Configuring Application Visibility and Control

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

AVC is configured by defining a class map in a QoS client policy to match a protocol.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

Note You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

Traffic flows are analyzed and recognized using the NBAR2 engine at the access point. For more information about the NBAR2 Protocol Library, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF).

AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. For example, if the policy has a filter based on an application name, and the traffic has also been classified to the same application name, then the action specified for this match in the policy will be applied.

Note When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

Cisco WLC Platform	Flow
Cisco 2504 WLC	26,250
Cisco 5508 WLC	183,750
Cisco WiSM2	393,750
Cisco 8510 WLC	336,000
Cisco 5520 WLC	336,000
Cisco 8540 WLC	336,000

Supported AVC Class Map and Policy Map Formats

Supported AVC Class Map Format

Class Map Format	Class Map Example	Direction
match protocol *protocol name*	`class-map match-any webex-class match protocol webex-media`	Both upstream and downstream
match protocol attribute category *category-name*	`class-map match-any IM match protocol attribute category instant-messaging`	Both upstream and downstream
match protocol attribute sub-category *sub-category-name*	`class-map match-any realtimeconferencing match protocol attribute sub-category voice-video-chat-collaboration`	Both upstream and downstream
match protocol attribute application-group *application-group-name*	`class-map match-any skype match protocol attribute application-group skype-group`	Both upstream and downstream
Combination filters	`class-map match-any webex-class match protocol webex match dscp 45 match wlan user-priority 6`	Upstream only

Supported AVC Policy Format

Policy Format	QoS Action
Upstream client policy based on match protocol filter	Mark, police, and drop
Downstream client policy based on match protocol filter	Mark and police

The following table describes the detailed AVC policy format with an example:

AVC Policy Format	AVC Policy Example	Direction

Basic set	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
		Upstream and downstream

Basic police	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
		Upstream and downstream

Basic set and police	`policy-map webex-policy`
	` class webex-class`
	` set dscp ef //or set up,cos`
	` police 5000000`
		Upstream and downstream

Multiple set and police including default	`policy-map webex-policy`
	` class webex-class`
	` set dscp af31 //or set up,cos`
	` police 4000000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`
		Upstream and downstream

Hierarchical police	`policy-map webex-policy`
	` class webex-class`
	` police 5000000`
	` service-policy client-in-police-only`
	
	` policy-map client-in-police-only`
	` class webex-class`
	` police 100000`
	` class class-webex-category`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` police 200000`
		Upstream and downstream

Hierarchical set and police	`policy-map webex-policy`
	` class class-default`
	` police 1500000`
	` service policy client-up-child`
	` policy-map webex-policy`
	` class webex-class`
	` police 100000`
	` set dscp ef`
	` class class-webex-category`
	` police 200000`
	` set dscp af31`	

Drop action		Upstream only

AVC Policy Format	AVC Policy Example	Direction

	Any of the above examples apply to this format with this additional example:
	`policy-map webex-policy`
	` class webex-class`
	` drop`
	` class netflix`
	` set dscp ef //or set up,cos`
	` police 6000000`
	` class class-default`
	` set dscp <>`	

Prerequisites for Application Visibility and Control

- The access points should be AVC capable.
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

Guidelines for Inter-Switch Roaming with Application Visibility and Control

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

- When a new QoS policy is added to the switch, a QoS policy with the same name should be added to other switch within the same roam or mobility domain.
- When a switch is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

Restrictions for Application Visibility and Control

- AVC is supported only on the following access points:
  - Cisco Aironet 1260 Series Access Points
  - Cisco Aironet 1600 Series Access Points
  - Cisco Aironet 2600 Series Access Point
  - Cisco Aironet 2600 Series Wireless Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3500 Series Access Points

