

Application Visibility and Control Feature Deployment Guide

Last Updated: August, 2014



Cisco Systems, Inc. www.cisco.com

Application Visibility and Control Release Update

Phase 1—AVC 7.4	• Application classification and control of 1039 applications with NBAR2 engine.
	• Support of 16 AVC profiles with 32 rules per profile.
	• One AVC profile support per WLAN; the same profile can be supported on multiple WLANs.
	• AVC profile mapped to WLAN has a rule for MARK or DROP action.
	• Graphical presentation on the controller for all classified applications
	• One NetFlow exporter and monitor can be configured on the WLC.
	• AVC NetFlow monitoring on PI with PAM license.
Phase 2—AVC 7.5	Protocol Pack 4.1 support in AVC Phase 2.
	Additional application support—Total of 1056 applications
	• Support for loading protocol pack dynamically to update applications.
Phase 3—AVC 8.0	Protocol Pack 9.0
	• NBAR Engine Release 3.1
	• AAA AVC Profile override for clients.
	• Application rate limiting per-user on WLAN.
	• Integration of AVC profiles to the Local Policy classification per user and per device.
	• AVC Directional QoS DSCP Marking for Upstream and Downstream traffic.
	Support for 1105 applications

Application Visibility and Control—Phase 1

Network Based Application Recognition (NBAR) provides application-aware control on a wireless network and enhances manageability and productivity. It also extends Cisco's Application Visibility and Control (AVC) as an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to take some action on the same.

NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which supports stateful L4 - L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a Common Flow Table for all IOS features which use NBAR. NBAR2 recognizes application and passes on this information to other features like QoS, NetFlow and Firewall, which can take action based on this classification.

The key use cases for NBAR are capacity planning, network usage base lining and better understanding of what applications are consuming bandwidth. Trending of application usage helps network admin to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

NBAR is supported on 2500, 5500, 7500, 8500 and WiSM2 controllers on Local, Mesh, and Flex Mode APs (for WLANs configured for central switching only).

NBAR Supported Feature

NBAR as a feature can perform the following tasks:

- 1. Classification–Identification of Application/Protocol.
- 2. AVC–Provides visibility of classified traffic and also gives an option to control the same using Drop or Mark (DSCP) action.
- 3. NetFlow–Updating NBAR stats to NetFlow collector like Cisco Prime Assurance Manager (PAM).

Application Visibility and Control–Phase 2

In phase two of the AVC support for Protocol Packs has been added. Protocol packs are software packages that allow update of signature support without replacing the image on the Controller. You have an option to load protocol packs dynamically when new protocol support is being added. There are two kinds of Protocol Packs—Major and Minor:

- Major protocol packs include support for new protocols, updates, and bug fixes.
- Minor protocol packs typically do not include support for new protocols.
- Protocol packs are targeted to specific platform types, software versions and releases separately.
 Protocol Packs can be downloaded from CCO using the software type "NBAR2 Protocol Pack".

Protocol packs are released with specific NBAR engine versions. For example, WLC 7.5 has NBAR engine 13, so protocol packs for it are written for engine 13 (pp-unified-wng-152-4.S-13-4.1.1.pack). Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (13 in the example above). Therefore for example – PP4.1 for 3.7 (version 13) can be loaded on top of 3.7 (version 13) and 3.8, but PP4.1 for 3.8 cannot be loaded on top of 3.7. It is strongly recommended to use the protocol pack that is the exact match for the engine.

For AVC phase 2, protocol packs can be downloaded directly from CCO–Protocol Pack 4.1.1 for engine XE 3.7. The protocol pack file "pp-AIR-7.5-13-4.1.1.pack" (Format: pp-AIR-{release}-{engine version}-M.m.r.pack) will be located in the same location with the controller code version 7.5. This is the only tested and supported protocol pack released with controller software version 7.5.



If you download the protocol pack from the below link where protocol packs for other Cisco devices is posted for download, the protocol packs might work but will not be supported. See http://software.cisco.com/download/release.html?mdfid=282993672&flowid=20841&softwareid=2845 09011&release=4.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Download So	ftware	Download Cart (0 tems) [4] Feedback Help
Downloads Home > Produc Cisco 5508 Wireless Contro Cisco 5508 Wireless	ts > Wireless > Wireless LAN Controller > Standalone Controllers > Cisi lier > NBAR2 Protocol Packs-4.1.1 Controller	co 5500 Series Wireless Controllers >
Search	Release 4.1.1	Release Notes for 4.1.1 📓 💩
Expand All Collapse All	File information	Release Date 👻 Size
= stact Palascac		

Complete list of the protocols supported in the release posted at the link below

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Note

For AVC Phase 2 the downloadable NBAR Protocol Packs are supported on 5500, 7500, 8500 and WiSM2 controllers on Local, Mesh, and Flex Mode APs (for WLANs configured for central switching only). The 2500 series controllers do not support Protocol Packs.

NBAR/AVC Facts

- NBAR/AVC phase 2 on WLC can classify and take action on 1054 different applications.
- Two actions, either DROP or MARK is possible on any classified application.
- Maximum 16 AVC profiles can be created on a WLC.
- Each AVC profile can be configured with a maximum 32 rules.
- Same AVC profile can be mapped to multiple WLANs. But one WLAN can have only one AVC profile.
- Only 1 NetFlow exporter and monitor can be configured on WLC.
- NBAR/AVC stats are displayed only for top 10 applications on GUI. CLI can be used to see all applications.
- NBAR/AVC is supported on WLANs configured for central switching only.
- If AVC profile mapped to WLAN has a rule for MARK action, that application will get precedence as per QOS profile configured in AVC rule overriding the QOS profile configured on WLAN.
- Any application, which is not supported/recognized by NBAR engine on WLC, is captured under the bucket of UNCLASSIFIED traffic.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- AVC profile can be configured per WLAN and cannot be applied per user basis.
- NBAR/AVC is not supported in vWLC and SRE WLC.

AVC and QoS Interaction on the WLAN

The AVC/NBAR2 engine on the controller interoperates with the QoS settings on the specific WLAN. The NBAR2 functionality is based on the DSCP setting. The following occurs to the packets in Upstream and Downstream directions if AVC and QoS are configured on the same WLAN:

Upstream

- 1. Packet comes with or without inner DSCP from wireless side (wireless client).
- 2. AP will add DSCP in the CAPWAP header that is configured on WLAN (QoS based configuration).
- 3. WLC will remove CAPWAP header.
- 4. AVC module on the controller will overwrite the DSCP to the configured **marked** value in the AVC profile and send it out.

Downstream

- 1. Packet comes from switch with or without inner DSCP wired side value.
- 2. AVC module will overwrite the inner DSCP value.
- **3.** Controller will compare WLAN QoS configuration (as per 802.1p value that is actually 802.11e) with inner DSCP value that NBAR had overwritten. WLC will choose the lesser value and put it into CAPWAP header for DSCP.
- 4. WLC will send out the packet to AP with QoS WLAN setting on the outer CAPWAP and AVC inner DSCP setting.
- 5. AP strips the CAPWAP header and sends the packet on air with AVC DSCP setting; if AVC was not applied to an application then that application will adopt the QoS setting of the WLAN.

AVC Operation with Anchor/Foreign Controller's Setup

In the case of Anchor and Foreign controller's configuration, the AVC has to be configured where the application control essentially is required. In most cases in Anchor/Foreign setups the AVC should be enabled on the Anchor controller. AVC profile enforcement will happen on the WLAN on the Anchor controller. If Anchor controller is release 7.4 or higher the above mentioned setup will work.

Loading AVC Protocol Pack–Phase 2

Loading of Protocol Packs is supported only via the command line interface. The command to load a protocol pack is shown in the example below:

(Cisco Controller) >transfer download datatype avc-protocol-pack
(Cisco Controller) >transfer download start
Mode FTP
Data Type AVC Protocol Pack
FTP Server IP A.B.C.D
FTP Server Port 21
FTP Path/
FTP Filename pp-unified-wng-152-4.S-13-4.1.1.pack
FTP Usernamecisco

```
FTP Password..... ********
Starting transfer of AVC Protocol Pack
This may take some time.
Are you sure you want to start? (y/N)
v
(5508-60-Active) >transfer download datatype avc-protocol-pack ┥
(5508-60-Active) >transfer download filename pp-adv-asr1k-152-4.S-13-4.1.1.pack
(5508-60-Active) >transfer download start
Node..... TFTP
Data Type..... AVC Protocol Pack
TFTP Server IP..... 10.70.0.59
TFTP Packet Timeout.....
TFTP Max Retries..... 10
TFTP Path.....
TFTP Filename.....pp-adv-asr1k-152-4.S-13-4.1.1.
pack
Starting tranfer of AVC Protocol Pack
This may take some time.
Are you sure you want to start? (y/N)
```

The download process might take some time.

