CHAPTER 13

QoS Configuration

The introduction of Cisco IOS® software on the WLC5760 controller brings a wide-range of wired/wireless QoS supports and capabilities:

- Consistent configuration CLI for both wired and wireless QoS through Modular QoS CLI
- Granular QoS policies per AP, SSID, radio, and client
- Fair bandwidth allocation across wireless clients on an AP
- Leverages proven Cisco IOS® and ASIC technology to provide line rate performance

Enabling QoS

Based on the Modular QoS CLI model, QoS is enabled by default on the WLC5760. Explicit marking of traffic is required in order to modify Class of Service (CoS) or Differentiated Services Code Point (DSCP) values for traffic from and to wired ports. Traffic from wireless to wireless ports or wireless to wired ports is considered untrusted. Though QoS is globally enabled if traffic passes through an SSID, it must be marked or trusted specifically, or all QoS values (DSCP, CoS) will be set to default (0).

Managing QoS

QoS policies on the WLC5760 are provisioned in a couple of ways.

- Via CLI
- Via AAA

The configuration examples herein demonstrate attachment of policies via CLI. AAA configuration of policies is shown later in this specific section. The QoS policy name, not the actual QoS policy, is passed from the AAA server to the WLC5760 platform. Due to this fact, the QoS policy configuration must be local to the platform regardless of which method is used to manage QoS on the platform.

Marking Models

The WLC5760 supports several marking models:

- Per-Port Marking (wired)
- Per-Client Marking (wireless)

- Per-SSID Marking (wireless)
- Per-VLAN Marking (wired)

From a unified policy standpoint, the Per-Port and Per-Client marking policy can be synonymous but applied to a different target (wireless client, physical client port). Each model is discussed herein.

Per-Port or Per-Client Marking

Similar to the Catalyst 4500, the Per-Port or Per-Client marking model matches VoIP on UDP/RTP ports 16384-32767. The signaling traffic is matched on SCCP ports (TCP 2000-2002), as well as on SIP ports (TCP/UDP 5060-5061). Transactional data traffic are matched on various ports. Unlike the Catalyst 3750-E examples, no explicit default class is required, because the implicit class default performs policy actions (such as marking or policing) on the WLC3850/5760.

!ACL configuration

```
ip access-list extended VOIP
remark Voice
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006
```

!Class-map configuration

```
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
```

```
match access-group name TRANSACTIONAL-DATA
```

!Per-Port or Per-Client Ingress Marking Policy-map Configuration

```
policy-map PER-PORT-MARKING
class VOIP
set dscp ef
class SIGNALING
set dscp cs3
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

!Policy attachment to interfaces

!Wireless Clients associating to WLAN OPEN

```
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9 load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-MARKING
session-timeout 1800
no shutdown
```

Policing Models

Several policing models are available on the WLC5760.

- Per-Port Policing
- Per-Client Policing
- Per-SSID Policing

Policing is offered in a number of ways and can be used in a hierarchical fashion as will be shown in the instance of client-based policies. In this instance, a policer can be used bi-directionally to police a client's traffic as an aggregate, as well as specific traffic classes associated with the client, such as voice.

Here is an example of FLAT Per-Port or Per-Client Policing configuration:

!ACL configuration

```
ip access-list extended VOIP
remark Voice
```

```
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006
```

!Class-map configuration

```
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
match access-group name TRANSACTIONAL-DATA
```

!Per-Port or Per-Client Ingress Policing Policy-map Configuration

```
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000conform-action transmitexceed-action drop
class SIGNALING
set dscp cs3
police 32000conform-action transmitexceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

!Policy attachment to interfaces

!Wireless Clients associating to WLAN OPEN Policed bi-directionally

```
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9
load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-POLICING
service-policy client output PER-PORT-POLICING
session-timeout 1800
```

Here is an example of Hierarchical Per-Client Policing configuration:

!Wireless Client Policy-map Client Aggregate policed to 2Mbps, Voice as a subset to 128k, signaling 32k

```
policy-map AGG-POLICE
class class-default
police 2000000 conform-action transmit exceed-action drop
service-policy PER-PORT-POLICING
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000 conform-action transmit exceed-action drop
class SIGNALING
set dscp cs3
police 32000 conform-action transmit exceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

Wireless Queuing

Wireless queuing by default provides a queuing policy. This policy is shown in the show run command and contains a static traffic class, which cannot be modified. This class is attached to multicast non-real-time traffic associated with the wireless port only. In order to enable the additional queues on egress of the wireless port, the static policy-map port_child_policy must be modified to include the three additional classes. Priority queuing is supported for two of the queues, while class-default makes up the rest of the queue.

Here is an example of egress wireless queuing policy:

```
policy-map port_child_policy
```

```
class non-client-nrt-class
bandwidth remaining ratio 7
class RT1
priority level 1
police 6400000 conform-action transmit exceed-action drop
class RT2
priority level 2
police 19200000 conform-action transmit exceed-action drop
class class-default
bandwidth remaining ratio 63
```

In this example, the policy limits as an aggregate the priority queues RT1 and RT2 to an aggregate policed rate as shown. The policy also provides the additional non-real-time classes with a bandwidth associated with the bandwidth remaining ratio command. This ratio of available bandwidth is provided to the non-client-nrt (or multicast and non-client non-real-time traffic queue) and class-default queues.

Wireless MultiMedia Configuration

Wireless MultiMedia (WMM) separates traffic types into four QoS access categories: background, best effort, video, and voice.

```
(config) wlan <your WLAN name> (config-wlan) shutdown
(config-wlan) broadcast
(config-wlan) radio all (to enable this WLAN configuration on both AP radios and all Wi-Fi
protocols)
(config-wlan) wmm require
(config-wlan) no security <your Current security setting>
(config-wlan) no shutdown
```

WMM configuration options include:

- WMM Required - only WMM enabled clients can join the WLAN
- WMM Optional - both non-WMM clients and WMM enabled client can join the WLAN
  - WMM enabled clients transmit all packets with WMM QoS header.
  - Non-WMM clients transmit no packets with WMM QoS header.

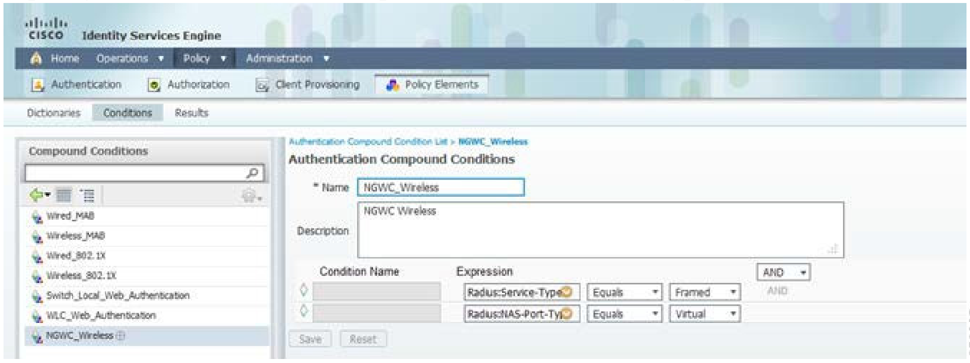
Note Note that non-WMM cannot receive packets from the AP that have a WMM QoS header.