  - Cisco Aironet 3600 Series Access Points

- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series Access Points.
- Dropping or marking of the data traffic (control part) is not supported for software Release 3.3.
- Dropping or marking of the data traffic (control part) is supported in software Release 3E.
- Only the applications that are recognized with application visibility can be used for applying QoS control.
- Multicast traffic classification is not supported.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- IPv6 including ICMPv6 traffic classifications are not supported.
- Datalink is not supported for NetFlow fields for AVC.
- The following commands are not supported for AVC flow records:
  - **collect flow username**
  - **collect interface** { **input** | **output**}
  - **collect wireless client ipv4 address**
  - **match interface** { **input** | **output**}
  - **match transport igmp type**
- The template timeout cannot be modified on exporters configured with AVC. Even if the template timeout value is configured to a different value, only the default value of 600 seconds is used.
- For the username information in the AVC-based record templates, ensure that you configure the options **records** to get the user MAC address to username mapping.
- When there is a mix of AVC-enabled APs such as 3600, and non-AVC-enabled APs such as 1140, and the chosen policy for the client is AVC-enabled, the policy will not be sent to the APs that cannot support AVC.
- Only ingress AVC statistics are supported. The frequency of statistics updates depends on the number of clients loaded at the AP at that time. Statistics are not supported for very large policy format sizes.
- The total number of flows for which downstream AVC QoS supported per client is 1000.
- The maximum number of flows supported for Cisco WLC 5700 Series is 360 K and Catalyst 3850 Series Switch is 48 K.
- These are some class map and policy map-related restrictions. For supported policy formats, see Supported AVC Class Map and Policy Map Formats, on page 3

  .

  - AVC and non-AVC classes cannot be defined together in a policy in a downstream direction. For example, when you have a class map with match protocol, you cannot use any other type of match filter in the policy map in the downstream direction.
  - Drop action is not applicable for the downstream AVC QoS policy.
  - Match protocol is not supported in ingress or egress for SSID policy.

- Google shares resources among several of their services because of which for some of the traffic it is not possible to say it is unique to one application. Therefore we added google-services for traffic that cannot be distinguished. The behavior you experience is expected.

How to Configure Application Visibility and Control

Configuring Application Visibility and Control (CLI)

To configure Application Visibility, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the flow record as an option.
3. Create a flow monitor based on the flow record and flow exporter.
4. Configure WLAN to apply flow monitor in IPv4 input or output direction.

To configure Application Control, follow these general steps:

1. Create an AVC QoS policy.
2. Attach AVC QoS policy to the client in one of three ways: configuring WLAN, using ACS or ISE, or adding local policies.

Creating a Flow Record

By default, **wireless avc basic** (flow record) is available. When you click **Apply** from the GUI, then the record is mapped to the flow monitor.

Default flow record cannot be edited or deleted. If you require a new flow record, you need to create one and map it to the flow monitor from CLI.

SUMMARY STEPS

1. **configure terminal**
2. **flow record** *flow_record_name*
3. **description** *string*
4. **match ipv4 protocol**
5. **match ipv4 source address**
6. **match ipv4 destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **match flow direction**
10. **match application name**
11. **match wireless ssid**
12. **collect counter bytes long**
13. **collect counter packets long**
14. **collect wireless ap mac address**
15. **collect wireless client mac address**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**flow record** *flow_record_name*
	
	Example:
	`Switch(config)# flow record record1`
	`Switch (config-flow-record)#`
		Enters flow record configuration mode.

Step 3	**description** *string* **Example:** `Switch(config-flow-record)# description IPv4flow`	(Optional) Describes the flow record as a maximum 63-character string.
Step 4	**match ipv4 protocol** **Example:** `Switch (config-flow-record)# match ipv4 protocol`	Specifies a match to the IPv4 protocol.

	Command or Action	Purpose
Step 5	**match ipv4 source address** **Example:** `Switch (config-flow-record)# match ipv4 source address`	Specifies a match to the IPv4 source address-based field.
Step 6	**match ipv4 destination address** **Example:** `Switch (config-flow-record)# match ipv4 destination address`	Specifies a match to the IPv4 destination address-based field.
Step 7	**match transport source-port** **Example:** `Switch (config-flow-record)# match transport source-port`	Specifies a match to the transport layer source-port field.
Step 8	**match transport destination-port** **Example:** `Switch (config-flow-record)# match transport destination-port`	Specifies a match to the transport layer destination-port field.
Step 9	**match flow direction** **Example:** `Switch (config-flow-record)# match flow direction`	Specifies a match to the direction the flow was monitored in.
Step 10	**match application name** **Example:** `Switch (config-flow-record)# match application name`	Specifies a match to the application name. **Note** This action is mandatory for AVC support, as this allows the flow to be matched against the application.
Step 11	**match wireless ssid** **Example:** `Switch (config-flow-record)# match wireless ssid`	Specifies a match to the SSID name identifying the wireless network.
Step 12	**collect counter bytes long** **Example:** `Switch (config-flow-record)# collect counter bytes long`	Specifies to collect counter fields total bytes.
Step 13	**collect counter packets long** **Example:** `Switch (config-flow-record)# collect counter bytes long`	Specifies to collect counter fields total packets.

