable **DHCP Profiling** and **HTTP Profiling** by checking the respective check boxes and click **Apply**.

I



di Channel Scanning Defe	205 Policy-Mapping	Advanced	Client Load Balancing	12		
Esso Defes Brinshi	01234567		Client Band Select			
acan Gener Priority	DEDEVVE		Passive Client			
Sano Defer Time(means)	100		Passive Client	2		
lexConnect	100		Voice			
ElexConnect Local	-		Media Session Snooping		Enabled	
Switching 2	Enabled		Re-anchor Roamed Voice Clients		Enabled	
FlexConnect Local Auth 🔝	Enabled		KTS based CAC Policy		Enabled	
Learn Client IP Address 2	Enabled		Radius Client Profiling			
Vian based Central	Eashied		DHCP Profiling			
Switching 12			HTTP Profiling			
Central DHCP Processing	Enabled		Local Client Profiling			
Override DNS	Enabled		DHCP Profiling			
NAT-PAT	Enabled		HTTP Profiling		-	
			DMTD		-	



To configure profiling through ISE use Radius Client Profiling.

Now, try associating a client to the WLAN on which profiling is enabled. In our setup we associated an Apple iPad, an Android device and a Windows machine.

From the WLC main menu bar, navigate to **Monitor > Clients** and under **Device Type** column, notice that there are three devices associated to the WLAN and all of them are being profiled. See the below figure – Windows PC as Microsoft-Workstation, iPad as an Apple-iPad and Motorola Zoom as an Android device.

Clients											Entries 1 - 3 of 3
Current Filter	None	[Change Filter] [Clear Fil	terl							1	*
Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	PHIP _{V6}	WG8	Device Type
00:27:10:d3:a3:c0	AP2600	Demo-Employee	Demo-Employee	Unknown	802.11an	Associated	Yes	1	No	No	Windows7-Works
40:10:89175164143	AP2600	Demo-Employee	Demo-Employee	Unknown	802.11an	Associated	Yes	1	No	No	Android
70:dere2:0erce:05	AP2600	Demo-Employee	Demo-Employee	Unknown	802.11an	Associated	Yes	1	No	No	Apple-iPad

The same can be viewed from CLI as well, run a command show client summary devicetype to see the clients being profiled.

We clearly see that the client devices are classified under Device Type.

(WLC) >show clien	t summary devicet	уре		
Number of Clients			. 3	
MAC Address	AP Name	Status	Device Туре	
00:27:10:7b:d9:e8 18:46:17:ec:84:e8 70:de:e2:0e:ce:05	AP2600 AP3600 AP2600	Associated Associated Associated	Microsoft-Workstation Android Apple-iPad	

Creating Policies on WLAN from WLC GUI

Once the policy has been configured you can create policies and apply them on the WLAN. On WLC menu bar, go to **Security > Local Policies** which will navigate you to the Policy List.



In Policy List page, click **New** to create a Policy Name. In our set up we are using "Employee-iPad" as a policy-name but you can use any name to define your own policy.

									Sage Configuration Eng Logout Befresh
MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Policy Lis	st								New
Policy Nar	me Profil	le ID							88 20 31 32
									Sage Configuration Ping Logout Befresh
MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
Policy >	New ame En	nployee-iPad		1					< Back Apply
									2

Once the Policy Name is created, click that policy name to configure the rules.

									Sage Configuration Ping	Logout Befresh
MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		
Policy Li	st									New
Policy Na	me			P	rofile ID					
Employee-	Pad			1						
	1									

Under **Policy Name**, you can create policies to match a Role, EAP Type and Device Type. You can also define what actions to take related to the Match criteria. In our setup we used Device Type for the Match Criteria but if required, you can use Role or EAP type as well.

To apply the policy based on a user device, go to **Device Type** and scroll down to select the device type from the drop down menu on which you want to enforce policy and then click **Add**.

Here we used Apple-iPad as a device type for Match Criteria.

MONITOR WLANS CONTRO	LLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Policy > Edit		-					
Policy Name				Employee-if	Pad		
Policy Id				1			
Match Criteria							
Match Role String							
Match EAP Type Device Type	none 🔻						
	A.44						
	Add						
List							
Action							
IPv4 ACL	none 🔻						
VLAN ID	0						
Qos Policy	none	•					
Session Timeout (seconds)	1800						
Sleeping Client Timeout (hours)	12						
Active Hours							
Day	Mon 👻						
Start Time	Hours	Mins					
End Time	Hours	Mins					
	Add						
Day Star	t	End	1				
bay Inne		110	ie i				

The device type will appear under the **Device List** section.

