Application Visibility and Control Feature Deployment Guide rel 7.4-8.8

Last Updated: July, 2018

Application Visibility and Control Release Update

Note, to get information and configuration on the specific AVC feature please refer to the specific update Phase.

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

Phase 4-**AVC** 8.2	■ Protocol Pack 14.0 ■ NBAR Engine 23 ■ Support for 1273 Applications ■ Support for 3rd party Netflow Collector ■ Support for two Flow Collectors ■ Support for 17 Data Flow Records in Flow Collector
Phase 5-**AVC** 8.3	■ Protocol Pack 19.1 ■ NBAR Engine version 23 ■ Support for 1317 Applications
Phase 6 - AVC 8.8	■ Protocol Pack 37 ■ NBAR Engine Version 31 ■ Support for 1408 applications ■ Enhancement to Default DSCP values. ■ Support Wi-Fi calling **Flex Connect AVC Wave-2 APs** ■ Protocol Pack 37 ■ NBAR2 Engine 31 ■ Support for 1408 applications ■ Enhancement to Default DSCP values ■ Support for Wi-Fi calling

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 series 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

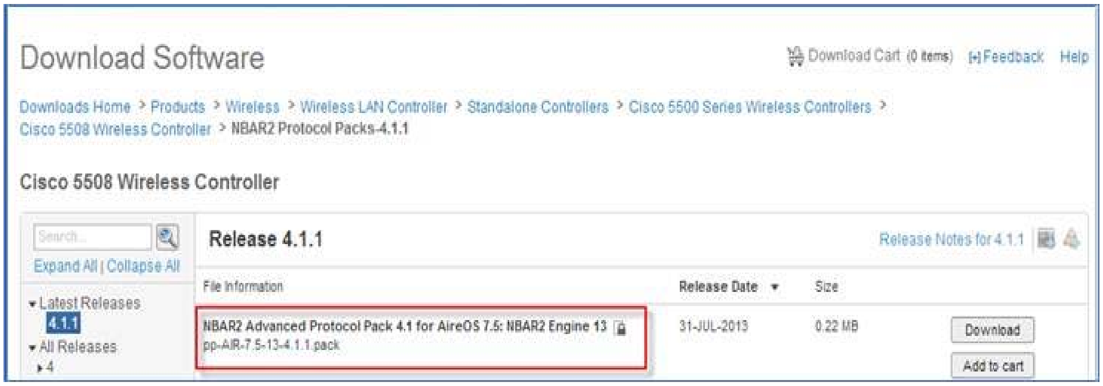
In phase two of the AVC support for Protocol Packs has been added. Protocol packs are software packages that allow update of signature support without replacing the image on the Controller. You have an option to load protocol packs dynamically when new protocol support is being added. There are two kinds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

Note: 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 https://software.cisco.com/download/home/282600534/type/284509011/release/24.0.0



Download Software

Downloads Home > Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless Controllers > Cisco 5508 Wireless Controller > NBAR2 Protocol Packs-4.1.1

Cisco 5508 Wireless Controller

Release 4.1.1

File Information	Release Date	Size
NBAR2 Advanced Protocol Pack 4.1 for AireOS 7.5: NBAR2 Engine 13 pp-AIR-7.5-13-4.1.1.pack	31-JUL-2013	0.22 MB

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.

Note: For AVC Phase -6 release 8.8 The latest NBAR2 and Protocol Packs are supported on the 3504, 5520 and 8540 series controllers. The PP in rel 8.8 only supports Wave-2 COS based APs.NBAR/AVC Facts

- NBAR/AVC phase 2 on WLC can classify and take action on 1317(rel8.3) 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

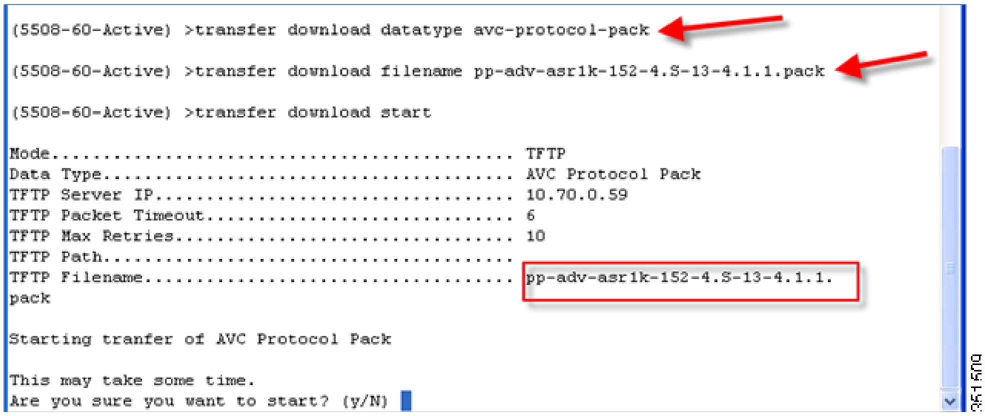
In the case of Anchor and Foreign controller's configuration, the AVC has to be configured where the application control essentially is required. In most cases in Anchor/Foreign setups the AVC should be enabled on the Anchor controller. AVC profile enforcement will happen on the WLAN on the Anchor controller. 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:

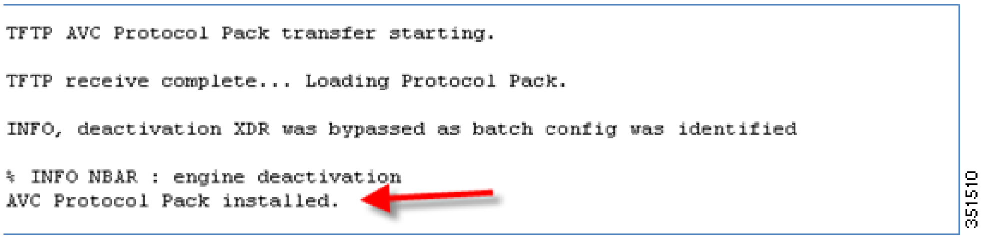
```
(Cisco Controller) >transfer download datatype avc-protocol-pack

(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 Username...................... cisco

FTP Password...................... *********

Starting transfer of AVC Protocol Pack

This may take some time.

Are you sure you want to start? (y/N)
```

Y



```
(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

Mode........................................... TFTP
Data Type...................................... AVC Protocol Pack
TFTP Server IP................................. 10.70.0.59
TFTP Packet Timeout............................ 6
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.
```

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

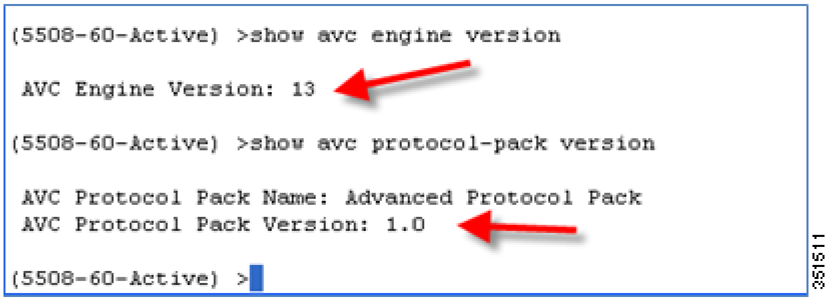
AVC Protocol Pack Version: 1.0

Use the show command to view the current Nbar2 Engine Version

(Cisco Controller) >show avc engine version

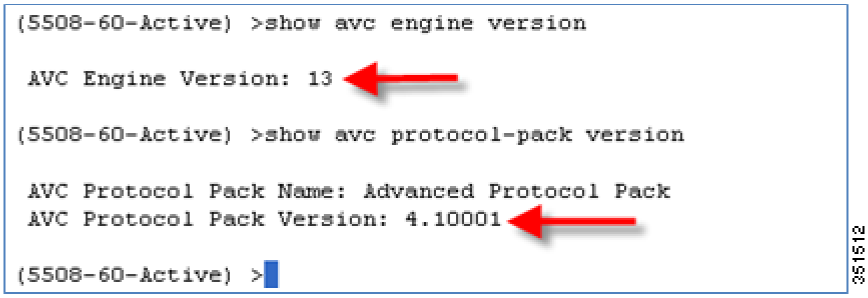
AVC Engine Version: 13

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



```
(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: 1.0

(5508-60-Active) >
```