TFTP AVC Protocol Pack transfer starting. TFTP receive complete... Loading Protocol Pack. INFO, deactivation XDR was bypassed as batch config was identified % INFO NBAR : engine deactivation AVC Protocol Pack installed.

1510

ñ

Use the show command to view the currently loaded protocol pack

```
(Cisco Controller) >show avc protocol-pack version
AVC Protocol Pack Name: Advanced Protocol Pack
AVC Protocol Pack Version: 1.0
```

Use the show command to view the current Nbar2 Engine Version

(Cisco Controller) >show avc engine version AVC Engine Version: 13

Before installing the Protocol Pack the default pack will show as follow:



After installing the Protocol Pack the AVC pack will show as version 4.10001:

(5508-60-Active) >show avc engine version	
AVC Engine Version: 13	
(5508-60-Active) >show avc protocol-pack version	
AVC Protocol Pack Name: Advanced Protocol Pack AVC Protocol Pack Version: 4.10001	512
(5508-60-Active) >	361

Debug Commands

(Cisco Controller) >debug avc events enable (Cisco Controller) >debug avc error enable

Configure Application Visibility

I

Complete these steps:

- 1. Open a web browser on the Wired Laptop. Enter your WLC IP Address.
- **2.** Create an OPEN WLAN with naming convention as for example: "POD1-Client" and enable Application Visibility on that WLAN under QOS TAB. Map this WLAN to management interface.

To enable Application visibility, click **WLAN ID** and then click the QOS tab and check the enable option for **Application Visibility** and click **Apply**.

ululu cisco		<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT
WLANS	WLANs >	New	WLAN	v 🗸		
Advanced	Profile Na SSID	ame	POD1 POD1	-Client -Client		
	ID		1	*		



3. Once Application Visibility is enabled on the specific WLAN, from the associated wireless client start different types of traffic using the applications (already installed) like Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, YouTube, Ping,

Trace route, etc. Once traffic is initiated from wireless client, visibility of different traffic can be observed globally for all WLANs, Per Client Basis and Per WLAN Basis which provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per client, per WLAN, and globally.

As mentioned above Visibility of traffic can be monitored:

- Globally for all WLANs
- Individual WLAN
- Individual Client
- 4. To check the visibility globally for all WLANs on WLC, click and scroll down.

									Say	e Configuration
MONITOR	WLANS	<u>c</u> 0	NTROLLER	WIREL	ESS SE	CURITY	MANAGEMENT	COMMANDS	HELP FE	EDBACK
			1.1			AAA A	uthentication Failu	re for UserNan	ne:c84c7579f45	5d User Type: W
Access Po	int Sum	mar	Y			View A	1	100		
	Total		Up	Down		Тор Ар	plications 👉			
802.11a/n Radios	1		1	0	Detail	Applic	ation Name		Packet Count	Byte Count
802.11b/g/n Radios	1		1	0	Detail	http		(U)	1216	0
All APs	1		1	0	Detail			(D)	2210	3164720
						youtub	e	(U)	846	21806
Cillant Cum								(D)	1495	1919261
client Sum	imary					ssl		(U)	186	19344
Current Clie	nts	4			Detail			(D)	214	154042
Current Clients Excluded Clients		0			Detail	skype		(U)	525	11189
Excluded Clients 0 Disabled Clients 0		Detail			(D)	561	24614			
					-	ms-live	accounts	(U)	33	3364
								(D)	28	13588
						ping		(U)	90	5760
								(D)	90	5760
						dns		(U)	7	305
								(D)	7	2590
						yahoo	voip-over-sip	(U)	1	86
								(D)	1	0
						webex	-meeting	(U)	3	37
								(D)	3	37
						poco		(U)	3	40
								(D)	2	0
						This pag	e refreshes every	30 seconds.		

<u>Note</u>

The monitor screen list the applications classified by NBAR engine running on WLC for all the WLANs. The top ten applications in the last 90 seconds in both Upstream (U) and Downstream (D) directions will be listed on this page.

5. To have more granular visibility per WLAN, navigate to **Monitor > Applications**. This page will list all the WLANs on which AVC visibility is enabled.

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Monitor Summary	WLANS	Туре	Profile Name		WLAN	551D	Admi	n Status	Avc Profile
 Access Points Cisco CleanAir Statistics CDP Rogues Clients Multicast Applications 	1	WLAN	POD1-Client		POD1-C	lient	Enable	d	None

Now click the individual WLAN ID and the below screen will be visible which will list aggregate data for the top ten applications running on that particular WLAN.

gregate Upstream	m Downstr	eam	1				_	
plication Last 90 Sec	Packet	Byte	Average	Usage	Application Cumulative 1	Packet Count	Byte Count	Usage(%)
App Name	Count	Count	Packet Size	(**)	VDC	544	529017	67.72
gtalk-chat	25	4010	160	28.86	http	163	132199	16.92
yahoo-messenger	9	3671	407	26.42	gtalk-chat	222	55448	7.10
webex-meeting	7	3232	461	23.26	webex-meeting	93	48925	6.26
http	19	2734	143	19.68	vahoo-messenger	41	14684	1.88
bittorrent	6	204	34	1.47	bitterrent	25	881	0.11
		gta yd we	alk-chat(28.86%) hoo-messenger(2 ibex-meeting(23.) 26.42%) 26%)			vnc(67	.72%) 5.92%) hat(7.10%)
		gt. yd we htt	alk-chat(28.86%) hoo-messenger(2 ibex-meeting(23. tp(19.68%) torrent(1.47%)) (6.42%) 26%)			vnc(67	.72%) 5.92%) hat(7.10%) meeting(6.26%) messenger(1.88%

<u>Note</u>

I

This page will provide more granular visibility per WLAN and will list the top ten applications in last the 90 seconds, as well as cumulative stats for the top ten applications. The above screen lists the aggregate traffic on a particular WLAN, which includes upstream as well as downstream data. You can view UPSTREAM and DOWNSTREAM stats individually per WLAN from same page by clicking the **Upstream** and **Downstream** tab.

6. To have further granular visibility of the top ten applications per client on a particular WLAN on which AVC visibility is enabled, navigate to **Monitor > Clients** and click any individual client MAC entry listed on that page.

cisco		CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	T COMMANDS	ation <u>P</u> ing	Logou	t i Bet
Monitor	Clients						Entr	ies 1 -	l of 1
Summary Maccess Points	Current Filter	None	(Change F	ilter] [Clear Fi	itter]				
Cisco CleanAir	Client MAC Add	AP Name		WLAN	Profile	WLAN SSID	Status	Auth	Port
 Statistics CDP 	00:40:96:59:25:60	POD1-AP		POD1	Client	POD1-Client	Associated	Yes	1
Rogues	-								

After clicking on an individual client MAC entry listed on the above page, the client details page will open which will have two tabs; one for general information and another tab with the name **AVC Statistics**. Click the **AVC Statistics** tab to see the NBAR statistics for the top ten applications for that particular client.

ina > Dorain	-					
neral AVC Statistics						
Aggregate Upstream	Downstrea	m				
Last 90 Secs Stats	•			Cumulative Stats	+	_
Last 90 Secs Stats	Average Packet Size	Packet Count	Byte Count	Cumulative Stats	Packet Count	Byte Cou
Last 90 Secs Stats Application Name gtalk-chat	Average Packet Size 174	Packet Count 25	Byte Count 4010	Application Name	Packet Count 555	Byte Cou 529060
Application Name gtalk-chat yahoo-messenger	Average Packet Size 174 611	Packet Count 25 10	Byte Count 4010 3671	Application Name	Packet Count 555 194	Byte Cou 529060 136257
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting	Average Packet Size 174 611 646	Packet Count 25 10 7	Byte Count 4010 3671 3232	Cumulative Stats Application Name vnc http gtalk-chat	Packet Count 555 194 247	Byte Cour 529060 136257 59458
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting http	Average Packet Size 174 611 646 245	Packet Count 25 10 7 21	Byte Count 4010 3671 3232 2942	Cumulative Stats Application Name vnc http gtalk-chat webex-meeting	Packet Count 555 194 247 100	Byte Cour 529060 136257 59458 52157
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting http bittorrent	Average Packet Size 174 611 646 245 68	Packet Count 25 10 7 21 6	Byte Count 4010 3671 3232 2942 204	Cumulative Stats Application Name vnc http gtalk-chat webex-meeting yahoo-messenger	Packet Count 555 194 247 100 51	Byte Court 529060 136257 59458 52157 18355



This page will provide further granular stats per client associated on WLAN on which Application Visibility is enabled and will list the top ten applications in last 90 seconds as well as cumulative stats for top ten applications. The above screen lists the aggregate traffic per client, which includes upstream as well as downstream stats. You can view UPSTREAM and DOWNSTREAM stats individually per client from same page by clicking the **Upstream** and **Downstream** tab.