	Command or Action	Purpose
Step 14	**collect wireless ap mac address** **Example:** `Switch (config-flow-record)# collect wireless ap mac address`	Specifies to collect the BSSID with MAC addresses of the access points that the wireless client is associated with.
Step 15	**collect wireless client mac address** **Example:** `Switch (config-flow-record)# collect wireless client mac address`	Specifies to collect MAC address of the client on the wireless network. **Note** The **collect wireless client mac address** is mandatory configuration for wireless AVC.
Step 16	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Flow Exporter (Optional)

You can create a flow export to define the export parameters for a flow. This is an optional procedure for configuring flow parameters.

SUMMARY STEPS

1. **configure terminal**
2. **flow exporter** *flow_exporter_name*
3. **description** *string*
4. **destination** *{hostname | ip-address}*
5. **transport udp** *port-value*
6. **option application-table timeout** *seconds* **(optional)**
7. **option usermac-table timeout** *seconds* **(optional)**
8. **end**
9. **show flow exporter**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**flow exporter** *flow_exporter_name*
	
	Example:
	`Switch(config)# flow exporter record1`
	`Switch (config-flow-exporter)#`
		Enters flow exporter configuration mode.

Step 3	**description** *string* **Example:** `Switch(config-flow-exporter)# description IPv4flow`	Describes the flow record as a maximum 63-character string.
Step 4	**destination** *{hostname | ip-address}* **Example:** `Switch (config-flow-exporter) # destination 10.99.1.4`	Specifies the hostname or IPv4 address of the system to which the exporter sends data.
Step 5	**transport udp** *port-value* **Example:** `Switch (config-flow-exporter) # transport udp 2`	Configures a port value for the UDP protocol.
Step 6	**option application-table timeout** *seconds* **(optional)** **Example:** `Switch (config-flow-exporter)# option application-table timeout 500`	(Optional) Specifies application table timeout option. The valid range is from 1 to 86400 seconds.
Step 7	**option usermac-table timeout** *seconds* **(optional)** **Example:** `Switch (config-flow-exporter)# option usermac-table timeout 1000`	(Optional) Specifies wireless usermac-to-username table option. The valid range is from 1 to 86400 seconds.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show flow exporter** **Example:** `Switch # show flow exporter`	Verifies your configuration.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

SUMMARY STEPS

1. **configure terminal**
2. **flow monitor** *monitor-name*
3. **description** *description*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **cache timeout** {**active** | **inactive**} **(Optional)**
7. **end**
8. **show flow monitor**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Switch (config)# flow monitor flow-monitor-1`	Creates a flow monitor and enters flow monitor configuration mode.
Step 3	**description** *description* **Example:** `Switch (config-flow-monitor)# description flow-monitor-1`	Creates a description for the flow monitor.
Step 4	**record** *record-name* **Example:** `Switch (config-flow-monitor)# record flow-record-1`	Specifies the name of a recorder that was created previously.
Step 5	**exporter** *exporter-name* **Example:** `Switch (config-flow-monitor)# exporter flow-exporter-1`	Specifies the name of an exporter that was created previously.

	Command or Action	Purpose

Step 6	**cache timeout** {**active** | **inactive**} **(Optional)**
	
	Example:
	`Switch (config-flow-monitor)# cache timeout active 1800`
	
	`Switch (config-flow-monitor)# cache timeout inactive 200`
		Specifies to configure flow cache parameters. You can configure for a time period of 1 to 604800 seconds (optional).
		
		Note To achieve optimal result for the AVC flow monitor, we recommend you to configure the inactive cache timeout value to be greater than 90 seconds.

Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show flow monitor** **Example:** `Switch # show flow monitor`	Verifies your configuration.

Creating AVC QoS Policy

To create AVC QoS policy, perform these general steps:

1. Create a class map with match protocol filters.
2. Create a policy map.
3. Apply a policy map to the client in one of the following ways:
   a. Apply a policy map over WLAN either from the CLI or GUI.
   b. Apply a policy map through the AAA server (ACS server or ISE) from the CLI.

      For more information, refer to the *Cisco Identity Services Engine User Guide* and *Cisco Secure Access Control System User Guide*.
   c. Apply local policies either from the CLI or GUI.

Creating a Class Map

You need to create a class map before configuring any match protocol filter. The QoS actions such as marking, policing, and dropping can be applied to the traffic. The AVC match protocol filters are applied only for the wireless clients. For more information about the protocols that are supported, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html.

SUMMARY STEPS

1. **configure terminal**
2. **class-map** *class-map-name*
3. **match protocol** {*application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Switch(config)# class-map webex-class`	Creates a class map.

Step 3	**match protocol** {*application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}
	
	Example:
	`Switch(config)# class-map webex-class`
	`Switch(config-cmap)# match protocol webex-media`
	
	`Switch(config)# class-map class-webex-category`
	`Switch(config-cmap)# match protocol attribute category webex-media`
	
	`Switch# class-map class-webex-sub-category`
	`Switch(config-cmap)# match protocol attribute sub-category webex-media`
	
	`Switch# class-map class-webex-application-group`
	`Switch(config-cmap)# match protocol attribute application-group webex-media`
		Specifies match to the application name, category name, subcategory name, or application group.

Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Policy Map

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** *policy-map-name*
3. **class** [*class-map-name* | **class-default**]
4. **police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]
5. **set** {**dscp** *new-dscp* | **cos** *cos-value*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**policy-map** *policy-map-name*
	
	Example:
	`Switch(config)# policy-map webex-policy`
	`Switch(config-pmap)#`
		Creates a policy map by entering the policy map name, and enters policy-map configuration mode.
		By default, no policy maps are defined.
		The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.
		Note To delete an existing policy map, use the **no policy-map** *policy-map-name* global configuration command.

Step 3	**class** [*class-map-name*	**class-default**]
		
		Example:
		`Switch(config-pmap)# class-map webex-class`
		`Switch(config-pmap-c)#`
			Defines a traffic classification, and enters policy-map class configuration mode.
			By default, no policy map and class maps are defined.
			If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for *class-map-name* in this command.
			A **class-default** traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied **match any** is included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**.
			Note To delete an existing class map, use the **no class** *class-map-name* policy-map configuration command.

Step 4	**police** *rate-bps burst-byte* [**exceed-action** {**drop**	**policed-dscp-transmit**}] **Example:** `Switch(config-pmap-c)# police 100000 80000 drop`	Defines a policer for the classified traffic. By default, no policer is defined. • For *rate-bps,* specify an average traffic rate in bits per second (b/s). The range is 8000 to 10000000000. • For *burst-byte,* specify the normal burst size in bytes. The range is 8000 to 1000000.

	Command or Action	Purpose
		• (Optional) Specifies the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action policed-dscp-transmit** keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet.
Step 5	**set** {**dscp** *new-dscp* | **cos** *cos-value*} **Example:** `Switch(config-pmap-c)# set dscp 45`	Classifies IP traffic by setting a new value in the packet. • For **dscp** *new-dscp*, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

What to Do Next

After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Configuring Local Policies (CLI)

Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.

Creating a Service Template (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **service-template** *service-template-name*
3. **access-group** *acl_list*
4. **vlan** *vlan_id*
5. **absolute-timer** *seconds*
6. **service-policy qos** {**input** | **output**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

Step 2	**service-template** *service-template-name*
	
	Example:
	`Switch(config)# service-template cisco-phone-template`
	`Switch(config-service-template)#`
		Enters service template configuration mode.