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

(5508-60-Active) >
```

Debug Commands

(Cisco Controller) >debug avc events enable

(Cisco Controller) >debug avc error enable

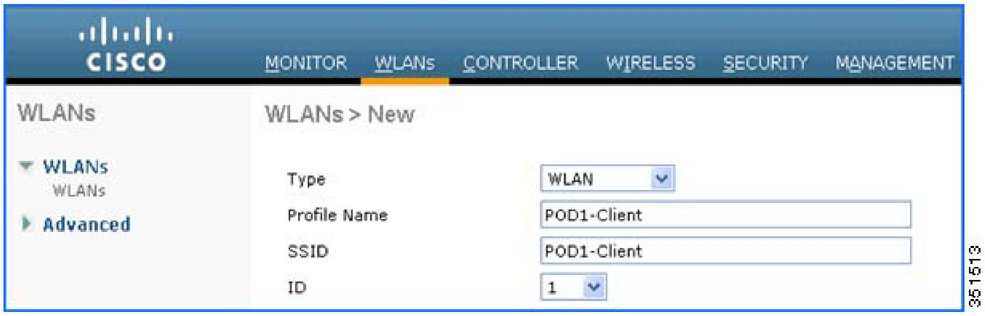
Configure Application Visibility

Complete these steps:

1. Open a web browser on the Wired Laptop. Enter your WLC IP Address.

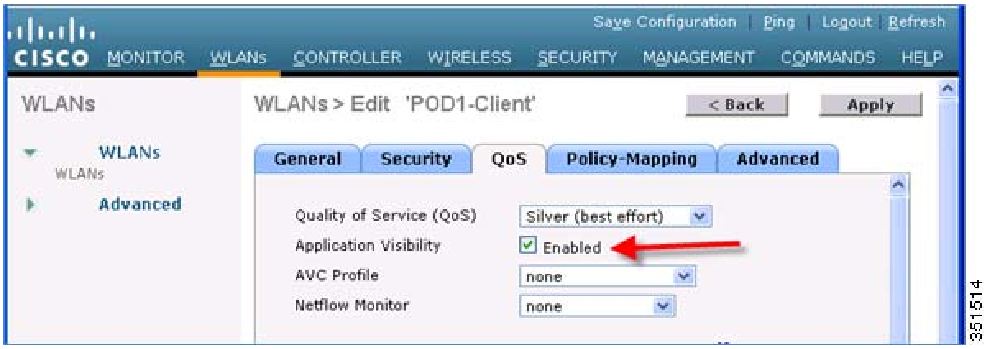
2. Create an OPEN WLAN with naming convention as for example: “POD1-Client” and enable Application Visibility on that WLAN under QOS TAB. Map this WLAN to management interface.

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



WLANs > New

Type: WLAN
Profile Name: POD1-Client
SSID: POD1-Client
ID: 1



WLANs > Edit 'POD1-Client'

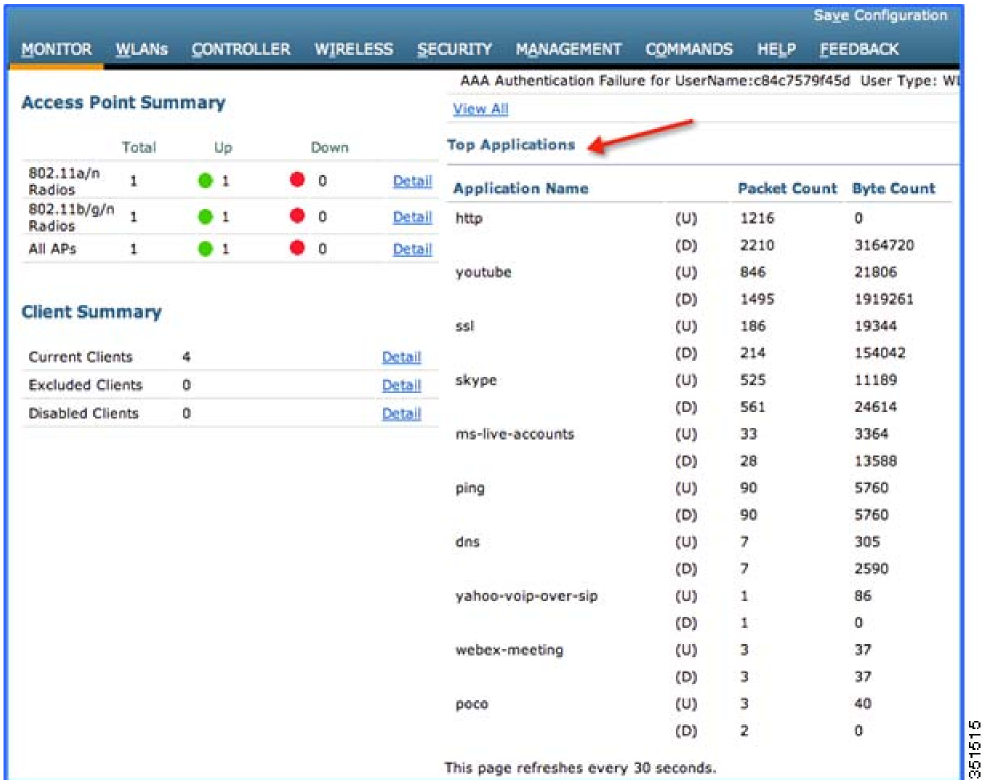
Quality of Service (QoS): Silver (best effort)
Application Visibility: ☑ Enabled
AVC Profile: none
Netflow Monitor: none

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.



AAA Authentication Failure for UserName:c84c7579f45d User Type: WL

View All

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	● 1	● 0	Detail
802.11b/g/n Radios	1	● 1	● 0	Detail
All APs	1	● 1	● 0	Detail

Client Summary

Current Clients	4	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

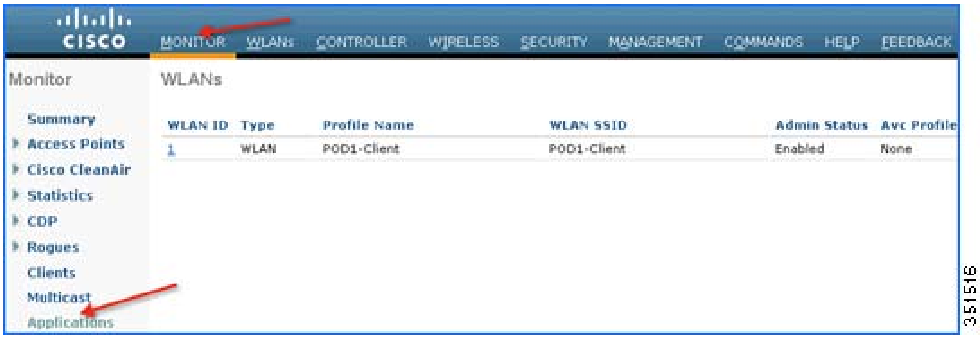
Top Applications

Application Name		Packet Count	Byte Count
http	(U)	1216	0
	(D)	2210	3164720
youtube	(U)	846	21806
	(D)	1495	1919261
ssl	(U)	186	19344
	(D)	214	154042
skype	(U)	525	11189
	(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 page refreshes every 30 seconds.

Note: 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.

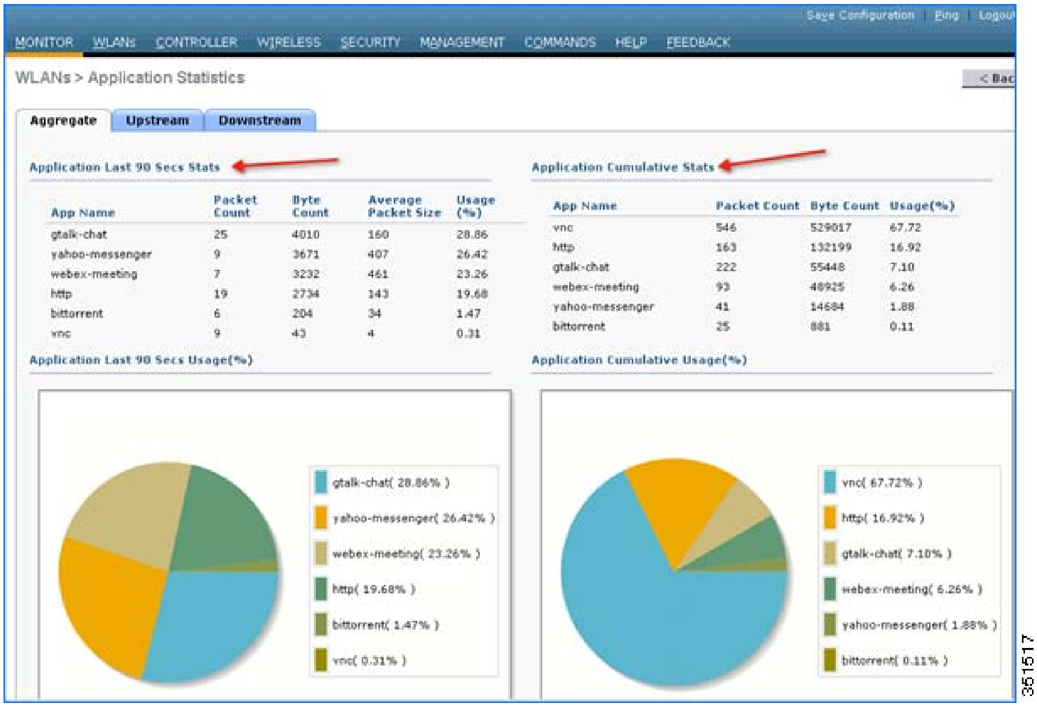
5. To have more granular visibility per WLAN, navigate to **Monitor > Applications**. This page will list all the WLANs on which AVC visibility is enabled.



WLANs

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Avc Profile
1	WLAN	POD1-Client	POD1-Client	Enabled	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.



WLANs > Application Statistics

Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage (%)
gtalk-chat	25	4010	160	28.86
yahoo-messenger	9	3671	407	26.42
webex-meeting	7	3232	461	23.26
http	19	2734	143	19.68
bittorrent	6	204	34	1.47
vnc	9	43	4	0.31

Application Cumulative Stats

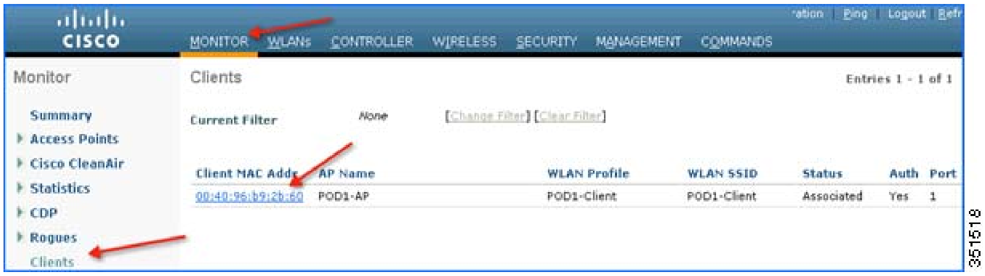
App Name	Packet Count	Byte Count	Usage(%)
vnc	546	529017	67.72
http	163	132199	16.92
gtalk-chat	222	55448	7.10
webex-meeting	93	48925	6.26
yahoo-messenger	41	14684	1.88
bittorrent	25	881	0.11

Application Last 90 Secs Usage(%)

Application Cumulative Usage(%)

Note: 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.



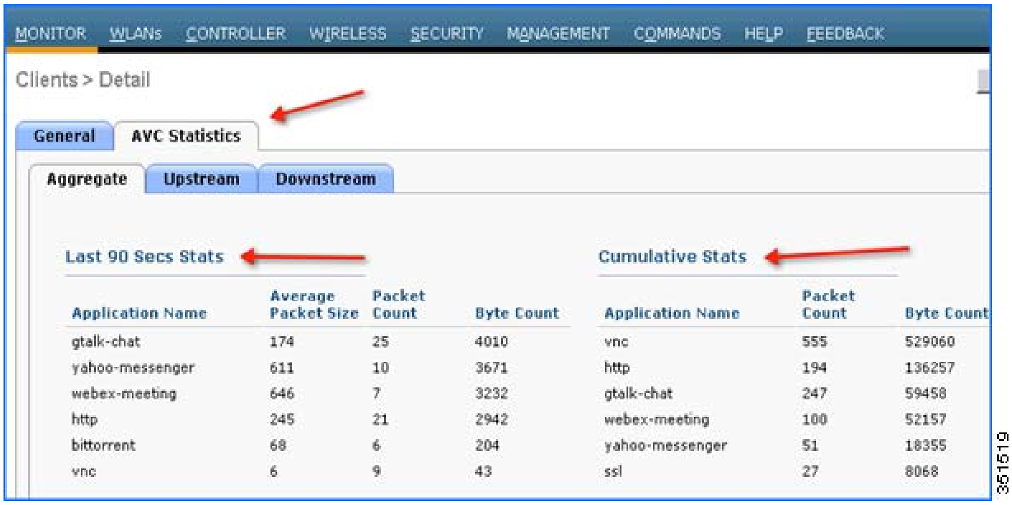
Clients

Entries 1 - 1 of 1

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Status	Auth	Port
00:40:96:b9:2b:60	POD1-AP	POD1-Client	POD1-Client	Associated	Yes	1

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.



Clients > Detail

Last 90 Secs Stats

Application Name	Average Packet Size	Packet Count	Byte Count
gtalk-chat	174	25	4010
yahoo-messenger	611	10	3671
webex-meeting	646	7	3232
http	245	21	2942
bittorrent	68	6	204
vnc	6	9	43

Cumulative Stats

Application Name	Packet Count	Byte Count
vnc	555	529060
http	194	136257
gtalk-chat	247	59458
webex-meeting	100	52157
yahoo-messenger	51	18355
ssl	27	8068

Note: 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

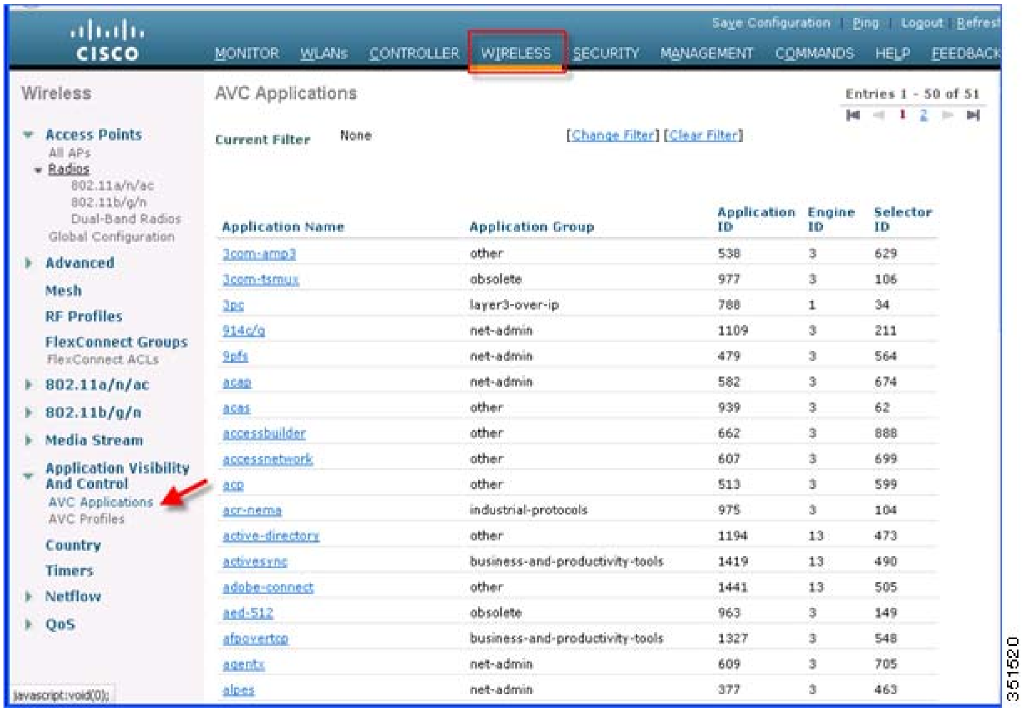
Complete these steps:

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)

2. 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.



AVC Applications

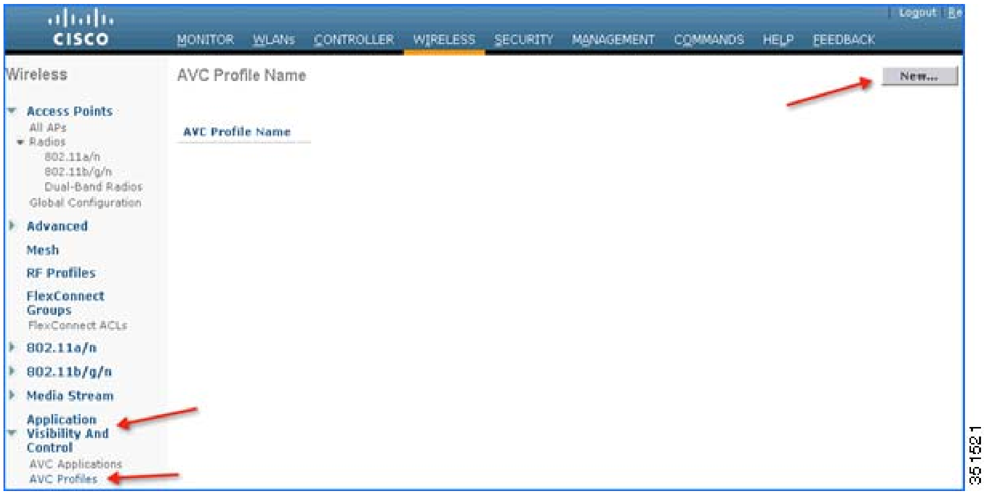
Entries 1 - 50 of 51

Current Filter None [Change Filter] [Clear Filter]

Application Name	Application Group	Application ID	Engine ID	Selector ID
3com-amp3	other	538	3	629
3com-tsmux	obsolete	977	3	106
3pc	layer3-over-ip	788	1	34
914c/g	net-admin	1109	3	211
9pfs	net-admin	479	3	564
acap	net-admin	582	3	674
acas	other	939	3	62
accessbuilder	other	662	3	888
accessnetwork	other	607	3	699
acp	other	513	3	599
acr-nema	industrial-protocols	975	3	104
active-directory	other	1194	13	473
activesync	business-and-productivity-tools	1419	13	490
adobe-connect	other	1441	13	505
aed-512	obsolete	963	3	149
afpovertcp	business-and-productivity-tools	1327	3	548
agentx	net-admin	609	3	705
alpes	net-admin	377	3	463

Note: 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.

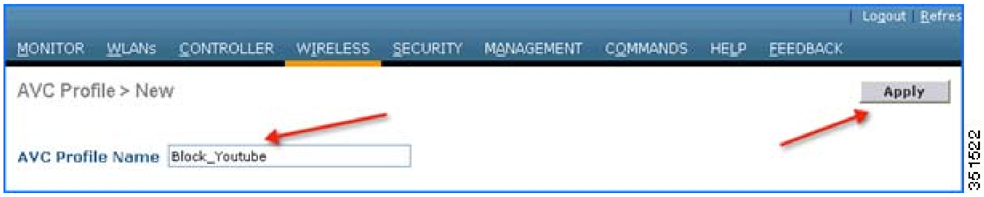
3. To configure any action (drop/mark), the AVC profile should be created first. To configure the AVC profile, navigate to **Wireless > Application Visibility And Control > AVC Profiles** and then click **New** to create the AVC profile.



AVC Profile Name

AVC Profile Name

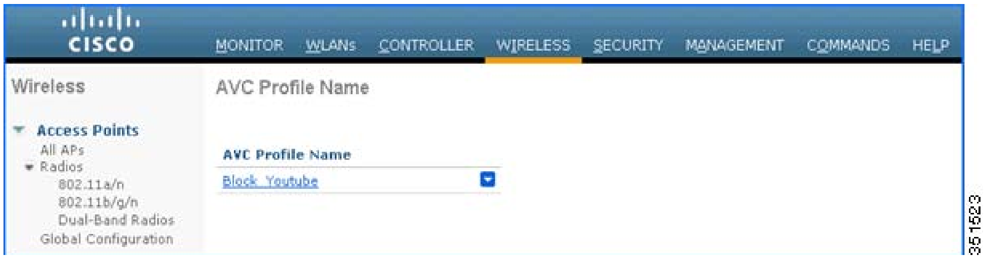
4. Enter AVC profile name and click **Apply**.



AVC Profile > New

AVC Profile Name Block_Youtube

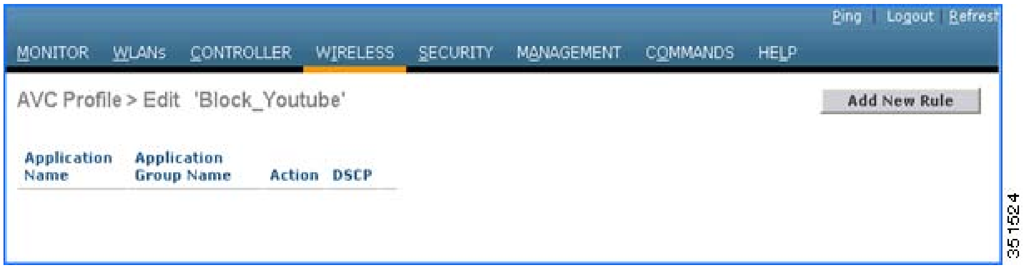
5. After Apply is clicked, the AVC profile will be created and you can see the above-created profile, which can be clicked further to create rules to take drop/mark action. Maximum of 16 AVC profiles can be created on a WLC.



AVC Profile Name

AVC Profile Name
Block_Youtube

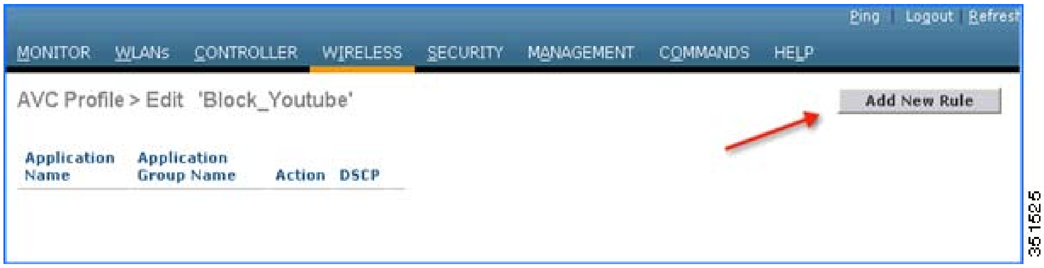
6. After creating the AVC profiles, you can click on any profile name and create rules for individual profiles. Maximum of 32 rules can be configured in each profile. Rules can be configured to take any of the two actions i.e. DROP or MARK. If no rule is configured for any application the default action 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.



AVC Profile > Edit 'Block_Youtube'

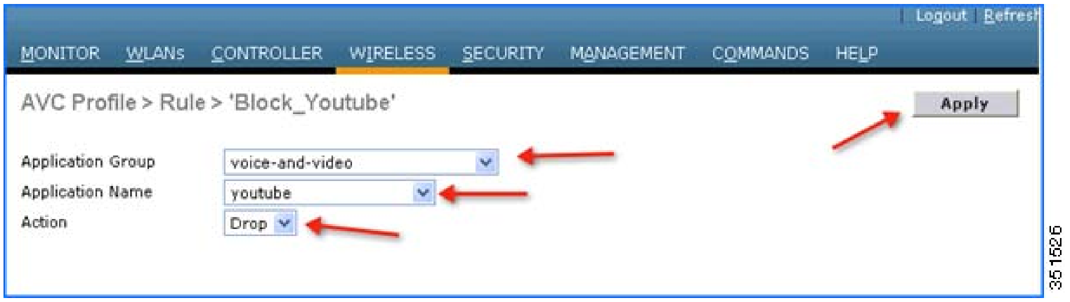
Application Name	Application Group Name	Action	DSCP

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.**



AVC Profile > Edit 'Block_Youtube'

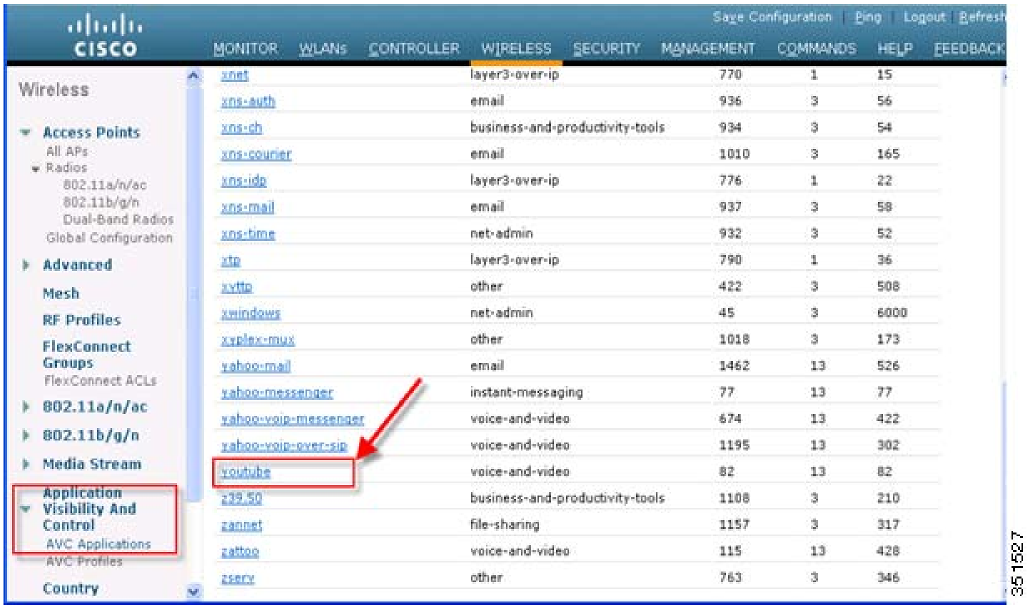
Application Name	Application Group Name	Action	DSCP


Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Apply
351526

AVC Profile > Rule > 'Block_Youtube'

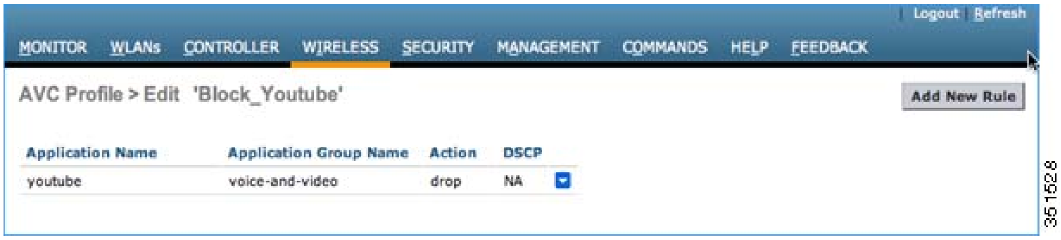
Application Group	voice-and-video
Application Name	youtube
Action	Drop

Note: 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.



xnet	layer3-over-ip	770	1	15
xns-auth	email	936	3	56
xns-ch	business-and-productivity-tools	934	3	54
xns-courier	email	1010	3	165
xns-idp	layer3-over-ip	776	1	22
xns-mail	email	937	3	58
xns-time	net-admin	932	3	52
xtp	layer3-over-ip	790	1	36
xyttp	other	422	3	508
xwindows	net-admin	45	3	6000
xyplex-mux	other	1018	3	173
yahoo-mail	email	1462	13	526
yahoo-messenger	instant-messaging	77	13	77
yahoo-voip-messenger	voice-and-video	674	13	422
yahoo-voip-over-sip	voice-and-video	1195	13	302
youtube	voice-and-video	82	13	82
z39.50	business-and-productivity-tools	1108	3	210
zannet	file-sharing	1157	3	317
zattoo	voice-and-video	115	13	428
zserv	other	763	3	346

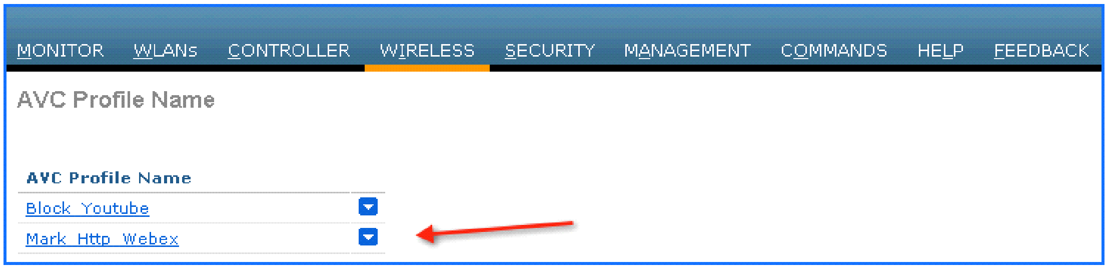
8. After Apply is clicked, the action rule will be created and displayed as captured in the below screen. You can add more rules under the AVC profile on the same page. Maximum of 32 rules can be configured in a single AVC profile.


Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Add New Rule
351528

AVC Profile > Edit 'Block_Youtube'

Application Name	Application Group Name	Action	DSCP
youtube	voice-and-video	drop	NA

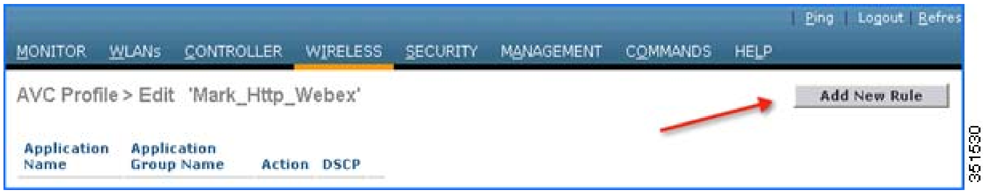
9. Another rule can be configured under the same AVC profile to MARK traffic with a different QOS profile or custom DSCP value. In this example, another AVC profile was created following step 3, 4 and 5 with the name “Mark_Http_Webex”. In this example this AVC profile is used to create a rule to mark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



AVC Profile Name

AVC Profile Name
Block_Youtube
Mark_Http_Webex

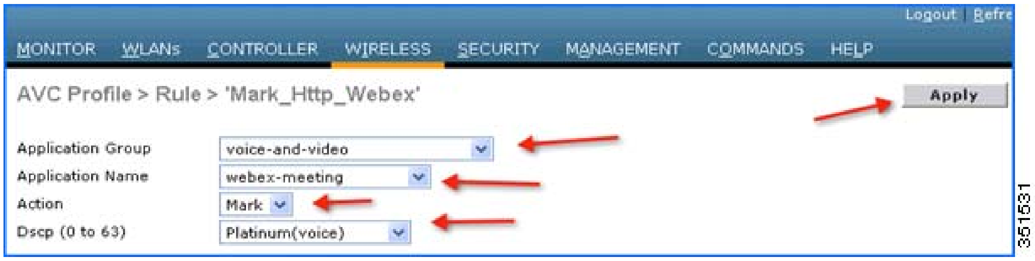
As discussed in previous steps 6, 7 and 8, click the AVC profile name to create rules for the profile. Click **Add New Rule.**



AVC Profile > Edit 'Mark_Http_Webex'

Application Name	Application Group Name	Action	DSCP

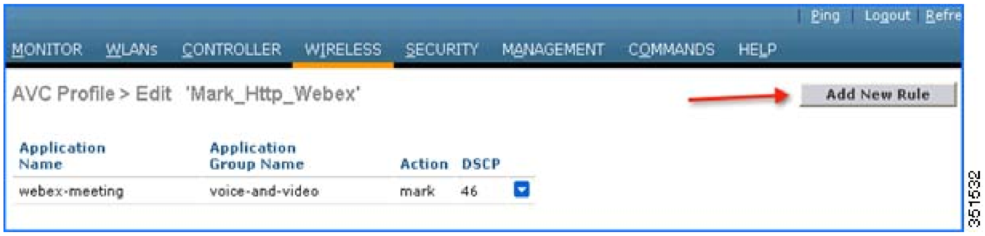
Select Application group from the first drop-down and Application name as **Webex** from second drop-down. Then, configure Action as **MARK** and select QOS profile as **Platinum** and the click **Apply**.



AVC Profile > Rule > 'Mark_Http_Webex'

Application Group voice-and-video
Application Name webex-meeting
Action Mark
Dscp (0 to 63) Platinum(voice)

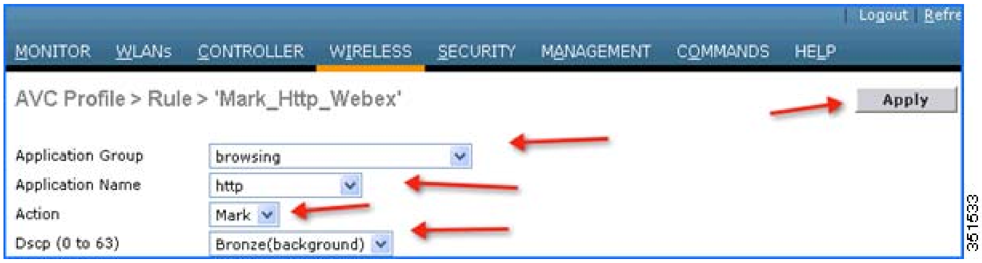
After **Apply** is clicked, the action rule will be created and displayed as captured in below screen. Click **Add New Rule** on same page to create another rule to MARK another application “Http”.



AVC Profile > Edit 'Mark_Http_Webex'

Application Name	Application Group Name	Action	DSCP
webex-meeting	voice-and-video	mark	46

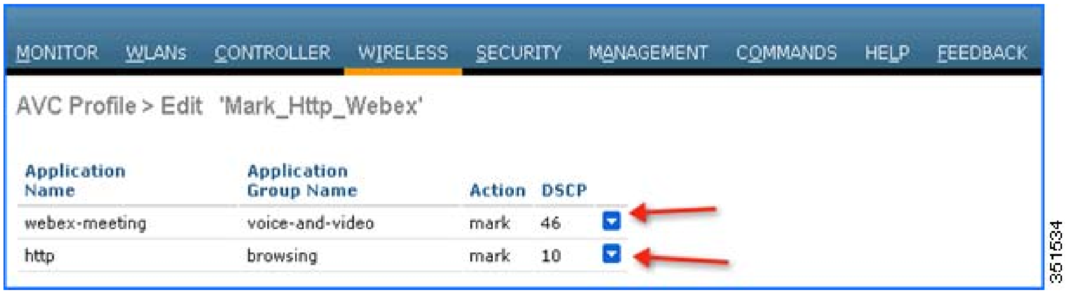
Create another rule in the same profile by just clicking **Add New Rule** on the same page. Select Application group from the first drop-down and Application name as **http** from second drop-down. Then, configure Action as **Mark** with QOS profile as Bronze. Then click **Apply**.



AVC Profile > Rule > 'Mark_Http_Webex'

Application Group	browsing
Application Name	http
Action	Mark
Dscp (0 to 63)	Bronze(background)

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

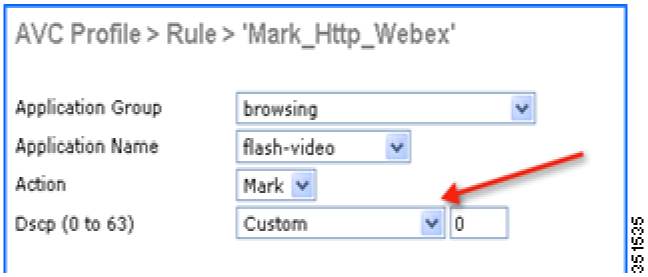


AVC Profile > Edit 'Mark_Http_Webex'

Application Name	Application Group Name	Action	DSCP
webex-meeting	voice-and-video	mark	46
http	browsing	mark	10

Note: 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.

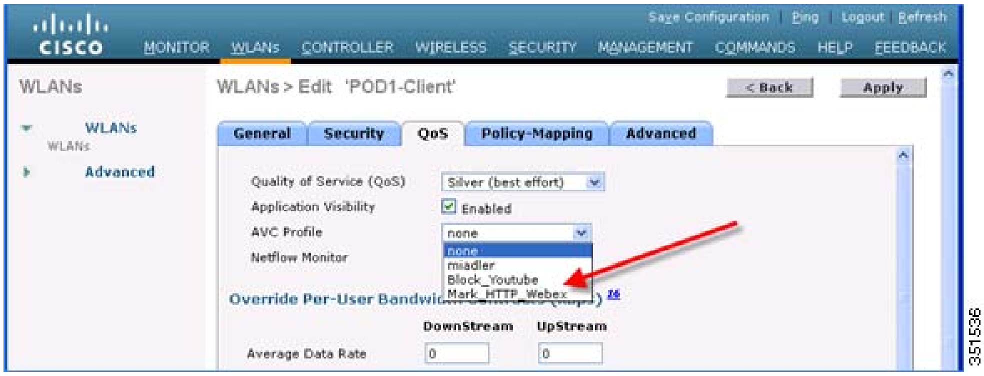
The administrator is also flexible while configuring Action as MARK to choose the Differentiated Services Code Point (DSCP) value as Custom instead of selecting “Platinum/Gold/Silver/Bronze”. Once Custom is selected as DSCP value, a text filed will be visible where admin can enter a custom DSCP value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



AVC Profile > Rule > 'Mark_Http_Webex'

Application Group	browsing
Application Name	flash-video
Action	Mark
Dscp (0 to 63)	Custom 0

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.


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
none
miadler
Block_Youtube
Mark_HTTP_Webex
Override Per-User Bandwidth Contracts (kbps)
DownStream UpStream
351536

WLANs > Edit 'POD1-Client'

Quality of Service (QoS): Silver (best effort)

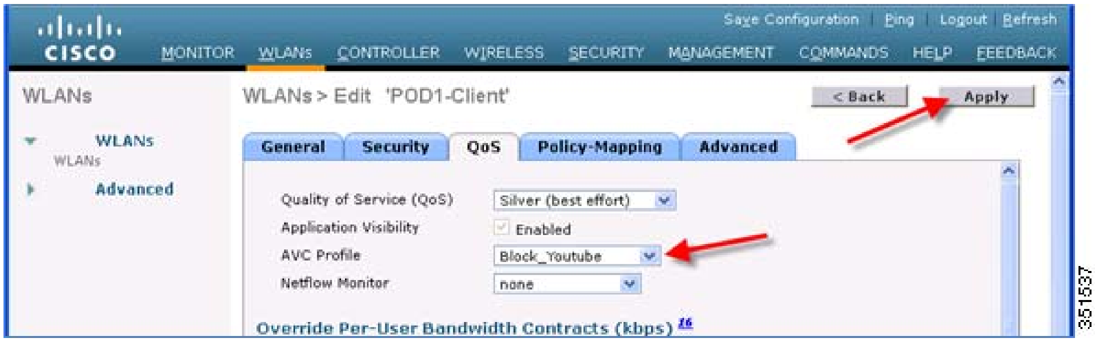
Application Visibility: ☑ Enabled

AVC Profile: none

Netflow Monitor

Average Data Rate: 0 0

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


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Override Per-User Bandwidth Contracts (kbps)
351537

WLANs > Edit 'POD1-Client'

Quality of Service (QoS): Silver (best effort)

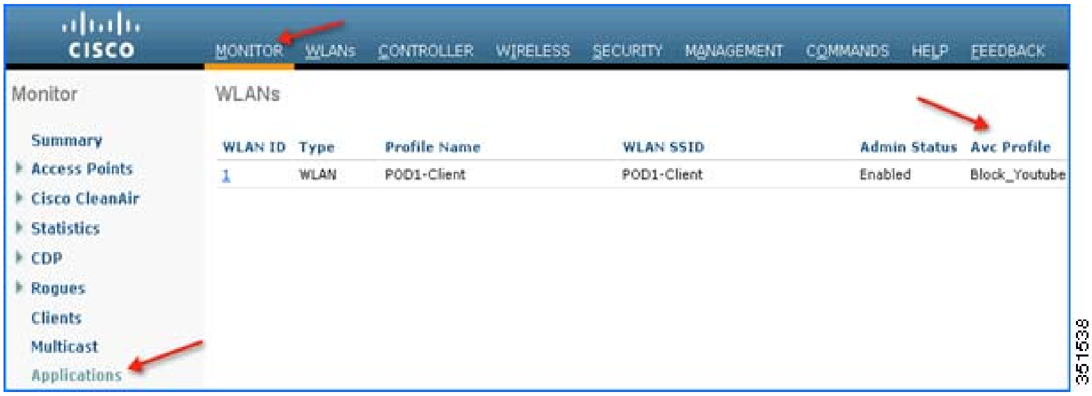
Application Visibility: ☑ Enabled

AVC Profile: Block_Youtube

Netflow Monitor: none

Note: 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



WLANs

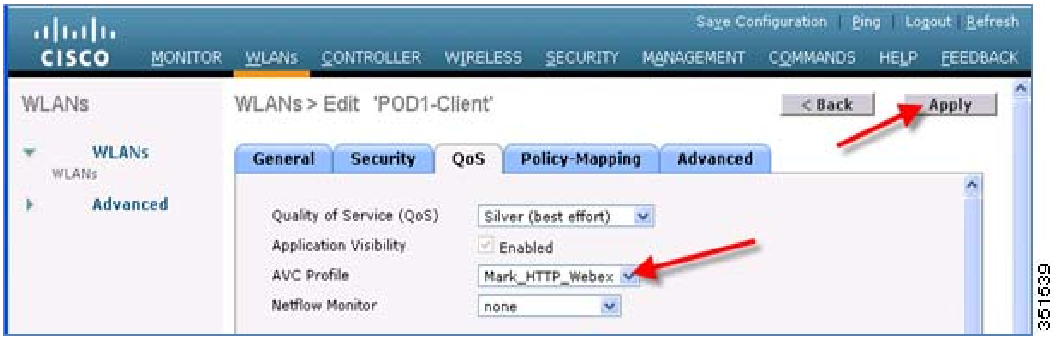
WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Avc Profile
1	WLAN	POD1-Client	POD1-Client	Enabled	Block_Youtube

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.

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

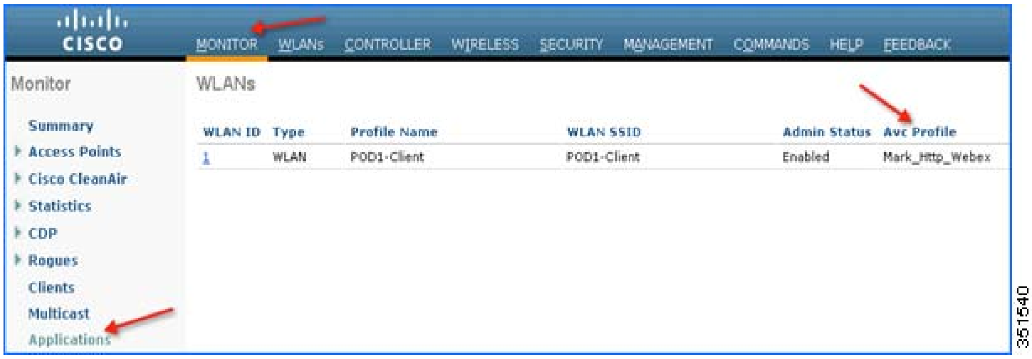
14. Now change the AVC profile on the WLAN to test the MARK operation of the NBAR feature. Select AVC profile **Mark_Http_Webex** from the drop-down under QOS tab on the WLAN and click **Apply.**



WLANs > Edit 'POD1-Client'

Quality of Service (QoS) Silver (best effort)
Application Visibility ☑ Enabled
AVC Profile Mark_HTTP_Webex
Netflow Monitor none

15. 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.



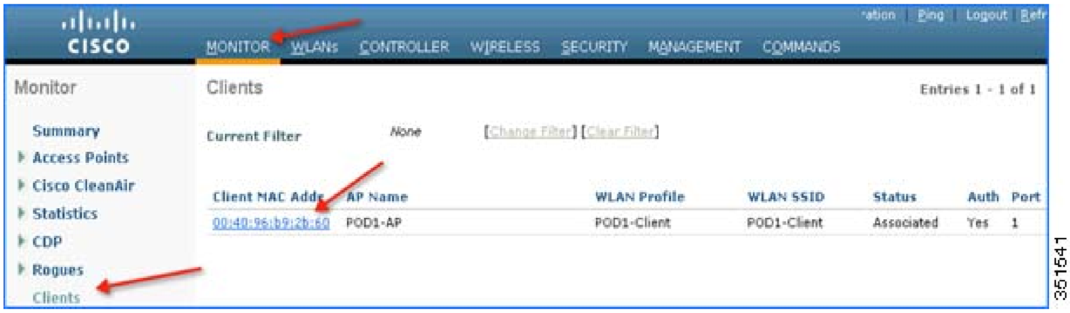
WLANs

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Avc Profile
1	WLAN	POD1-Client	POD1-Client	Enabled	Mark_Http_Webex

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.



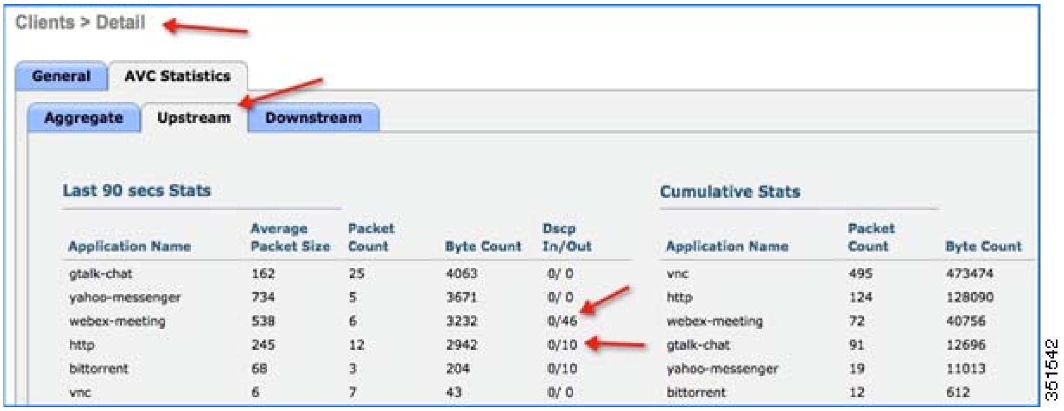
Clients

Entries 1 - 1 of 1

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Status	Auth	Port
00:40:96:b9:2b:60	POD1-AP	POD1-Client	POD1-Client	Associated	Yes	1

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.



Last 90 secs Stats

Application Name	Average Packet Size	Packet Count	Byte Count	Dscp In/Out
gtalk-chat	162	25	4063	0/ 0
yahoo-messenger	734	5	3671	0/ 0