L

Γ

	OLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Policy > Edit						
Daliau Nama				Employee-if	n.d	
Policy Name				Employee-n	Pag	
Poney 10						
Match Criteria						
Match Role String						
Match EAP Type	none 🔻					
Device Type	Android		-			
	Add					
Device List						
Apple-iPad 📉						
Action						
IPv4 ACL	none 🔻					
IPv4 ACL VLAN ID	none 🔻					
Action IPv4 ACL VLAN ID Qos Policy Section Timeout (seconds)	none V D none					
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours	none 0 none 1800 12					
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours)	none • 0 none 1800) 12					
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours Active Hours	none 0 none 1800) 12	-				
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours Active Hours Day	none • 0 1800) 12 Mon •					
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours) Active Hours Day Start Time	none V 0 none 1800 12 Mon V Hours	• Mins				
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours) Active Hours Day Start Time End Time	none 0 none 1800 12 Mon Hours Hours	• Mins Mins				
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours Active Hours Day Start Time End Time	none V 0 none 1800) 12 Mon V Hours Add	• Mins Mins				
Action IPv4 ACL VLAN ID Qos Policy Session Timeout (seconds) Sleeping Client Timeout (hours) Active Hours Day Start Time End Time	none 0 none 1800) 12 Mon Hours Add	Mins Mins				



There are 88 device profiles listed under **Device Type**, but you can add/list only 16 devices per policy.

Now to apply the appropriate action, choose from the parameters under the **Action** menu to enforce the Policy. There are five attributes ACL, VLAN ID, QoS Policy, Session Timeout and Sleeping Client Timeout. You can configure these attributes and enforce clients with specified policies. By default the Session timeout is 1800 seconds and Sleeping client timeout is 12 Hrs.

The **Sleeping Client** refers to the clients already in RUN state after successful web authentication and are allowed to sleep and wakeup without the need to re-authenticate through the login page. The sleep client's duration for which client needs to be remembered for re-authentication is based on user configuration.

The Sleeping Client timeout configuration set in policy overrides the global sleeping client timeout configuration set on WLAN. These configurations and details are discussed later in this document, refer Appendix-A.

Active Hours menu allows configuration to be defined/set for what time of the day clients are allowed on the network.

<u>Note</u>

For the purpose of ease and demonstration only device parameters and vlan attributes are used to do profiling and policy enforcement in our setup.

Now Assign a VLAN ID and click Apply.

ONITOR HLANS CONTRO	LLER WORELESS SECURITY MANAGEMENT	COMMANDS HELP ETERDIACK	
Policy > Edit			< Back Apply
Policy Name		Employee-the	
Palicy 3d		1	
Match Criteria			
Match Role String			
Match EAP Type	1014 W		
Device Type	Andreid		
	Add		
Device List			
Apple-iPed		•	
Action			
IPv4 ACL			
WLAN ID	22		

As discussed in previous sections, we created a separate interface on the WLC when enforcing policy through vlan attributes. We have VLAN 20 for management and VLAN 22 for Employees iPads and Apple devices. Any iPad or Apple device connecting to a policy enforced WLAN will be redirected to a different VLAN. In the case of the given example, it is VLAN 22.

	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>o</u> mmand:	s help	FEEDBACK	
Interfaces								
Interface Name		VLAN Identifier	IP Address	Interface	Type Dyr	namic AP	Management	
Interface Name		VLAN Identifier 23	IP Address	Interface Dynamic	Type Dyr Disi	amic AP	Management	
Interface Name android apple		VLAN Identifier 23 22	IP Address 10.0.23.2 10.0.22.2	Interface Dynamic Dynamic	Type Dyr Disi Disi	abled	Management	
Interface Name android apple dynamic		VLAN Identifier 23 22 21	IP Address 10.0.23.2 10.0.22.2 10.0.21.2	Interface Dynamic Dynamic Dynamic	Type Dyr Disi Disi Disi	abled abled abled	Management	

Mapping a Policy on WLAN

I

Go to WLANs from WLC menu and click the WLAN ID on which you want the policy to be implemented. As you can see in the **WLAN> General** tab, Interface/Interface Group is tied to management interface which is on VLAN 20.

				Saye	e Configuration
MONITOR WLANS O	ontroller Wireless	SECURITY MANAGEMENT	COMMANDS HELP EE	EDBACK	
WLANs					
Current Filter: None	[Change Filter] [Clea	ar Filter]	Create New	▼ Go	
WLAN ID Type	Profile Name	WLAN SSID	Admin State	s Security Policies	2
WLAN	Demo-Employee	Demo-Employee	Enabled	None	

From the WLAN edit menu choose the Policy-Mapping tab.