  - All packets from and to non-WMM clients are sent with best effort Wi-Fi channel access.

Configure ISE in order to Authenticate and Push QoS Policies

Complete these steps to authenticate and push QoS policies.

1. Specify a condition where the expression is of NAS-Port-Type **Virtual**.



Authentication Compound Conditions

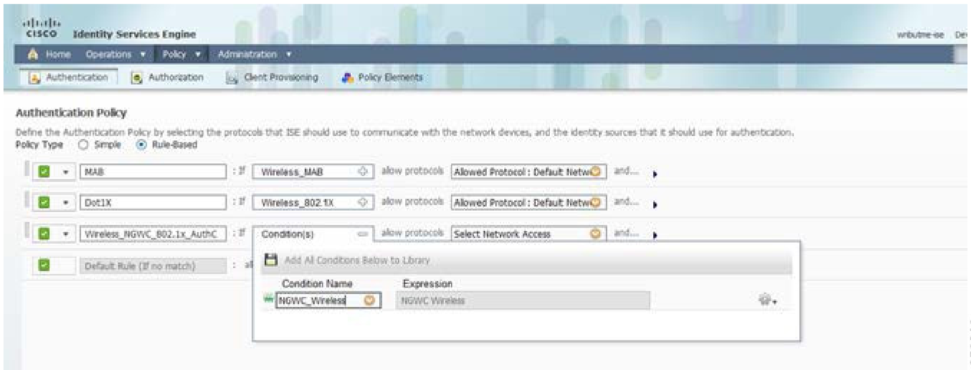
* Name: NGWC_Wireless

Description: NGWC Wireless

Condition Name	Expression			AND ▾
	Radius:Service-Type	Equals ▾	Framed ▾	AND
	Radius:NAS-Port-Ty	Equals ▾	Virtual ▾	

350265

2. Create authentication parameters.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

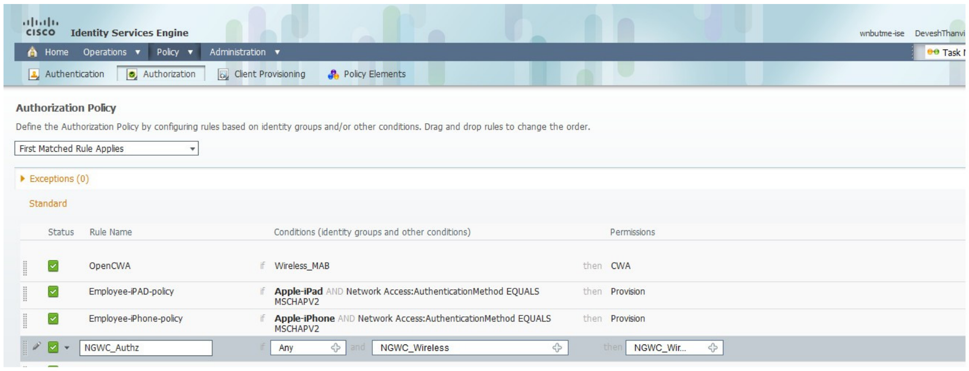
Policy Type ○ Simple ● Rule-Based

☑	MAB	: If	Wireless_MAB	allow protocols	Allowed Protocol : Default Netw	and...
☑	Dot1X	: If	Wireless_802.1X	allow protocols	Allowed Protocol : Default Netw	and...
☑	Wireless_NGWC_802.1x_AuthC	: If	Condition(s)	allow protocols	Select Network Access	and...
☑	Default Rule (If no match)	: al				

Condition Name	Expression
NGWC_Wireless	NGWC Wireless

350266

3. Authorization - Define result and use same condition.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies ▾

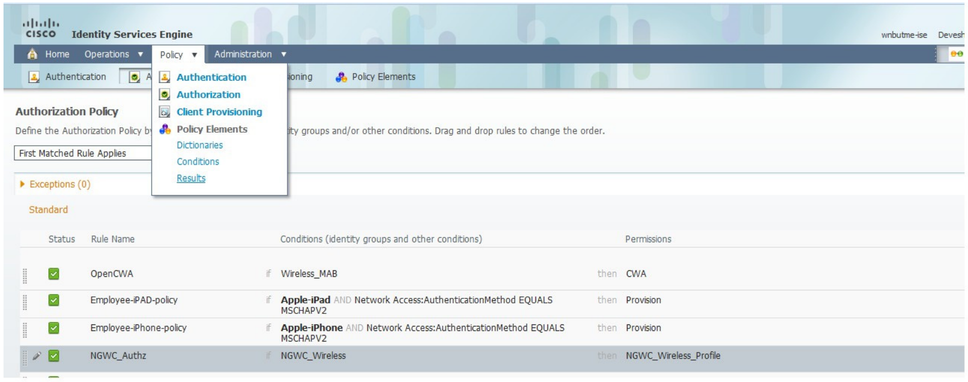
▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	OpenCWA	if	Wireless_MAB	then	CWA
☑	Employee-iPAD-policy	if	**Apple-iPad** AND Network Access:AuthenticationMethod EQUALS MSCHAPV2	then	Provision
☑	Employee-iPhone-policy	if	**Apple-iPhone** AND Network Access:AuthenticationMethod EQUALS MSCHAPV2	then	Provision
☑ ▾	NGWC_Authz	if	Any and NGWC_Wireless	then	NGWC_Wir...

350267

4. Go to **Policy > Results**.



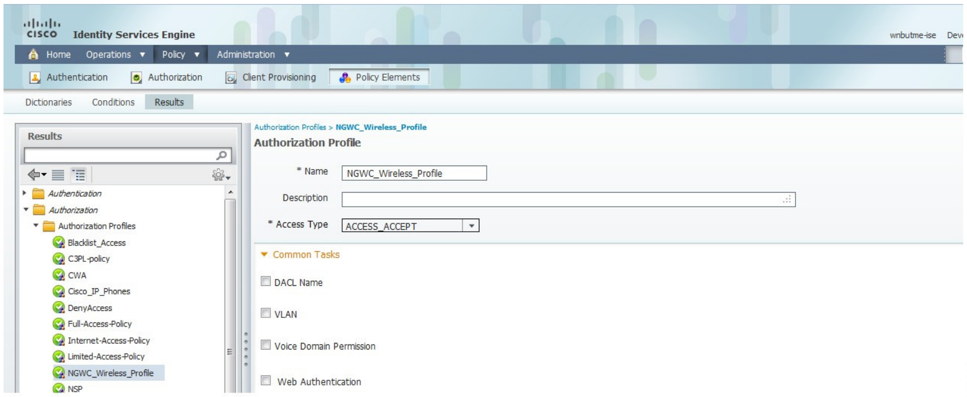