webex-meeting	538	6	3232	0/46
http	245	12	2942	0/10
bittorrent	68	3	204	0/10
vnc	6	7	43	0/ 0

Cumulative Stats

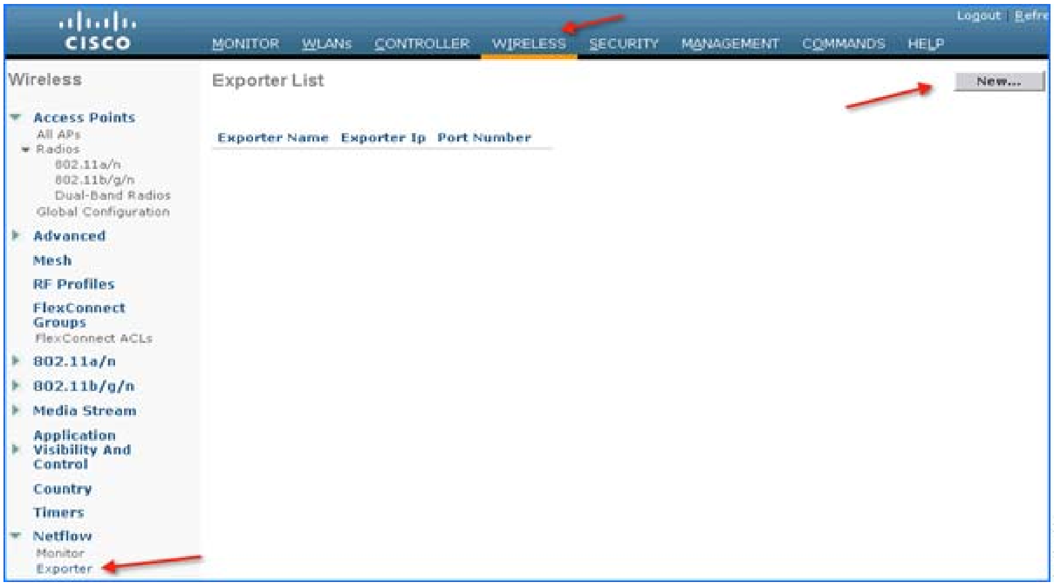
Application Name	Packet Count	Byte Count
vnc	495	473474
http	124	128090
webex-meeting	72	40756
gtalk-chat	91	12696
yahoo-messenger	19	11013
bittorrent	12	612

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.

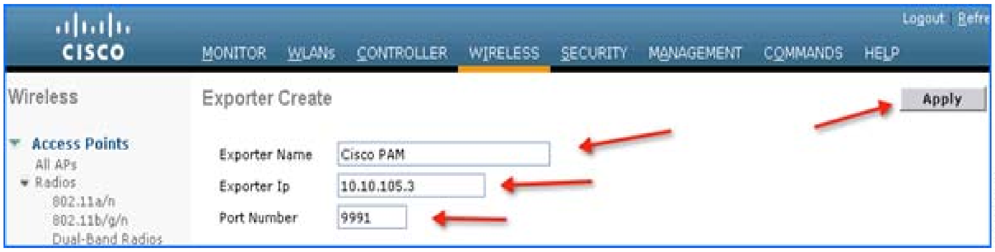
1. Add NetFlow Exporter first on WLC by configuring Exporter (NetFlow collector). In this example Cisco PAM is an exporter. It collects all the NetFlow stats generated by the WLC. To add an exporter in the WLC, navigate to **Wireless > NetFlow > Exporter**, then click **New.**



Exporter List

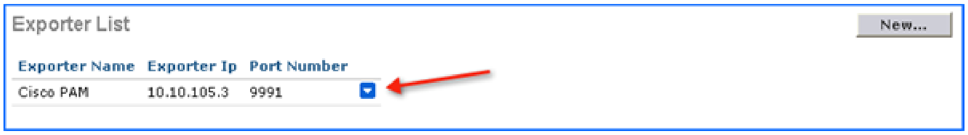
Exporter Name	Exporter Ip	Port Number

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.**



Exporter Create

Exporter Name: Cisco PAM
Exporter Ip: 10.10.105.3
Port Number: 9991

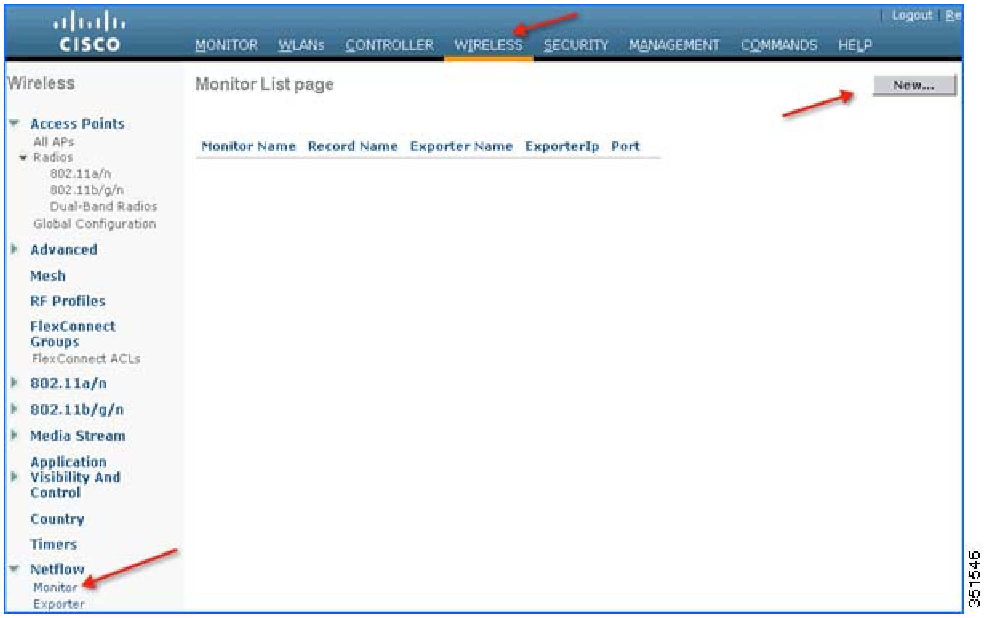


Exporter List

Exporter Name	Exporter Ip	Port Number
Cisco PAM	10.10.105.3	9991

Note: Only one exporter can be added in the WLC.

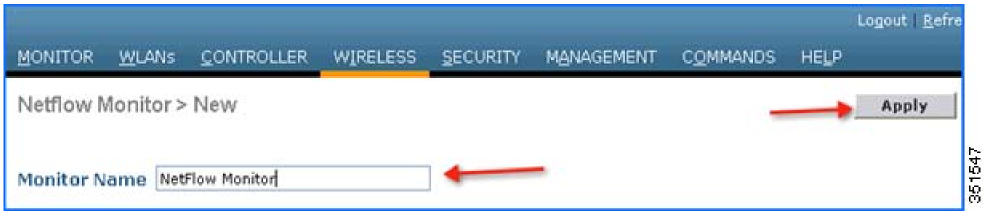
3. After adding Exporter details on the WLC i.e. PAM server, a monitor needs to be created which will store the NetFlow stats and export the same to the PAM server. To create a Monitor, navigate to **Wireless > NetFlow > Monitor**, then click **New.**



Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp	Port

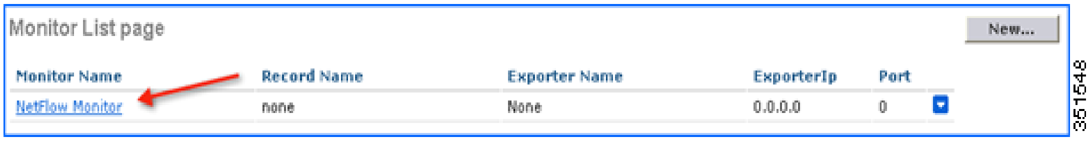
4. Enter any name to create the Monitor entry on WLC and click **Apply**.



Netflow Monitor > New

Monitor Name: NetFlow Monitor

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

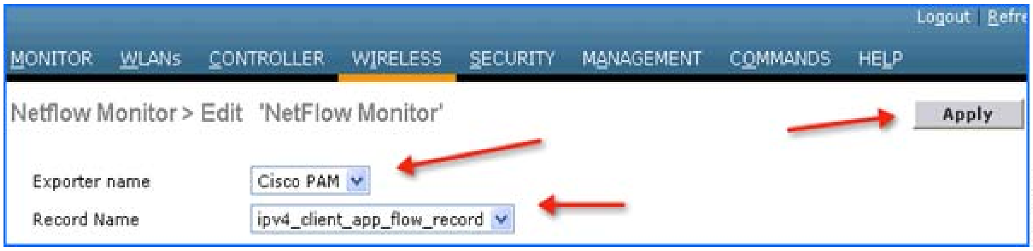


Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp	Port
NetFlow Monitor	none	None	0.0.0.0	0

Note: 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**.

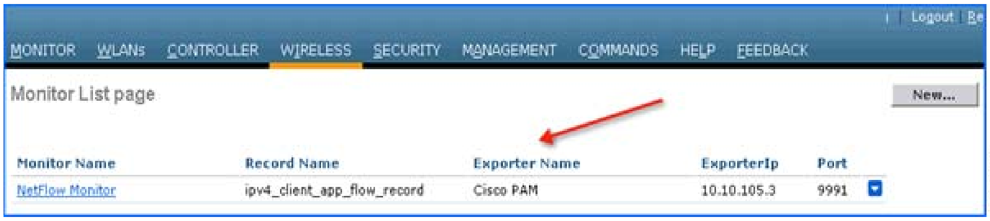


Netflow Monitor > Edit 'NetFlow Monitor'

Exporter name: Cisco PAM

Record Name: ipv4_client_app_flow_record

351549



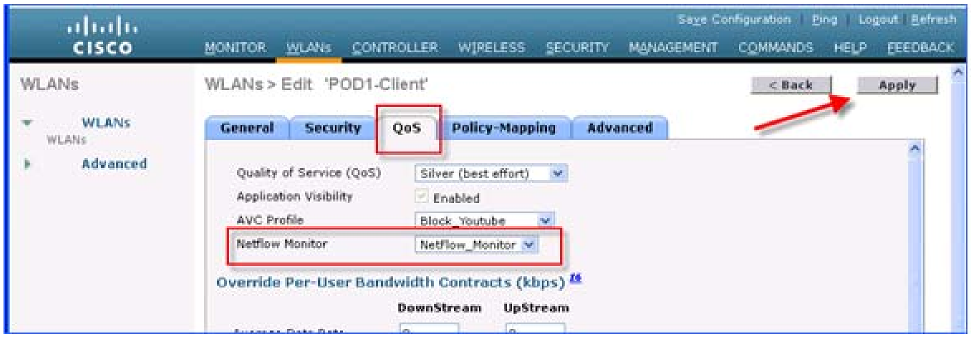
Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp	Port
NetFlow Monitor	ipv4_client_app_flow_record	Cisco PAM	10.10.105.3	9991

351550

7. 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.

Note: Please make sure the configured Exporter Port is 9991.



WLANs > Edit 'POD1-Client'

Quality of Service (QoS): Silver (best effort)

Application Visibility: ☑ Enabled

AVC Profile: Block_Youtube

Netflow Monitor: NetFlow_Monitor

Override Per-User Bandwidth Contracts (kbps)

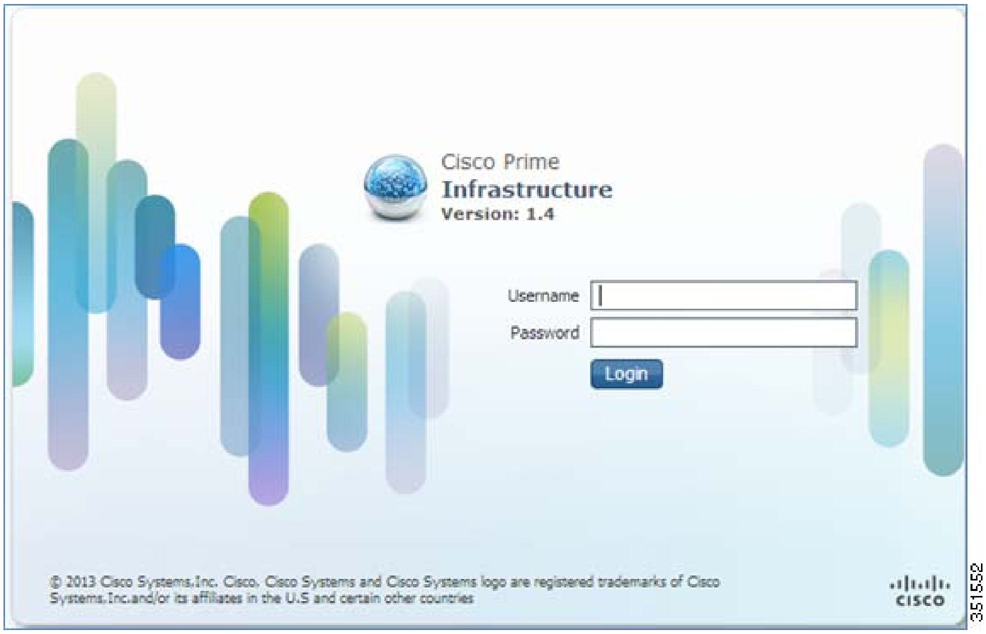
DownStream UpStream

351551

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

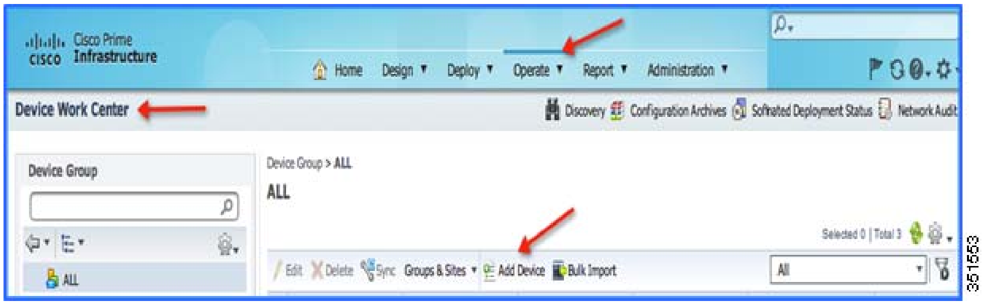
   Username: XXXXXX

   Password: XXXXXXX

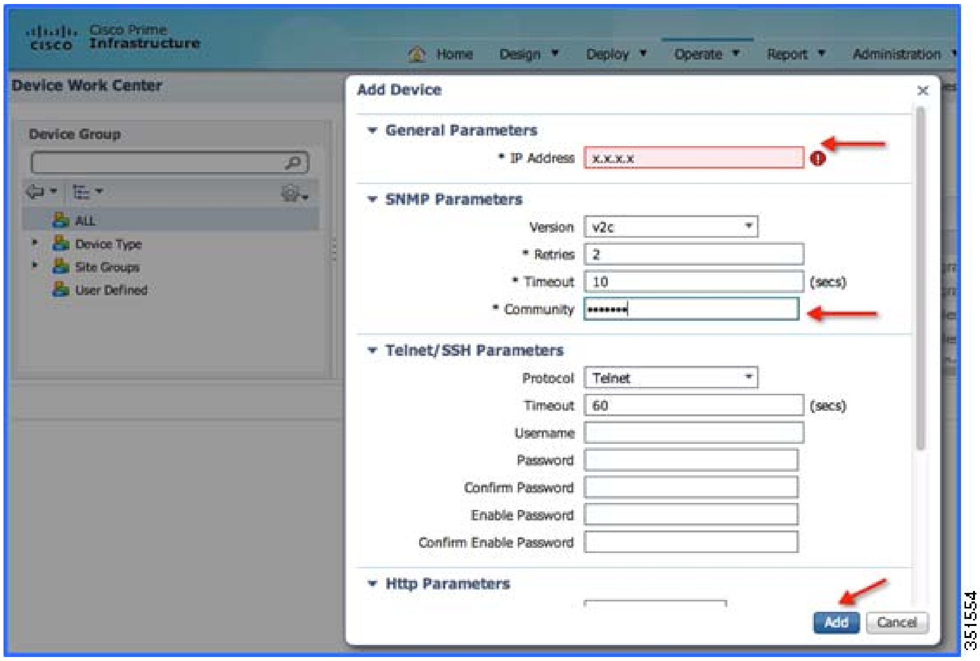


© 2013 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc.and/or its affiliates in the U.S and certain other countries

9. 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.



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**.



Add Device

General Parameters

* IP Address: x.x.x.x

SNMP Parameters

Version: v2c
* Retries: 2
* Timeout: 10 (secs)
* Community: •••••••

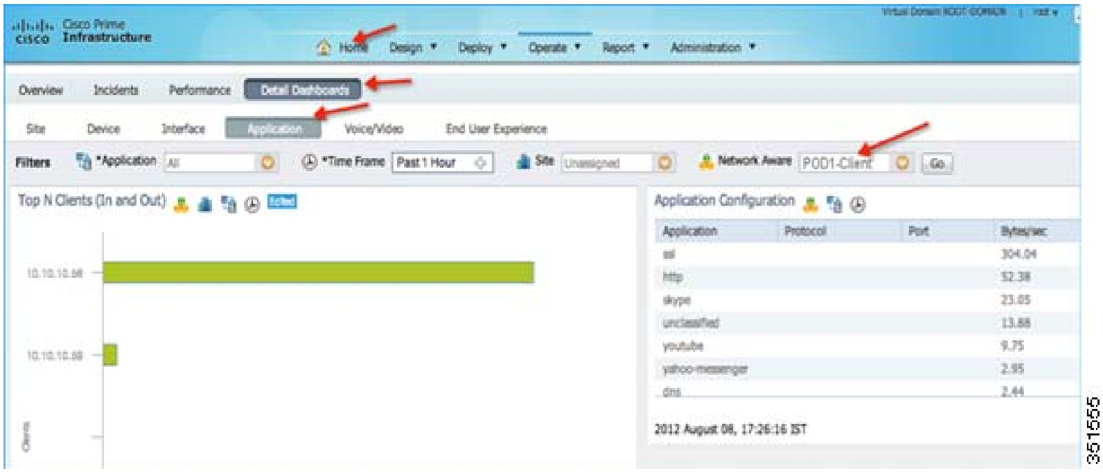
Telnet/SSH Parameters

Protocol: Telnet
Timeout: 60 (secs)
Username:
Password:
Confirm Password:
Enable Password:
Confirm Enable Password:

Http Parameters

Add Cancel

11. 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**.



Filters: *Application: All | *Time Frame: Past 1 Hour | Site: Unassigned | Network Aware: POD1-Client | Go

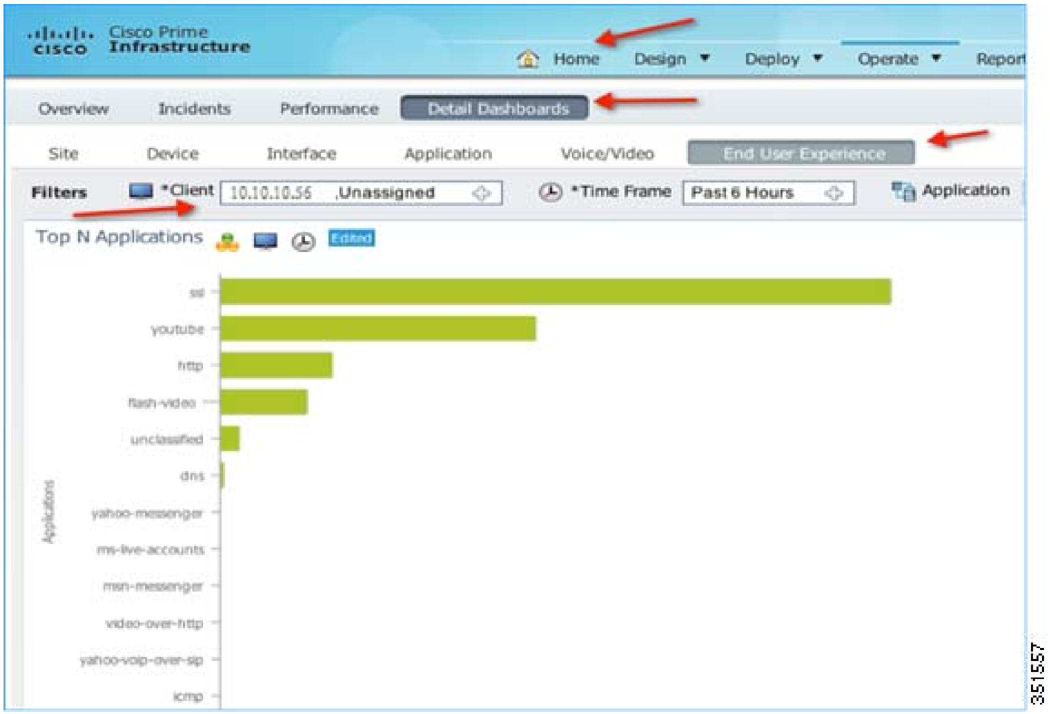
Application Configuration

Application	Protocol	Port	Bytes/sec
ssl			304.04
http			52.38
skype			23.05
unclassified			13.88
youtube			9.75
yahoo-messenger			2.95
dns			2.44

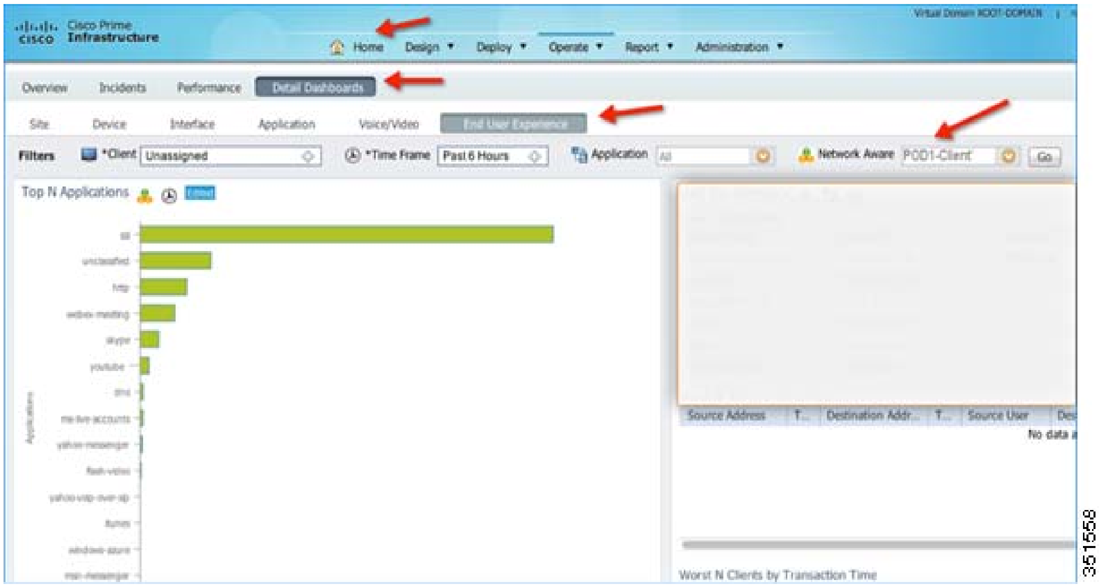
2012 August 08, 17:26:16 IST

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.

12. 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.



13. 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**.



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

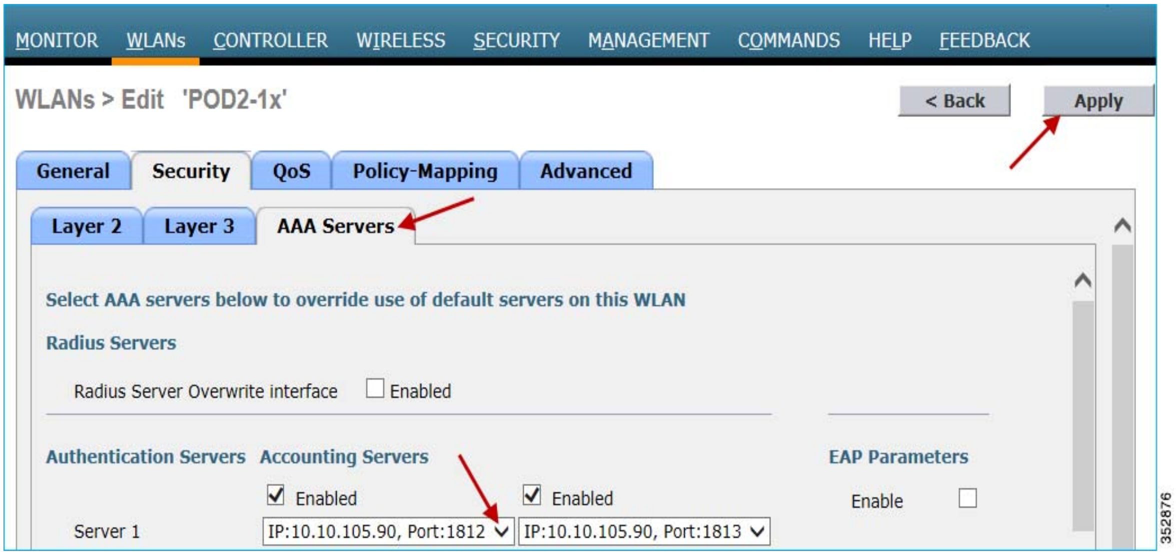
As mentioned above in releases 7.4, 7.5, and 7.6, the AVC Profile is configured on a WLAN and all clients connected to that WLAN inherit the same AVC profile. The value proposition to allow for the AAA AVC profile override is to enable different clients (logging in as different users) to obtain different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

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**.



WLANs > Edit 'POD2-1x'

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

Radius Servers

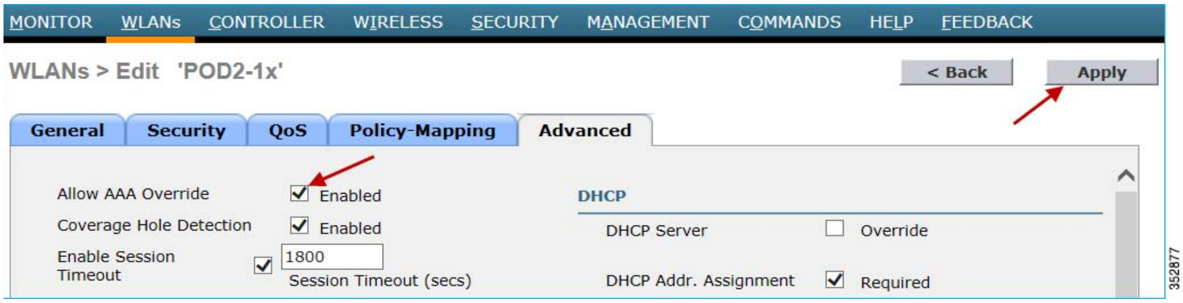
Radius Server Overwrite interface □ Enabled

Authentication Servers Accounting Servers EAP Parameters

☑ Enabled ☑ Enabled Enable □

Server 1 IP:10.10.105.90, Port:1812 IP:10.10.105.90, Port:1813

Click the **Advanced** tab and enable “AAA Override” as shown below.



WLANs > Edit 'POD2-1x'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

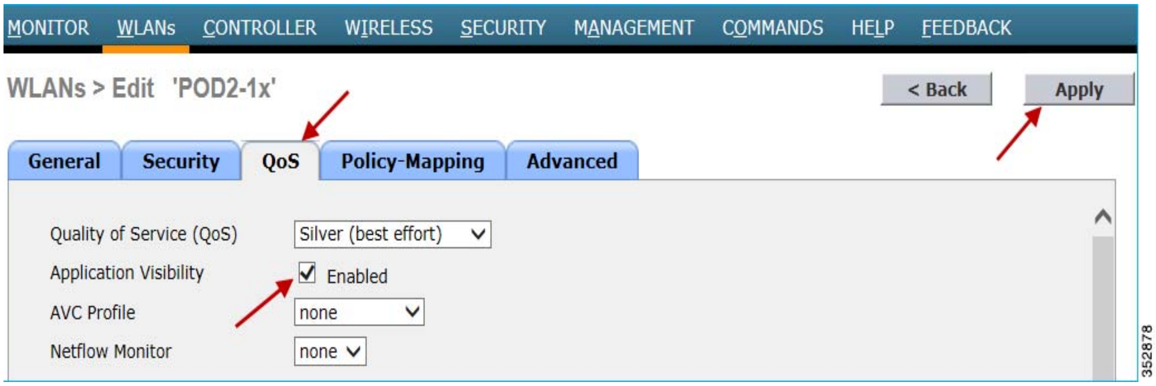
Enable Session Timeout ☑ 1800 Session Timeout (secs)

DHCP

DHCP Server □ Override

DHCP Addr. Assignment ☑ Required

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



WLANs > Edit 'POD2-1x'

Quality of Service (QoS) Silver (best effort)

Application Visibility ☑ Enabled

AVC Profile none

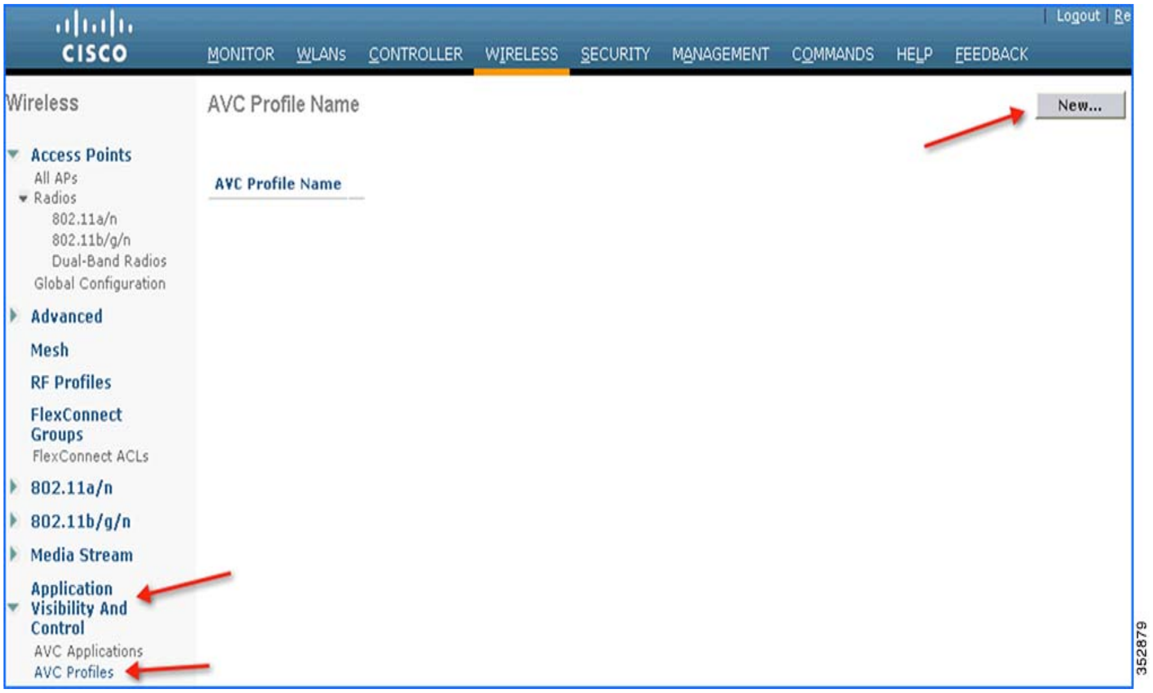
Netflow Monitor none

AAA Configuration for AVC Profile

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:

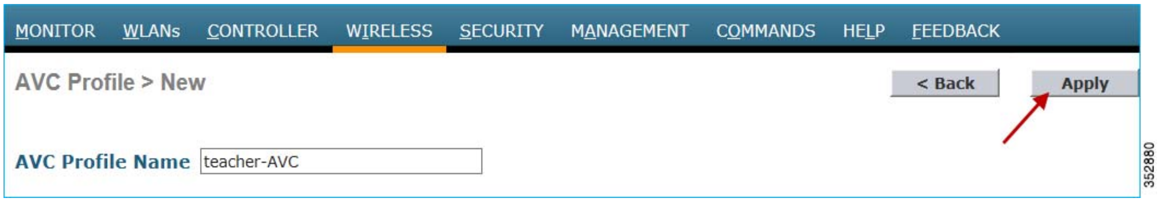
1. To demonstrate the AVC profile being applied per user through AAA server, create AVC profiles by navigating to **Wireless > Application Visibility And Control > AVC Profiles** and click **New.** In this setup/example, we created a teacher-AVC and student-AVC. We will mark specific traffic (YouTube 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.



AVC Profile Name

AVC Profile Name

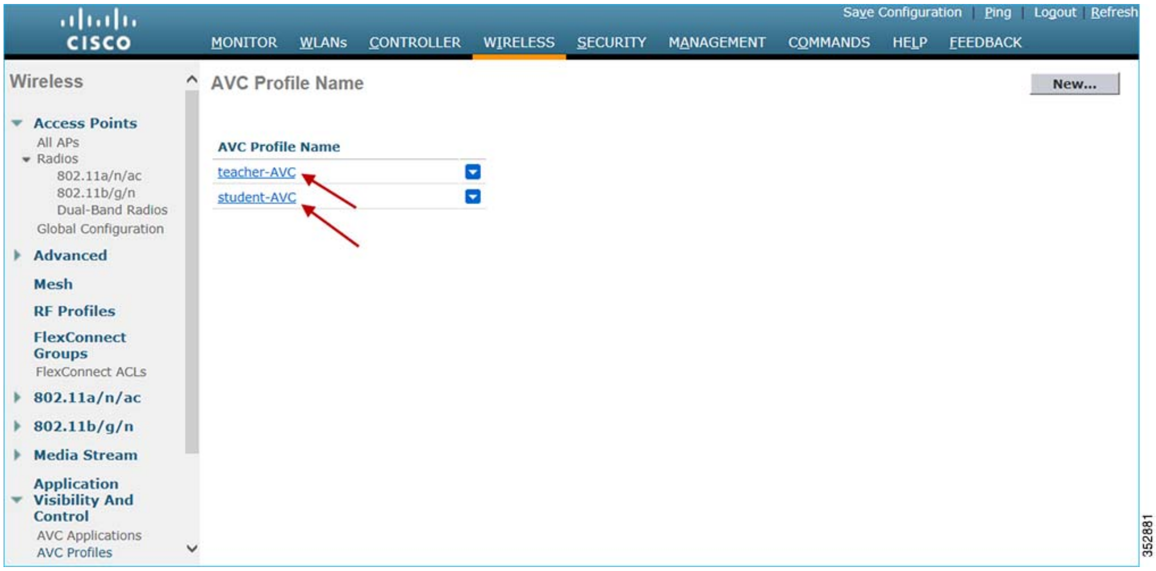
2. Enter the AVC profile name and click **Apply**. Similarly, create another profile.


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
< Back
Apply
352880

AVC Profile > New

AVC Profile Name teacher-AVC

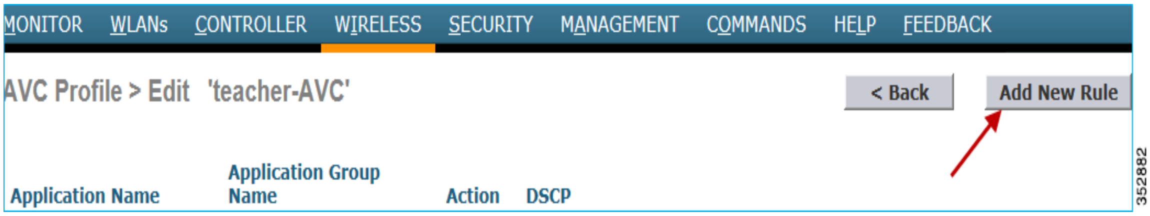
3. The AVC profile is created and you can view the above created profile, which can be clicked to create rules to take drop/mark/Rate Limit action from the GUI. A maximum of 16 AVC profiles can be created on the WLC.



AVC Profile Name

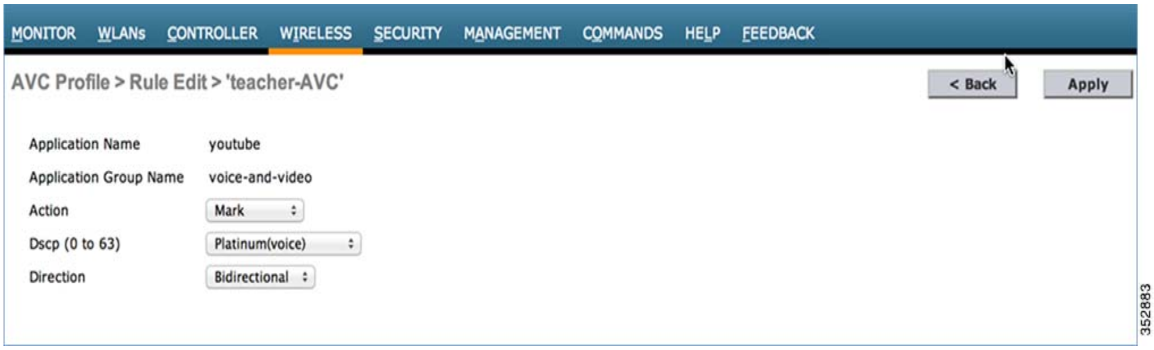
AVC Profile Name
teacher-AVC
student-AVC

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 WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
< Back
Add New Rule
352882

AVC Profile > Edit 'teacher-AVC'

Application Name	Application Group Name	Action	DSCP

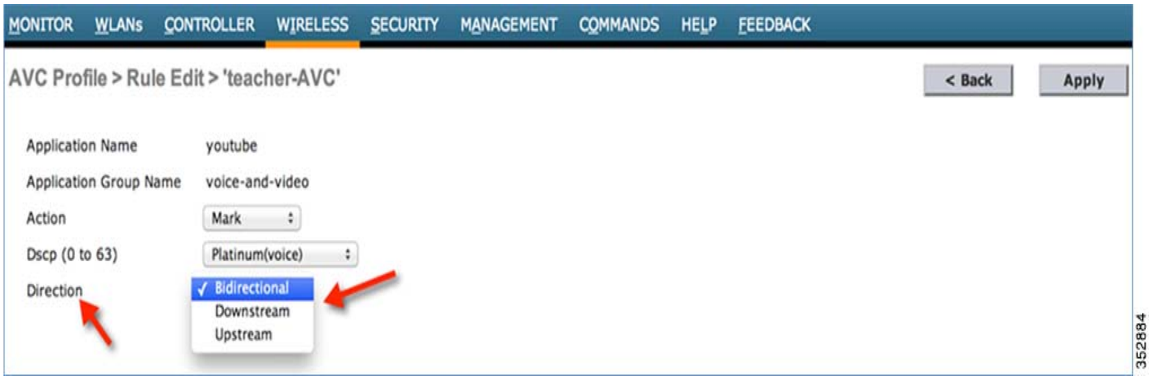

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
< Back
Apply
352883

AVC Profile > Rule Edit > 'teacher-AVC'

Application Name	youtube
Application Group Name	voice-and-video
Action	Mark
Dscp (0 to 63)	Platinum(voice)
Direction	Bidirectional

Note: 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.



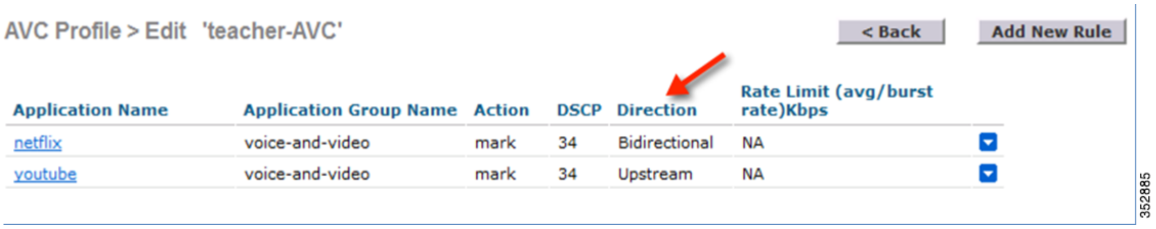
AVC Profile > Rule Edit > 'teacher-AVC'

Application Name	youtube
Application Group Name	voice-and-video
Action	Mark
Dscp (0 to 63)	Platinum(voice)
Direction	✓ Bidirectional Downstream Upstream

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.

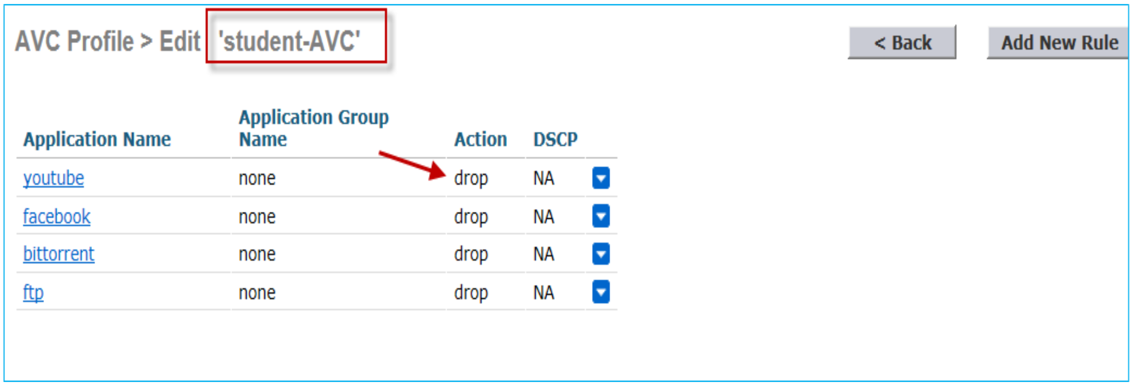
Here, we configured Netflix and YouTube to be marked for the AVC profile “teacher-AVC” with DSCP 34 (Gold) with the direction set to Bidirectional and Upstream, respectively.



AVC Profile > Edit 'teacher-AVC'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
netflix	voice-and-video	mark	34	Bidirectional	NA
youtube	voice-and-video	mark	34	Upstream	NA

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.

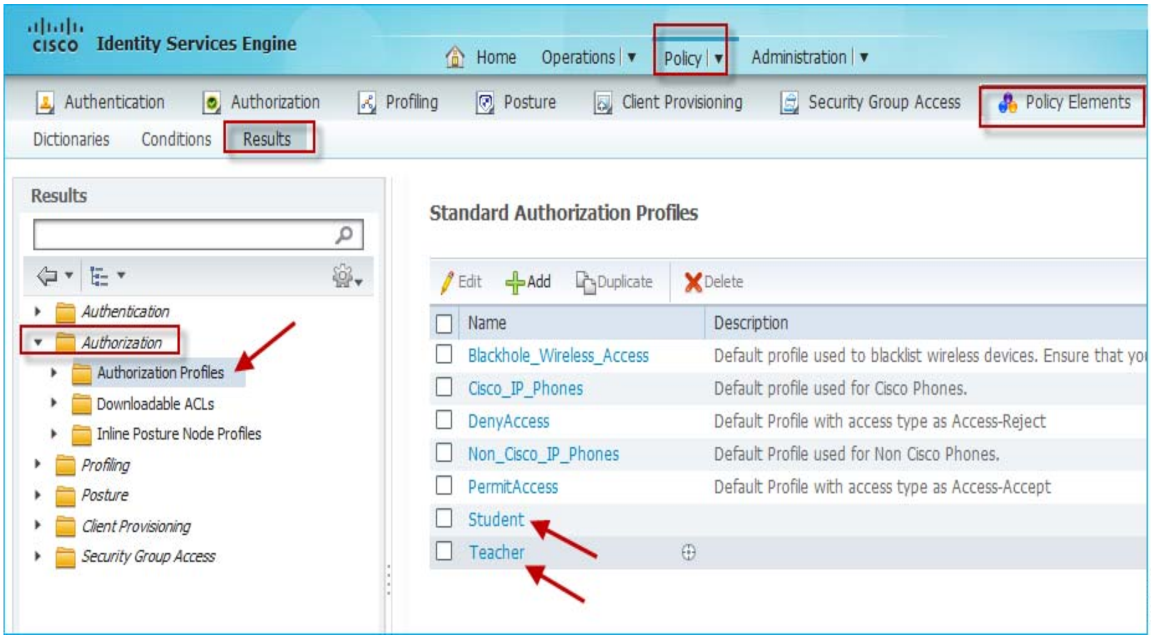


AVC Profile > Edit 'student-AVC'

Application Name	Application Group Name	Action	DSCP
youtube	none	drop	NA
facebook	none	drop	NA
bittorrent	none	drop	NA
ftp	none	drop	NA

352886

7. Now, assume that the user/administrator has already configured the AAA server (ISE/ACS/Open Radius) 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.

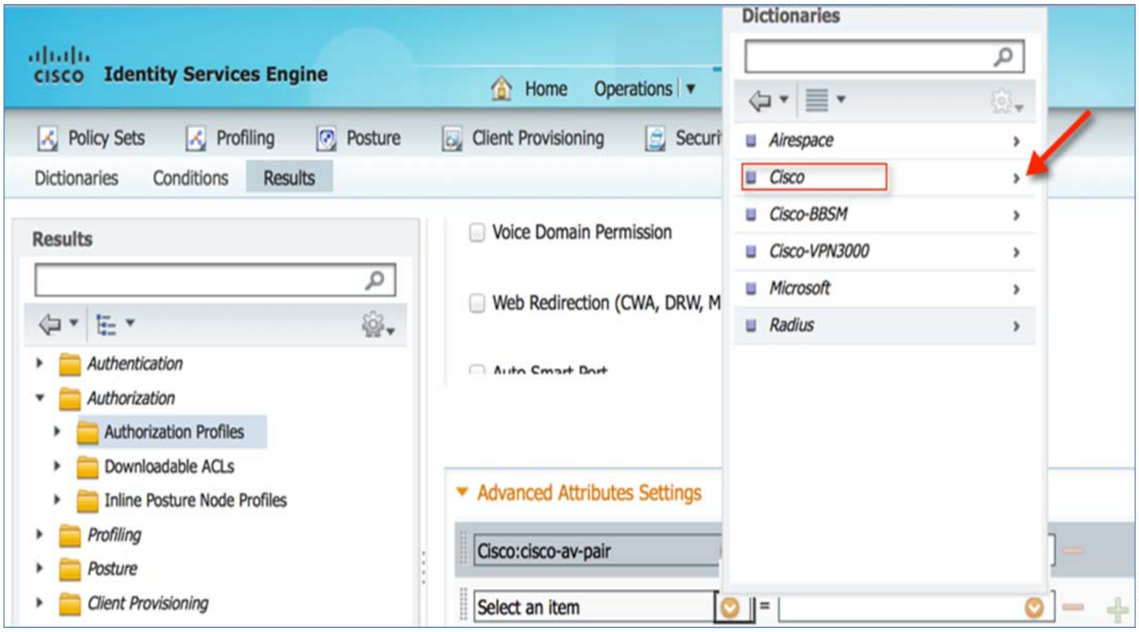


Standard Authorization Profiles

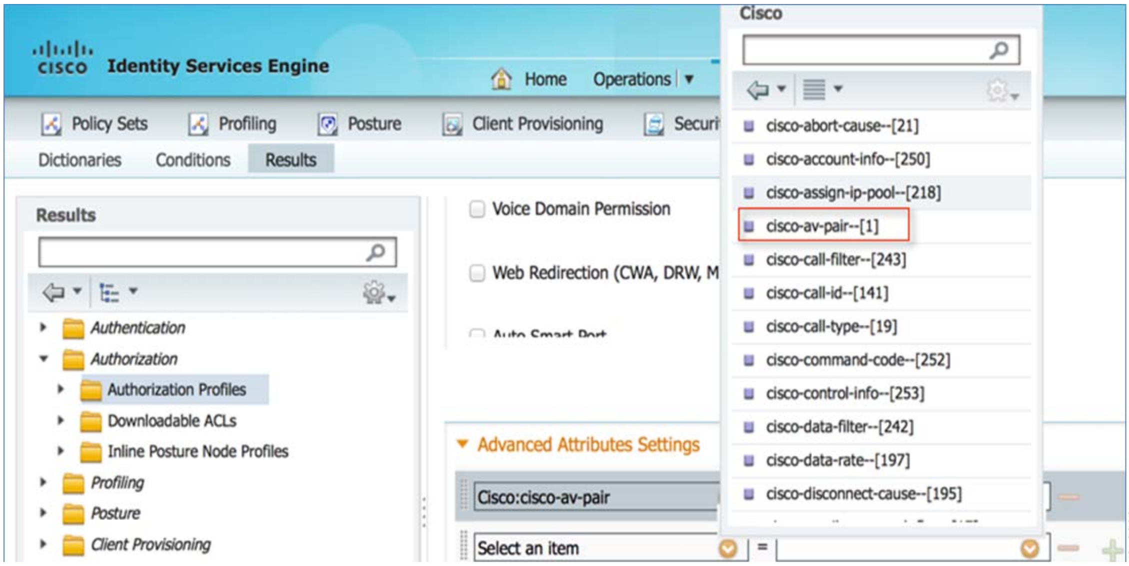
	Name	Description
□	Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure that yo
□	Cisco_IP_Phones	Default profile used for Cisco Phones.
□	DenyAccess	Default Profile with access type as Access-Reject
□	Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
□	PermitAccess	Default Profile with access type as Access-Accept
□	Student	
□	Teacher	

352887

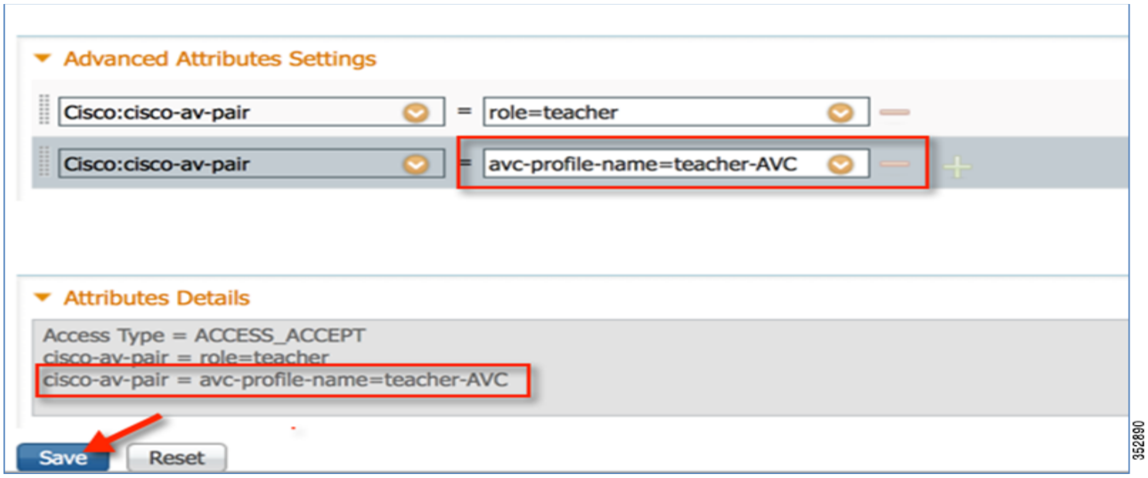
8. Click the authorization profile which you created for the role Teacher, and under **Advanced Attributes Settings**, configure AVC Profile Name by adding **cisco-av-pair=avc-profile-name=*The AVC profile name created on the WLC,*** as shown below.



352888



352889



Advanced Attributes Settings

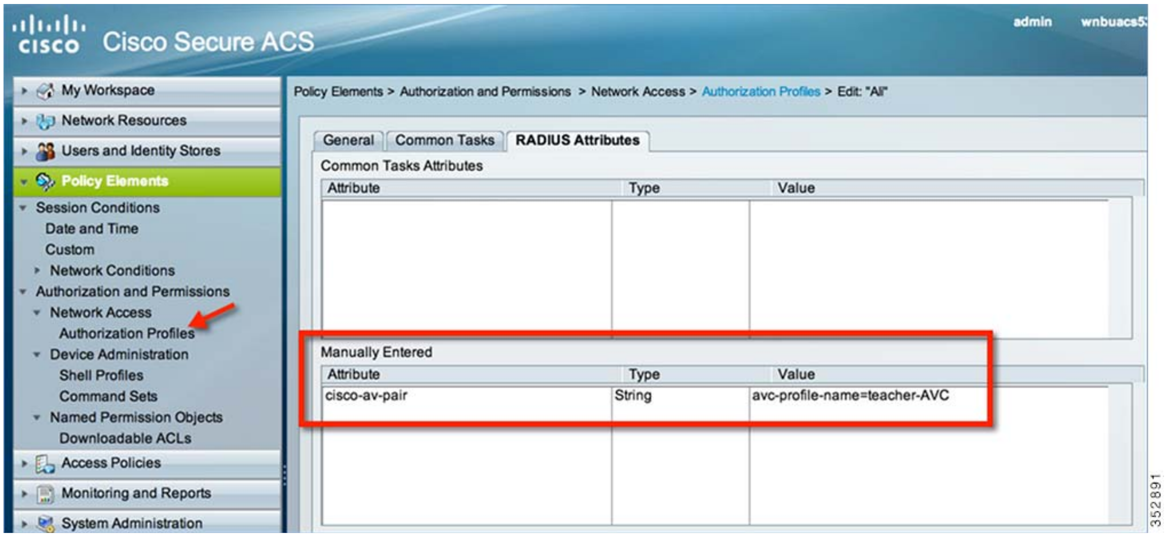
Cisco:cisco-av-pair = role=teacher

Cisco:cisco-av-pair = avc-profile-name=teacher-AVC

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=teacher
cisco-av-pair = avc-profile-name=teacher-AVC

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*.**



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "All"

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	avc-profile-name=teacher-AVC

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.

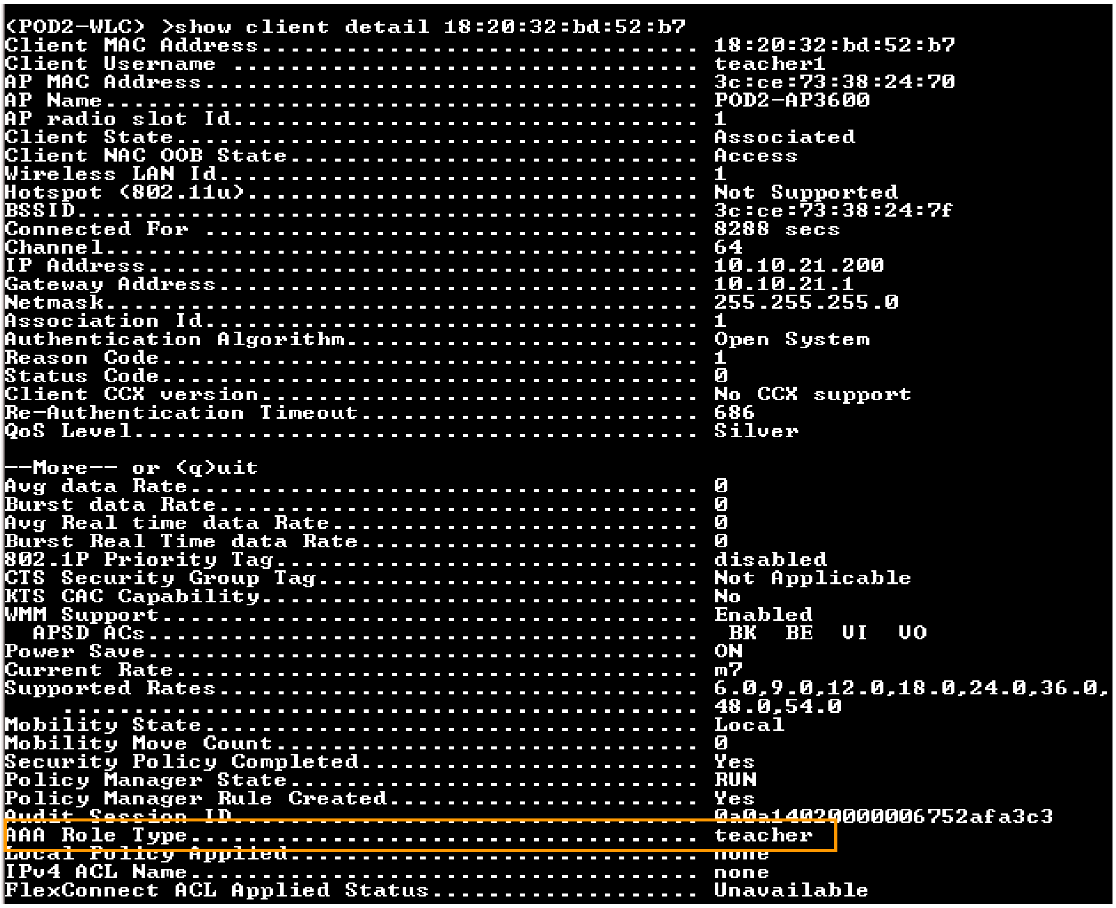
When the wireless client (with role student) connects to the same 802.1x WLAN, the client cannot play any videos on YouTube. Also, if the client tries to access a Facebook page and tries to open any YouTube video from the Facebook account, the YouTube video will not be played.

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:bd:52:b7
Client MAC Address............................... 18:20:32:bd:52:b7
Client Username ................................. teacher1
AP MAC Address................................... 3c:ce:73:38:24:70
AP Name.......................................... POD2-AP3600
AP radio slot Id................................. 1
Client State..................................... Associated
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 1
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 3c:ce:73:38:24:7f
Connected For ................................... 8288 secs
Channel.......................................... 64
IP Address....................................... 10.10.21.200
Gateway Address.................................. 10.10.21.1
Netmask.......................................... 255.255.255.0
Association Id................................... 1
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Status Code...................................... 0
Client CCX version............................... No CCX support
Re-Authentication Timeout........................ 686
QoS Level........................................ Silver

--More-- or (q)uit
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
Burst Real Time data Rate........................ 0
802.1P Priority Tag.............................. disabled
CTS Security Group Tag........................... Not Applicable
KTS CAC Capability............................... No
WMM Support...................................... Enabled
  APSD ACs....................................... BK  BE  VI  VO
Power Save....................................... ON
Current Rate..................................... m7
Supported Rates.................................. 6.0,9.0,12.0,18.0,24.0,36.0,
    ............................................. 48.0,54.0
Mobility State................................... Local
Mobility Move Count.............................. 0
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Policy Manager Rule Created...................... Yes
Audit Session ID................................. 0a0a140200000006752afa3c3
AAA Role Type.................................... teacher
Local Policy Applied............................. none
IPv4 ACL Name.................................... none
FlexConnect ACL Applied Status................... Unavailable
```