	<u>w</u> lans <u>c</u> on	ITROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
WLANs > E	Edit 'Demo-	Employe	e'					
General	Security	QoS	Policy-Mappi	ng Adva	inced			
Profile N	ame	Den	no-Employee	\sim				
Туре		WLA	N		•			
SSID		Den	no-Employee					
Status		V (inabled					
Security	Policies	Nor	e					
		(Mod	ifications done i	under security	r tab will appear af	fter applying the	changes.)
Radio Po	licy	All						
Interface	e/Interface Grou	ip(G) mai	nagement 💌					
Multicast	Vlan Feature	Е Е	nabled					
Broadcas	st SSID	🗹 E	nabled					

Set the **Priority index** to any value from 1-16. Then select the policy which you already created, from the **Local Policy** drop down menu. To Apply the policy on WLAN click **Add.** The policy will be mapped to WLAN and can be seen under Policy Name.

	ANs <u>C</u> ON	TROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
WLANs > Edit	t 'Demo-	Employe	e'					
General	Security	QoS	Policy-Mapp	ing Adva	anced			
Priority Index Local Classifi	x (1-16) cation Policy	((1 Employee-iPad					
Priority Index	×	-	Add Policy	Name				

MONITOR	<u>W</u> LANs		TROLLER	WIRELESS	<u>S</u> ecurity	M <u>a</u> na	GEMENT	C <u>O</u> MMANI	DS I	HELP	EEEDBACK
WLANs >	Edit 'D	emo-l	Employe	ee'							
General	Secur	rity	QoS	Policy-Mapp	ing Adva	anced					
Priority Local C	Index (1-1 lassification	6) Policy		Employee-iPa	d 💌						
				Add							
Priority 1	Index			Policy Nam Employee-iP	ad I						

Now when an iPad associates to a policy enforced WLAN it is redirected to a VLAN tied to that policy. Scrolling down to Security Information will show you the local policy applied.

MONITOR WLANS	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Clients > Detail							
Client Properties					AP Properties		
MAC Address	70:de:e2:	:0e:ce:05			AP Address		3c:ce:73:1b:39:cl
IPv4 Address	10.0.22.5	3			AP Name		AP2600
IPv6 Address	fe80::72	de:e2ff:fe0e:c	e05,		АР Туре		802.11an
					WLAN Profile		Demo-Employee
					Status		Associated
					Association ID		1
					802.11 Authen	tication	Open System
					Reason Code		1
					Status Code		0
					CF Pollable		Not Implemented
				h	CF Poll Reques	t	Not Implemented
Client Type	Regular				Short Preamble	e	Not Implemented
User Name					PBCC		Not Implemented
Port Number	1.4	_			Channel Agility	,	Not Implemented
Interface	apple				Timeout		1800
VLAN ID	22				WEP State		WEP Disable
CCX Version	Not Suppo	orted			DIATO Deserved		
E2E Version	Not Suppl	orted			PMIP Properti	es	
Mobility Role	Local				Mobility type		Simple
Mobility Peer IP Addres	ss N/A						
Policy Manager State	RUN						

I

Γ

Security Policy Completed	Yes	
Policy Type	N/A	
Auth Key Mgmt	N/A	
Encryption Cipher	None	
EAP Type	N/A	
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	
IPv4 ACL Applied Status	Unavailable	
IPv6 ACL Name	none	
IPv6 ACL Applied Status	Unavailable	
mDNS Profile Name	default-mdns-profile	
mDNS Service Advertisement Count	0	
AAA Role Type	none	

Mapping the Policy to an AP Group

Disable the WLAN on which you want to configure the policy.

To apply the policy on an AP group we assume that you already have AP Groups configured on the WLC. If AP Groups has already been configured in your setup, please skip Step1 to 3.

If not, create an AP Group by going to WLC menu.

Step 1 Navigate to WLANs > Advanced> AP Groups and click Add Group.



Then type in the name to define your AP Group Name and click Add button.



Step 2 Now click on the AP Group Name and then from the menu click WLANs and Add New

MONITOR WLANS CONTROLL	er W <u>i</u> reless	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
AP Groups						
AP Group Name	AP	Group Descr	iption			
Employee-AppleDevice						
default-group						

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
Ap Group	s > Edit	'Employee-A	ppleDevice					
General	WLAN	Ns RF Profile	e APs	802.11u				
1								Add New
WLAN ID	WLAN	SSID Inter	face/Interfa	ce Group(G)	SNMP N/	AC State	_ /	1
							1	
0								

Step 3 From the drop down menu for WLAN SSID and Interface, select the required SSID and Interface respectively. Once selected click **Add** button to apply the selected WLAN on the AP Group.