Step 3	**access-group** *acl_list* **Example:** `Switch(config-service-template)# access-group foo-acl`	Specifies the access list to be applied.
Step 4	**vlan** *vlan_id* **Example:** `Switch(config-service-template)# vlan 100`	Specifies VLAN ID. You can specify a value from 1 to 4094.
Step 5	**absolute-timer** *seconds* **Example:** `Switch(config-service-template)# absolute-timer 20`	Specifies session timeout value for service template. You can specify a value from 1 to 65535.
Step 6	**service-policy qos** {**input** | **output**} **Example:** `Switch(config-service-template)# service-policy qos input foo-qos`	Configures QoS policies for the client.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type subscriber attribute-to-service** *parameter-map-name*
3. *map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* }
4. **service-template** *service-template-name*
5. **interface-template** *interface-template-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	Specifies the parameter map type and name.
Step 3	*map-index* **map** { **device-type**	**mac-address**	**oui**	**user-role**	**username**} {**eq**	**not-eq**	**regex** *filter-name* } **Example:** `Switch(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	Specifies parameter map attribute filter criteria.

Step 4	**service-template** *service-template-name*
	
	Example:
	`Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 5	**interface-template** *interface-template-name*
	
	Example:
	`Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

	Command or Action	Purpose
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Policy Map (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type control subscriber** *policy-map-name*
3. **event identity-update** {**match-all** | **match-first**}
4. *class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**}
5. *action-index* **map attribute-to-service table** *parameter-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Switch(config)# policy-map type control subscriber Aironet-Policy`	Specifies the policy map type.
Step 3	**event identity-update** {**match-all**	**match-first**} **Example:** `Switch(config-policy-map)# event identity-update match-all`	Specifies match criteria to the policy map.
Step 4	*class_number* **class** {*class_map_name*	**always** } {**do-all**	**do-until-failure**	**do-until-success**} **Example:** `Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options: • **always—**Executes without doing any matching but return success. • **do-all—**Executes all the actions.

	Command or Action	Purpose
		• **do-until-failure—**Execute all the actions until any match failure is encountered. This is the default value. • **do-until-success—**Execute all the actions until any match success happens.
Step 5	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	Specifies parameter map table to be used.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Applying a Local Policy for a Device on a WLAN (CLI)

Before You Begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

Note You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name*
3. **service-policy type control subscriber** *policymapname*
4. **profiling local http (optional)**
5. **profiling radius http (optional)**
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch(config)# wlan wlan1`	Enters WLAN configuration mode.
Step 3	**service-policy type control subscriber** *policymapname* **Example:** `Switch(config-wlan)# service-policy type control subscriber Aironet-Policy`	Applies local policy to WLAN.
Step 4	**profiling local http (optional)** **Example:** `Switch(config-wlan)# profiling local http`	Enables only profiling of devices based on HTTP protocol (optional).
Step 5	**profiling radius http (optional)** **Example:** `Switch(config-wlan)# profiling radius http`	Enables profiling of devices on ISE (optional).
Step 6	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Specifies not to shut down the WLAN.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Local Policies (GUI)

Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create a policy map.
3. Apply a local policy that you have created to a WLAN.

Creating a Service Template (GUI)

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Service Template** to open the **Service Template** page.

Step 2 Create a new template as follows:

a) Click **New** to open the **Service Template > New** page.
b) In the Service Template name text box, enter the new service template name.
c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
h) Click **Apply** to save the configuration.

Step 3 Edit a service template as follows:

a) From the **Service Template** page, click the service template to open the **Service Template > Edit** page.
b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
g) Click **Apply** to save the configuration.

Step 4 Remove a service template as follows:

a) From the **Service Template** page, select the service template.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Creating a Policy Map (GUI)

Step 1 Choose **Configuration** > **Security** > **Local Policies** > **Policy Map** to open the **Policy Map** page.

Step 2 Create a new policy map as follows:

a) Click **New** to open the **Policy Map > New** page.
b) In the Policy Map name text box, enter the new policy map name.
c) Click **Add** to open the Match Criteria area.
d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.

e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.
f) From the Service Template drop-down list, choose the service template to be mapped to the policy.
g) Click **Add**. The match criteria is added to the Match Criteria Lists.
h) In the Match Criteria Lists area, click **Add** to add the match criteria to the policy.
i) Click **Apply** to save the configuration.