Configure AVC Profile

Complete these steps:

- 1. The NBAR feature on a WLC not only gives a visibility of applications running in the network, but also gives the administrator an option to control the applications running in the network by creating an AVC profile. AVC profiles can be configured to take the following actions on the recognized applications:
 - **a.** Action DROP (Traffic for that application will be dropped)
 - **b.** Action MARK (Particular applications can be marked with different QOS profiles available on WLC, or the administrator can custom define the DSCP value for that application)

 To see all the applications supported by NBAR engine for stats, visibility and control action (DROP/MARK), navigate to Wireless > Application Visibility And Control > AVC Applications. This page will list down all the applications in sorted order with the application group they belong.

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY M	Saye Configur	ation E	ng Logout Befre HELP FEEDBA
cisco	Tenner Tenne Jennerer	There are a second the second se			Teres
Wireless	AVC Applications			En	tries 1 - 50 of 51
Access Points All APs * <u>Redios</u> 802.11a/n/ac	Current Filter None	[Change Filter] [6	(lear Filter)	P4	4 I 2 - H
802.11b/g/n Dual-Band Radios Global Configuration	Application Name	Application Group	Application ID	Engine 10	Selector ID
Advanced	3com-amp3	other	538	3	629
Mesh	3com-tsmux	obsolete	977	3	106
PE Deofiles	380	layer3-over-ip	788	1	34
ElexConnect Groups	914c/g	net-admin	1109	3	211
FlexConnect ACLs	9pfs	net-admin	479	3	564
▶ 802.11a/n/ac	0000	net-admin	582	3	674
▶ 802.11b/g/n	asas	other	939	3	62
Media Stream	accessbuilder	other	662	3	888
Application Visibility	accessnetwork	other	607	3	699
And Control	ace	other	513	3	599
AVC Applications	acr-nema	industrial-protocols	975	3	104
Country	active-directory	other	1194	13	473
Timers	activesync	business-and-productivity-tools	1419	13	490
Netflow	adobe-connect	other	1441	13	505
Oos	aed-512	obsolete	963	3	149
And I	afpovertcp	business-and-productivity-tools	1327	3	548
	agents	net-admin	609	3	705
vascript:void(0):	aloes	net-admin	377	3	463

<u>Note</u>

ſ

While creating the drop/mark action for any application under AVC profile, application group need to be selected first. This page list down all the applications with application group they belong and with simple lookup for application using browser "FIND" option, an administrator can find applications and its group and use this group in AVC profile to configure drop/mark action which is discussed further in this guide. NBAR on WLC supports visibility of 1054 different applications.

To configure any action (drop/mark), the AVC profile should be created first. To configure the AVC profile, navigate to Wireless > Application Visibility And Control > AVC Profiles and then click New to create the AVC profile.



4. Enter AVC profile name and click Apply.



5. After Apply is clicked, the AVC profile will be created and you can see the above-created profile, which can be clicked further to create rules to take drop/mark action. Maximum of 16 AVC profiles can be created on a WLC.

cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Wireless	AVC Prof	file Name	•					
Access Points All APs Padies	AVC Profi	le Name						
802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration	Block Yout	tube						

6. After creating the AVC profiles, you can click on any profile name and create rules for individual profiles. Maximum of 32 rules can be configured in each profile. Rules can be configured to take any of the two actions i.e. DROP or MARK. If no rule is configured for any application the default action will be "Allow" with QOS policy configured on a WLAN. To create rules under profile, navigate to **Wireless > Application Visibility And Control > AVC Profiles** and then click any of the above created profile.

	₩LANs		LLER \	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	нецр	Ping Logout <u>R</u> efrest
AVC Profil	e > Edit	'Block	_Youtu	be'					Add New Rule
Application Name	Applica Group	ation Name	Action	DSCP					

7. Now click **Add New Rule** and the below page (2nd screen shot) is displayed where the administrator can select the application group from the first drop-down which filters the applications that belong to that group only. Then, from the second drop-down application can be selected. Once the application is selected from second drop down, the administrator can select what action should be taken on that application from third the drop-down. Once the action is selected click **Apply**.

MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Ping Logout Refrest
AVC Profi	le > Edit	'Block_Yo	utube'				1	Add New Rule
Application Name	n Applic Group	ation Name Ac	tion DSCP			-		

MONITOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Logout Refres
AVC Profile > Ru	ile > 'Block_Yo	utube'				~	Apply
Application Group	voice-and-vid	eo	× +			-	
Application Name Action	youtube Drop 🌱 4	~					



In 7.5 release, WLC is capable of classifying 1054 applications and provide an option to take any action. To take an action on any application, the administrator has to select application group first to which that application belongs which will filter the list of applications for that application group only. The reason for this implementation is all 1054 applications cannot be displayed in a single drop-down. Also in release 7.5, the Application Names are now selectable and by hovering over and clicking the application name in the list the above profile rule can be created.

CISCO		MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
All all and	^	xnet			layer3-over-ip		770	1	15	
Wireless		xns-auth			email		936	3	56	
Access Points		xns-ch			business-and-p	productivity-too	ols 934	3	54	
All APs		xns-courier			email		1010	3	165	
 Radios 802.11a/n/ac 		xns-idp			layer3-over-ip		776	1	22	
802.11b/g/n		xns-mail			email		937	3	58	
Global Configuration		xns-time			net-admin		932	3	52	
Advanced		ate			layer3-over-ip		790	1	36	
Mesh		ayttp			other		422	3	508	
RF Profiles		xwindows			net-admin		45	3	6000	
FlexConnect		xyplex-mux			other		1018	3	173	
Groups		yahoo-mail			email		1462	13	526	
FlexConnect ACLs		yahoo-mess	enger	1	instant-messag	ping	77	13	77	
802.11a/n/ac		yahoo-voip-	messenge		voice-and-vide	0	674	13	422	
802.11b/g/n		yahoo-voip-	over-sip		voice-and-vide	0	1195	13	302	
Media Stream		xoutube			voice-and-vide	0	82	13	82	
Application Visibility And	L.	239.50		1	business-and-p	productivity-too	ols 1108	3	210	
Control		zannet			file-sharing		1157	3	317	
AVC Applications		zattoo			voice-and-vide	0	115	13	428	
Country		zsery			other		763	3	346	

8. After Apply is clicked, the action rule will be created and displayed as captured in the below screen. You can add more rules under the AVC profile on the same page. Maximum of 32 rules can be configured in a single AVC profile.

		WIDELECC	SECURITY	MANAG	EMENT	COMMANDS	HEID	FEEDBACK	Logout Befresh	
MONTION MOANS	CONTROLLER	WIRELESS	SECORIT	MANAG	EMENT	COMMANDS	ncith	LCCODACK		
AVC Profile > Edit	t 'Block_You	utube'							Add New Rule	
Application Name	Applicat	ion Group Nam	e Action	DSCP						
youtube	voice-an	d-video	drop	NA						52
										35.1

Another rule can be configured under the same AVC profile to MARK traffic with a different QOS profile or custom DSCP value. In this example, another AVC profile was created following step 3, 4 and 5 with the name "Mark_Http_Webex". In this example this AVC profile is used to create a rule to mark "Http" with low priority and give "Webex" more precedence.



As discussed in previous steps 6, 7 and 8, click the AVC profile name to create rules for the profile. Click **Add New Rule.**

MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>P</u> ing Logout <u>R</u> efres
AVC Prof	file > Edit	: 'Mark_Http	Webex'				1	Add New Rule
Applicatio Name	on Applie Group	ation Name Acti	on DSCP					

Select Application group from the first drop-down and Application name as **Webex** from second drop-down. Then, configure Action as **MARK** and select QOS profile as **Platinum** and the click **Apply**.

								Logout Refre
MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
AVC Prof	file > Rul	e > 'Mark_Http	_Webex'				_	Apply
Application	Group	voice-and-vid	eo	v 🔶				
Application I	Name	webex-meetin	9 4					
Action		Mark 🛩 ┥	_					
Dscp (0 to 6	3)	Platinum(voice	e) 🗸					

After **Apply** is clicked, the action rule will be created and displayed as captured in below screen. Click **Add New Rule** on same page to create another rule to MARK another application "Http".

									<u>Ping Logout R</u> efr
MONITOR	WLANS	CONTROLLER	WIRELESS	SECUR	UTY .	MANAGEMENT	COMMANDS	HELP	
AVC Prof	file > Edit	'Mark_Http_	Webex'				_	-	Add New Rule
Applicatio Name	'n	Application Group Nam	n ne	Action	DSCP				
webex-me	eting	voice-and-vi	ideo	mark	46				

Create another rule in the same profile by just clicking **Add New Rule** on the same page. Select Application group from the first drop-down and Application name as **http** from second drop-down. Then, configure Action as **Mark** with QOS profile as Bronze. Then click **Apply**.