352892

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:

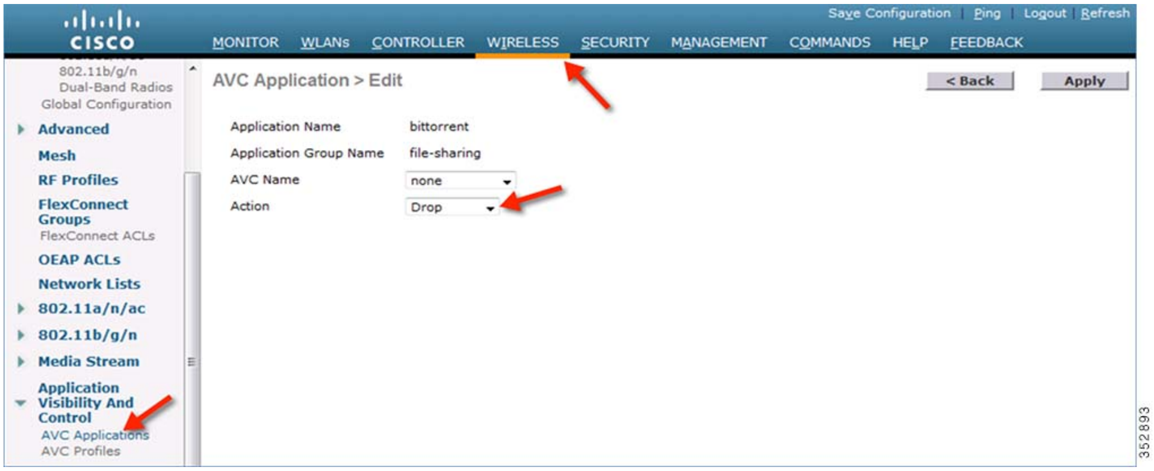
(WLC) >config avc profile <prof-name> {add|remove} rule application <app-name> {drop|mark <dscp-value>|ratelimit <avg_rate> <burst_rate>}

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**.

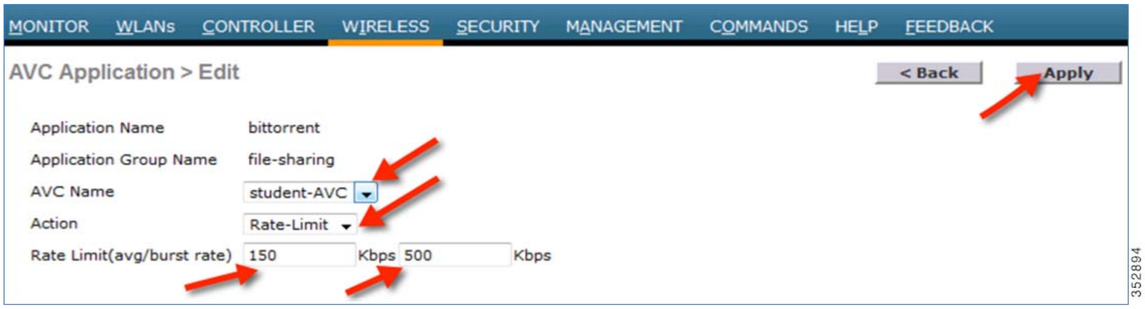


AVC Application > Edit

Application Name	bittorrent
Application Group Name	file-sharing
AVC Name	none
Action	Drop

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**.

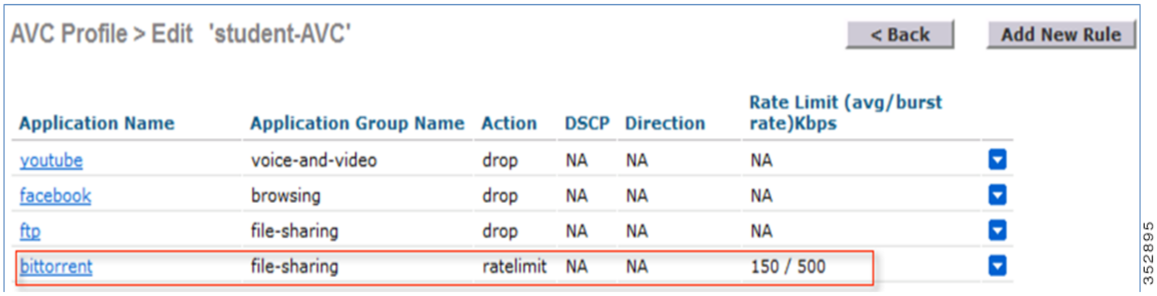
In this example, we are rate limiting the BitTorrent application with the average rate set to 150 Kbps and burst rate set to 500 Kbps and applying this to the AVC profile "student-AVC".



AVC Application > Edit

Application Name	bittorrent
Application Group Name	file-sharing
AVC Name	student-AVC
Action	Rate-Limit
Rate Limit(avg/burst rate)	150 Kbps 500 Kbps

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



AVC Profile > Edit 'student-AVC'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	drop	NA	NA	NA
facebook	browsing	drop	NA	NA	NA
ftp	file-sharing	drop	NA	NA	NA
bittorrent	file-sharing	ratelimit	NA	NA	150 / 500

NBAR Facts (AVC Phase 3)

- 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 points and policies applicable per device.

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

Scope and Objectives

In this section, the user will be configuring and implementing Profiling and Policy on a Cisco WLC running AireOS 8.0 code.

The profiling and policy enforcement will be configured as two separate components. The configuration on the WLC is based on defined parameters specific to clients joining the network. 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:

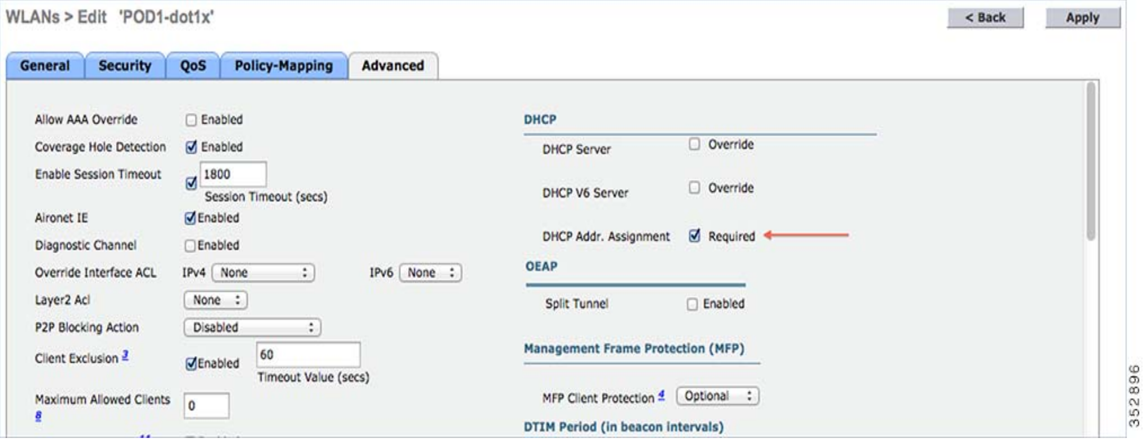
- VLAN
- ACL
- Session Timeout
- QoS
- Sleeping Client
- Flexconnect ACL
- AVC profile (added in 8.0 release)
- mDNS profile (added in 8.0 release)

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:

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.**



WLANs > Edit 'POD1-dot1x'

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients [8] 0

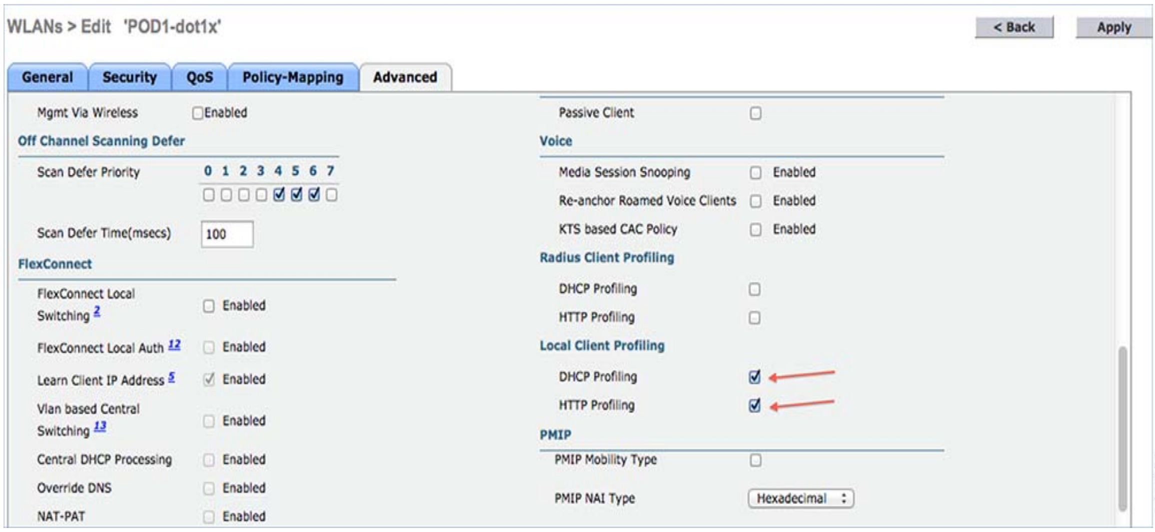
DHCP
DHCP Server □ Override
DHCP V6 Server □ Override
DHCP Addr. Assignment ☑ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

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



WLANs > Edit 'POD1-dot1x'

Mgmt Via Wireless □Enabled

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
□ □ □ □ ☑ ☑ ☑ □

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] □ Enabled

FlexConnect Local Auth [12] □ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] □ Enabled

Central DHCP Processing □ Enabled

Override DNS □ Enabled

NAT-PAT □ Enabled

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Local Client Profiling

DHCP Profiling ☑

HTTP Profiling ☑

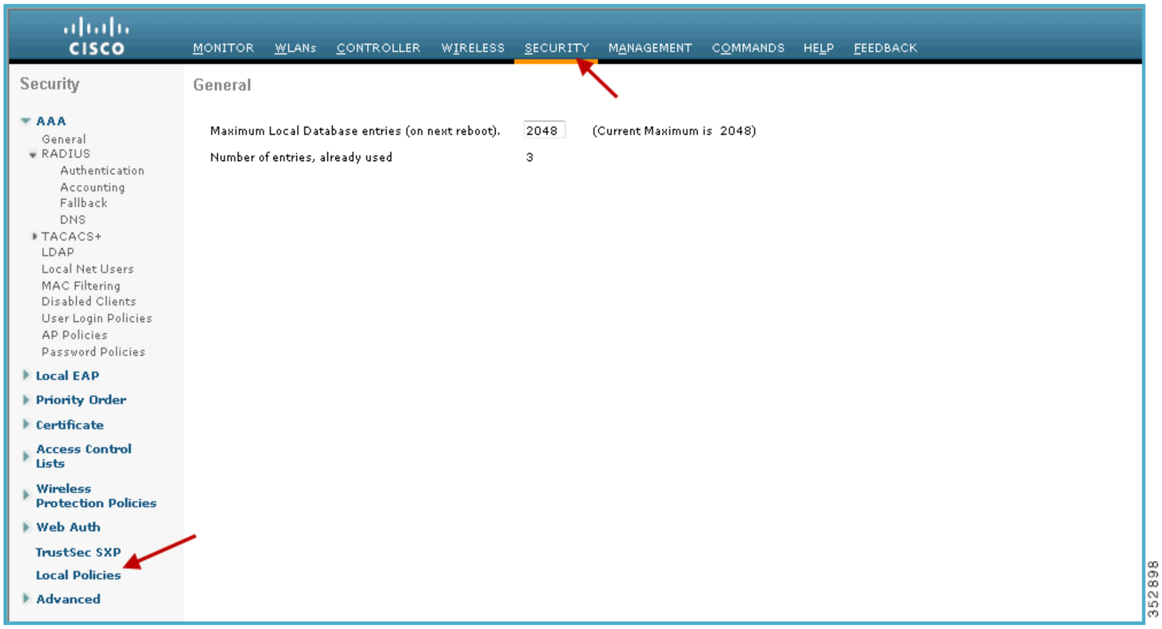
PMIP

PMIP Mobility Type □

PMIP NAI Type Hexadecimal

Creating Policies on the WLAN from the WLC GUI

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.

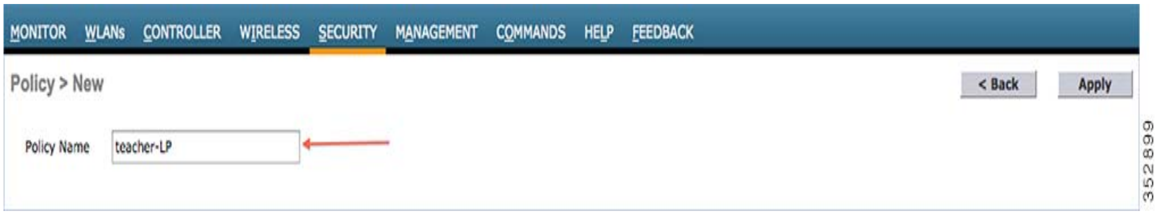


General

Maximum Local Database entries (on next reboot). 2048 (Current Maximum is 2048)

Number of entries, already used 3

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.



Policy > New

Policy Name: teacher-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.

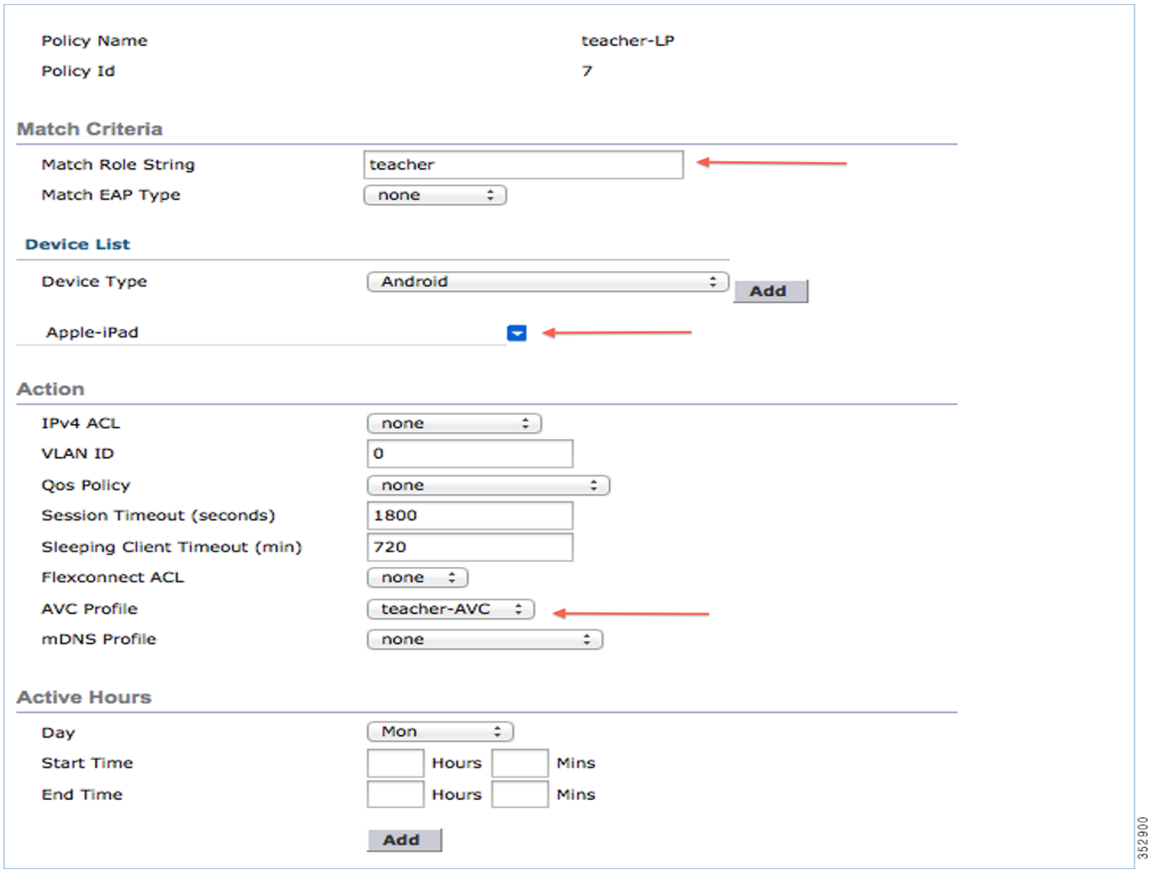
Note: Make sure Match Role string is the same as AAA defined role name. In this example, it is configured as teacher.

5. Enter User Role and click **Apply**. Here the role name “teacher” is used as an example.
6. To apply the policy based on a user device, in the **Device List** area, from the **Device Type** drop-down list, choose the device type on which you want to enforce the policy and then click **Add**.

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

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

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

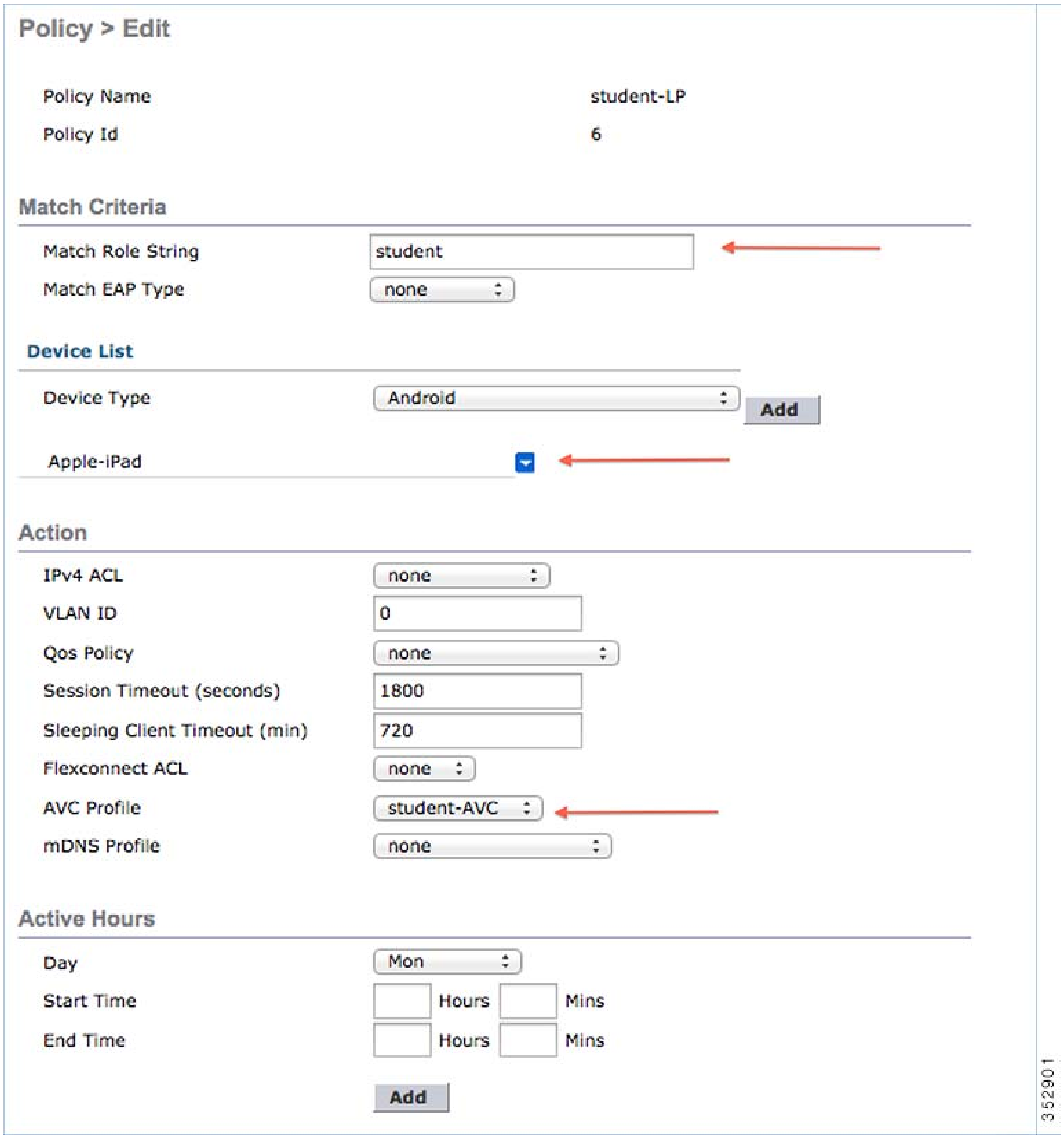
Day	Mon
Start Time	Hours Mins
End Time	Hours Mins

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

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

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.