Step 3 Edit a policy map as follows:

a) In the **Policy Map** page, select the policy map that you want to edit, and click **Edit** to open the **Policy Map > Edit** page.
b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user
d) From the Service Template drop-down list, choose the service template to be mapped to the policy.
e) Click **Ok** to save the configuration or **Cancel** to discard the configuration.
f) Click **Add** to add more match criteria based on device type, user role, and service template to the policy.
g) In the Match Criteria Lists area, select the match criteria and click **Move to** to move the match criteria with respect to a value entered in the row text box.
h) Select the match criteria and click **Move up** to move the match criteria up in the list.
i) Select the match criteria and click **Move down** to move the match criteria down in the list.
j) Select the match criteria and click **Remove** to remove the match criteria from the policy map list.
k) Click **Apply** to save the configuration.

Step 4 Remove a policy map as follows:

a) From the **Policy Map** page, select the policy map.
b) Click **Remove**.
c) Click **Apply** to save the configuration.

Applying Local Policies to WLAN (GUI)

Step 1 Choose **Configuration** > **Wireless** > **WLAN** to open the **WLANs** page.
Step 2 Click the corresponding WLAN profile. The **WLANs > Edit** page is displayed.
Step 3 Click the **Policy-Mapping** tab.
Step 4 Check the **Device Classification** check box to enable classification based on device type.
Step 5 From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.
Step 6 Select **Local HTTP Profiling** to enable profiling on devices based on HTTP (optional).
Step 7 Select **Radius HTTP Profiling** to enable profiling on devices based on RADIUS (optional).
Step 8 Click **Apply** to save the configuration.

Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-id*
3. **ip flow monitor** *monitor-name* **{input | output}**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id* **Example:** `Switch (config) # wlan 1`	Enters WLAN configuration submode. For *wlan-id*, enter the WLAN ID. The range is 1 to 64.
Step 3	**ip flow monitor** *monitor-name* **{input | output}** **Example:** `Switch (config-wlan) # ip flow monitor flow-monitor-1 input`	Associates a flow monitor to the WLAN for input or output packets.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Application Visibility and Control (GUI)

Configuring Application Visibility (GUI)

You can apply the default flow record (**wireless avc basic**) to the default flow monitor (**wireless-avc-basic**).

If you are using the flow record and flow monitor you have created, then the record name and monitor name should be same. This is specific only for configuring AVC from GUI and not for the CLI configuration.

You can use the flow monitor you have created either for upstream or downstream, or both, but ensure that you use the same record name while mapping with the flow monitor.

Step 1 Choose **Configuration** > **Wireless** > **WLAN**.
The **WLAN** page appears.

Step 2 Click on the corresponding WLAN ID to open the **WLAN > Edit** page and click **AVC**.
The **Application Visibility** page appears.

a) Select the **Application Visibility Enabled** check box to enable AVC on a WLAN.
b) In the **Upstream Profile** text box, enter the name of the AVC profile.
c) In the **Downstream Profile** text box, enter the name of the AVC profile.

To enable AVC, you need to enter the profile names for the upstream and downstream profiles. The profile names are the flow monitor names. By default, the flow monitor names (**wireless-avc-basic**) appear in the **Upstream Profile** and **Downstream Profile** text boxes. For the default flow monitor, the default flow record (**wireless avc basic**) will be taken. The default flow record is generated by the system and is available.

You can change the profile names for the upstream and downstream profiles but ensure that the same flow records are available for the flow monitors.

The upstream and downstream profiles can have different profile names but there should be flow records available for the flow monitors.

Step 3 Click **Apply** to apply AVC on the WLAN.

Step 4 To disable AVC on a specific WLAN, perform the following steps:

- Choose **Configuration** > **Wireless** > **WLAN** to open the **WLAN** page.
- Click on the corresponding WLAN ID to open the **WLAN > Edit** page.
- Click **AVC** to open the **Application Visibility** page.
- Uncheck the **Application Visibility Enabled** check box.
- Click **Apply** to disable AVC on the specific WLAN.

Configuring Application Visibility and Control (GUI)

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **QoS** node by clicking the left pane and choosing **QOS-Policy**.
The **QOS-Policy** page is displayed.

Step 3 Click **Add New** to create a new QoS Policy.
The **Create QoS Policy** page is displayed.