I

NITOR <u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Groups > Edit	t 'Employee-A	ppleDevice					
eneral WLA	Ns RF Profile	APs	802.11u				
							Add New
id New							
WLAN SSID	Demo-Employ	ee(1)					
Interface	beine employe			-			
In the second second	management			K			
Group(G)							
Group(G) SNMP NAC State	Enabled						

Step 4 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the Policy. Then select **Policy-Mapping** from the drop-down menu.

ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>o</u> mmands	HELP	FEEDBACK
Group	s > Edit	'Employee-A	opleDevic	e'				
General	WLAP	s RF Profile	APs	802.11u				
WLAN ID	WLAN	SSID		Interface/In	terface Group(G)	SNMP NAC State	1	Add New
1	Demo	-Employee		management		Disabled		NAC Enable
							Ċ	Remove Policy-Mapping

Set the Priority Index to any value from 1-16, and then select the policy which you already created from Local Policy drop down list. To apply the policy on AP Group click Add. The policy will be mapped to AP Group and can be seen under Policy Name.

Click **Back** to go to the AP Group menu.

ſ



Step 6 If the APs are not added to group go ahead and add them by selecting the AP and clicking the **Add APs** button. Here we added AP2600 to the AP Group.



1



Once the AP has joined the specific AP group then Enable the WLAN on which the policy is enforced.

Test the policy enforcement by associating an iPad/Client to the WLAN. Once the device is associated and profiled, it gets redirected to the VLAN matching the policy.

MONITOR WLANS	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Clients > Detail							
Client Properties					AP Properties		
MAC Address	70:de:e2	:0e:ce:05			AP Address		3c:ce:73:1b:39:c0
IPv4 Address	10.0.22.5	53			AP Name		AP2600
IPv6 Address	fe80::72	de:e2ff:fe0e:c	e05,		АР Туре		802.11an
					WLAN Profile		Demo-Employee
					Status		Associated
					Association ID		1
					802.11 Authent	tication	Open System
					Reason Code		1
					Status Code		0
					CF Pollable		Not Implemented
				h	CF Poll Reques	t	Not Implemented
Client Type	Regular				Short Preamble	e	Not Implemented
User Name					PBCC		Not Implemented
Port Number	1				Channel Agility	,	Not Implemented
Interface	apple	_			Timeout		1800
VLAN ID	22				WEP State		WEP Disable
CCX Version	Not Supp	orted					
E2E Version	Not Supp	orted			PMIP Properti	es	
Mobility Role	Local				Mobility type		Simple
Mobility Peer IP Addres	s N/A						
Policy Manager State	RUN						

For	get this Netwo	orik
IP Address		
DHCP	BootP	Static
IP Address		10.0.22.53
Subnet Mask	-	255.255.255.0
Router		10.0.22.3
DNS		171,75,168,183
Search Domains		cisco.com
Client ID		
	Renew Lease	
HTTP Proxy		
Off	Manual	Auto



If your device is not being profiled correctly then the policy would not be enforced.

Example of Policy Enforcement on Other Device Types

Example

Policies were created for different device types (Android, Macbook, and Windows) coming into our network to be redirected to particular VLANs once they get profiled and policies are being enforced.

For this, dynamic interfaces such as "android" mapped to VLAN 23, Interface "apple" mapped to VLAN 22 and interface "dynamic" mapped to VLAN 21 was created.

Interfaces					
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
android	23	10.0.23.2	Dynamic	Disabled	
apple	22	10.0.22.2	Dynamic	Disabled	
dynamic	21	10.0.21.2	Dynamic	Disabled	
management	20	10.0.20.2	Static	Enabled	

In the following example, we are demonstrating profiling and policy implementation for Android and MAC devices.

For Employee MacBooks we created a policy name **Employee-Mac-Device** and added the Profiles from the WLC predefined profile list from the **Device Type** drop down menu.

Once the profile is matched, the policy enforcement is based on VLAN attribute. Here, the device should be redirected to VLAN 22 if it is a MacBook and to VLAN 23 if it is an Android device.