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

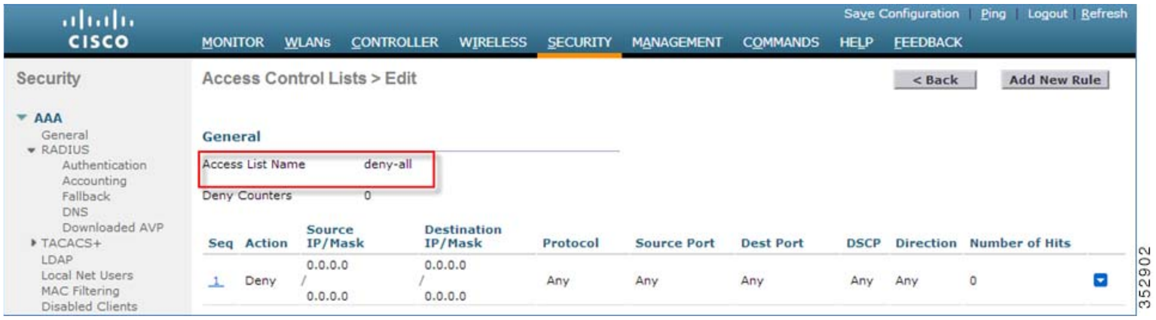
Day	Mon
Start Time	Hours Mins
End Time	Hours Mins

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

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

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

   Create an ACL to deny all IPv4 flow.



Access Control Lists > Edit

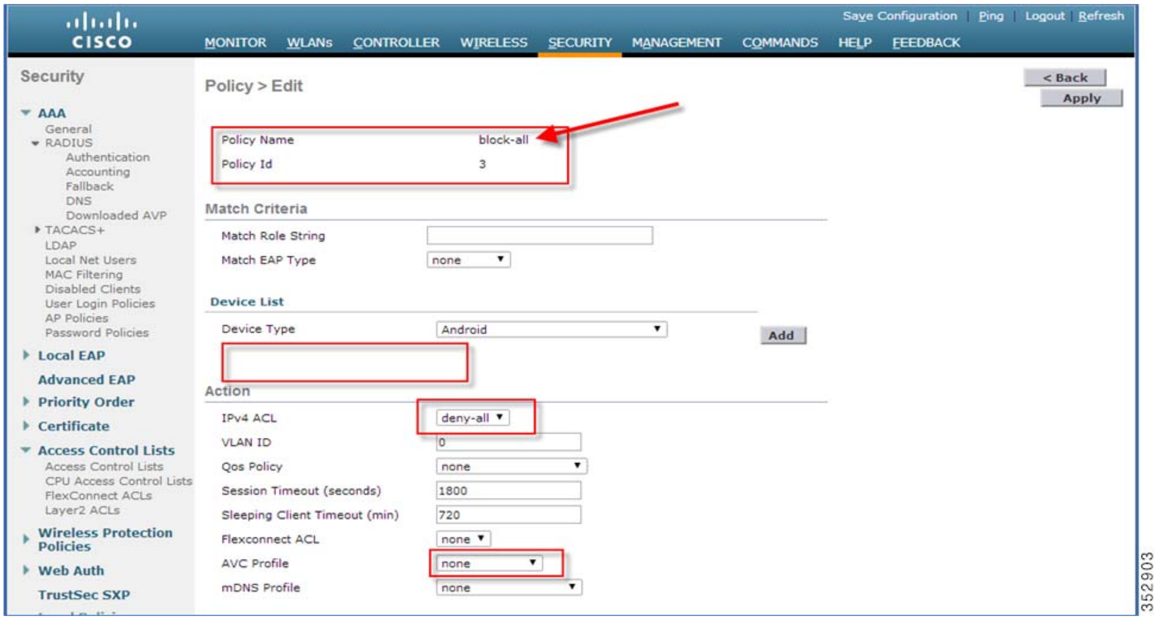
General

Access List Name deny-all

Deny Counters 0

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

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



Policy > Edit

Policy Name block-all

Policy Id 3

Match Criteria

Match Role String

Match EAP Type none

Device List

Device Type Android

Action

IPv4 ACL deny-all

VLAN ID 0

Qos Policy none

Session Timeout (seconds) 1800

Sleeping Client Timeout (min) 720

Flexconnect ACL none

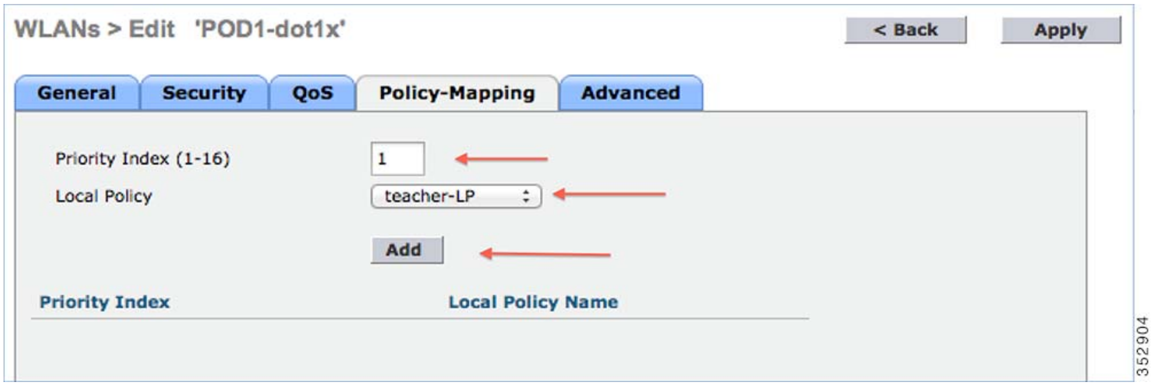
AVC Profile none

mDNS Profile none

Mapping Policy on WLAN

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.



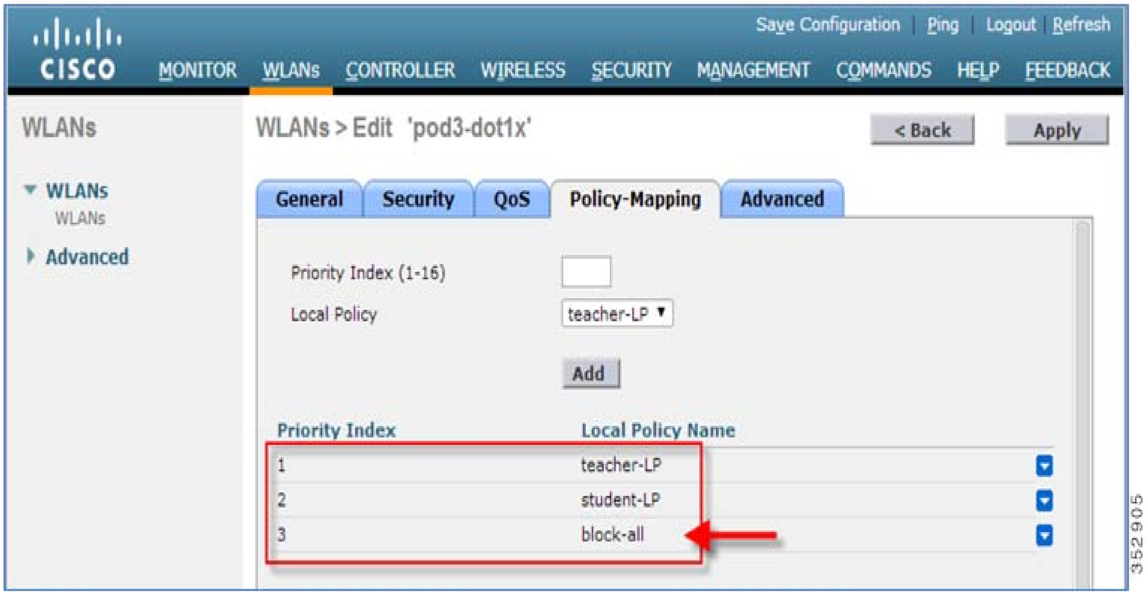
WLANs > Edit 'POD1-dot1x'

Priority Index (1-16): 1

Local Policy: teacher-LP

Priority Index	Local Policy Name

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



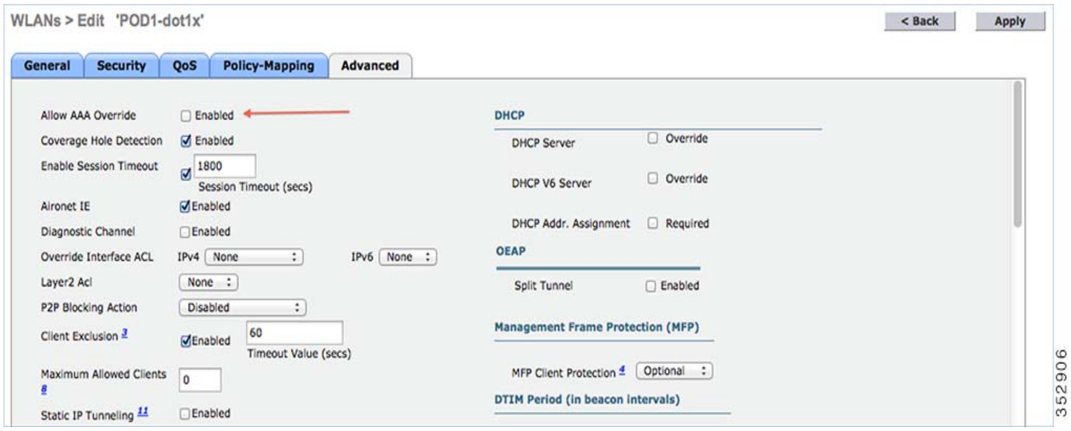
WLANs > Edit 'pod3-dot1x'

Priority Index (1-16):

Local Policy: teacher-LP

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

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



WLANs > Edit 'POD1-dot1x'

Allow AAA Override ☐ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel ☐ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8] 0

Static IP Tunneling [11] ☐ Enabled

DHCP

DHCP Server ☐ Override

DHCP V6 Server ☐ Override

DHCP Addr. Assignment ☐ Required

OEAP

Split Tunnel ☐ Enabled

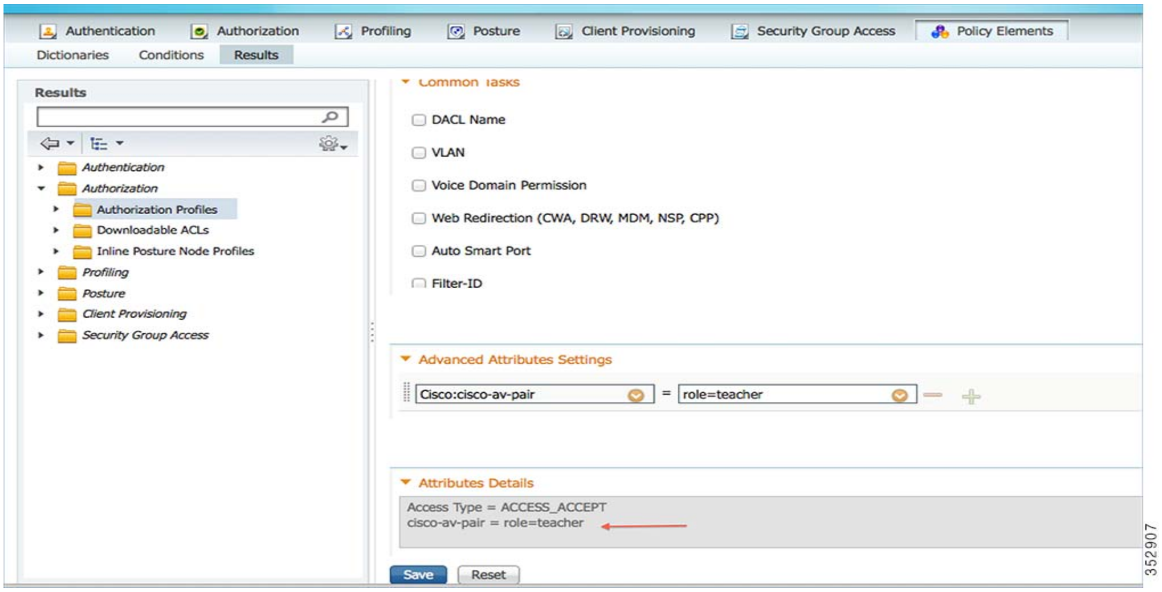
Management Frame Protection (MFP)

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

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:



- ☐ DACL Name
- ☐ VLAN
- ☐ Voice Domain Permission
- ☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)
- ☐ Auto Smart Port
- ☐ Filter-ID

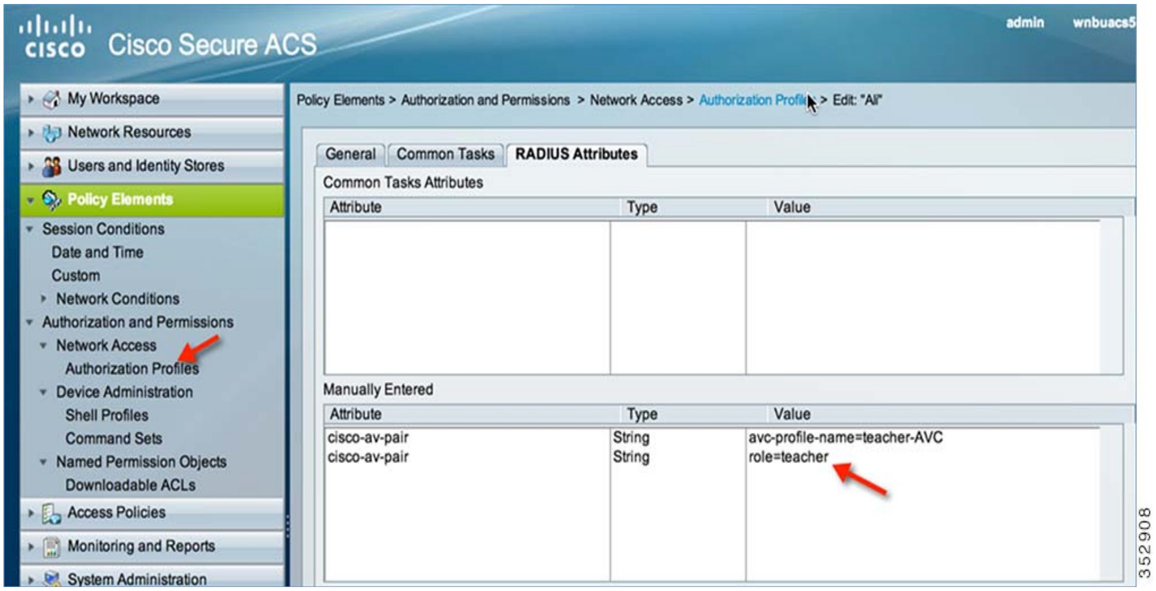
Advanced Attributes Settings

Cisco:cisco-av-pair = role=teacher

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=teacher

ACS:



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "All"

Common Tasks Attributes

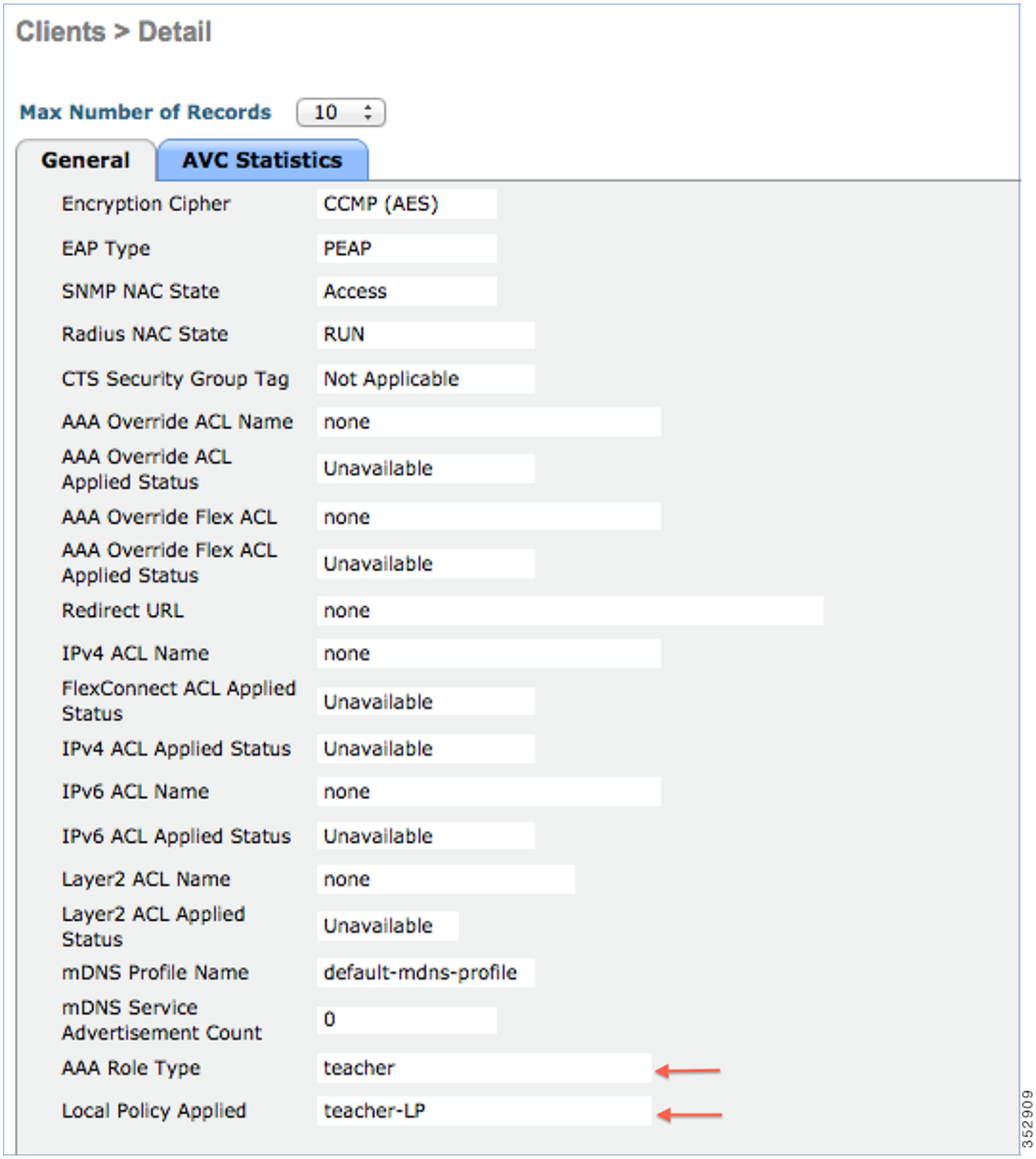
Attribute	Type	Value

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	avc-profile-name=teacher-AVC
cisco-av-pair	String	role=teacher

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.**



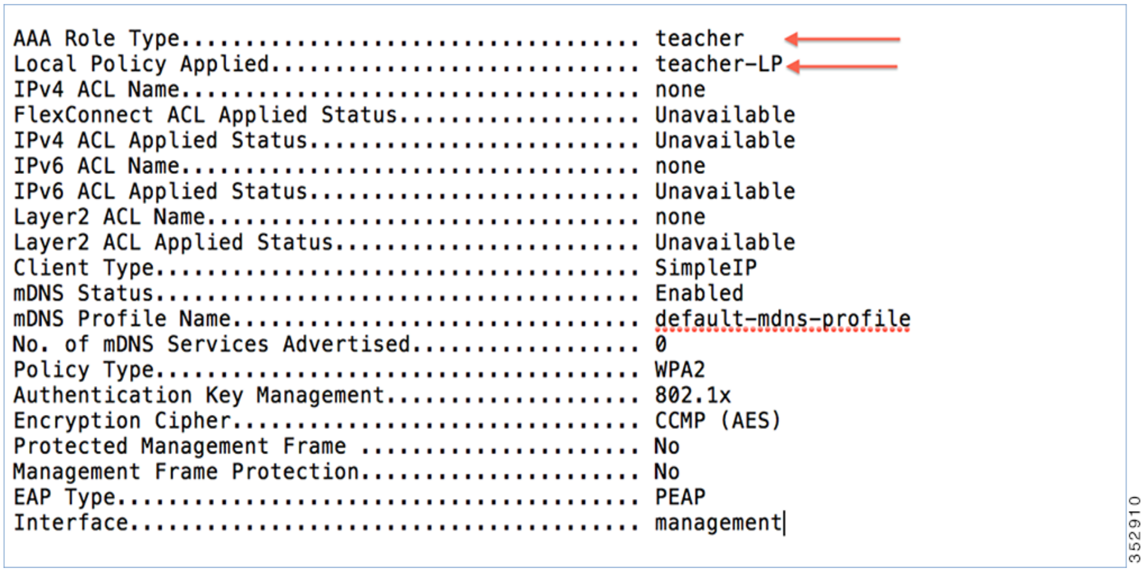
Clients > Detail

Max Number of Records 10

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:

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



```
AAA Role Type.................................... teacher
Local Policy Applied............................. teacher-LP
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
Client Type...................................... SimpleIP
mDNS Status...................................... Enabled
mDNS Profile Name................................ default-mdns-profile
No. of mDNS Services Advertised.................. 0
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ management
```

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

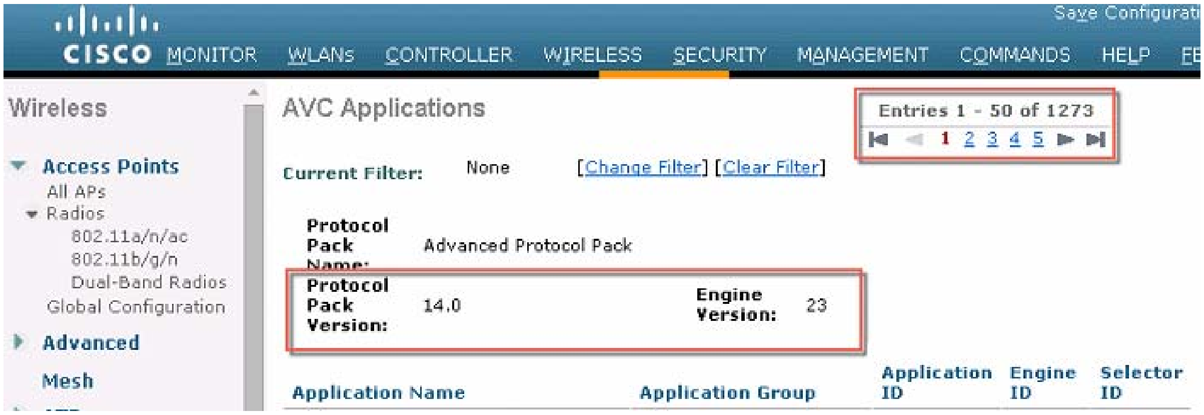
- By default, profiling is disabled on all WLANs
- Each WLAN can have mapped profiling policies configured.
- Each Policy can have matching Role Type, Device Type, EAP type configured and an associated policy index mapped.
- The policy index signifies which policy needs to be matched first.
- The corresponding 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.

AVC–Phase 4 in CUWN Release 8.2

Protocol Pack and NBAR Engine Update

Up to release 8.2, NBAR Engine (16) is integrated in WLC for centralized AVC support, which supports Protocol Pack (PP) up to version-12. In release 8.2, the new and improved NBAR Engine 23 and Protocol Pack 14 are introduced. The new versions allow customers to classify 1273 application like Netflix, Jabber, Bittorrent and YouTube and other a lot more reliably with higher precision and less impact on the controller performance. It is also important to note that Protocol Pack 14 requires NBAR engine 23 and will not work with the previous NBAR released version in the prior WLC releases. When PP version 15 is released and posted on CCO, it will operate with NBAR engine 23.



AVC Applications

Entries 1 - 50 of 1273
1 2 3 4 5

Current Filter: None [Change Filter] [Clear Filter]

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 14.0 Engine Version: 23

Application Name	Application Group	Application ID	Engine ID	Selector ID

Netflow Support in release 8.2

An IP traffic flow is a sequence of packets passing through a network device with common attributes like source and destination IP address & transport ports, direction, etc. Additional common attributes for wireless flow are SSID, AP MAC. These packets with common attributes are aggregated into flows and exported to the Netflow Collectors. Prior to relase 8.2, controller exported Netflow data was analyzed only by PI (Prime Infrastructure) and wasn't compatible with any third party Netflow collectors.

In release 8.2 nenhanced Netflow records exporter is introduced. New Netflow v9 is sending 17 different data records (as defined in RFC 3954) to the External 3rd Party Netflow collector such as Stealthwatch and others. Support for the Enhanced Flow Record Data Export was added on the WLC 5520, 8510 and 8540.

Prior to release 8.2 Netflow feature available on the controller sends only the IP address of the client, SSID and Application statistics. While this helps for compatible Netflow collectors like Cisco Prime to show the application statistics, it does not provide the full 5 tuple flow information and is also not compatible with many 3rd party Netflow collectors who expect 5 tuples.

The current netflow record prior to release 8.2 that WLC exports support only the following fields

- applicationTag
- ipDiffServCodePoint
- octetDeltaCount
- packetDeltaCount

- postIpDiffServCodePoint
- staIPv4Address
- staMacAddress
- wtpMacAddress

The newly introduced flow record exporter in the release 8.2 supports the following flow data records

- Application Tag
- Client Mac Address
- AP Mac address
- WlanID
- Source IP
- Dest IP
- Source Port
- Dest Port
- Protocol
- Flow Start Time
- Flow End Time
- Direction
- Packet count
- Byte count
- VLAN Id - Mgmt/Dyn
- TOS - DSCP Value
- Dot1x username

Netflow Deployment Considerations

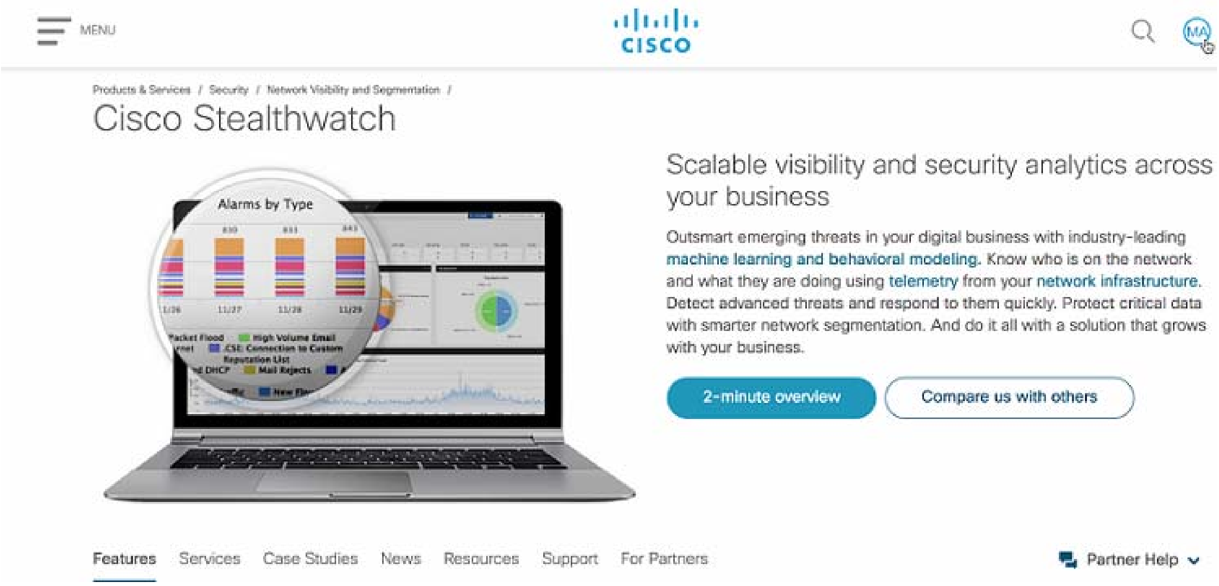
- WLC supports only one monitor and exporter.
- WLC will support only one type of Netflow record globally per controller.
- Flow records are exported directly and will not be shown on the controller.
- Application visibility statistics present today will continue on the controller.
- Change to monitor parameters will required the WLAN to be disabled and enabled.
- The new record will be supported on 8510 , 5520 and 8540 controllers only.
- 2500, 5508, 7500 and WiSM2 controllers will not be supported.
- Netflow statistics are sent at an interval of 30 seconds (Not user configurable. Current value is 90 seconds).
- Netflow record will be sent even for the unclassified applications with new flow record.

- Netflow will be sent on enabling AVC on that WLAN.
- IPv6 traffic is not supported in Netflow in release 8.2.
- Netflow sending initial template will be sent from Control plane.
- Netflow export on service port is not supported.

Obtaining Stealthwatch Software for Evaluation Purposes

The software is available for web download on the URL as indicated below: https://www.Stealthwatch.com/stealthwatch-evaluation-application

1. Sign up for Stealth Watch Evaluation and download the software



Products & Services / Security / Network Visibility and Segmentation /

Cisco Stealthwatch

Scalable visibility and security analytics across your business

Outsmart emerging threats in your digital business with industry-leading machine learning and behavioral modeling. Know who is on the network and what they are doing using telemetry from your network infrastructure. Detect advanced threats and respond to them quickly. Protect critical data with smarter network segmentation. And do it all with a solution that grows with your business.

Netflow Configuration on the WLC

Prior to release 8.2 Netflow configuration on WLC was done by associating the fixed record ipv4_client_app_flow_record to the Netflow monitor. Now along with this we will support a new fixed record called ipv4_client_src_dst_flow_record the same will be allowed in cli and GUI at the places shown below.

Note: Since only one netflow exporter is present per controller, it has to be between the old and new record formats.

Configuration from CLI

Configuration Change

```
(Cisco Controller) > config flow add monitor <My_Netflow_Monitor record>
```

Configuration steps from CLI

```
config flow create monitor <My_Netflow_Monitor>
config flow create exporter My_Netflow_Exporter A.B.C.D port 2055
config flow add monitor My_Netflow_Monitor exporter My_Netflow_Exporter
config flow add monitor My_Netflow_Monitor record ipv4_client_src_dst_flow_record config wlan flow 1
monitor My_Netflow_Monitor enable
```

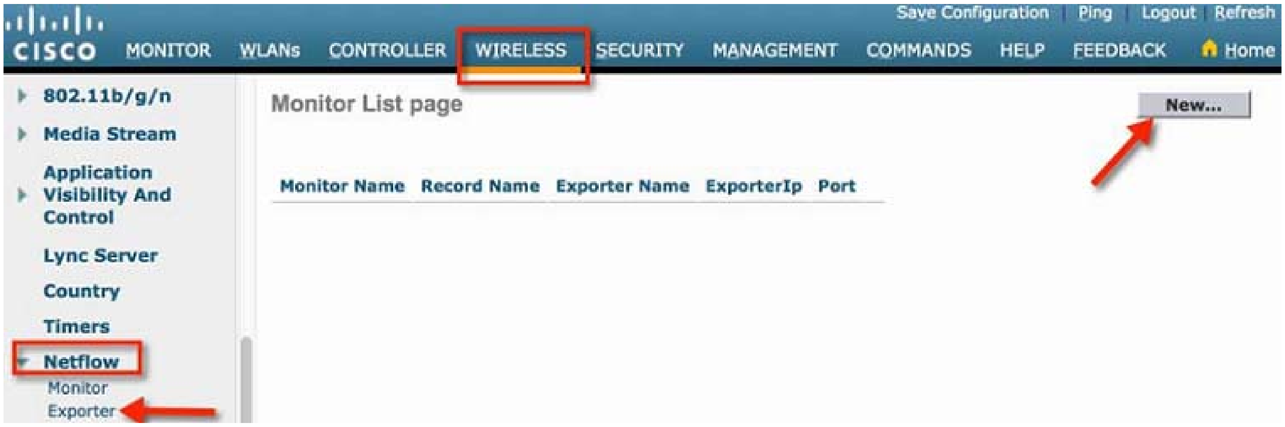
Debug commands

```
debug fastpath cfgtool --flowdb.dump debug fastpath dump wlandb
debug flow info enable
```

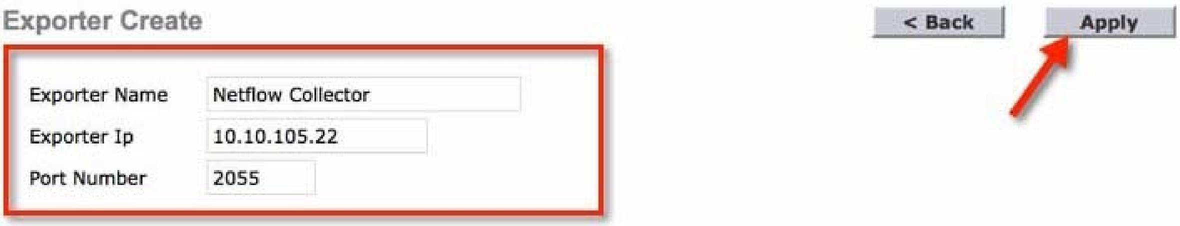
Configuration using WebUI

Screen shots below illustrate examples of the Stealthwatch Netflow Collector VM on the USC box with IP Address 10.10.105.22 and it is listening on UDP port 2055.