							15	Logout <u>R</u> ef
MONITOR	<u>W</u> LANs	CONTROLLER W	IRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Prof	file > Rul	e > 'Mark_Http_V	/ebex'				-	Apply
Application (Group	browsing		× (
Application 1	Name	http	~ 4	_				
Action		Mark 💌 🔶	-					
Dscp (0 to 6	3)	Bronze(backgrou	nd) 💌					

After Apply is clicked, the action rule will be created and displayed as captured in below screen.

MONITOR WLANS	CONTROLLER WIRELESS	SECUR	RITY	MANAGE	MENT	COMMANDS	HELP	EEEDBACK
AVC Profile > Edit	'Mark_Http_Webex'							
Application Name	Application Group Name	Action	DSCP					
webex-meeting	voice-and-video	mark	46					
http	browsing	mark	10	•	_			

<u>Note</u>

For the same AVC profile two rules are created. The Administrator can configure up to 32 rules in the same AVC profile. Individual rules can be configured for action MARK or DROP in the same profile. A single rule can only be configured with a single action i.e. either MARK or DROP.

The administrator is also flexible while configuring Action as MARK to choose the Differentiated Services Code Point (DSCP) value as Custom instead of selecting "Platinum/Gold/Silver/Bronze". Once Custom is selected as DSCP value, a text filed will be visible where admin can enter a custom DSCP value in range of 0 - 63.

AVC Profile > Rul	e > 'Mark_Http_Webe	ex'
Application Group	browsing	×
Application Name	flash-video 🔽	
Action	Mark 💌	
Dscp (0 to 63)	Custom	0
		9

10. The Next step will be to apply these AVC profiles on the WLAN. Only one AVC profile can be mapped to a single WLAN. A single AVC profile can be mapped to multiple WLANs. Once an AVC profile is mapped to a WLAN and if it has a rule for MARK action, that application will get precedence as per QoS profile configured in AVC rule interacting with the QOS profile configured on the WLAN. All the AVC profiles created will be visible under AVC Profile drop-down in WLAN under QOS TAB. To see the AVC profile in the drop-down on WLAN, navigate to WLANs > WLAN ID and then click QOS tab. All the AVC profiles created are visible under the AVC Profile drop-down. The administrator can select the AVC profile on the WLAN as per network requirement.



11. For example, select the AVC profile Block_Youtube from the drop-down and click Apply.

cisco	MONITOR	₩LANs		WIRELESS	SECURITY	Sage Co MANAGEMENT	nfiguration <u>B</u> C <u>Q</u> MMANDS	ing Log HELP	eout <u>B</u> efresh EEEDBACK
WLANs		WLANs>	Edit 'POD1-	Client'			< Back	-	Apply
WLANS	Ns	General	Security	QoS P	olicy-Mapping	Advanced			100
▶ Adva	nced	Quality	r of Service (QoS ation Visibility) Silver	(best effort)				
		AVC Pr Netflow	rofile v Monitor	Block_	Youtube 💌				
		Override	e Per-User Ba	ndwidth Co	ntracts (kbps	s) 16			



If Application visibility is not enabled on the WLAN, and users selects an AVC profile and Apply is clicked, this automatically enables Application visibility. But to disable Application visibility from WLAN, AVC profile, which is mapped to WLAN, should be removed first by selecting **None** from drop-down.

12. Once AVC profiles are applied on WLAN it is also visible under **Monitor > Applications**. All the WLANs which has Application Visibility enabled will be displayed

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS HELF	EEEDBACK
Monitor Summary	WLANS	Туре	Profile Name		WLAN	SSID	Admin State	as Avc Profile
Access Points Cisco CleanAir Statistics CDP Rogues	1	WLAN	P0D1-Client		POD1-C	lient	Enabled	Block_Youtube
Clients Multicast Applications								

13. Now try to open www.youtube.com from wireless clients. Make sure that the client cannot play any videos on YouTube. Also try to open your Facebook account (in case you have one) and try to open any YouTube video from your Facebook account. You will observe YouTube videos cannot be played.

Because YouTube is blocked in the AVC profile and AVC profile is been mapped to WLAN, clients will not be able to access YouTube videos via browser or even via YouTube application or from any other website.



If your browser was already open and running Youtube.com, refresh the browser for the AVC profile to take effect.

Now change the AVC profile on the WLAN to test the MARK operation of the NBAR feature. Select AVC profile Mark_Http_Webex from the drop-down under QOS tab on the WLAN and click Apply.

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	Saye Cor MANAGEMENT	ifiguration ging COMMANDS I	Logout <u>R</u> efresh HELP <u>F</u> EEDBACK
WLANs		WLANs>	Edit 'POD1-	Client'			< Back	Apply
WLANS	Ns	General	Security	QoS	Policy-Mapping	Advanced		
▶ Adva	inced	Quality	r of Service (QoS) ation Visibility	Silver	r (best effort)	•		
		AVC Pr Netfloy	rofile v Monitor	Mark	_HTTP_Webex 🛩			

 Once the AVC profiles are applied on the WLAN, it is also visible under Monitor > Applications. All the WLANs which has Application Visibility enabled will be displayed.

uluulu cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS HE	LP EEEDBACK
Monitor Summary	WLANS	Туре	Profile Name		WEAN	5510	Admin Sta	tus Avc Profile
Access Points Cisco CleanAir Statistics CDP Rogues	1	WLAN	POD1-Client		POD1-C	lient	Enabled	Mark_Http_Webex
Clients Multicast Applications								

16. Once the AVC profile Mark_Http_Webex is applied on the WLAN, initiate or login to your individual WebEx account (if you have one) and also initiate some HTTP connections and observe the marking for these two applications under client details. Once the AVC profile is mapped to a WLAN and if it has a rule for the MARK action, that application will get precedence as per QoS profile configured in AVC rule overriding the QoS profile configured on the WLAN.

Although the WLAN in this example is mapped to the default QOS profile **SILVER**, the AVC profile has been created and mapped to this WLAN to MARK application WebEx and HTTP with a different QOS profile. Traffic for application WebEx will be marked with **PLATINUM** profile and traffic for all HTTP application will be marked with **BRONZE** profile. Rest of the applications that do not match any rules in the AVC profile; will be marked with QOS profile configured on WLAN i.e. SILVER in this example.

17. To see the markings stats for client traffic, navigate to **Monitor > Clients** and then click any individual client MAC entry listed on that page.

iliilii cisco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	ration <u>P</u> ing	Logou	t Befr
Monitor Summary	Clients Current Filter	None	[Change F	iter] [Clear Fi	her]		Entr	ies 1 - 1	l of 1
Access Points Cisco CleanAir Statistics	Client MAC Add	AP Name		WLAN	Profile	WLAN 551D	Status	Auth	Port
CDP Rogues Clients	00140196109120160	-ODI-AP		7001	Client	POD1-Client	Associated	165	

After clicking on the individual client MAC entry listed on the above page, the client details page will open which will have two tabs; one for general information and another tab with name AVC **Statistics**. Click the **AVC Statistics** tab and further click the **UPSTREAM** tab to notice the MARKING operation of the AVC profile.

AVC Statist	cs						
Aggregate Upstrea	Downstre	am					
Last 90 secs Stats					Cumulative Stats		
Application Name	Average Packet Size	Packet Count	Byte Count	Dscp In/Out	Application Name	Packet Count	Byte Coun
gtalk-chat	162	25	4063	0/0	vnc	495	473474
yahoo-messenger	734	5	3671	0/0	http	124	128090
webex-meeting	538	6	3232	0/46	webex-meeting	72	40756
http	245	12	2942	0/10 🔶	gtalk-chat	91	12696
bittorrent	68	3	204	0/10	yahoo-messenger	19	11013
			47		hitterment		613

Notice the above output and make sure the WebEx application is getting OUT DSCP value as 46 because the WebEx application is been configured with Platinum QOS profile and HTTP application is getting OUT DSCP value as 10 because the HTTP application is been configured with Bronze profile.

Configure NBAR NetFlow Monitor

A NetFlow monitor can also be configured on the WLC to collect all the stats generated on a WLC and these can be exported to the NetFlow collector. In the following example, Cisco Performance Application Manager (PAM) is shown as being used as a NetFlow collector. PAM is a licensed application running on Cisco Prime Infrastructure.

 Add NetFlow Exporter first on WLC by configuring Exporter (NetFlow collector). In this example Cisco PAM is an exporter. It collects all the NetFlow stats generated by the WLC. To add an exporter in the WLC, navigate to Wireless > NetFlow > Exporter, then click New.