Step 4 Select **Client** from the Policy Type drop-down list.

Step 5 Select the direction into which the policy needs to be applied from the Policy Direction drop-down list.

The available options are:

- **Ingress**
- **Egress**

Step 6 In the **Policy Name** text box, specify a policy name.

Step 7 In the **Description** text box, provide a description to the policy.

Step 8 Check the **Enable Application Recognition** check box to configure the AVC class map for a client policy.

Note For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.

The following options are available:

- **Trust—**Specify a classification type for this policy.
  - **Protocol—**Allows you to choose the protocols and configure the marking and policing of the packets.
  - **Category—**Allows you to choose the category of the application, for example, browsing.
  - **Subcategory—**Allows you to choose the subcategory of the application, for example, file-sharing.
  - **Application-Group—**Allows you to choose the application group, for example, ftp-group.
- **Protocol Choice—**Choose the protocols, category, subcategory, or application group from the **Available Protocols** list into the **Assigned Protocols** to apply the marking and policing of the packets.
- **Mark—**Specify the marking label for each packet. The following options are available:
  - **DSCP—**Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  - **CoS—**Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  - **None—**Does not mark the packets.
- **Police (kbps)—**Specify the policing rate in kbps. This option is available when the **Policy Direction** is egress.
- **Drop—**Specify to drop the ingress packets that correspond to the chosen protocols.

Note You can add a maximum of five AVC classes for each client policy.

Step 9 Click **Add** to create an AVC class map. The new class map is listed in a tabular format.

Step 10 Click **Apply** to create an AVC QoS policy.

Step 11 Click the QoS policy link in the **QOS-Policy** page to edit the QoS policy. The **QOS-Policy** > **Edit** page is displayed. Make changes and click **Apply** to commit your changes.

Step 12 Remove an AVC class map from the QoS policy by navigating to the corresponding AVC class map row in the AVC class map table and clicking **Remove**. Click **Apply** to commit your changes.

Monitoring Application Visibility and Control

Monitoring Application Visibility and Control (CLI)

This section describes the new commands for application visibility.

The following commands can be used to monitor application visibility on the switch and access points.

Table 1: Monitoring Application Visibility Commands on the switch

Command	Purpose
show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given client MAC.
show avc wlan *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given SSID.
avc top user[enable | disable]	Enables or disables the information about top "N" application.
show avc wlan *wlan-id* **application** *app name* **top***N* [**aggregate** | **upstream** | **downstream**]	Displays to know network usage information on a per user basis within an application. **Note** On Catalyst 4500E Supervisor Engine 8-E, in the information about top N users that is displayed, the client's MAC address and username are not displayed. This issue occurs only within 90 seconds after the client is disconnected.
show wlan id *wlan-id*	Displays information whether AVC is enabled or disabled on a particular WLAN.
show flow monitor *flow_monitor_name* **cache**	Displays information about flow monitors.
show wireless client mac-address *mac-address* **service-policy** { **input** | **output** }	Displays information about policy mapped to the wireless clients.

Table 2: Clearing Application Visibility Statistics Commands

Command	Purpose
clear avc client *mac* **stats**	Clears the statistics per client.
clear avc wlan *wlan-name* **stats**	Clears the statistics per WLAN.

Monitoring Application Visibility and Control (GUI)

You can view AVC information on a WLAN in a single shot using a **AVC on WLAN** pie chart on the **Home** page of the switch. The pie chart displays the AVC data (Aggregate - Application Cumulative usage %) of the first WLAN. In addition, the top 5 WLANs based on clients are displayed first. Click on any one of the WLANs to view the corresponding pie chart information. If AVC is not enabled on the first WLAN, then the **Home** page does not display the AVC pie chart.

Step 1 Choose **Monitor** > **Controller** > **AVC** > **WLANs**.
The **WLANs** page appears.

Step 2 Click the corresponding WLAN profile.
The **Application Statistics** page appears.

From the **Top Applications** drop-down list, choose the number of top applications you want to view and click **Apply**. The valid range is between 5 to 30, in multiples of 5.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

Step 3 Choose **Monitor** > **Clients** > **Client Details** > **Clients**.
The **Clients** page appears.