1. From WLC main menu configure a Netflow Exporter by going to **Wireless> Netflow> Exporter**. Click **New**.



2. Configure an **Exporter Name**, **Exporter IP** and Port Number, then click **Apply**.

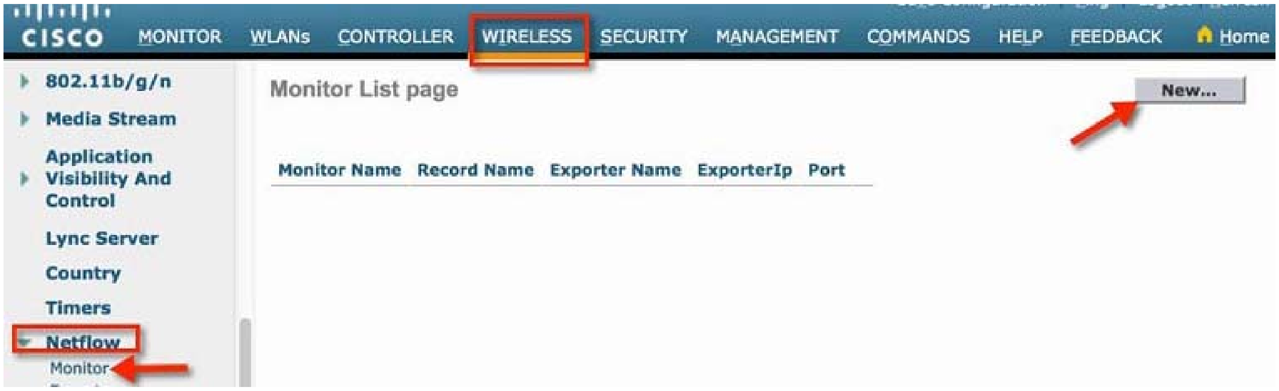


Exporter Name Netflow Collector

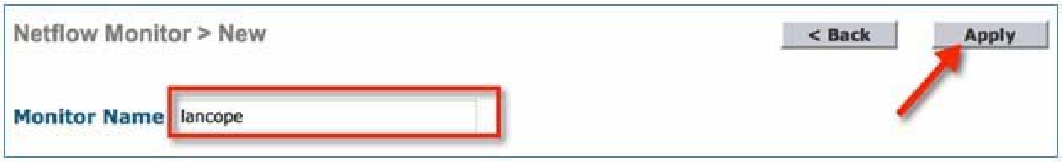
Exporter Ip 10.10.105.22

Port Number 2055

3. Now, we will create a Flow monitor for the Netflow Exporter which we created above. Under **Netflow,** go to **Monitor**. Click **New**..



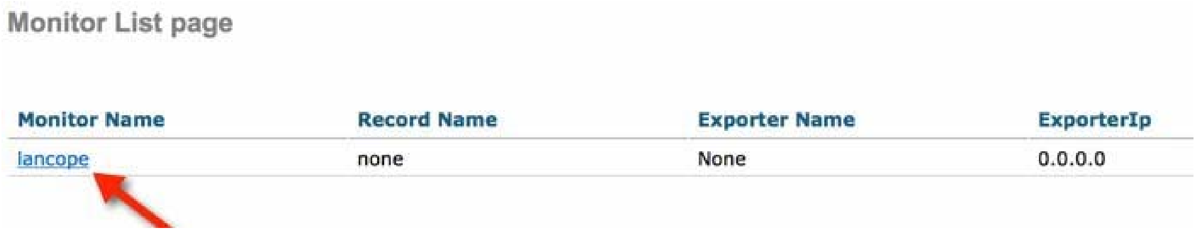
4. Create a monitor with the name " Stealthwatch " and click **Apply** as shown below.



Netflow Monitor > New

Monitor Name: lancope

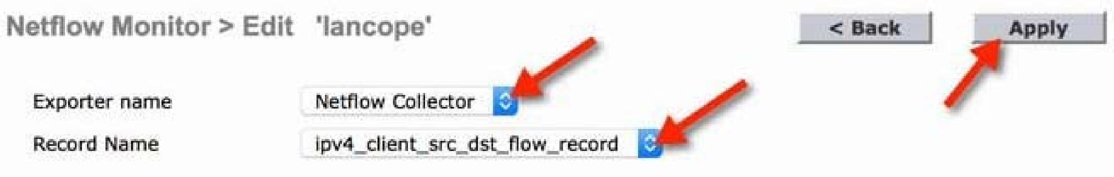
5. Click on the created Monitor name.



Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp
lancope	none	None	0.0.0.0

6. Select '**Netflow Collector**' from the Exporter Name drop down menu and choose '**ipv4_client_src_dst_flow_record**' from the Record Name list. Click **Apply**.

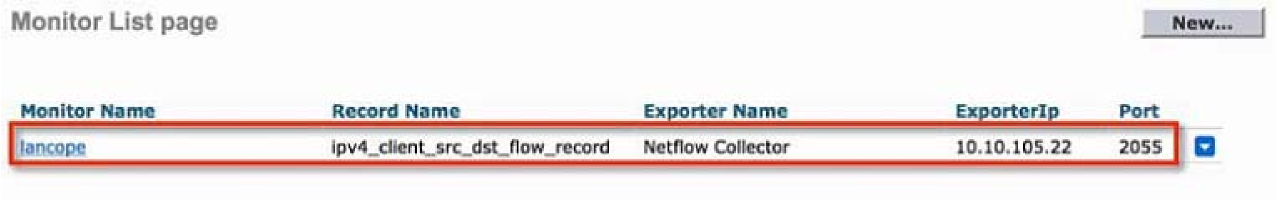


Netflow Monitor > Edit 'lancope'

Exporter name: Netflow Collector

Record Name: ipv4_client_src_dst_flow_record

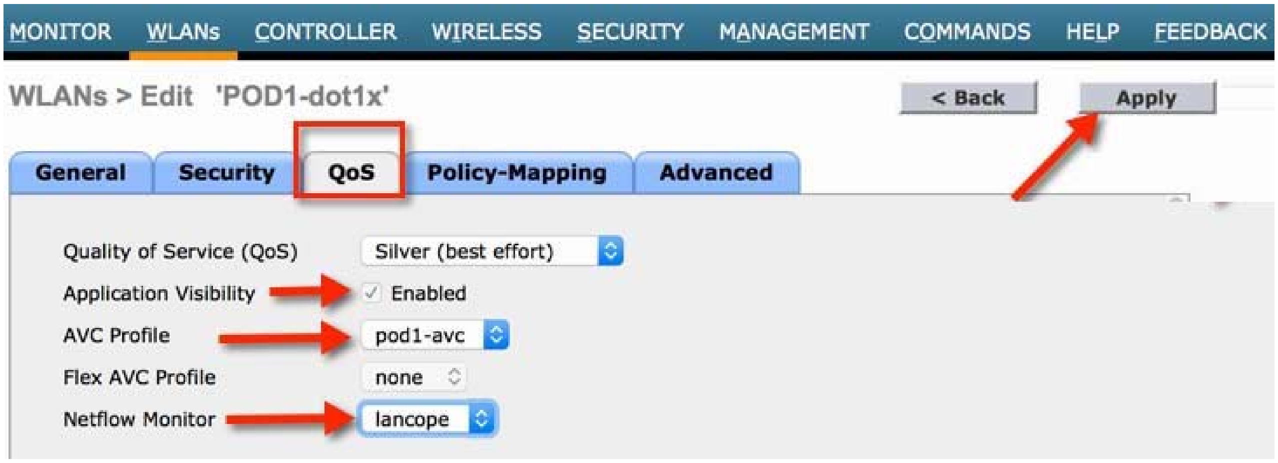
User should see the following under **Wireless> Netflow> Monitor**



Monitor List page

Monitor Name	Record Name	Exporter Name	ExporterIp	Port
lancope	ipv4_client_src_dst_flow_record	Netflow Collector	10.10.105.22	2055

7. Browse to the **WLAN** on which we need to enable AVC and Netflow Monitor. From the WLAN edit parameters, go to **QoS** tab and check **Application Visibility** box. Then select the **Netflow Monitor** and click **Apply**.



WLANs > Edit 'POD1-dot1x'

Quality of Service (QoS): Silver (best effort)

Application Visibility: ☑ Enabled

AVC Profile: pod1-avc

Flex AVC Profile: none

Netflow Monitor: lancope

Netflow Reporting

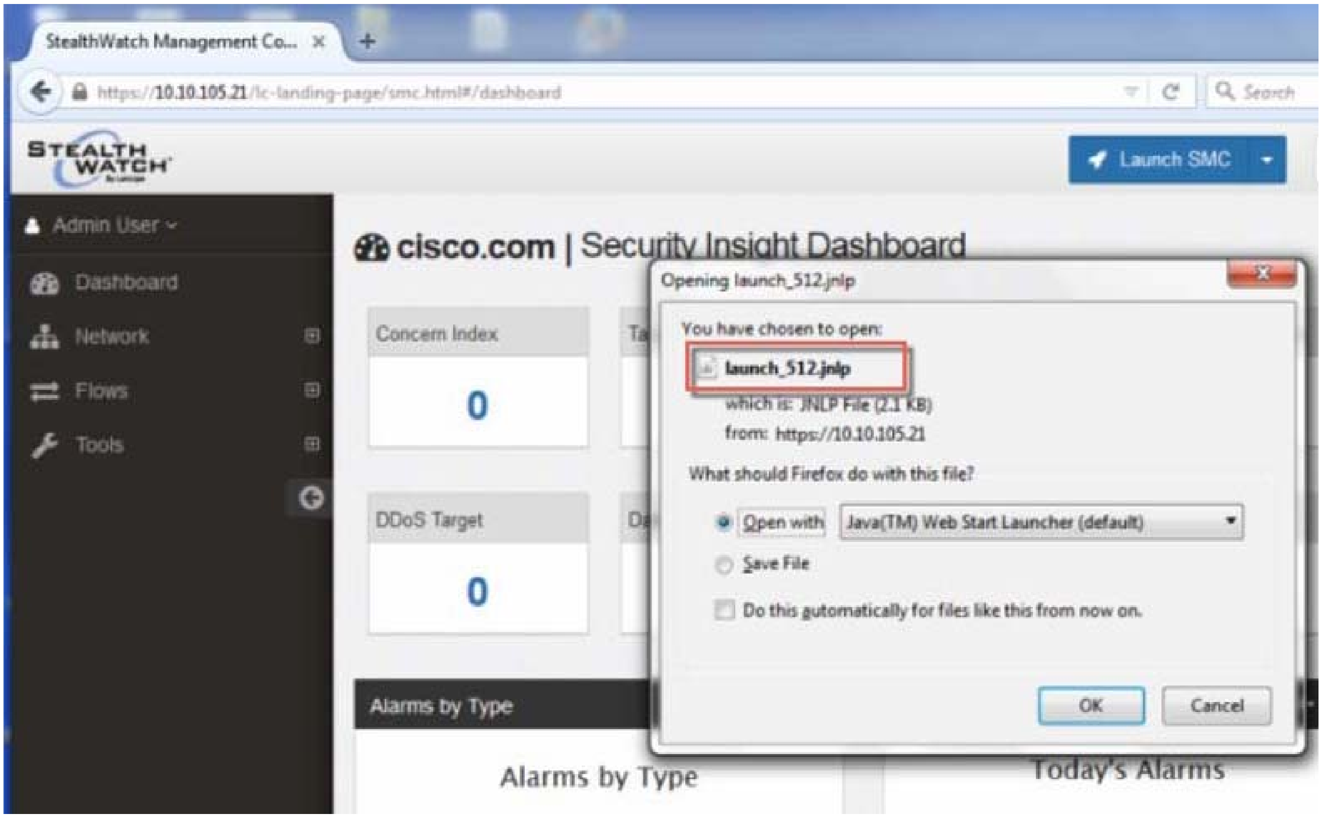
Stealthwatch Netflow reporting setup comprises of a flow collector and a central management console.

Stealthwatch FlowCollector collects data from various sources (in this case Wireless Lan Controller), analyzes them, creates a profile for normal activity and generates an alarm (to the SMC) for any activity that falls outside of the normal profile.

SMC manages, coordinates, and configures different components of the system through a web browser. It offers centralized management and reporting for up to 25 flow collectors with graphical charts for visualizing traffic.

Examples below illustrate FlowCollector residing at 10.10.105.22 (configured on the WLC above) and SMC at 10.10.105.21.

1. Log into SMC with username and password.
2. Click on " Launch SMC" from the dashboard. It will prompt you to download the Application " **launch_512**" .Save it locally and Launch it as shown above.



Opening launch_512.jnlp

You have chosen to open:

launch_512.jnlp

which is: JNLP File (2.1 KB)

from: https://10.10.105.21

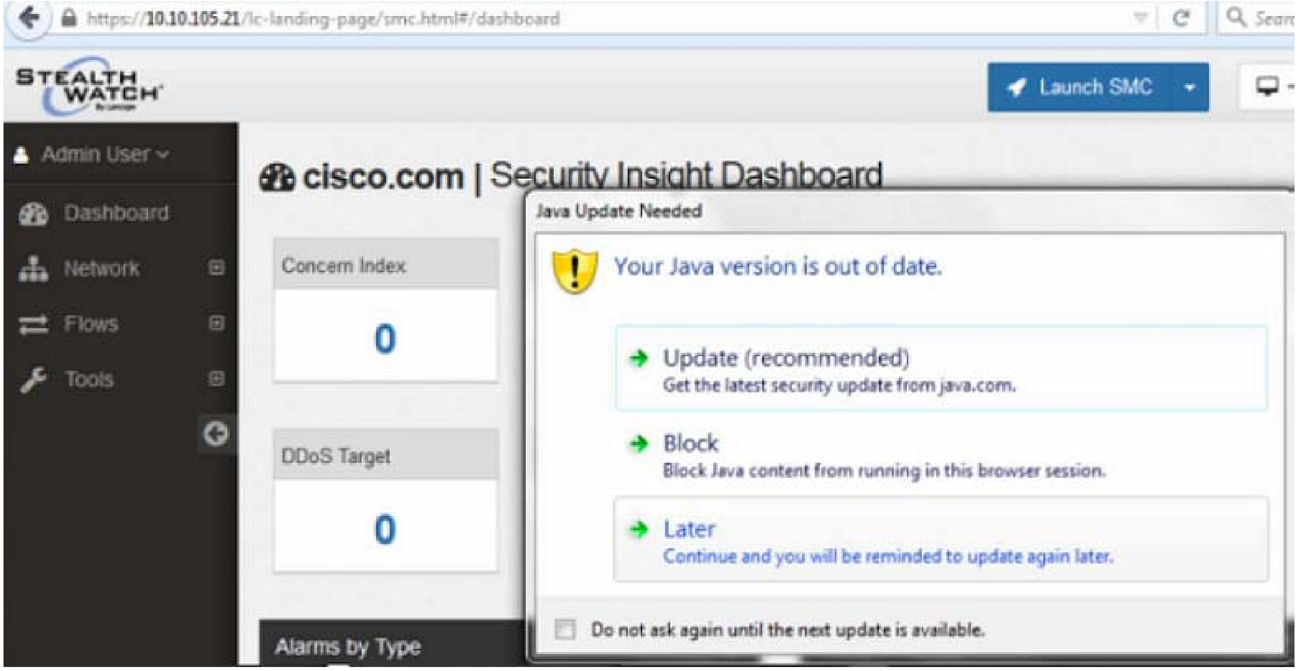
What should Firefox do with this file?

● Open with Java(TM) Web Start Launcher (default)

○ Save File

□ Do this automatically for files like this from now on.

3. Follow the steps as shown below when pop up window appears.



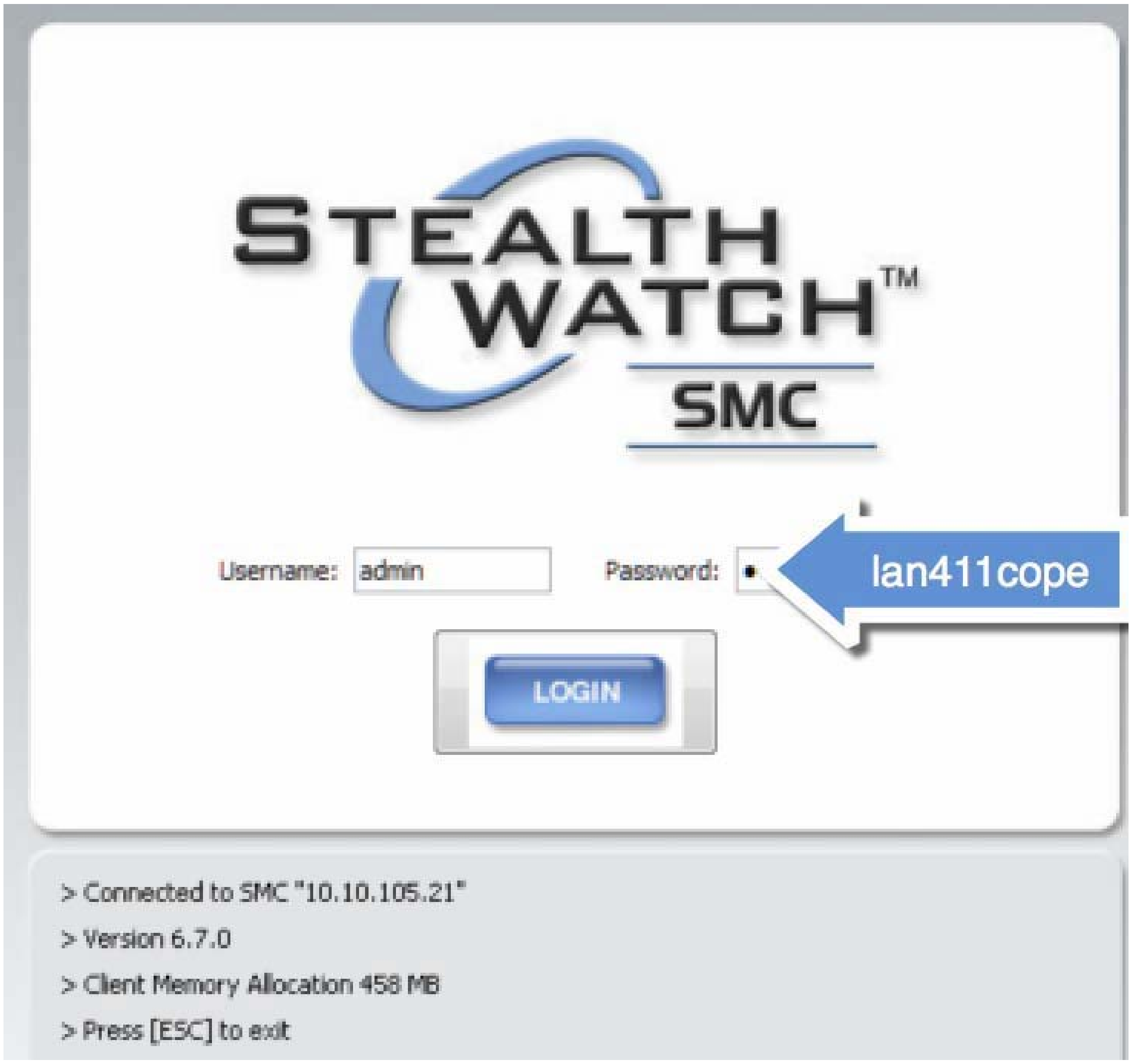
Java Update Needed

Your Java version is out of date.

- Update (recommended)
  Get the latest security update from java.com.
- Block
  Block Java content from running in this browser session.
- Later
  Continue and you will be reminded to update again later.

□ Do not ask again until the next update is available.

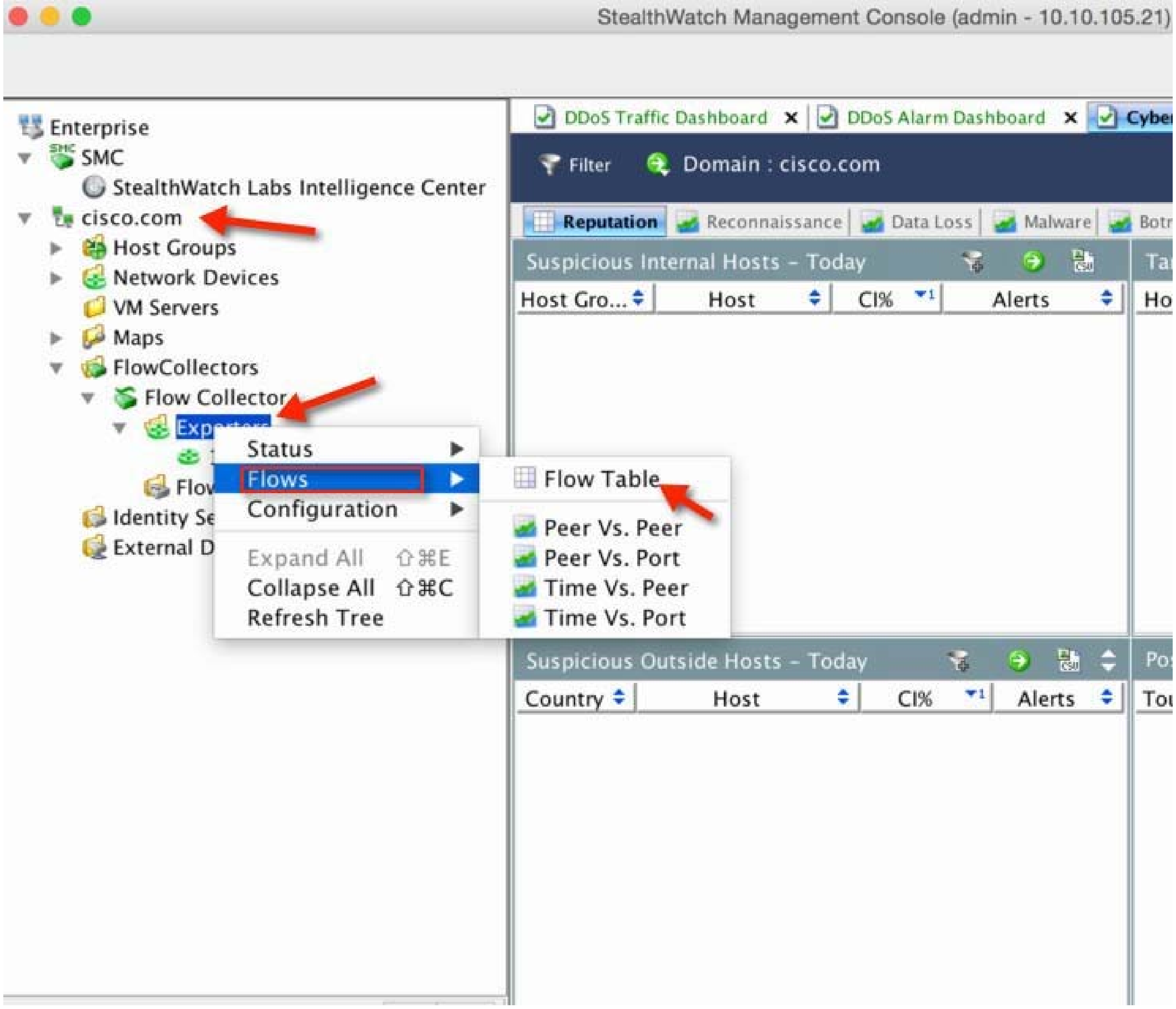
4. Continue Loading the Stealth Watch Monitor.



> Connected to SMC "10.10.105.21"
> Version 6.7.0
> Client Memory Allocation 458 MB
> Press [ESC] to exit

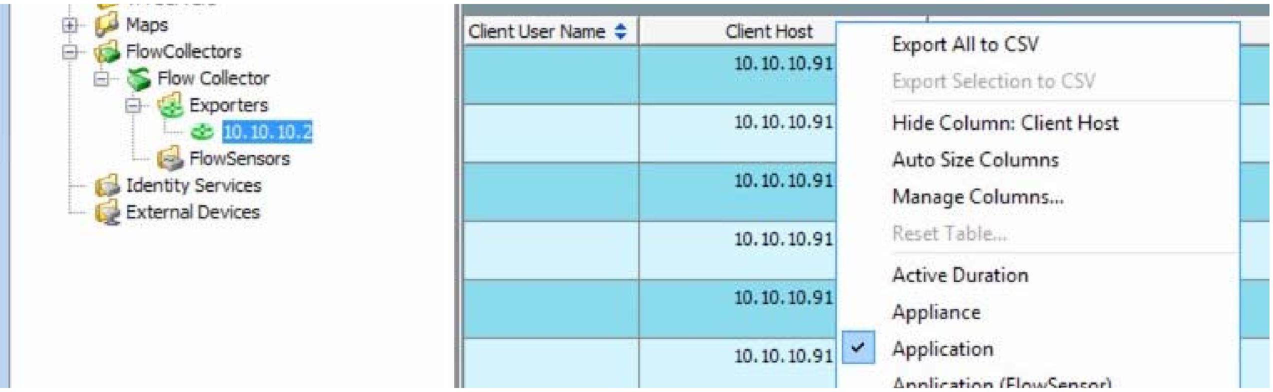
5. Finally Login to Stealthwatch Collector Monitor with credentials as per your setup.

6. From the dashboard, right click **Exporters-> <Controller IP> -> Flows-> Flow Table** to view client flows.



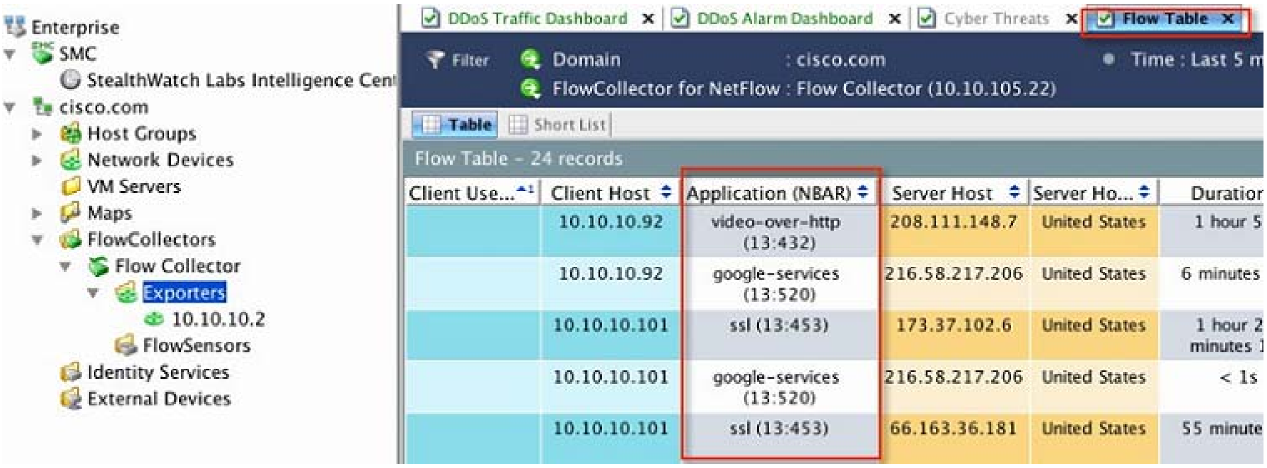
7. You will see multiple client flows here. You can filter the flows on various attributes by right clicking against a column name and selecting parameter/s as shown below. In the example illustrated below , WLC with IP address 10.10.10.2 is selected with Application (NBAR) attribute.

Note: In order to see the flows please make sure the clients are connected to the AVC and Netflow enabled SSID.



Client User Name	Client Host
	10.10.10.91
	10.10.10.91
	10.10.10.91
	10.10.10.91
	10.10.10.91
	10.10.10.91

If user is connected with dot1x credentials, they will also be visible on the Stealthwatch flow table dashboard



Domain : cisco.com
FlowCollector for NetFlow : Flow Collector (10.10.105.22)
Time : Last 5 m

Flow Table - 24 records

Client Use...	Client Host	Application (NBAR)	Server Host	Server Ho...	Duratior
	10.10.10.92	video-over-http (13:432)	208.111.148.7	United States	1 hour 5
	10.10.10.92	google-services (13:520)	216.58.217.206	United States	6 minutes
	10.10.10.101	ssl (13:453)	173.37.102.6	United States	1 hour 2 minutes 1
	10.10.10.101	google-services (13:520)	216.58.217.206	United States	< 1s
	10.10.10.101	ssl (13:453)	66.163.36.181	United States	55 minute

Note: If you are planning to upgrade the Protocol Pack file on the controller the latest Protocol Pack can be found at the link below

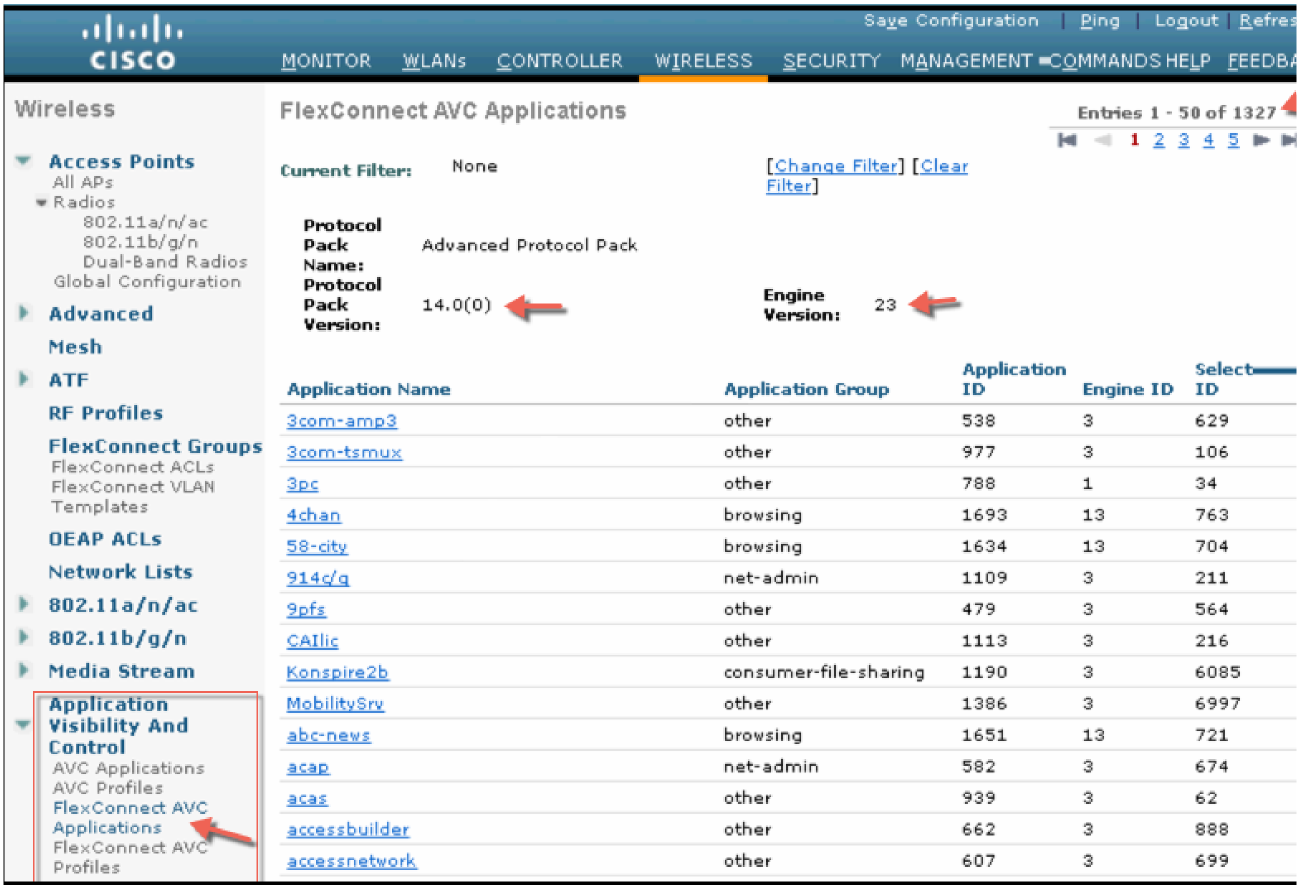
https://software.cisco.com/download/home/282600534/type/284509011/release/24.0.0

.

AVC–Phase 5 in CUWN Release 8.3

AVC in FlexConnect Mode ver 8.3

In release 8.3 ,the Protocol Pack and the NBAR engine got upgraded for Flex Connect Applications and now supports Protocol Pack 14 and NBAR engine 23 with a total support of the 1327 applications.