2. Enter the details of PAM, Exporter IP, as an example below 10.10.105.3 and Port Number as 9991 which will collect all the NetFlow stats generated by the WLC and then click **Apply**.

 After adding Exporter details on the WLC i.e. PAM server, a monitor needs to be created which will store the NetFlow stats and export the same to the PAM server. To create a Monitor, navigate to Wireless > NetFlow > Monitor, then click New.

Note

cisco	Logout Be MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless	Monitor List page
Access Paints All APs Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration	Monitor Name Record Name Exporter Name ExporterIp Port
Advanced	
Mesh	
RF Profiles	
FlexConnect Groups FlexConnect ACLs	
▶ 802.11a/n	
▶ 802.11b/g/n	
Media Stream	
Application Visibility And Control	
Country	
Timers	
Netflow Monitor Exporter	

4. Enter any name to create the Monitor entry on WLC and click Apply.

MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Logout <u>R</u> efre
Netflow N	/onitor >	New				-	-	Apply
Monitor N	ame Net	Flow Monitor		-	-			

5. Once applied, the Monitor entry will be created which will need to be further mapped to the Exporter created in step 2.

Monitor List page					New
Monitor Name	Record Name	Exporter Name	ExporterIp	Port	
NetFlow Monitor	none	None	0.0.0.0	0	



I

Only one Monitor entry can be added in the WLC.

6. Click the Monitor entry and map it to the Exporter entry, which is Cisco PAM. The exporter name drop-down list the "Exporter" entry that is created above. Record name "ipv4_client_app_flow_record" is auto generated by WLC, which records all the NBAR statistics and exports to the Cisco PAM. Select this record entry in the record name drop-down and click Apply.



											Logout Be
MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	8		
Monitor L	.ist page					-				1	New
Monitor N	ame	Rec	ord Name		Exporter Nan	ne	Енр	orterIp	Port		
NetFlow Mo	nitor	īpv4	_client_app_fl	ow_record	Cisco PAM		10.1	0.105.3	9991		

Once the Monitor entry is created and the Exporter entry is mapped to the same, it should be mapped to the WLAN. To map the exporter entry to WLAN, click WLANs and then click the specific WLAN ID. Click the QOS tab and choose the Monitor entry created above from the NetFlow Monitor drop-down and then click Apply on the WLAN Edit page.

uluili. cisco	Sage Config MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT C	guration <u>Bing</u> Logout <u>B</u> efresh COMMANDS HELP <u>E</u> EEDBACK
WLANs	WLANs > Edit 'POD1-Client'	< Back Apply
WLANS	General Security QoS Policy-Mapping Advanced	
▶ Advanced	Quality of Service (QoS) Silver (best effort) v Application Visibility Enabled AVC Profile Block Youtube v	0
	Netflow Monitor Netflow_Monitor 💌	
	Override Per-User Bandwidth Contracts (kbps) ¹⁴ DownStream UpStream	

8. Now open a new tab on the browser and login to the Cisco Prime Infrastructure Server to add individual WLCs to PAM.

Username: XXXXXX Password: XXXXXX

Cisco Prime Infrastructure Version: 1.4 Username Password Login	
© 2013 Cisco Systems.Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems.Inc.and/or its affiliates in the U.S and certain other countries	-dhadh cisco

 Add the WLC in Cisco PAM. To add WLC into Cisco PAM, login to Cisco PAM and navigate to Operate > Device Work Center, then click Add Device in the Lifecycle Theme.

Julu Cisco Prime	-	ρ.
cisco Infrastructure		P 0 0.4
Device Work Center 🔶	📕 Discovery 🤨 Configuration Archives 🤅	🕽 Sofhated Deployment Status 🚼 Network Audit
Device Group	Device Group > ALL ALL	
Q+E+ 1		Selected 0 Total 3 🔞 🥁 🗸
ALL	/ Edit X Delete % Sync Groups & Sites ▼ 😤 Add Device 🔛 Bulk Import	Al 🔹 🖌

ſ

10. Enter the details of individual WLC i.e. WLC Management IP Address (Example WLC-POD4 = 10.10.40.2) and **Community String** as public and then click **Add**.

evice Work Center	Add Device		2
Device Group	▼ General Parameters		-
(٩	* IP Address	X.X.X.X	0
Ø• E• Ø•	▼ SNMP Parameters		
Ba All	Version	v2c *	
Convice Type	* Retries	2	
B User Defined	* Timeout	10	(secs)
	* Community		
	▼ Telnet/SSH Parameters		
	Protocol	Teinet *	
	Timeout	60	(secs)
	Username		
	Password	2	
	Confirm Password		
	Enable Password		
	Confirm Enable Password		
			-

Once the WLC is added, start some traffic from wireless clients. You can view the number of clients per WLAN and usage per client. To see the usage by clients, navigate to Home > Detail Dashboards > Application. Now filter the Application Box as All, Site as Unassigned, and Network Aware as Wireless > PODX-Client and then click Go.

1

Holife Design * Deploy * Operate * Repo	ot • Administration •	
ars the Application All 🔘 🛞 *Time Frame Past Hour 🔿 🔒 Sfle Unamigned	0 & Network Aware POD1-Client 0 Go	
p N Clients (In and Out) 🙇 👔 🐏 🛞 💷	Application Configuration 🔔 🍢 🛞	
	Application Protocol Port	Bytes/sec
		304.04
a 10.10.00	http	52.38
	skype	23.05
	unclessified	13.88
0 10 10 40	youtube	9.75
	yahoo-messenger	2.95
	dris	2.44

Note

- You can see the number of clients on WLAN "POD1-Client" which is filtered under Network Aware. Also, in same screen, you can see the applications used by both the clients.
- To see the application usage by a particular client, navigate to Home > Detail Dashboards > End User Experience > Under Filter and then select the client IP.



 To see application usage per WLAN, navigate to Home > Detail Dashboards > End User Experience > Under Filter and then select the Network Aware as WLAN i.e. POD1-Client in this example. Click GO.

cisco	Cisco Prime Infrastructure		A Home	e Design • Deploy •	Operate • Report •	Administration	Vistual Dom	un XOOT COMADIN - 1 - A
Overvie	w Incidents	Performance	Artail Dashboards	←				
Site	Device	Interface App	lication Voice	te/Video End User Exp	Carlos -			
Filters	Clent Ur	assigned	 (a) • Te 	ime Frame Past 6 Hours	Application A	0	. Network Aware POD1-Cla	nt 🔘 Ga
Top N	Applications	(b) [[[]]					CHIER	
						-		
	unclassified -							
	Mp -							
	ware metry							
	mype -							
	poster-							
-E	214-					Country & Address	T Destanting Mile T	Formalium Day
1	me live accounts					Source Address	The Description Address Tax	No data a
	and the second s							
	COLUMN THE R							
	Autor -							
	andoni azura -					-		
	ra-renerjer -					Worst N Clients by	Transaction Time	

ſ

AVC—Phase 3 in CUWN Release 8.0

In this release, a lot of enhancement has been made on the AVC feature set that includes the following:

- AAA AVC Profile override for clients.
- Application rate limiting per-user on WLAN.
- Integration of AVC profiles to the Local Policy classification per user and per device.
- AVC Directional QoS DSCP Marking for Upstream and Downstream traffic.
- Support for 1105 applications with Protocol Pack 9.0 and NBAR Engine release 3.1.

AAA AVC Profile Override for Clients

As mentioned above in releases 7.4, 7.5, and 7.6, the AVC Profile is configured on a WLAN and all clients connected to that WLAN inherit the same AVC profile. The value proposition to allow for the AAA AVC profile override is to enable different clients (logging in as different users) to obtain different AVC profiles even though they are connected to the same WLAN.

The AAA attribute for a client or user profile can be configured on AAA servers, for example, Cisco ACS or ISE. The AAA attribute is defined as a generic Cisco AV Pair and can be defined as a string and value pair in AAA. This attribute is processed during L2/L3 Authentication by the WLC and the same is overridden by what is configured on the WLAN.

Steps to Configure Application Visibility Per User Role

Complete these steps:

Step 1 Create/Configure a WLAN with L2 Security set for WPA2/802.1x authentication. Assuming that the user/administrator has already configured the AAA server for dot1x authentication, choose the AAA server from the **Authentication Servers** drop-down list and click **Apply**.

MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
WLANs >	Edit 'P	OD2-1x'						< Back	Apply
General	Secur	rity QoS	Policy-Map	ping Adv	vanced			/	
Layer	2 Laye	er 3 AAA Se	ervers	-					^
Select A	AA server	s below to overr	ide use of de	fault servers	on this WLAN				^
Radius	Servers								
Radiu	us Server O	verwrite interface	Enabled						
Authent	ication Se	rvers Accountir	ig Servers	1		EA	P Param	eters	
		✓ Enable	ed	🔪 🗹 En	abled		Enable		
Serve	er 1	IP:10.10.	105.90, Port:1	812 🗸 IP:10.	10.105.90, Port:18	13 🗸			

Click the Advanced tab and enable "AAA Override" as shown below.