Policy "Employee-Mac-Device"

MONITOR WLANS CONTROLL	ER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Policy > Edit						
Policy Name		Employee-Ma	ac-Device			
Policy Id		6				
Match Criteria						
Match Role String						
Match EAP Type	none 💌					
Device Type						
OS_X_Lion-Workstation					i i	
OS_X_Leonard-Workstation						
OS X SnowLeopard-Workstation						
OS_X_Tiger-Workstation						
OS_X-Workstation						
Apple-MacBook					1	
Apple-Device					(
Action						
IPv4 ACL	none 💌					
VLAN ID	22					
Qos Policy	none					
	0					

1

Policy "Employee-Android"

MONITOR WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Policy > Edit							
Policy Name			Employee-And	biont			
Policy Id			4				
Match Criteria							
Match Role String							
Match EAP Type	n	one 💌					
Device Type							
	1	Vdd					
Device List							
Android							
Action							
IPv4 ACL	n	one 💌	-				
VLAN ID	23						
Qos Policy	n	one					
Session Timeout (secon	ds) 0						

WLANs > Edit 'Demo-Employee' Security Policy-Mapping Advanced General QoS Priority Index (1-16) Local Classification Policy Employee-Mac-Device -Add **Priority Index** Policy Name 1 Employee-iPad 2 Employee-WindowsClient 3 Employee-Android 4 Employee-iPhone 350926 5 Employee-Mac-Device

These policies are mapped to the WLAN "Demo-Employee"

In the above example, an Android device and a Macbook is associated to SSID **Demo-Employee** and both the device is being redirected to the VLAN 23 and VLAN 22 respectively.

Client details for Android Device:

MONITOR WLANS C	ONTROLLER WIRELESS S	ECURITY MANAGEMENT	COMMANDS HEL	EEEDBACK
Clients > Detail				
lient Properties			AP Properties	
MAC Address	18:45:17:ec:84:e8	-	AP Address	3croe:73:1b:39:c0
IPv4 Address	10.0.23.52		AP Name	AP2600
IPv6 Address	fe80::1a46:17ff:feec:84e8		AP Type	802.11bn
			WLAN Profile	Demo-Employee
			Status	Associated
			Association ID	1
			802.11 Authentication	Open System
			Reason Code	1
			Status Code	0
			CF Pollable	Not Implemented
		h	CF Poll Request	Not Implemented
Client Type	Regular		Short Preamble	Implemented
User Name			PBCC	Not Implemented
Port Number	1		Channel Agility	Not Implemented
Interface	android		Timeout	1800
VLAN ID	23		WEP State	WEP Disable
CCX Version	CCXv4			
E2E Version	Not Supported	P	MIP Properties	
Mobility Role	Local		Mobility type	Simple
Mobility Peer IP Address	s N/A			
Policy Manager State	RUN			

Client details for Apple MacBook:

ſ

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Clients >	Detail							
Client Pro	operties					AP Properties		
MAC Add	iress	f8:1e:df:	e2:e8:0e			AP Address		3c:ce:73:1b:39:c0
IPv4 Address		10.0.22.5	56 🗲	-		AP Name		AP2600
IPv6 Address		fe80::fa	le:dfff:fee2:e8	0e,		AP Type		802.11an
						WLAN Profile		Demo-Employee
					Status		Associated	
					Association ID		1	
					802.11 Authen	tication	Open System	
						Reason Code		1
						Status Code		0
						CF Pollable		Not Implemented
					h	CF Poll Reques	t	Not Implemented
Client Ty	pe	Regular				Short Preamble	e	Not Implemented
User Nan	ne					PBCC		Not Implemented
Port Num	nber	1				Channel Agility	1	Not Implemented
Interface	,	apple				Timeout		1800
VLAN ID		22	20725			WEP State		WEP Disable
CCX Ver	sion	Not Supp	orted				508	
E2E Vers	Version Not Supported			PMIP Properti	es			
Mobility R	Role	Local				Mobility type		Simple
Mobility P	Peer IP Addres	ss N/A						
Policy Ma	anager State	RUN						

1

Device Profile:

<pre><wlc> >show client</wlc></pre>	t summary device	type	
Number of Clients.			. 2
MAC Address	AP Name	Status	Device Type
18:46:17:ec:84:e8 f8:1e:df:e2:e8:0e	AP2600 AP2600	Associated Associated	Android OS_X_SnowLeopard-Workstation

Role Based Policy

Role is identified as a Cisco AV-pair from the AAA server and a user needs to configure the role as per user on the AAA server as:

Cisco:cisco-av-pair= role= <role-type>

The following example shows the role type "student" configured on ISE.