FlexConnect AVC Applications

Entries 1 - 50 of 1327

Current Filter: None [Change Filter] [Clear Filter]

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 14.0(0)

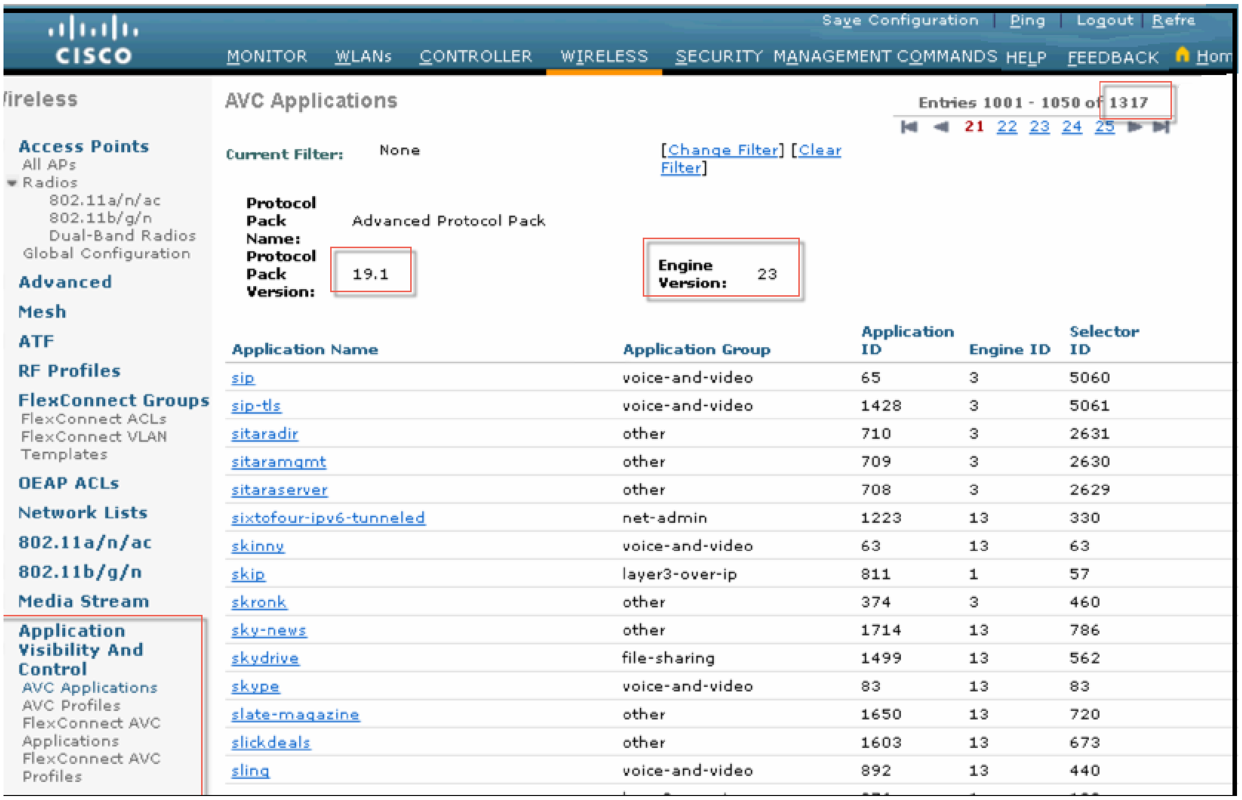
Engine Version: 23

Application Name	Application Group	Application ID	Engine ID	Selector ID
3com-amp3	other	538	3	629
3com-tsmux	other	977	3	106
3pc	other	788	1	34
4chan	browsing	1693	13	763
58-city	browsing	1634	13	704
914c/g	net-admin	1109	3	211
9pfs	other	479	3	564
CAIlic	other	1113	3	216
Konspire2b	consumer-file-sharing	1190	3	6085
MobilitySrv	other	1386	3	6997
abc-news	browsing	1651	13	721
acap	net-admin	582	3	674
acas	other	939	3	62
accessbuilder	other	662	3	888
accessnetwork	other	607	3	699

For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/Flex-7500/Flex_7500_DG.html#pgfId-131717.

Protocol Pack and NBAR Engine Update in rel 8.3

Up to release 8.3 NBAR Engine 23 is integrated in WLC for centralized AVC support, which supports Protocol Pack (PP) version-16. In release 8.3, the new and improved NBAR Engine 23 and Protocol Pack 19.1 are introduced. The new versions allow customers to classify up to1317 application like Skype, Jabber and other a with lot more reliability and higher precision and less impact on the controller performance. It is also important to note that Protocol Pack 19.1 requires NBAR engine 23 and will not work with the previous NBAR released version in the prior WLC releases. When PP version 19.1 is released and posted on CCO, it will operate with NBAR engine 23 or higher.



AVC Applications

Entries 1001 - 1050 of 1317

Current Filter: None

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 19.1

Engine Version: 23

Application Name	Application Group	Application ID	Engine ID	Selector ID
sip	voice-and-video	65	3	5060
sip-tls	voice-and-video	1428	3	5061
sitaradir	other	710	3	2631
sitaramgmt	other	709	3	2630
sitaraserver	other	708	3	2629
sixtofour-ipv6-tunneled	net-admin	1223	13	330
skinny	voice-and-video	63	13	63
skip	layer3-over-ip	811	1	57
skronk	other	374	3	460
sky-news	other	1714	13	786
skydrive	file-sharing	1499	13	562
skype	voice-and-video	83	13	83
slate-magazine	other	1650	13	720
slickdeals	other	1603	13	673
sling	voice-and-video	892	13	440

AVC–Phase 6 in CUWN Release 8.8

Prior to rel 8.8, WLC supported NBAR engine version 23 (3.16.3) and default protocol pack version 19.1. There a significant customer demand to support additional applications on the WLC especially the new Wi-Fi calling, Zoom etc. These new applications are supported in the protocol pack version 37. But the protocol pack 35 is not supported on NBAR engine 23 (3.16.3) thus, to support new PP 37 application for classification NBAR engine and protocol pack needs to be upgraded to latest version. In release 8.8 NBAR engine 31 and PP 37 are supported with Wave-2 APs.

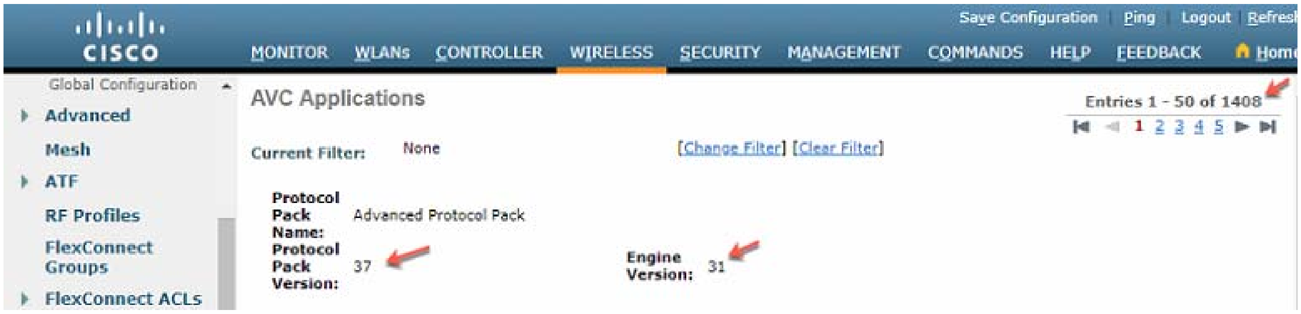
COS based Wave-2 AP will also be upgraded to support NBAR 31 and PP37 in FC mode.

IOS APs will not upgrade to the latest NBAR engine and protocol pack. So new applications will be shown as “UNKNOWN” for the FC deployed Wave-1 APs.

With release 8.8 only 3504, 5520, 8540 and vWLC support the latest PP37 and NBAR2 31 with Wave-2 APs 1800, 2800, 3800 and 4800 series.

Configurations Steps for AVC Enhancement

There is really no configuration steps required to load the latest NBAR engine or the protocol pack.



AVC Applications

Entries 1 - 50 of 1408

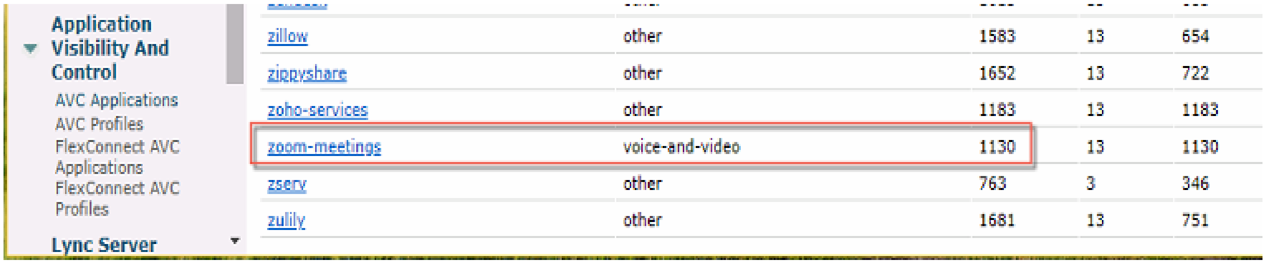
Current Filter: None

Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 37

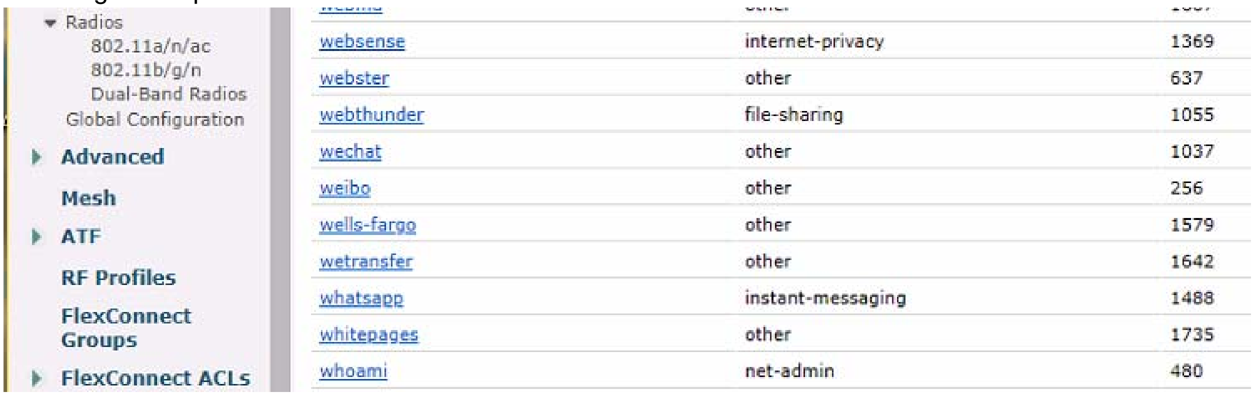
Engine Version: 31

Zoom Calling is now showing in the PP 37.



zillow	other	1583	13	654
zippyshare	other	1652	13	722
zoho-services	other	1183	13	1183
zoom-meetings	voice-and-video	1130	13	1130
zserv	other	763	3	346
zulily	other	1681	13	751

Wi-Fi Calling is also part of the PP37.



websense	internet-privacy	1369
webster	other	637
webthunder	file-sharing	1055
wechat	other	1037
weibo	other	256
wells-fargo	other	1579
wetransfer	other	1642
whatsapp	instant-messaging	1488
whitepages	other	1735
whoami	net-admin	480

Managing 8.8 AVC Features through CLI

CLI Output:

```
(Cisco Controller) >show avc protocol-pack version
AVC Protocol Pack Name: Advanced Protocol Pack
AVC Protocol Pack Version: 37
(Cisco Controller) >show avc engine version
AVC Engine Version: 31
(Cisco Controller) >
```

Default DSCP Value for AVC Profile Feature Overview

Prior to rel 8.8 with AVC enabled, we can no override all applications DSCP values only for Application flows configured on the AVC profile. Furthermore, the AVC profile can contain maximum 32 Applications rules.

For a flow where a rule is not configured in the AVC Profile, NO action is performed & DSCP is left intact. As it is, the AVC can't be used as PEP (Policy Enforcement Point).

For Managed Service, to control and rewrite DSCP values (example with DSCP 0) for all flows that are not presented on the AVC profile is not possible.

The new AVC enhancement allows a “default-class” rule to override the DSCP values for all application flows where AVC Rule is not configured. It is more like last rule with Any/Any conditions. The goal is to protect the network from all flows with unwanted/controlled DSCP values.

AVC at present supports Marking, Rate Limiting or Drop for any application it recognizes. AVC supports 32 Rules. For any applications which are not configured as part of these rules, no action will be taken.

For local mode, these rules are plumbed down to Data Plane. At the Data Plane, for those applications action will be taken including DSCP marking.

As part of the new feature in rel 8.8, “default rule” can be configured as part of the 32 Rules supported.

For any application which doesn’t match the existing rules, this “default rule” will be applied.

For Flex Connect AVC, we send App Name in the TLV Type TLV_FLEX_AVC_CLASS_MAP_APP_NAME_PAYLOAD along with APP ID in the TLV Type TLV_FLEX_AVC_CLASS_MAP_APP_ID_PAYLOAD.

In rel 8.8 enhancement will be made to support “default-class” Application Name and APP ID while sending to AP. AP also has to handle these values and correspondingly update the class map.

AVC Default DSCP Value Limitations in rel 8.8

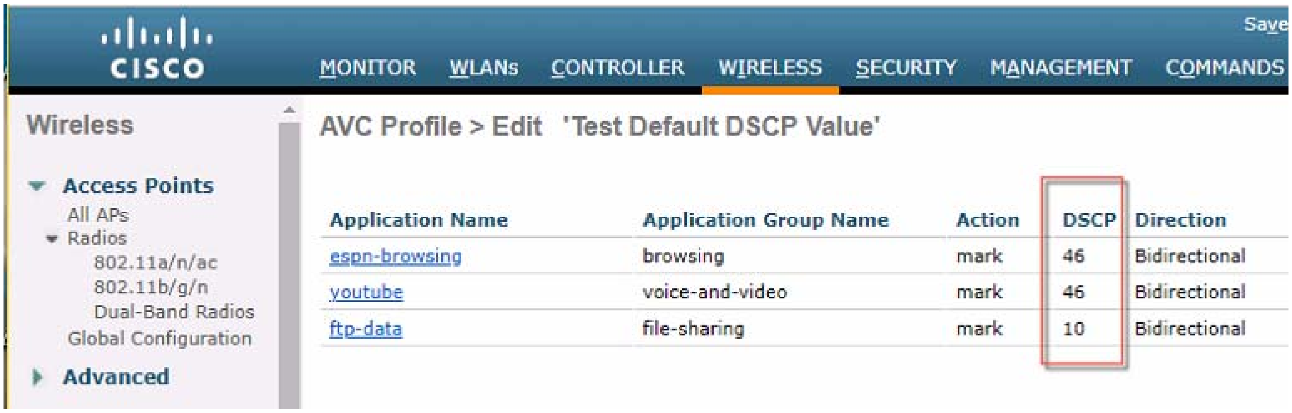
- Supported only Marking, Rate Limit or Drop is not supported.
- Default DSCP will work only when AVC is enabled.
- 32 Rules per profile supported, including “Default-class” Rule. If default Rule is configured than the user can configure only 31 Rules.
- “default-class" application name configured will not be shown in stats pages/CLI output.
- It will not be supported to Multicast and Broadcast flows.
- At present AVC doesn’t support IPv6
- AVC doesn’t allow cascading for Rules, means for same flow we can’t have Rate Limiting and Marking. Hence if for a flow where Rate Limiting is done, for that flow “default” Marking will not happen.

Note: “default-class” setting will overwrite all DSCP values for all not configured application when the profile is applied to the WLAN.

Configurations Steps for Default DSCP setting

Follow steps for creating, configuring AVC profiles and applying them to the WLAN as desribed in the previous sections of this deployment guide and then after creating AVC profiles please follow the steps below.

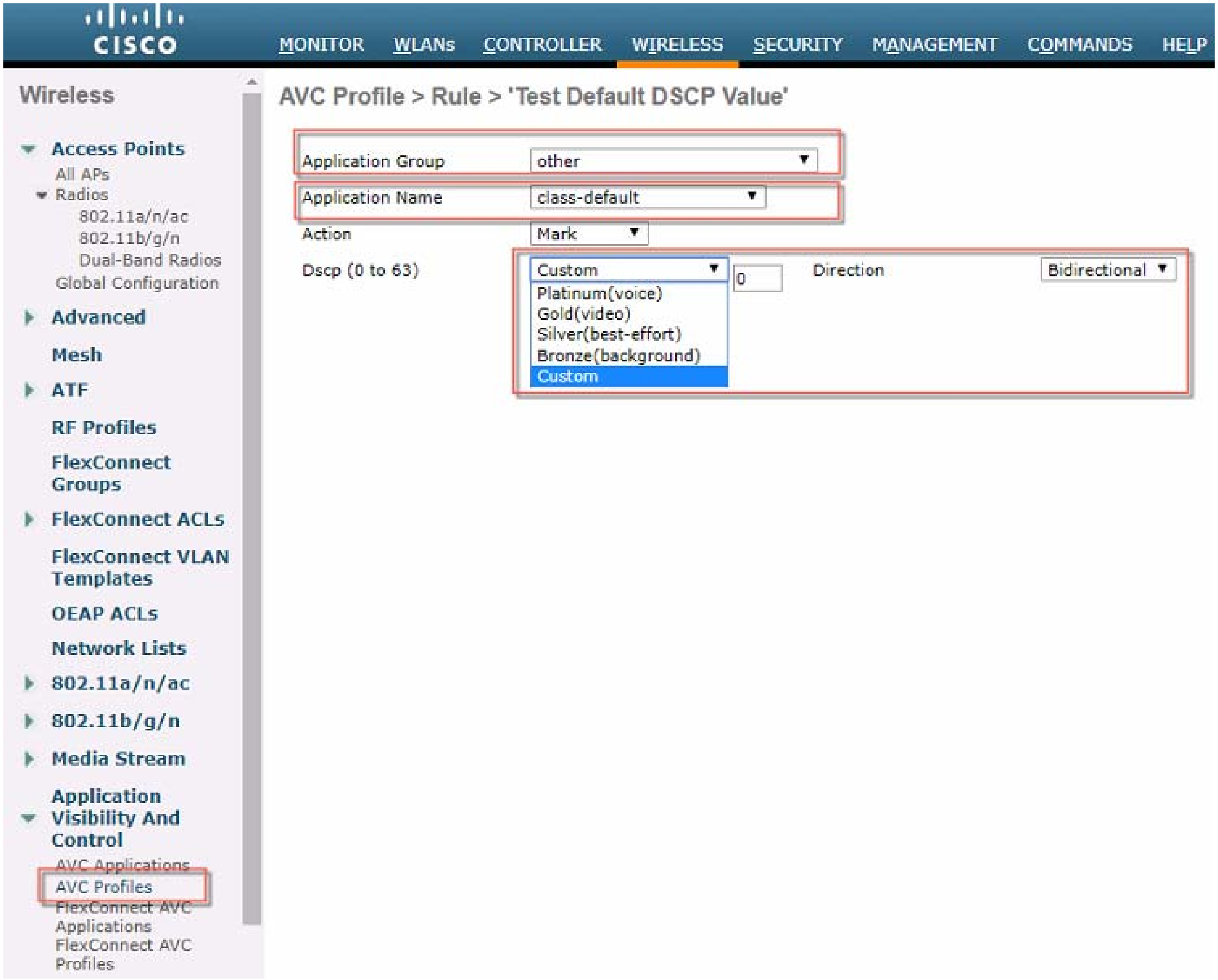
1. After creating an AVC profile you should have something as in the example below:



AVC Profile > Edit 'Test Default DSCP Value'

Application Name	Application Group Name	Action	DSCP	Direction
espn-browsing	browsing	mark	46	Bidirectional
youtube	voice-and-video	mark	46	Bidirectional
ftp-data	file-sharing	mark	10	Bidirectional

2. To add a default-class application, create a new rule from application group " other" and application name " class-default" and at the same time select a DSCP action desired or configure a custom DSCP value as shown in the example below.



AVC Profile > Rule > 'Test Default DSCP Value'

Application Group: other

Application Name: class-default

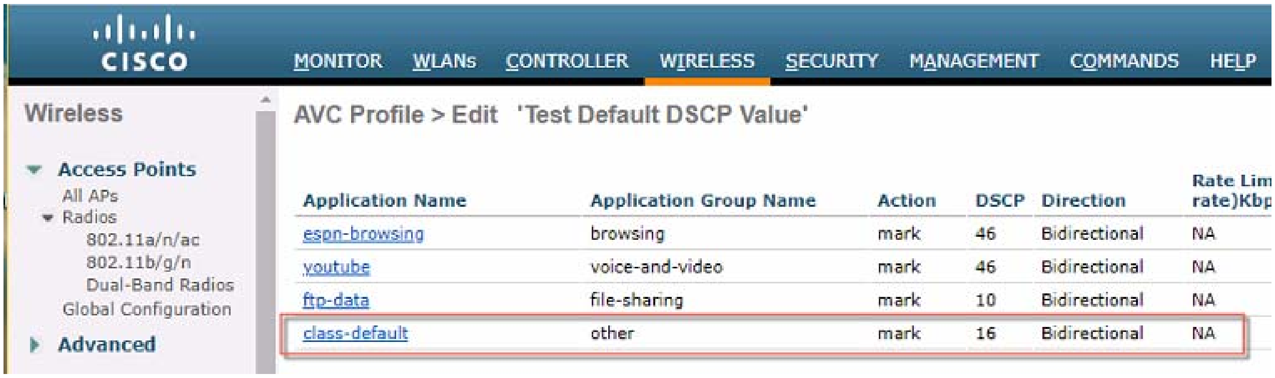
Action: Mark

Dscp (0 to 63): Custom 0

Direction: Bidirectional

Note: Same applies to the AVC profiles created for the Flex Connect mode.

3. Apply the newly created rule to the Profile and you will see it appear now in the profile.



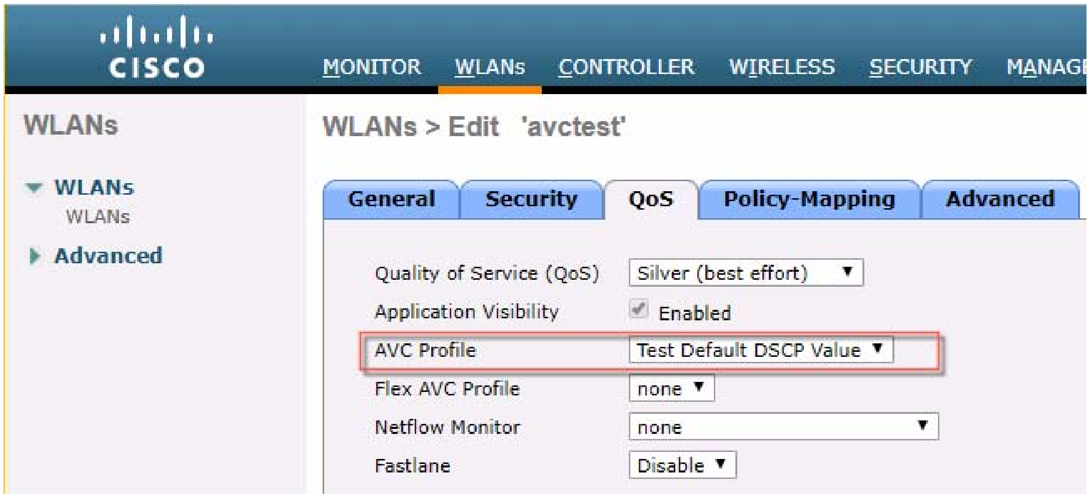
AVC Profile > Edit 'Test Default DSCP Value'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Lim rate)Kbp
espn-browsing	browsing	mark	46	Bidirectional	NA
youtube	voice-and-video	mark	46	Bidirectional	NA
ftp-data	file-sharing	mark	10	Bidirectional	NA
class-default	other	mark	16	Bidirectional	NA

The existing application list will be appended with “class-default” application.

GUI will automatically show it.

4. Apply the newly created profile to the WLAN, as shown in the example below the profile created applied to the WLAN "avctest"



WLANs > Edit 'avctest'

Quality of Service (QoS) Silver (best effort)
Application Visibility ☑ Enabled
AVC Profile Test Default DSCP Value
Flex AVC Profile none
Netflow Monitor none
Fastlane Disable

Default DSCP CLI Configuration command:

Create an AVC profile with application name "class-default"

```
# config avc profile <profile_name> rule add application <application name> mark <dscp>
```

Show command Changes:

```
# show avc profile detailed <profile_name>
Application-Name          Application-Group-Name           Action      DSCP    DIR   AVG-RATELIMIT
BURST-RATELIMIT
  ================          =======================           ======      ====   ===== =============
=============
 default       -                              Mark      46
```

Example Config Command:

```
(Cisco Controller) >config avc profile temp rule add application class-default mark 16
(Cisco Controller) >show avc profile detailed temp
Application-Name  Application-Group-Name  Action DSCP  DIR  AVG-RATELIMIT -RATELIMIT  ================
=======================           ======     ====   ===== =
telnet                    net-admin                            Mark      7 Bidirectional
 ping                      net-admin                            Mark      6 Bidirectional
class-default             other                                Mark     16 Bidirectional
Associated WLAN IDs       :
Associated Remote LAN IDs :
Associated Guest LAN IDs  :
(Cisco Controller) >
```

Application Visibility and Control for FlexConnect rel 8.1-8.8

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and WLC platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following components:

- Next-generation Deep Packet Inspection (DPI) technology, called as Network Based Application Recognition (NBAR2), allows for identification and classification of applications. 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 that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS), and Access Control List (ACL), which can take action based on this classification.
- Ability to Apply Mark using QoS, Drop and Rate-limit applications.

The key use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator 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.

AVC is supported on the 5520, 8540, 2500, 5508, 7500, 8500, and WiSM2 controllers on Local and FlexConnect modes (for WLANs configured for central switching only) since release 7.4. Release 8.1 introduces support for Application Visibility and Control for locally switched WLANs on FlexConnect APs on 5508, 7500, 75100, WiSM2, and vWLC.

- In release 8.3 the Protocol Pack and the NBAR engine got upgraded for Flex Connect Applications and now supports Protocol Pack 14 and NBAR engine 23 with a total support of the 1327 applications.
- In release 8.8 the Protocol Pack and the NBAR engine got upgraded for Flex Connect Applications and now supports Protocol Pack 37 and NBAR engine 31 with a total support of the 1408 applications.

Begin with release 8.6 AVC is supported on 3504, 5520 and 8540 series controllers and vWLC also supports AVC for FC mode only.

Note: For AVC Phase -6 release 8.8 The latest NBAR2 and Protocol Packs are supported on the 3504, 5520 and 8540 series controllers and vWLC supports AVC for Flex Connect APs only. The PP in rel 8.8 only supports Wave-2 COS based APs.

AVC Facts and Limitations

AVC on the FlexConnect AP can classify and take action on 1000+ different applications.

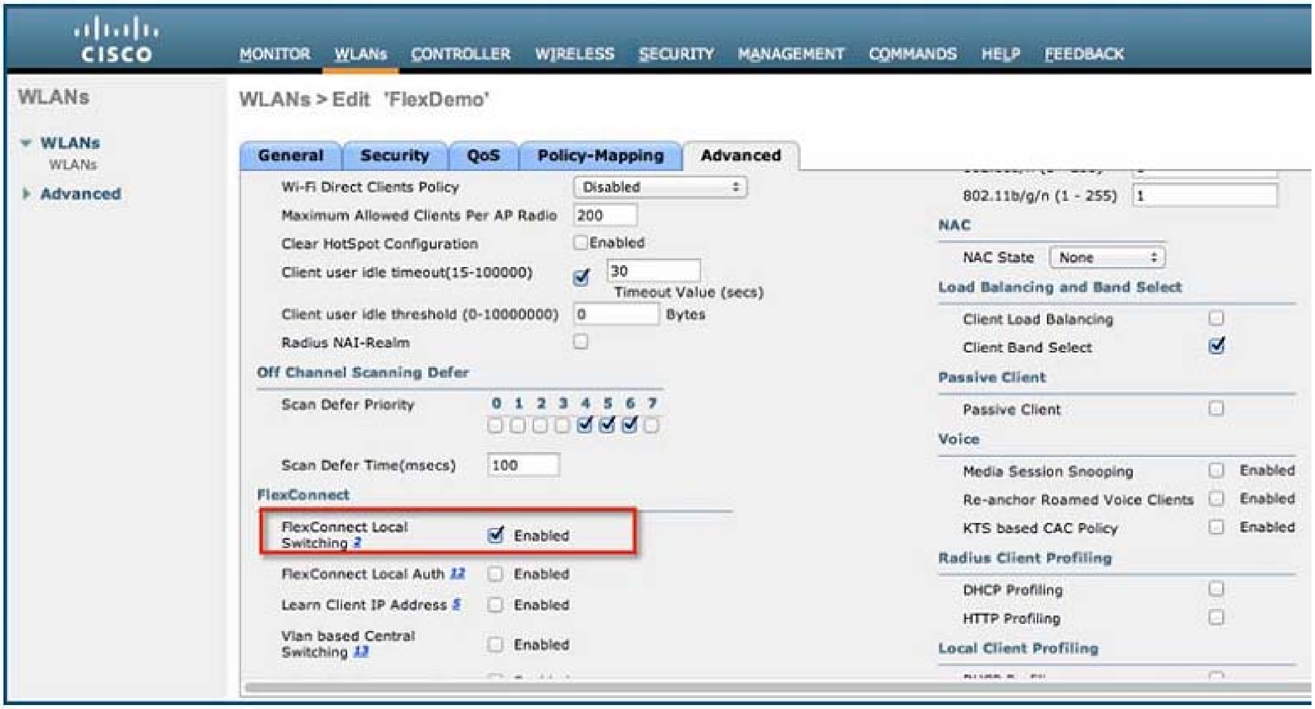
- The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- Intra FlexConnect Group roaming support.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- Multicast traffic is not supported by AVC application.
- Netflow export for FlexConnect AVC is not supported

Configuring Application Visibility

To configure the application visibility, perform these steps:

1. Open a web browser on the wired laptop, and then enter your WLC IP Address.
2. Create an OPEN WLAN with naming convention, for example, “FlexDemo”.

3. Enable FlexConnect Local Switching on the WLAN and then click Apply.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced

WLANs > Edit 'FlexDemo'

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Clear HotSpot Configuration: □ Enabled

Client user idle timeout(15-100000): ☑ 30 Timeout Value (secs)

Client user idle threshold (0-10000000): 0 Bytes

Radius NAI-Realm: □

Off Channel Scanning Defer

Scan Defer Priority: 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □

Scan Defer Time(msecs): 100

FlexConnect

FlexConnect Local Switching 2: ☑ Enabled

FlexConnect Local Auth 12: □ Enabled

Learn Client IP Address 5: □ Enabled

Vlan based Central Switching 13: □ Enabled

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

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing: □

Client Band Select: ☑

Passive Client

Passive Client: □

Voice

Media Session Snooping: □ Enabled

Re-anchor Roamed Voice Clients: □ Enabled

KTS based CAC Policy: □ Enabled

Radius Client Profiling

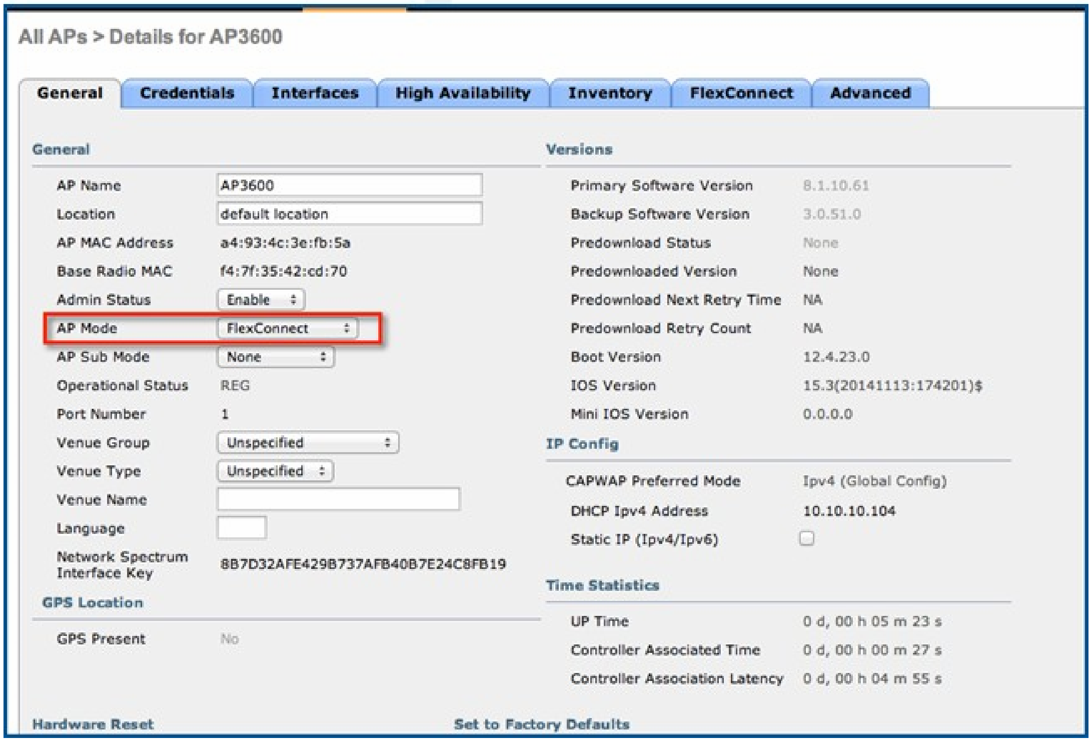
DHCP Profiling: □

HTTP Profiling: □

Local Client Profiling

4. Make sure that the APs connected to this WLAN are among the list of supported access points for this feature.

5. Convert the AP to FlexConnect mode by selecting FlexConnect in the AP Mode drop-down menu, and then click **Apply.** The mode changes to FlexConnect without a reboot.