MONITOR	<u>W</u> LANs	<u>C</u> ONT	ROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
WLANs >	Edit 'P	OD2-	1x'						< Back	Apply
General	Secu	rity	QoS	Policy-Map	ping Ad	vanced			/	~
Allow A	AA Overric	ie	Er	abled		DHCP				^
Covera	ge Hole De	tection	Er	abled		DHCP Server		Override	e	
Enable Timeou	Session		Sessio	n Timeout (sec	s)	DHCP Addr. /	Assignment 🔽	Require	d	

Step 2 To enable Application Visibility, click the **WLAN ID** and in the **QoS** tab, check the **Enabled** check box for **Application Visibility**. Click **Apply**.

<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTR	OLLER	WIRELESS	<u>S</u> ECURITY	M <u>a</u> nagement	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
WLANs >	Edit 'F	OD2-1	x'	/					< Back	Apply
General	Secu	rity	QoS	Policy-Map	ping Ad	vanced			/	
Quality	of Service	(QoS)	Silve	er (best effort)	~					^
Applica	tion Visibili	ty		nabled						
AVC Pr	ofile	1	none	• •						
Netflow	Monitor		none	• 🗸						

AAA Configuration for AVC Profile

I

The AAA AVC Profile is defined as a Cisco AV Pair. The string is defined as **avc-profile-name** and this has to be configured for any AVC profile existing on the WLC.

Complete these steps:

Step 1 To demonstrate the AVC profile being applied per user through AAA server, create AVC profiles by navigating to Wireless > Application Visibility And Control > AVC Profiles and click New. In this setup/example, we created a teacher-AVC and student-AVC. We will mark specific traffic (YouTube and so on) for user/role teacher and block/drop the specific application/traffic (YouTube, Facebook and so on) for user/role student. You can create your own AVC profiles according to your network requirements.



1

Step 2 Enter the AVC profile name and click Apply. Similarly, create another profile.

<u>M</u> ONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
AVC Prof	file > Nev	W]	< Back Apply	
AVC Profi	le Name	teacher-AVC							Veecac

Step 3 The AVC profile is created and you can view the above created profile, which can be clicked to create rules to take drop/mark/Rate Limit action from the GUI. A maximum of 16 AVC profiles can be created on the WLC.

ահահո									Sa <u>v</u> e	Configura	tion <u>P</u> ing	Logout Refre
	CISCO		MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
W	ireless	^	AVC Prot	file Name	e							New
• •	Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration		AVC Profil teacher-AV student-AV	e Name		3						
۲	Advanced				•							
	Mesh											
	RF Profiles											
	FlexConnect Groups FlexConnect ACLs											
Þ	802.11a/n/ac											
Þ	802.11b/g/n											
۶	Media Stream											
•	Application Visibility And Control AVC Applications AVC Profiles	~										

Step 4 After creating the AVC profiles, you can click any profile name and create rules for individual profiles. A maximum of 32 rules can be configured in each profile. Rules can be configured to take any of the 3 actions, that is, DROP, MARK, and RATE LIMIT. If no rule is configured for any application, the default action will be "Allow" with the QOS policy configured on the WLAN. To create rules for a profile, go to Wireless > Application Visibility And Control > AVC Profiles, and then click any *Profile*.

MONITOR	<u>W</u> LANs	<u>C</u> ontrol	LER W	IRELESS	<u>s</u> ecurit	ΥM	I <u>a</u> nagement	г с <u>о</u>	MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK		
AVC Prof	file > Edi	t 'teach	er-AVC'							<	Back A	dd New Rul	e
Applicatio	n Name	Appli Name	cation Gro	oup	Action	DSCP							352882
	<u>w</u> LANs <u>C</u> C	ONTROLLER	WIRELESS	SECURITY	MANAGE	MENT	COMMANDS	HELP	FEEDBACK		< Back	Apply	
Application Application Action Dscp (0 to Direction	n Name n Group Name 63)	youtube voice-and Mark Platinum(Bidirection	-video ÷ voice) ÷	1									352883

ſ



WLC is capable of classifying 1105 applications with Protocol Pack 11.0 and gives an option to take action. To take an action on any application, the administrator has to select the application group first to which that application belongs, which will filter the list of applications for that application group only. The reason for this implementation is all 1105 applications cannot be displayed in a single drop-down. The administrator is also flexible while configuring Action as MARK to choose the Differentiated Services Code Point (DCSP) value as Custom instead of selecting "Platinum/Gold/Silver/Bronze". Once Custom is selected as the DSCP value, a text field will be visible where the admin can enter the custom DSCP value in the range of 0 - 63.

Prior to Release 8.0, the DSCP Marking is only applied bi-directionally for traffic. But in Release 8.0, an extra configuration parameter of "Direction" is available where marking can be specified with respect to direction, that is, Upstream or Downstream as shown below.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELES	S SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			
AVC Pro	file > Ru	e Edit > 'teac	her-AVC'						< Back	Apply	
Applicatio Applicatio Action Dscp (0 t Direction	on Name on Group N to 63)	youtube ame voice-and Mark Platinum V Bidirecti	d-video (voice)								
		Upstream	m								52884

Step 5 Once the appropriate Marking is selected, click Apply. The action rule will be created and is displayed as captured in the below screen. You can add more rules under the same AVC profile on the same page. A maximum of 32 rules can be configured in a single AVC profile.

Another rule can be configured under the same AVC profile to MARK traffic with a different QoS profile or custom DSCP value with a specific direction.

Here, we configured Netflix and YouTube to be marked for the AVC profile "teacher-AVC" with DSCP 34 (Gold) with the direction set to Bidirectional and Upstream, respectively.

AVC Profile > Edit	'teacher-AVC'				< Back	Add New Rule	
Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps		
netflix	voice-and-video	mark	34	Bidirectional	NA		
voutube	voice-and-video	mark	34	Upstream	NA		85
							3528

I

Step 6 Similarly, the following example displays another AVC profile (student-AVC) for a different role type, which is student in our setup and is configured to drop Facebook, YouTube, and BitTorrent traffic.

Application Name	Application Group Name	Action	DSCP	
<u>youtube</u>	none	≯ drop	NA	-
<u>facebook</u>	none	drop	NA	-
<u>bittorrent</u>	none	drop	NA	-
ftp	none	drop	NA	-

Now, assume that the user/administrator has already configured the AAA server (ISE/ACS/Open Radius) Step 7 with users (teacher and student), devices (WLC), and Authorization Profiles. To configure the AAA Server to match the profile for the AVC set on the WLC, from ISE main menu bar, go to **Policy > Policy** Elements > Results > Authorization > Authorization Profiles. Here, you see the configured profiles (Student and Teacher) displayed in the example screenshot below.



Step 8

Click the authorization profile which you created for the role Teacher, and under Advanced Attributes Settings, configure AVC Profile Name by adding cisco-av-pair=avc-profile-name=The AVC profile name created on the WLC, as shown below.

cisco Identity Services Engine	Home Operations ▼	Dictionaries	ρ
🔀 Policy Sets 🔣 Profiling 👩 Posture	😡 Client Provisioning 📓 Securi	Airespace	
Dictionaries Conditions Results		Cisco	>
	Voice Domain Permission	Cisco-BBSM	>
Results	Voice Domain Permission	Cisco-VPN3000	>
م	Web Redirection (CWA, DRW, M	Microsoft	>
@• E•		Radius	>
Authentication	Auto Crost Dart		
 Authorization 			
Authorization Profiles			
Downloadable ACLs	w Advanced Attributes Cottings		
 Inline Posture Node Profiles 	 Advanced Attributes Settings 		
Profiling	Cisco:cisco-av-pair]
Posture			
Client Provisioning	Select an item	2 =	S - +

1



Advanced Attributes Settings
Cisco:cisco-av-pair 📀 = role=teacher 📀 —
Cisco:cisco-av-pair 📀 = avc-profile-name=teacher-AVC 📀 — +
▼ Attributes Details
Access Type = ACCESS_ACCEPT <u>cisco-av-pair = role=teacher</u> <u>cisco-av-pair = avc-profile-name=teacher-AVC</u>
Save Reset

If you are using the Cisco ACS, go to **Policy Elements > Authorization and Permissions > Network** Access > Authorization Profiles. Add cisco-av-pair to match the string value avc-profile-name=*The* AVC profile name created on the WLC.



Similarly, configure the Authorization profile for student as well. Once configuration is done, you can connect a wireless client to the 802.1x WLAN with teacher credentials. You will be able to access Netflix and YouTube.