L

Γ

Results	
٩	▼ Common Tasks
@• ⊞• @•	DACL Name
Authentication	
🔻 🚞 Authorization	VLAN
Authorization Profiles	
 Downloadable ACLs 	Voice Domain Remission
Inline Posture Node Profiles	Li voice boman Pernisson
Profiling	
Posture	Web Redirection (CWA, DRW, MDM, NSP, CPP)
Client Provisioning	_
Security Group Access	
	 Advanced Attributes Settings
	Cisco:cisco-av-pair 📀 = role=student 📀 — 🕂
	 Attributes Details
	Access Type = ACCESS_ACCEPT
	cisco-av-pair = role=student
	Save Reset

Example of similar role type configured on ACS:

	Llear Catur	
ahaha	User Setup	
CISCO	0	^ Help
		Account Disabled
User Setup		Deleting a Usemanne
Group	Circo LOC /DIV 6 x DADIUS Attributos	Password Authentication
Setup	CISCO IUS/PIX 6.X RADIUS Attributes	Group to which the user is assigned Callback
Shared Profile Components	☑[009\001] cisco-av-pair	Client IP Address Assignment
Network Coofigeration	role=student	Network Access Restrictions
Sustan		Usage Quotas
Configuration		Account Disable Downloadable ACLs
Configuration	4	Advanced TACACS+ Settings TACACS+ Englisher Control
Administration		TACACS+ Enable Password
Secontrol		TACACS+ Shell Command Authorization
Databases		<u>Command Authorization for Network Device Management Applications</u> <u>TACACS+ Unknown Services</u>
Donna Posture Validation	IETF RADIUS Attributes ?	IETF RADIUS Attributes RADIUS Vendor-Specific Attributes
Sel Network Access		Time Bound Alternate Group
Step Profiles	E [UU0] Service-Type	Account Disabled Status
Reports and Activity	Authenticate only	
Online	[UU/] Framed-Protocol	the account Disabled check box to disable this account; clear the check box to enable the account.
CIII-2 Documentation	Ascend MPP V	[Back to Top]
	[UU9] Framed-IP-Netmask	Deleting a Username
	0.0.0.0	The Delete button appears only when you are editing an existing user account, not when
	[010] Framed-Routing	you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click DK.
	None 🔻	* [Back to Top]
	Submit Delete Cancel	fundamentary lines to fe

1

Now, to apply the role based policy on WLC, navigate to **Policy > Edit** page and under **Match Criteria** define the **Match Role String** that the user created earlier on the AAA server. In the example, the **Match Role String** is configured as **student**. Once the policy is created, the user can tie the policy to a specific WLAN (with L2 Security set to 802.1x).

Policy > Edit		< Back Apply
Policy Name	student	
Policy Id	1	
Match Criteria		
Match Role String	student	
Match EAP Type	none 👻	
Device Type	Android 👻	
	Add	

Flex-Connect Support

The following table explains the Policy application support matrix for FlexConnect mode.

Flex Operation	Feature Support	Comments
Central Switched	Yes	The policy application will work for central switching as per design.
Local Switched	Partial support	Only VLAN override is supported.
Central Authentication	Yes	The policy application will work as per design.
Local Authentication	No	No local authentication support.
Standalone mode	No	When in standalone mode the clients will be out of policy. The clients need to be centrally authenticated to get the policies applied again. Same would apply for external web-authenticated clients.

Limitations

ſ

- When local profiling is enabled, radius profiling is not allowed on a particular WLAN, both configurations are mutually exclusive.
- If AAA override is enabled and you get any AAA attributes from AAA server other than role type, the configured policy action is not applied. The AAA override attributes will have higher precedence.

- Wired clients behind the WGB won't be profiled and policy action will not be done.
- Only the first Policy rule which matches will be given precedence. Each policy profile will have an associated policy rule which will be used for matching the policies.
- Only sixteen policies per WLAN can be configured and globally sixty four policies will be allowed.
- Policy action will be done after L2 authentication is complete or after L3 authentication or when device sends http traffic and gets the device profiled. Due to which certain scenarios profiling and policy actions will happen more than once per client.
- This release will support only IPv4 clients to be profiled.
- No support for WGB wired clients for profiling as http profiling is not supported on WGB wired clients

Summary

- By default profiling is disabled on all WLANs.
- Each WLAN can have mapped profiling policies configured.
- Each Policy can have matching Role Type, Device Type, EAP type configured and an associated policy index mapped.
- The policy index signifies which policy needs to be matched first.
- The corresponding policy name will be deduced from the policy Index.
- The policy matching will exit at the first policy match and the corresponding policy action attributes will be set per client.
- The order of applying the policies per client will be based on security type.
- If a device is profiled once, the client is stored and the corresponding policy actions is applied.