Step 4 Click **Client MAC Address** and then click **AVC Statistics** tab.
The **Application Visibility** page appears.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

Monitoring SSID and Client Policies Statistics (GUI)

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the switch. The frequency of the statistics depends on the number of clients associated with the access point.

Type of Statistics	Method	Details
SSID Policies	Choose **Monitor > Controller > Statistics > QoS**.	The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click **Apply** to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.
Client Policies	Choose **Monitor > Clients > Client Details** .	The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the **QoS Statistics** tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.

Examples: Application Visibility and Control

Examples: Application Visibility Configuration

This example shows how to create a flow record, create a flow monitor, apply the flow record to the flow monitor, and apply the flow monitor on a WLAN:

```
Switch# configure terminal
Switch(config)# flow record fr_v4
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match application name
Switch(config-flow-record)# match wireless ssid
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
```

```
Switch(config-flow-record)# collect wireless ap mac address
Switch(config-flow-record)# collect wireless client mac address
Switch(config)#end
```

```
Switch# configure terminal
Switch# flow monitor fm_v4
Switch(config-flow-monitor)# record fr_v4
Switch(config-flow-monitor)# cache timeout active 1800
Switch(config)#end
```

```
Switch(config)#wlan wlan1
Switch(config-wlan)#ip flow monitor fm_v4 input
Switch(config-wlan)#ip flow mon fm-v4 output
Switch(config)#end
```

Examples: Application Visibility and Control QoS Configuration

This example shows how to create class maps with apply match protocol filters for application name, category, and subcategory:

```
Switch# configure terminal
Switch(config)# class-map cat-browsing
Switch(config-cmap)# match protocol attribute category browsing
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map cat-fileshare
Switch(config-cmap)# match protocol attribute category file-sharing
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map match-any subcat-terminal
Switch(config-cmap)# match protocol attribute sub-category terminal
Switch(config-cmap)#end

Switch# configure terminal
Switch(config)# class-map match-any webex-meeting
Switch(config-cmap)# match protocol webex-meeting
Switch(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 150000
Switch(config-pmap-c)# set dscp 12
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 1000000
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 120000
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)#end
```

```
Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# set dscp 21
Switch(config-pmap-c)#end
```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```
Switch# configure terminal
Switch(config)# policy-map test-avc-down
Switch(config-pmap)# class cat-browsing
Switch(config-pmap-c)# police 200000
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)#end


Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class cat-fileshare
Switch(config-pmap-c)# police 300000
Switch(config-pmap-c)# set wlan user-priority 2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)#end


Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class subcat-terminal
Switch(config-pmap-c)# police 100000
Switch(config-pmap-c)# set dscp 25
Switch(config-pmap-c)#end

Switch# configure terminal
Switch(config)# policy-map test-avc-up
Switch(config-pmap)# class webex-meeting
Switch(config-pmap-c)# police 60000000
Switch(config-pmap-c)# set dscp 41
Switch(config-pmap-c)#end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Switch# configure terminal
Switch(config)#wlan  alpha
Switch(config-wlan)#shut
Switch(config-wlan)#end
Switch(config-wlan)#service-policy client input test-avc-up
Switch(config-wlan)#service-policy client output test-avc-down
Switch(config-wlan)#no shut
Switch(config-wlan)#end
```

Example: Configuring QoS Attribute for Local Profiling Policy

The following example shows how to configure QoS attribute for a local profiling policy:

```
Switch(config)# class-map type control subscriber match-all local_policy1_class
Switch(config-filter-control-classmap)# match device-type android
Switch(config)# service-template local_policy1_template
Switch(config-service-template)# vlan 40
Switch(config-service-template)# service-policy qos output local_policy1
Switch(config)# policy-map type control subscriber local_policy1
Switch(config-event-control-policymap)# event identity-update match-all
Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success
Switch(config-action-control-policymap)# 1 activate service-template local_policy1_template
Switch(config)# wlan open_auth 9
```

```
Switch(config-wlan)# client vlan VLAN40
Switch(config-wlan)# service-policy type control subscriber local_policy1
```

Additional References for Application Visibility and Control

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow configuration	*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow commands	*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
QoS configuration	*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*
QoS commands	*QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Application Visibility and Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	AVC control with QoS was introduced.