When the wireless client (with role student) connects to the same 802.1x WLAN, the client cannot play any videos on YouTube. Also, if the client tries to access a Facebook page and tries to open any YouTube video from the Facebook account, the YouTube video will not be played.

Because both YouTube and Facebook are blocked in the AVC profile for Student-AVC, therefore clients with student role will not be able to access YouTube videos via a browser or even via a YouTube application or from any other website nor they can access Facebook.

On the other hand, when the client logs in with Teacher credentials, the traffic is just marked and no application is dropped.

To verify if the policy is applied, from the WLC CLI prompt, run the following command:

show client detail mac_address, then scroll down to see the applied profile.

(POD2-WLC) >show client detail 18:20:32:hd:52:h7	
Client MAC Address	18:20:32:bd:52:b7
Client Usewname	teachew1
AP MAC Addwess	3c : ce : 73 : 38 : 24 : 70
AP Name	POD2-AP3600
AP wadio slot Id	1
ni radio site internet interne	Associated
Client NGC OOB State	Access
	ACCESS
Wireless LHM IU.	L Nat Currented
	Not supported 2
	JC.CC.7J.J0.24.7I
	8288 Secs
	04 40 40 04 000
IF Haaress.	
Gateway Haaress	10.10.21.1
Netmask	255.255.255.0
Association Id.	
Authentication Algorithm	Open System
Reason Code	1
Status Code	U
Client CCX version	No CCX support
Re-Authentication Timeout	686
QoS Level	Silver
More or (g)uit	
Avg data Rate	0
Burst data Rate	Ø
Aug Real time data Rate	0
Burst Real Time data Rate	0
802.1P Priority Tag	disabled
CTS Security Group Tag.	Not Annlicable
KTS CAC Canability	No
MMM Support	Fnabled
	ON DE VI VV
Curwent Bate	m7
Surrent all stoc	6 0 0 10 0 10 0 0 10 0 0 0 0 0
Supported Nates	AO A EA A
Mability Ctata	
Mobility State	DUCAL O
Mobility move Count	
Security Policy Completea	Yes
Policy Manager State	RUN
Policy Manager Rule Created	
Hudit Section III	134314424000006752a1a3c3
ннн које јуре	teacher
LUCAL FULLCY Applied	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable

Application Rate Limiting Through AVC

In this release, we can configure only 3 applications for rate limiting which can be done from the WLC CLI through the following command:

(WLC) >config avc profile <prof-name> {add|remove} rule application <app-name> {drop|mark <dscp-value>|ratelimit <avg_rate> <burst_rate>}

Note

The minimum ratelimit value can be set from minimum 0 Kbps to maximum 2147483647 Kbps.

The configuration example below is performed on the profile "student-AVC" when using the BitTorrent application:

(WLC) >config avc profile student-AVC rule add application bittorrent ratelimit 150 500 Similarly, from the WLC GUI, the Rate Limiting can be configured by selecting the application on which the user wants to apply Rate Limit and from the **Action** drop-down list, choose **Rate-Limit**.

uluilu cisco	MONITOR WLANS CONT		<u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration HELP	n <u>P</u> ing Lo <u>F</u> EEDBACK	gout <u>R</u> efresh
802.11b/g/n Dual-Band Radios Global Configuration	AVC Application > Edit		~				< Back	Apply
Advanced	Application Name	torrent						
Mesh	Application Group Name	e-sharing						
RF Profiles	AVC Name	ne 👻						
FlexConnect Groups FlexConnect ACLs	Action	op 🗸						
OEAP ACLS								
Network Lists								
▶ 802.11a/n/ac								
▶ 802.11b/g/n								
Media Stream								
Application Visibility And Control AVC Applications AVC Profiles								0000

This brings up an option for the user to configure the average and burst rates for the desired application that the user needs to rate limit. The user can assign any value in Kbps from 0 to 2147483647. Once the Rate-Limit is set, the user can choose the "AVC Name" on which he wants to apply the Rate Limit and click **Apply**.

In this example, we are rate limiting the BitTorrent application with the average rate set to 150 Kbps and burst rate set to 500 Kbps and applying this to the AVC profile "student-AVC".

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
AVC App	lication >	Edit					1	< Back	Apply
Applicatio Applicatio	on Name on Group Nar	bittorrent ne file-sharin	g 🧹						
AVC Nam Action	ie	student-A Rate-Limit							
Rate Limi	t(avg/burst r	ate) 150	Kbps 500	Kbps	1				00074

The BitTorrent application displays **ratelimit** in the **Action** column with Rate Limit average and burst rate values.

AVC Profile > Edit 's	tudent-AVC'				< Back	Add New Rule
Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps	
voutube	voice-and-video	drop	NA	NA	NA	
facebook	browsing	drop	NA	NA	NA	
<u>ftp</u>	file-sharing	drop	NA	NA	NA	
bittorrent	file-sharing	ratelimit	NA	NA	150 / 500	

NBAR Facts (AVC Phase 3)

I

- NBAR Engine 13 and PP 11.0 can support 1105 different applications.
- Three actions DROP, MARK and RATE LIMIT is possible on any classified application.

- A maximum of 16 AVC profiles can be created on the WLC.
- Each AVC profile can be configured with a maximum of 32 rules.
- The same AVC profile can be mapped to multiple WLANs. But one WLAN can have only one AVC profile.
- Only one NetFlow exporter and monitor can be configured on the WLC.
- NBAR statistics are displayed only for the top 30 applications on the GUI. The CLI can be used to see all applications.
- NBAR is supported on WLANs configured for central switching only.
- If the AVC profile mapped to the WLAN has a rule for MARK action, that application will get precedence as per QOS profile configured in the AVC rule overriding the QOS profile configured on the WLAN.
- Directional Marking can only be applied either Bidirectional, Upstream or Downstream on a particular application.
- Currently, Rate Limit can only be applied to three applications.
- Any application that is not supported/recognized by the NBAR engine on the WLC is captured under bucket of UNCLASSFIED traffic.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is supported in 8.0 release.
- The AVC profile can be configured per WLAN and applied per user basis.
- NBAR is not supported in vWLC and SRE WLC.

AVC Profiles Attached to Local Policies

In Release 8.0, an AVC profile can be mapped to a local policy for a client with a particular device type. Ensure that each local policy can be configured with a different AVC/mDNS profile name based on the AAA override to restrict the policy from being able to use the services not allowed by the profile on the same WLAN.

Introduction to Profiling and Policy Engine on the WLC

Cisco currently offers a rich set of features which provide device identification, onboarding, 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 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, the user will be configuring and implementing Profiling and Policy on a Cisco WLC running AireOS 8.0 code.

I

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. The policy attributes which are of interest are:

a. Role—Role defines the user type or the user group the user belongs to.

For example: Student or Employee

b. Device—Device defines the type of device.

For example: Windows machine, Smart phone, Apple device such as iPad, iPhone and so on.

- **c.** Time of day—Allows configuration to be defined at what time of the day end-points are allowed on the network.
- d. EAP Type—Checks what EAP method the client is getting connected to.

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 (added in 8.0 release)
- mDNS profile (added in 8.0 release)

The user can configure these policies and enforce end-points with specified policies. The wireless clients will be profiled based on the 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

Complete these steps:

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 the Advanced tab. Disable Allow AAA Override if it is enabled. In the DHCP area, check the Required check box for DHCP Addr. Assignment.

neral Security	QoS Policy-Mapping	Advanced			
Allow AAA Override			DHCP		
Coverage Hole Detection	S Enabled		DHCP Server	Override	
Enable Session Timeout	Session Timeout (secs)		DHCP V6 Server	Override	
Aironet IE Diagnostic Channel	Enabled Enabled		DHCP Addr. Assignment	🗹 Required ←	
Override Interface ACL	IPv4 None :	IPv6 None :	OEAP		
Layer2 Acl	None :		Split Tunnel	Enabled	
P2P Blocking Action	Disabled :				
Citerat Evolution 3	60		Management Frame Prote	ction (MFP)	

1

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**.

General	Security	QoS	Policy-Mapping	Advanced				
Mgmt Via Wireless Enabled					Passive Client	0		
Off Channel	Scanning Defe	r			Voice			
Scan Defe	er Priority	0 1	234567		Media Session Snooping		Enabled	
		00			Re-anchor Roamed Voice Clients		Enabled	
Scan Defe	er Time(msecs)	100			KTS based CAC Policy		Enabled	
lexConnect	t	1.0			Radius Client Profiling			
FlexConne	ect Local		and a second		DHCP Profiling	0		
Switching	2	0 6	napled		HTTP Profiling			
FlexConne	ect Local Auth 12	. E	nabled		Local Client Profiling			
Learn Clie	ent IP Address 5	✓ E	nabled		DHCP Profiling	☑		
Vian based Central Enabled			HTTP Profiling	Ø				
			PMIP					
Central D	HCP Processing	OE	nabled		PMIP Mobility Type			
Override	DNS	E	nabled		PMIP NAL Type	(F	fexadecimal :	
NAT-PAT		DE	nabled			-		

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.