See Cisco Wireless Device Profiling and Policy video for more information on setup and configuration.

Show Commands

show user <username> devices
show client wlan <WLAN Id>
show client wlan <WLAN Id> device-type <ipad | ipod | macbook ..>
show wlan <wlan-id>

Debug Commands

debug policy [events|errors] <enable|disables>
Debugs for profiler will be enabled by the existing "debug profiling <enable | disable>"
CLI

I

Commands to Configure Profiling through CLI

```
config wlan disable<wlan-id>
config wlan profiling <radius/local> <all/dhcp/http> enable <wlan-id>
config wlan enable <wlan-id>
```

Commands to Configure Policy through CLI

config policy <policy-name> create

config policy <policy-name> match device-type add <device name>

config policy <policy-name>action vlan <enable|disable> <vlan #>

config wlan policy add <policy index number> <policy-name> <WLAN Id>

To configure the policy and match it to a corresponding AP group, we need the policy Index also, which signifies which policies need to be matched first. The CLI command will be:

config wlan apgroup policy add <policy index number> <policy-name> <apgroup name> <WLAN Id>

To configure the policy and match it with time of day, the CLI command will be:

config policy <policy-name>active add hours <08:00 - 17:00> days <Mon | Tue | Wed | Thurs
| Fri | Daily | Weekdays >

To configure the policy match with EAP type, the CLI command will be:

config policy <policy-name> match eap-type add <peap | leap | eap-fast | eap-tls>

For policy action as ACL, the CLI command will be:

config policy <policy-name> action acl <acl-name> <enable/disable>

For policy action as QoS, the CLI command will be:

config policy<policy-name> action qos <bronze | gold | platinum | silver>
<enable|disable>

For policy action as Session-Timeout, the CLI command will be:

config policy <policy-name> action session-timeout <timeout in sec> <enable|disable> For policy action as Sleeping Client Timeout, the CLI command will be:

config policy <policy-name> action sleeping-client-timeout <enable|disable><timeout in

Appendix-A

Sleeping Client Support

hours>

Currently in 7.4 release, guest client devices connected to the WLC on web-auth enabled WLANs have to enter login credentials every time the client goes to sleep and wakes up.

From 7.5 release, clients already in RUN state after successful web authentication are allowed to sleep and wakeup without the need to re-authenticate through the login page. The sleep client duration for which client needs to be remembered for re-authentication is based on the configuration.

Other salient features are as follows:

- Feature is configurable per wlan.
- Supported only for L3 security enabled WLANs. Not applicable to Guest LAN or Remote LAN.
- Sleep client duration is configurable for 1hrs to 30days (720 Hrs) with a default value set to 12 hours. This duration is configurable on WLAN as well as on the policy mapped to the WLAN. The policy mapped configuration takes precedence over WLAN configuration.
- The maximum number of sleeping clients supported is based on the platform.
 - WiSM/5508 1000
 - 7500/8500 9000
 - 2500 500
- Flex connect AP Support Sleep client support feature works with flexconnect mode AP's in local switching case for both internal and external web-auth.
- High Availability– Only configuration sync is supported. Sleep cache entries are not synchronized across active and standby.

WLAN Configuration for Sleeping Client

As sleeping client is only supported for L3 security WLANs, navigate to the particular WLAN on which you want to enable the sleeping client feature. Navigate to **Security > Layer 3** and select **Web Policy** from the Layer 3 Security drop-down list.

Select the radio button **Authentication** and enable **Sleeping Client** by checking the box as shown in the image below.



Navigate to **Advanced** tab and make sure that the session timeout is greater than the client idle timeout, otherwise the sleeping client entry would not be created.

I

eneral Security QoS Polic	y-Mapping Advanced
Allow AAA Override	Enabled
Coverage Hole Detection	C Enabled
Enable Session Timeout	neout (secs)
Aironet IE	Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None
P2P Blocking Action	Disabled
Client Exclusion 2	Enabled 60 Timeout Value (secs
Maximum Allowed Clients	0
Static IP Tunneling 11	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
Clear HotSpot Configuration	Enabled
Client user idle timeout (15-100000)	300 Seconds
Client user idle threshold (0-10000000)	0 Bytes
Off Channel Scanning Defer	