General Credentials Interfaces High Availability Inventory FlexConnect Advanced
Hardware Reset
Set to Factory Defaults

All APs > Details for AP3600

General

AP Name: AP3600

Location: default location

AP MAC Address: a4:93:4c:3e:fb:5a

Base Radio MAC: f4:7f:35:42:cd:70

Admin Status: Enable

AP Mode: FlexConnect

AP Sub Mode: None

Operational Status: REG

Port Number: 1

Venue Group: Unspecified

Venue Type: Unspecified

Venue Name:

Language:

Network Spectrum Interface Key: 8B7D32AFE429B737AFB40B7E24C8FB19

GPS Location

GPS Present: No

Versions

Primary Software Version: 8.1.10.61

Backup Software Version: 3.0.51.0

Predownload Status: None

Predownloaded Version: None

Predownload Next Retry Time: NA

Predownload Retry Count: NA

Boot Version: 12.4.23.0

IOS Version: 15.3(20141113:174201)$

Mini IOS Version: 0.0.0.0

IP Config

CAPWAP Preferred Mode: Ipv4 (Global Config)

DHCP Ipv4 Address: 10.10.10.104

Static IP (Ipv4/Ipv6): □

Time Statistics

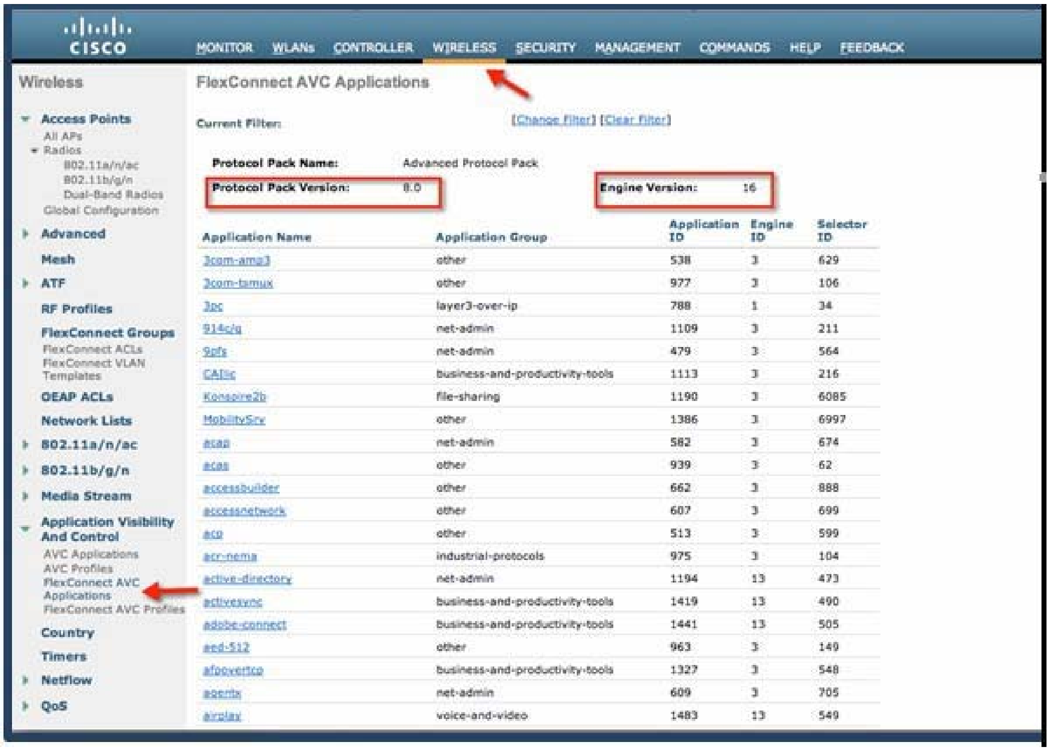
UP Time: 0 d, 00 h 05 m 23 s

Controller Associated Time: 0 d, 00 h 00 m 27 s

Controller Association Latency: 0 d, 00 h 04 m 55 s

6. Create a FlexConnect Group and add the AP to the FlexConnect Group. In the following example, “FlexGroup” is the FlexConnect Group and the access point AP3600 is added to it.

7. Applications that can be identified, classified, and controlled are listed under **Wireless > Application Visibility and Control > FlexConnect AVC Applications**. The access points support Protocol Pack version 8.0 and NBAR engine version 16.



FlexConnect AVC Applications

Current Filter:

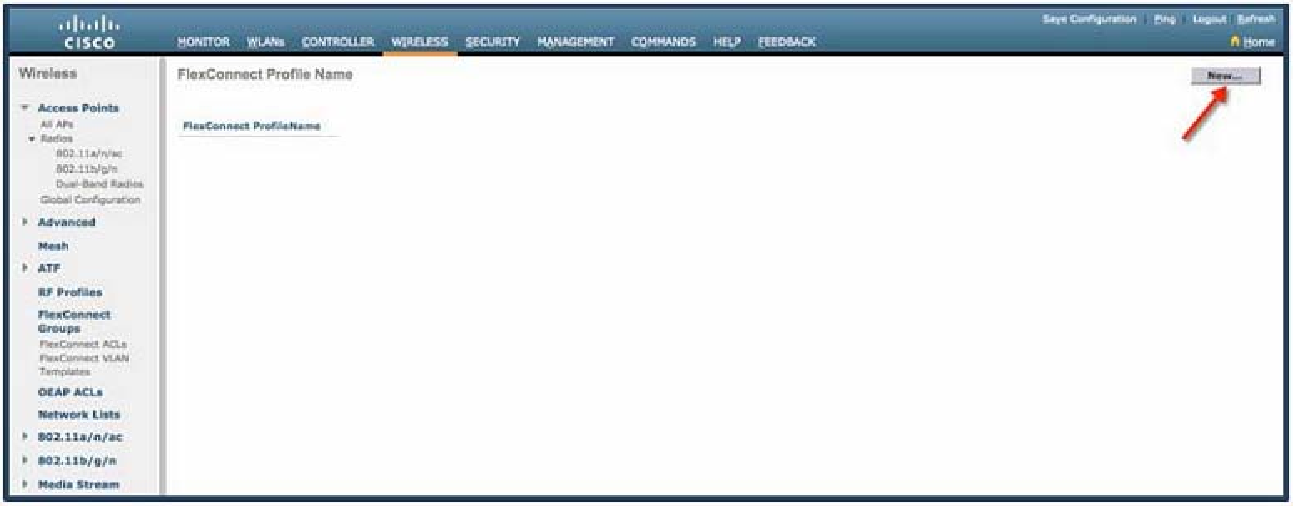
Protocol Pack Name: Advanced Protocol Pack

Protocol Pack Version: 8.0

Engine Version: 16

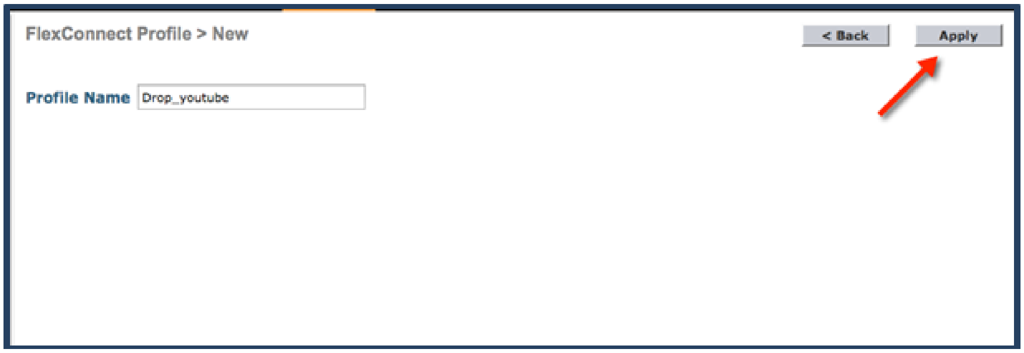
Application Name	Application Group	Application ID	Engine ID	Selector ID
3com-amp3	other	538	3	629
3com-tsmux	other	977	3	106
3pc	layer3-over-ip	788	1	34
914c/g	net-admin	1109	3	211
9pfs	net-admin	479	3	564
CAIlic	business-and-productivity-tools	1113	3	216
Konspire2b	file-sharing	1190	3	6085
MobilitySrv	other	1386	3	6997
acap	net-admin	582	3	674
acas	other	939	3	62
accessbuilder	other	662	3	888
accessnetwork	other	607	3	699
acp	other	513	3	599
acr-nema	industrial-protocols	975	3	104
active-directory	net-admin	1194	13	473
activesync	business-and-productivity-tools	1419	13	490
adobe-connect	business-and-productivity-tools	1441	13	505
aed-512	other	963	3	149
afpovertcp	business-and-productivity-tools	1327	3	548
agentx	net-admin	609	3	705
airplay	voice-and-video	1483	13	549

8. Create an AVC profile under **Wireless > Application Visibility and Control > FlexConnect AVC Profiles > New** with name “Drop_youtube”. And then Click **Apply**.



FlexConnect Profile Name

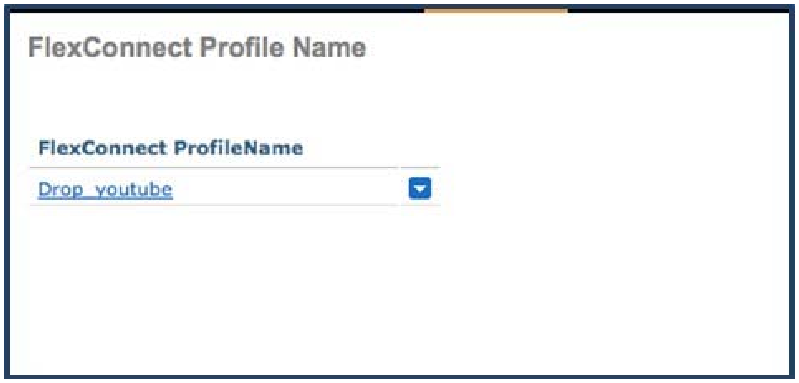
FlexConnect ProfileName



FlexConnect Profile > New

Profile Name: Drop_youtube

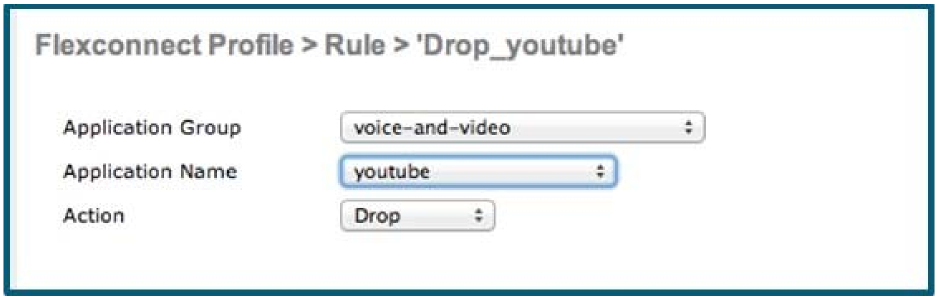
The AVC profile is created with the new name “Drop_youtube”.



FlexConnect Profile Name

FlexConnect ProfileName
Drop_youtube

9. Click the Profile name and then click **Add New Rule.** Select the **Application Group, Application Name**, and **Action**, and then click **Apply**.



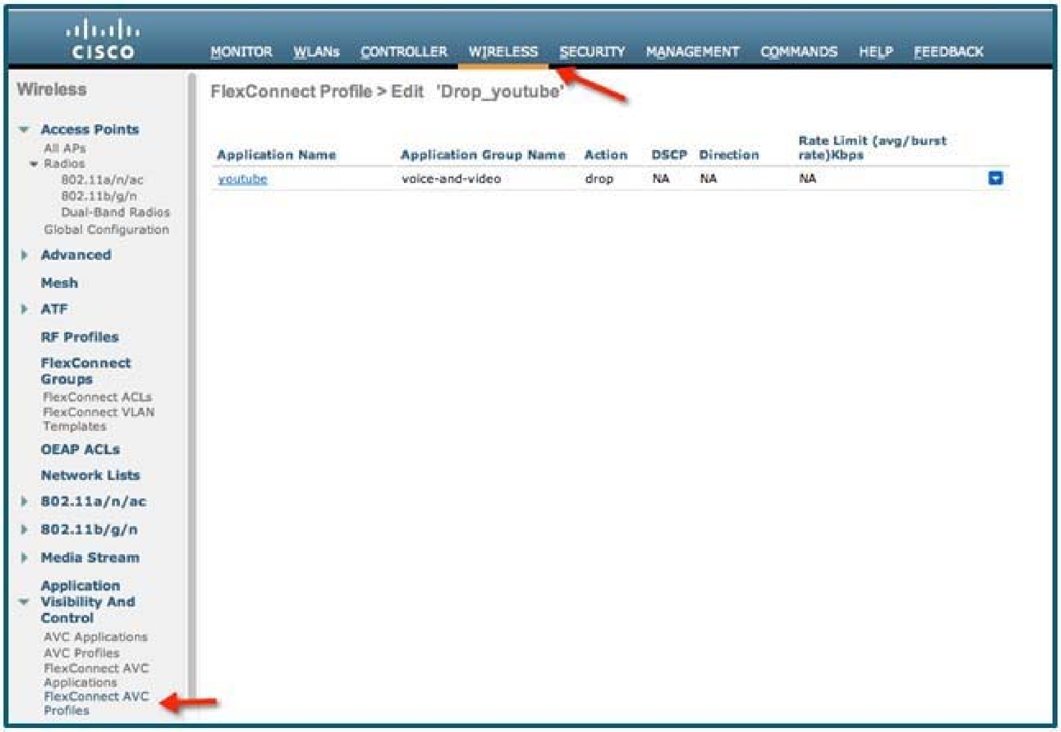
Flexconnect Profile > Rule > 'Drop_youtube'

Application Group: voice-and-video

Application Name: youtube

Action: Drop

10. Verify that the rule is added as shown in the following figure.

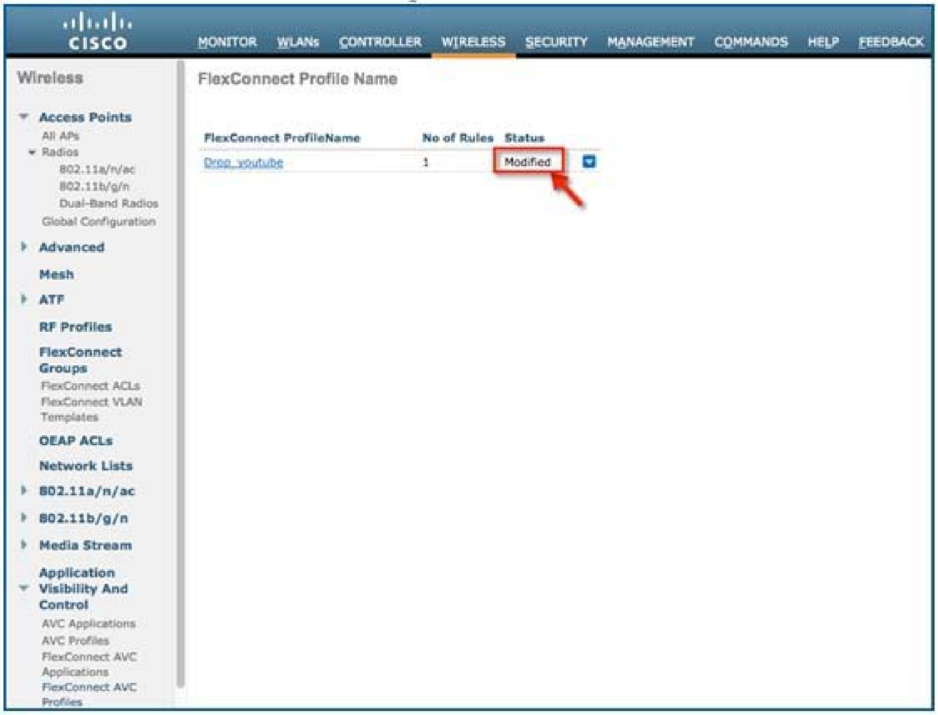


FlexConnect Profile > Edit 'Drop_youtube'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
youtube	voice-and-video	drop	NA	NA	NA

The status of the FlexConnect AVC profile at this point is **Modified.**

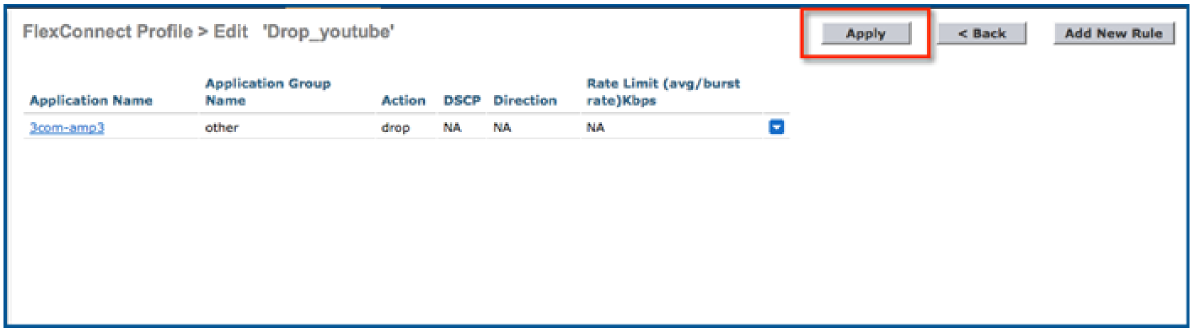
11. Select the profile and click **Apply** for the profile to be applied and to take effect.



FlexConnect Profile Name

FlexConnect ProfileName	No of Rules	Status
Drop_youtube	1	Modified

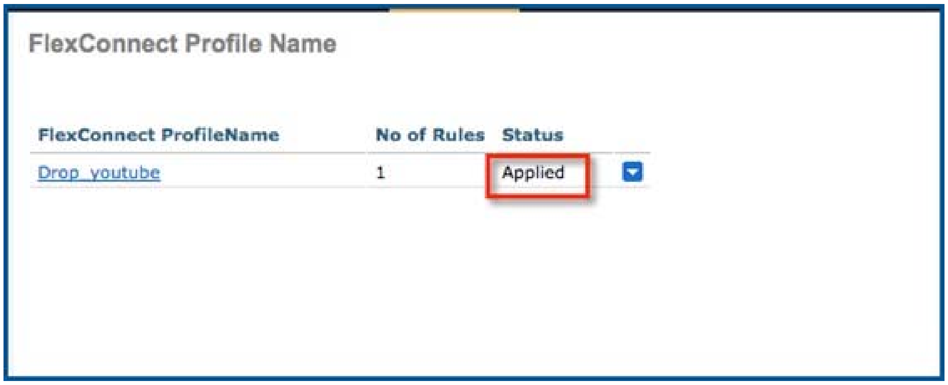
12. Select the profile and click **Apply** for the profile to be applied and to take effect.



FlexConnect Profile > Edit 'Drop_youtube'

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
3com-amp3	other	drop	NA	NA	NA

The status of the FlexConnect AVC profile is changed to **Applied**.

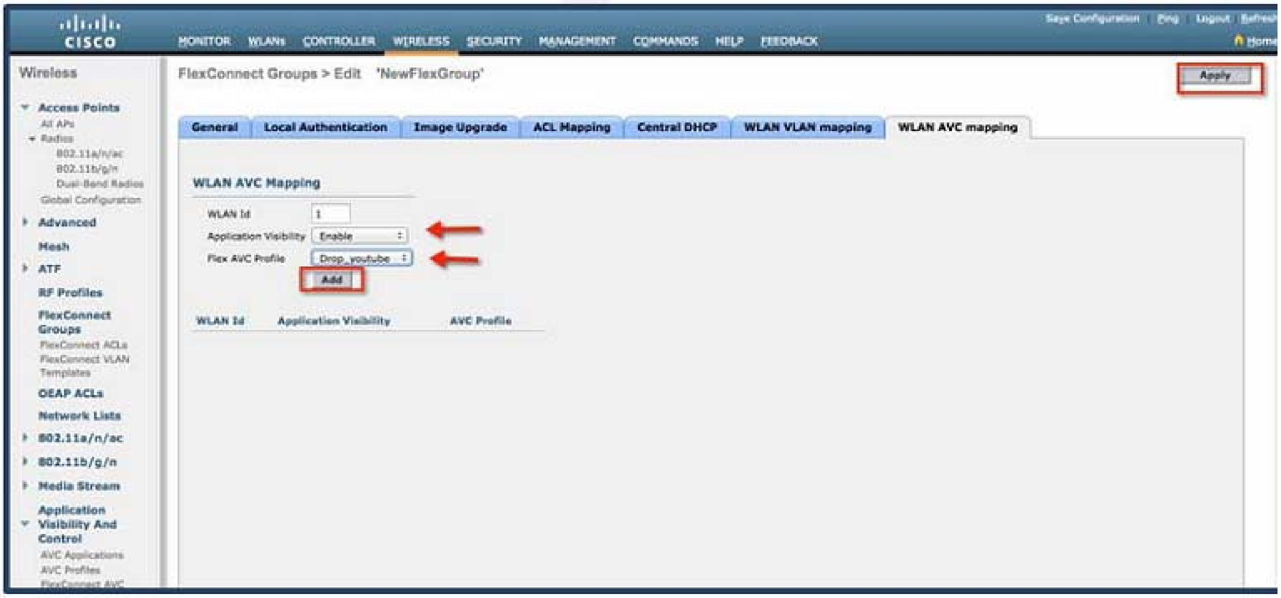


FlexConnect Profile Name

FlexConnect ProfileName	No of Rules	Status
Drop_youtube	1	Applied

13. Enable Application Visibility on the FlexConnect group under **Wireless > FlexConnect Group > FlexConnect Group name > WLAN AVC Mapping** by selecting the WLAN ID and choosing Enable from the drop-down menu.

14. Apply the FlexConnect AVC profile by selecting the profile created in the previous set from the Flex AVC Profiledrop-down menu. Click **Add** and then click **Apply**.



FlexConnect Groups > Edit 'NewFlexGroup'

WLAN AVC Mapping

WLAN Id: 1

Application Visibility: Enable

Flex AVC Profile: Drop_youtube

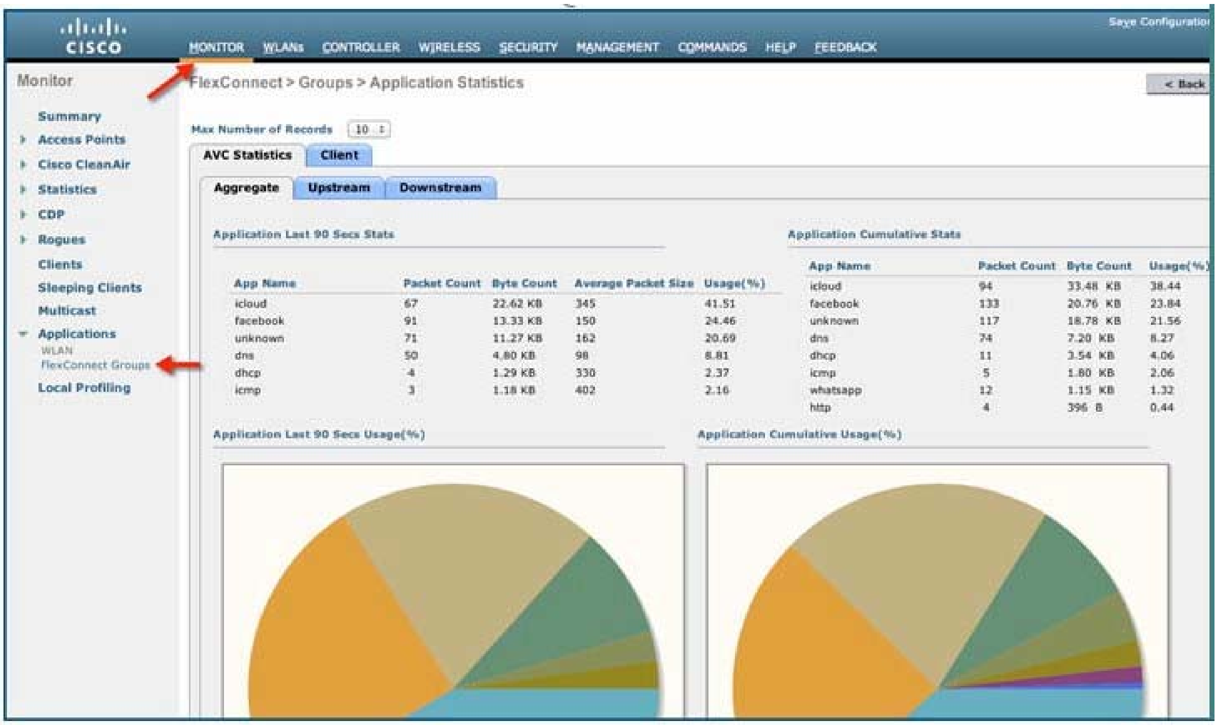
WLAN Id	Application Visibility	AVC Profile

15. Once AVC is enabled on the FlexConnect Group, from the associated wireless client, start different types of traffic using the applications (already installed) such as Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, Ping, Trace route, and so on.

Once traffic is initiated from the wireless client, visibility of different traffic can be observed on a per FlexConnect Group and per client basis. This provides the administrator a good overview of the network bandwidth utilization and type of traffic in the network per client and per branch site

16. To check the visibility globally for all WLANs on a FlexConnect Group, click **Monitor > Applications > FlexConnect > FlexConnect Groups** and then select the FlexConnect group created earlier.

The following screen is visible which lists aggregate data for the top 10 applications running on that particular FlexConnect group.



FlexConnect > Groups > Application Statistics

Max Number of Records 10

Application Last 90 Secs Stats

App Name	Packet Count	Byte Count	Average Packet Size	Usage(%)
icloud	67	22.62 KB	345	41.51
facebook	91	13.33 KB	150	24.46
unknown	71	11.27 KB	162	20.69
dns	50	4.80 KB	98	8.81
dhcp	4	1.29 KB	330	2.37
icmp	3	1.18 KB	402	2.16

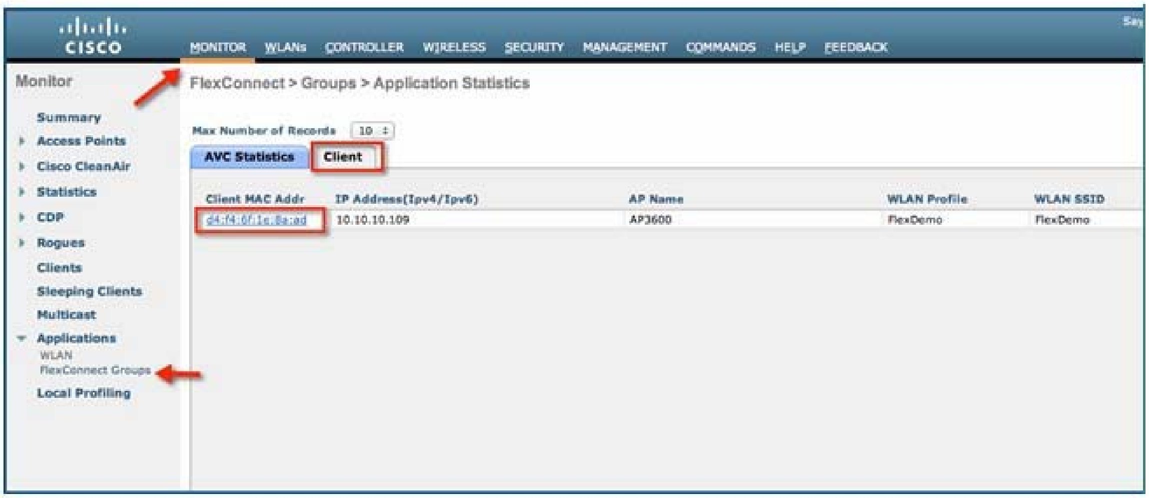
Application Cumulative Stats

App Name	Packet Count	Byte Count	Usage(%)
icloud	94	33.48 KB	38.44
facebook	133	20.76 KB	23.84
unknown	117	18.78 KB	21.56
dns	74	7.20 KB	8.27
dhcp	11	3.54 KB	4.06
icmp	5	1.80 KB	2.06
whatsapp	12	1.15 KB	1.32
http	4	396 B	0.44

This page provides more granular visibility per FlexConnect Group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect Group from the same page by clicking the Upstream and Downstream tabs.

Note: The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the Max Number of Records field on this page. The default value is 10.

17. To have more granular visibility of the top 10 applications per client on a particular locally switched WLAN where AVC visibility is enabled, click **Monitor > Applications > FlexConnect Group > FlexConnect Group name > Clients**. Then, click any individual client MAC entry listed on that page.

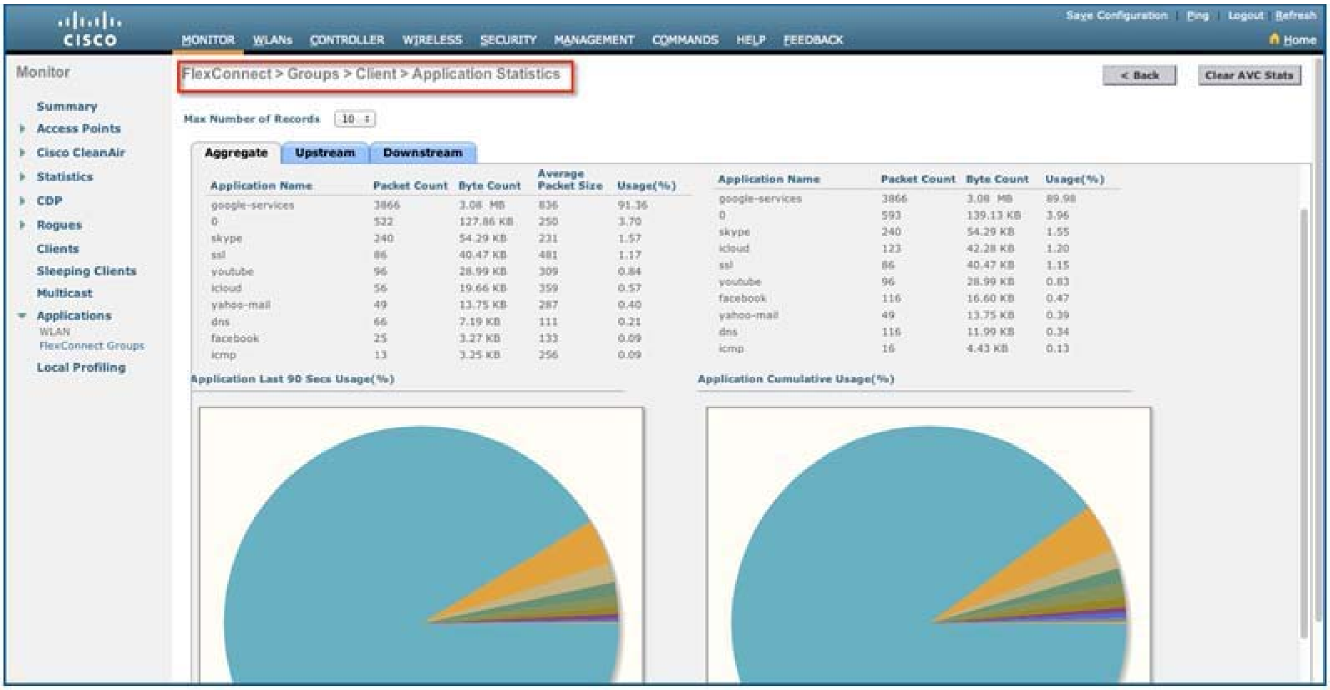


FlexConnect > Groups > Application Statistics

Max Number of Records 10

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID
d4:f4:6f:1e:8a:ad	10.10.10.109	AP3600	FlexDemo	FlexDemo

After clicking on an individual client MAC entry, the client details page appears.



FlexConnect > Groups > Client > Application Statistics

Max Number of Records 10

Application Name	Packet Count	Byte Count	Average Packet Size	Usage(%)
google-services	3866	3.08 MB	836	91.36
0	522	127.86 KB	250	3.70
skype	240	54.29 KB	231	1.57
ssl	86	40.47 KB	481	1.17
youtube	96	28.99 KB	309	0.84
icloud	56	19.66 KB	359	0.57
yahoo-mail	49	13.75 KB	287	0.40
dns	66	7.19 KB	111	0.21
facebook	25	3.27 KB	133	0.09
icmp	13	3.25 KB	256	0.09

Application Name	Packet Count	Byte Count	Usage(%)
google-services	3866	3.08 MB	89.98
0	593	139.13 KB	3.96
skype	240	54.29 KB	1.55
icloud	123	42.28 KB	1.20
ssl	86	40.47 KB	1.15
youtube	96	28.99 KB	0.83
facebook	116	16.60 KB	0.47
yahoo-mail	49	13.75 KB	0.39
dns	116	11.99 KB	0.34
icmp	16	4.43 KB	0.13

This page provides further granular stats per client associated on locally switched WLANs, where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group as in this example. The page lists the top 10 applications in last the 90 seconds as well as cumulative stats for top 10 applications.

18. You can view upstream and downstream stats individually per client from the same page by clicking the **Upstream** and **Downstream** tabs

.**Note:** The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the **Max Number of Records Field** on this page. The default value is 10.

19. You can clear the AVC stats for the particular client by clicking the Clear AVC Stats button.

Now, if you open YouTube, from wireless clients, you will observe that client cannot play any YouTube videos. Also, if applicable, open your Facebook account and try to open any YouTube video. You will observe YouTube videos cannot be played. Because YouTube is blocked in the FlexConnect AVC profile, and AVC profile is mapped to WLAN on the FlexConnect Group. You cannot access YouTube videos via browser, or even via YouTube application or from any other website.

.**Note:** If your browser was already open with YouTube, refresh the browser for the AVC profile to take effect.

Appendix

VOD Reference

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