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	General
 AAA General RADIUS Authentication Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password 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	s <u>C</u> ONTROLLEF	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	Heļp	FEEDBACK	
Policy > I	New								< Back Apply
Policy Nar	me	eacher-LP							

Once policy name is configured, you can create policies to match a Role, EAP Type, and Device Type. 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.



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.

Policy Name	teacher-LP	
Policy Id	7	
Match Criteria		
Match Role String	teacher	
Match EAP Type	none ‡	
Device List		
Device Type	Android	
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	teacher-AVC 🗘 🚽	
mDNS Profile	none 🛟	
Active Hours		
Day	Mon ‡	-
Start Time	Hours Mins	
End Time	Hours Mins	
	Add	

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

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

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 (Apple-iPad) on which you want to enforce the policy and then click **Add**.

To apply the appropriate action, choose from the parameters under the **Action** area to enforce the Policy. Select the AVC profile (student-AVC) that should be defined in the last section.

<u>Note</u>

Policy > Edit	
Policy Name	student-LP
Policy Id	6
Match Criteria	
Match Role String	student
Match EAP Type	none 🛟
Device List	
Device Type	Android
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

I

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.

ululu cisco	MON	TOR	<u>w</u> lans	CONTROLLE	r W <u>i</u> reless	SECURITY	MANAGEMENT	C <u>o</u> mmands	Sa <u>v</u> e C HE <u>L</u> P	onfiguration FEEDBACK	Ping Logout	<u>R</u> efrest
Security	Acc	ess Co	ontrol Li	sts > Edit						< Back	Add New R	ule
AAA General PADIUS	Gen	eral										
Authentication	Acces	s List Na	ime	deny-all								
Fallback DNS Downloaded AVP TACACS+	Deny	Counter	Source IP/M	0 ce l ask l	Destination	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
TACACS+ LDAP Local Net Users MAC Filtering Disabled Cliente	1	Deny	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.

ludu					Sa <u>v</u> e	Configuration	Ping	Logout Refresh
CISCO	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS	HELP	FEEDBACK		
Security	Policy > Edit							< Back
AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP	Policy Name Policy Id Match Criteria	block-all 4 3						
TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Match Role String Match EAP Type Device List	none						
Password Policies Local EAP Advanced EAP Delicies Octoor	Device Type Action	Android	×	Add				
Priority Order Certificate	IPv4 ACL	deny-all 🔻						
 Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Layer2 ACLs 	Qos Policy Session Timeout (seconds) Sleeping Client Timeout (m	1800 720						
Wireless Protection Policies	Flexconnect ACL AVC Profile	none V						
F Web Auth TrustSec SXP	mDNS Profile	none						

Mapping Policy on WLAN

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 mapped to the WLAN and can be seen under Policy Name.

Seneral Security	QoS Policy-Mapping Advanced	
Priority Index (1-16)		
Local Policy	teacher-LP ‡	
	Add	

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

	TOR <u>w</u> lans <u>c</u> ontroller w <u>i</u> f	Sa <u>v</u> e Conf RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT	figuration <u>P</u> ing Logout <u>R</u> efresh C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'pod3-dot1	x,	< Back Apply
WLANs	General Security Q	oS Policy-Mapping Advanced	
Advanced	Priority Index (1-16) Local Policy	teacher-LP ▼ Add	
	Priority Index	Local Policy Name	
	1	teacher-LP	
	2	student-LP	
	3	block-all	

Step 3 In the Advanced tab, disable Allow AAA Override if it is enabled.

Γ

Allow AAA Override Enabled DHCP Coverage Hole Detection Ø Enabled DHCP Server Override Enable Session Timeout Ø Ession Timeout (secs) DHCP V6 Server Override Alronet IE Ø Enabled DHCP Addr. Assignment Required Diagnostic Channel Enabled DHCP Addr. Assignment Required Override Interface ACL IPv6 None 1 OEAP	
Coverage Hole Detection Ø Enabled DHCP Server Override Enable Session Timeout Session Ti	
Enable Session Timeout (secs) DHCP V6 Server Override Alronet IE Genabled Diagnostic Channel Enabled Override Interface ACL IPv4 None : IPv6 None : OPAP	
Aironet IE Image: Channel Image: Channel DHCP Addr. Assignment Required Override Interface ACL IPv4 (None : IPv6 (None :) OEAP OEAP	
Diagnostic Channel Enabled DHCP Addr. Assignment Required Override Interface ACL IPv4 None : IPv6 None : OEAP	
Override Interface ACL IPv4 None : IPv6 None : OEAP	
Layer2 Acl None : Split Tunnel Enabled	
P2P Blocking Action Disabled :	
Client Exclusion 2 Genabled 60 Management Frame Protection (MFP)	
Timeout Value (secs)	

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 and Cisco ACS.

ISE:

Results		▼ Lommon lasks
	Q	DACL Name
↓ E •	÷∰.≁	VLAN
Authorization Authorization Profiles Downloadable ACLs Downloadable ACLs Profiling Profiling Client Provisioning Security Group Access		Voice Domain Permission Web Redirection (CWA, DRW, MDM, NSP, CPP) Auto Smart Port Filter-ID
		Advanced Attributes Settings Cisco:cisco-av-pair Cisco:cisco-av-
		Attributes Details Access Type = ACCESS_ACCEPT cisco-av-pair = role=teacher

1

1

ACS:

cisco Cisco Secure	ACS			admin	wnbuacs5
A My Workspace Age Network Resources	Policy Elements > Authorization and	Permissions > Network Access >	Authorization Profile > Edit: "Al"		
Bollow Elements	General Common Tasks Common Tasks Attributes	RADIUS Attributes			
 Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access Authorization Profiles 		lype	Value		
 Device Administration 	Manually Entered				
Shell Profiles	Attribute	Туре	Value		
Command Sets Named Permission Objects Downloadable ACLs 	cisco-av-pair cisco-av-pair	String String	avc-profile-name=teacher-AVC role=teacher		
Access Policies			-		
Monitoring and Reports					
System Administration					

Once the client associates to SSID with teacher credentials through Apple iPad, it should be able to access Internet and different applications per its AVC profile configuration. If the user tries to connect from any device other than Apple iPad, then it will not be able to access the Internet.

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

Clients > Detail	
Max Number of Records	10 ‡
General AVC Statist	ics
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 🔶

To verify if the policy is applied from WLC CLI prompt, run the following command:

Γ

show client detail mac_address and then scroll down to the end to see the applied profile.

AAA Role T	⁻ ype	teacher	
Local Poli	cy Applied	teacher-LP 🛶 🛶 🛶	
IPv4 ACL N	lame	none	
FlexConnec	ct ACL Applied Status	Unavailable	
IPv4 ACL A	Applied Status	Unavailable	
IPv6 ACL N	lame	none	
IPv6 ACL A	Applied Status	Unavailable	
Layer2 ACL	Name	none	
Layer2 ACL	Applied Status	Unavailable	
Client Typ	e	SimpleIP	
mDNS Statu	IS	Enabled	
mDNS Profi	le Name	default-mdns-profile	
No. of mDN	IS Services Advertised	0	
Policy Typ	e	WPA2	
Authentica	tion Key Management	802.1x	
Encryption	Cipher	CCMP (AES)	
Protected	Management Frame	No	
Management	: Frame Protection	No	
EAP Type		PEAP	0
Interface.		management	5
		- ·	ŝ

To verify if the AVC policy is applied from the WLC:

AVC Profile Name: teacher-AVC

Try to connect SSID with student credentials, you should see another policy applied (student-AVC) and if the client device is not an Apple-iPad, the user will not be able to access the network.

Native Profiling Limitations

- Wired clients behind the WGB will not be profiled and policy action will not be done.
- Only 16 policies per WLAN can be configured, and globally 64 policies will be allowed.
- Policy action will be done after L2 authentication is complete or after L3 authentication or when the 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 because 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 the security type.

VOD Reference

ſ

Cisco AVC - Per User Application Control: http://www.youtube.com/watch?v=ESg53o3ufDQ&feature=youtu.be

Web Links and Terminology

Cisco WLAN Controller Information: http://www.cisco.com/en/US/products/hw/wireless/products.html http://www.cisco.com/cisco/web/support/index.html Cisco Prime Management Software Information: http://www.cisco.com/en/US/products/ps11686/index.html Cisco MSE Information: http://www.cisco.com/en/US/products/ps9742/index.html Cisco LAP Documentation: http://www.cisco.com/en/US/products/ps10981/index.html