Now connect a client to the WLAN on which sleeping client feature is enabled. Then navigate to Monitor > Clients, the status of the client shows that it is in **Associated** state but Not Authenticated as username/password required for web-auth.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS SECUR	ITY NANAGEMENT	COMMANDS HELP	TEEDBACK							Sage	Configurati
Monitor Summary > Access Peints > Cisco CleanAir > Statistics > CDP Regues Clients Sleeping Clients Hulticast Applications	Clients Current Filter Client RAC Adde 70:de:e2:0e:ce.0	None IP Address 10.0.10.135	(Chanse Fiber) (Cle AP Name AP3600-1	wLAN Profile Quest-Services	WLAN SSID Guest-Services	User Name Unknown	Protocol 802.11an	Status Associated	Auth Por No 1	Slot Id	PHIPv6	WGB No	Device Type Apple-iPad	

Γ

Seneral	AVC Statistics					
lient Pro	perties		A	P Properties		
MAC Address		70:de:e2:0e:ce:05		AP Address	9c:4e:20:72:e1:d0	-
IPv4 Address		10.0.10.135		AP Name	AP5	
IPv6 Address				AP Type	802.11bn	
				AP radio slot Id	0	
				WLAN Profile	Guest-Services	
				Status	Associated	
				Association ID	1	
				802.11 Authentication	Open System	
				Reason Code	1	
				Status Code	0	
			4	CF Pollable	Not Implemented	
Client Typ	pe	Regular		CF Poll Request	Not Implementer	
User Nam				Short Preamble	Implemented	
Port Num	ber	1		PBCC	Not Implemented	
Interface		management		Channel Agility	Not Implementer	
VLAN ID		10		Timeout	1800	
CCX Versi	ion	Not Supported		WEP State	WEP Disable	
E2E Versio	on	Not Supported	100	0.000000000000		
Mobility R	ole	Local	P	MIP Properties		-
Mobility P	eer IP Address	N/A		Mobility type	Simple	
Policy Man	nager State	WEBAUTH_REQD				
Protection		No				
UpTime (Sec)	10				
Power Sav	ve Mode	OFF				
Current T	xRateSet					
Data Rate	eSet	1.0,2.0,5.5,11.0,6.0,9.0,12.0 ,18.0,24.0,36.0,48.0,54.0 ×				
KTS CAC Capability		No				
802.11u		Not Supported				

Under Client Properties menu, it is seen that the client is in Web-auth required state.

1

After entering the appropriate login credentials for web-auth, the client get authenticated and moves to RUN state.

eral AVC Statist	ics		
nt Properties		AP Properties	
C Address	70:de:e2:0e:ce:05	AP Address	9c:4e:20:72:e1:d0
v4 Address	10.0.10.135	AP Name	AP5
v6 Address		AP Type	802.11an
		AP radio slot Id	1
		WLAN Profile	Guest-Services
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
ent Tune	Deside:	CF Pollable	Not Implemented
ent rype	Regular	CF Poll Request	Not Implemented
er name	an .	Short Preamble	Not Implemented
re number	1	PBCC	Not Implemented
	management	Channel Agility	Not Implemented
AN ID	10	Timeout	1800
E Version	Not Supported	WEP State	WEP Disable
e version	Not Supported	DMID Dreporties	
billty Role	Local	Phile Properties	
line Managers Shake		Mobility type	Simple
inagement Frame	No		
Time (Sec)	89		
wer Save Mode	ON		
rrent TxRateSet			
ta RateSet	6.0,9.0,12.0,18.0,24.0,36.0,4 8.0,54.0		
S CAC Capability	No		
2.11u	Not Supported		

After successful web-auth, the user is successfully authenticated.

Γ



Now if the client configured is idle for 300 seconds (default idle timeout value) or disconnects from the WLAN it is connected to, then the client will move to sleeping clients. Click **Sleeping Clients** option to check if the client entry exists.



Once the client is moved to the Sleeping Clients, the timeout session starts and the remaining time before the client entry is deleted/cleared is displayed.

If the client wakes up or joins back to the same WLAN, it doesn't require re-authentication.

Sleeping Client CLI commands

To enable the sleeping-client feature on wlan: (controller) >config wlan custom-web sleep-client enable/disable <wlan-id> To configure sleeping-client interval on wlan: (controller) > config wlan custom-web sleep-client timeout <1- 720hours> <wlan-id> To check sleep client configuration on wlan: (controller) > show wlan <wlan-id> To delete any unwanted sleeping-client entries: (controller) > config custom-web sleep-client delete <mac-addr> To show summary of all the sleeping-client entries: (controller) > show custom-web sleep-client summary To show the details of sleeping-client entry based on mac address: (controller) > show custom-web sleep-client detail <mac-addr>

I