Authorization Policy

Define the Authorization Policy by ...ity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	OpenCWA	if	Wireless_MAB	then	CWA
☑	Employee-iPAD-policy	if	Apple-iPad AND Network Access:AuthenticationMethod EQUALS MSCHAPV2	then	Provision
☑	Employee-iPhone-policy	if	Apple-iPhone AND Network Access:AuthenticationMethod EQUALS MSCHAPV2	then	Provision
☑	NGWC_Authz	if	NGWC_Wireless	then	NGWC_Wireless_Profile

5. Choose Cisco-AV-Pair at bottom shown in Step 6.



Authorization Profiles > NGWC_Wireless_Profile

Authorization Profile

* Name NGWC_Wireless_Profile

Description

* Access Type ACCESS_ACCEPT

Common Tasks

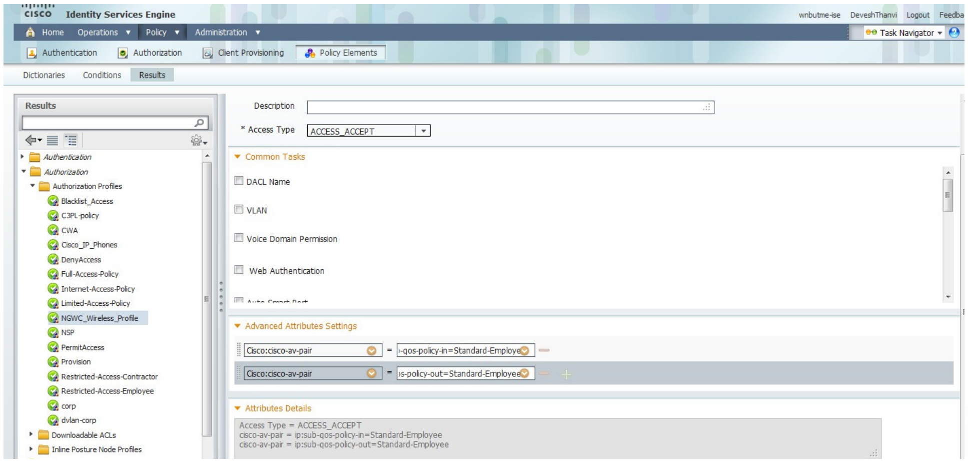
□ DACL Name

□ VLAN

□ Voice Domain Permission

□ Web Authentication

6. Modify **Advanced Attribute Settings** with the **Cisco av-pair name**, **ip:sub-qos-policy-in**, or **ip:sub-qos-polify-out**, plus name of QoS policy local to the WLC3850/5760. When clients are associated and authenticated, the policy name is pushed to the WLC3850/5760.



Description

* Access Type ACCESS_ACCEPT

Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

□ Web Authentication

□ Auto Smart Port

Advanced Attributes Settings

Cisco:cisco-av-pair = ı-qos-policy-in=Standard-Employe

Cisco:cisco-av-pair = ›s-policy-out=Standard-Employee

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:sub-qos-policy-in=Standard-Employee
cisco-av-pair = ip:sub-qos-policy-out=Standard-Employee
```

Cisco IOS® Tool Command Language Scripting

With the introduction of the Cisco IOS® software on the WLC5760 controller, users can now implement the Tool Command Language (TCL) scripting feature on the controller.