EVOLVE IP

Soft Client Deployment

Quality of Service (QoS) Best Practices

Table of Contents

Overview

In order to ensure the best possible experience with softphone clients for audio and video calling, Evolve IP has identified several recommended designs for both local installations and virtual. Each design has independent Quality of Service (QoS) recommendations that ensure soft client traffic is properly tagged and prioritized from the end user machine, across the LAN, and optimally across the WAN to the Evolve IP data center depending on WAN access.

Evolve IP offers best practices recommendations for Windows-only deployments because the Windows operating system is able to tag voice packets while the MAC operating system does not currently su pport voice packet tagging.

Once those packets are tagged, the network needs to honor DSCP values for QoS on soft clients for audio and video calling: switches, routers, and firewalls.

Deployment Topologies

Over the Top (Public Bandwidth)

Clients with smaller locations and/or users working from home choose to connect VoIP services to Evolve IP using public bandwidth. While call quality cannot be guaranteed, Evolve IP still takes measures and provides recommendations for those situations.

- ❖ Voice Gateway – Deployed for offices with 3 or more phones. This unit will proxy voice traffic and get a static IP from the 3rd party ISP. It will gather MOS scoring and provide an endpoint at locations for troubleshooting in the event of issues.
- ❖ Microsoft O/S Configuration – Even though traffic cannot be managed across the WAN due to public bandwidth, Evolve IP still recommends pushing the group policy for QoS on the Operating System. At least on the PC with applications, browsing, downloads, and streaming, the voice traffic is prioritized locally over the data traffic.

Dedicated Evolve IP Circuit

In this topology, Evolve IP is providing a dedicated circuit to the customer premise in the form of Fiber, Ethernet over copper, T1/E1, or DS3 back to the Evolve data center.

Local Operating System Deployment
- The **onsite router** should be configured to pass DSCP values and prioritize traffic to EvolveIP voice services (Completed by Evolve IP, unless customer owned router)
  - o A template for Cisco IOS routers is available
- **Switches** should be configured to trust DSCP values from end user machines (Completed by customer unless the customer has contracted Evolve IP for a managed on-site switches)
  - o A template for Cisco switches is available
- **End users' machines** should be configured to tag soft client traffic as EF (Completed by Customer)
  - o Instructions to do this on Windows machines is available

Virtual Desktop using Evolve IP Desktop as a Service Solution
- The onsite **router** should be configured to guarantee bandwidth to EvolveIP DaaS servers (Completed by Evolve IP, unless customer owned router)
  - o A template for Cisco IOS routers is available
- **Switches** should be configured to trust DSCP values from end user machines (Completed by customer unless the customer has contracted Evolve IP for a managed on-site switches)
  - o A template for Cisco switches is available
- **End users machine** should be configured to tag soft client traffic as EF (Completed by customer)
  - o Instructions to do this on Windows machines is available

NOTE: This process is the same for customers bringing their own Virtual Desktop infrastructure with the exception of prioritizing DaaS traffic back to Evolve's network

Private Customer Network to Evolve Network

In this topology, a customer provided circuit is utilized to provide direct connectivity to EvolveIP's data center. The circuit terminates to an onsite router with the other end terminating to a hosted services router in EvolveIP's data center.

Local Operating System Deployment

- The EvolveIP **hosted services router** is configured to pass DSCP values and prioritize EvolveIP voice services (Completed by EvolveIP)
- The **onsite router** should be configured to pass DSCP values and prioritize traffic to EvolveIP voice services (Completed by customer unless the customer has contracted for a managed on-site router)
  - A template for Cisco IOS routers is available
- **Switches** should be configured to trust DSCP values from end user machines (Completed by customer unless the customer has contracted Evolve IP for a managed on-site switches)
  - A template for Cisco switches is available
- End users' machines should be configured to tag soft client traffic as EF (Completed by Customer)
  - Instructions to do this on Windows machines is available
- If applicable, the circuit provider should be configured to prioritize EF traffic on both sides of the circuit

Virtual Desktop using Evolve IP Desktop as a Service Solution

- The EvolveIP hosted services router is configured to pass DSCP values and prioritize DaaS traffic (Completed by EvolveIP)
- The onsite router should be configured to guarantee bandwidth to EvolveIP DaaS servers (Completed by customer unless the customer has contracted for a managed on-site router)
  - A template for Cisco IOS routers is available
- The circuit carrier's edge equipment should be configured to prioritize DaaS traffic on both sides of the circuit
  - This configuration will be dependent on the circuit vendor and may require QoS changes to the local router
- End users machine should be configured to tag soft client traffic as EF (Completed by customer)
  - Instructions to do this on Windows machines is available

NOTE: This process is the same for customers bringing their own Virtual Desktop infrastructure with the exception of prioritizing DaaS traffic back to Evolve IP's network

Cloud Connect with an onsite firewall

In this topology, EvolveIP provides a managed Cloud Connect device delivering internet connectivity to an onsite firewall.

Local Operating System Deployment

- The Cloud Connect device is configured to prioritize all traffic to EvolveIP voice services. (Completed by EvolveIP)
- The onsite firewall should be configured to pass DSCP values and prioritize EF traffic. (Completed by customer unless the customer has contracted for a managed on-site firewall)
  - A template for Cisco ASA is available
- Switches should be configured to trust and prioritize EF traffic from end user machines and the Cloud Connect (Completed by customer unless the customer has contracted for managed on-site switches)
  - A template for Cisco switches is available
- End users machine should be configured to tag soft client traffic as EF (Completed by the customer)
  - Instructions to do this on Windows machines is available

Virtual Desktop using Evolve IP Desktop as a Service Solution:

- The Cloud Connect device is configured to guarantee bandwidth to EvolveIP DaaS servers. (Completed by EvolveIP)
- End users machine should be configured to tag soft client traffic as EF (Completed by customer)
  - Instructions to do this on Windows machines is available

NOTE: This process is the same for customers bringing their own Virtual Desktop infrastructure with the exception of prioritizing DaaS traffic back to Evolve's network

Cloud Connect with an onsite router

In this topology, EvolveIP provides a managed Cloud Connect device delivering private connectivity to an onsite router.

Local Operating System Deployment

- The Cloud Connect device is configured to prioritize all traffic to EvolveIP voice services. (Completed by EvolveIP)
- The onsite router should be configured to pass DSCP values and prioritize traffic to EvolveIP voice services. (Completed by customer unless the customer has contracted for a managed on-site router)
  - A template for Cisco IOS routers is available
- Switches should be configured to trust and prioritize EF traffic from end user machines and the Cloud Connect (Completed by customer unless the customer has contracted for managed on-site switches)
  - A template for Cisco switches is available
- End users machine should be configured to tag soft client traffic as EF (Completed by the customer)
  - Instructions to do this on Windows machines is available

Virtual Desktop using Evolve IP Desktop as a Service Solution

- The Cloud Connect device is configured to guarantee bandwidth to EvolveIP DaaS servers. (Completed by EvolveIP)
- The onsite router should be configured to guarantee bandwidth to EvolveIP DaaS servers (Completed by customer unless the customer has contracted for a managed on-site router)
  - A template for Cisco IOS routers is available

NOTE: This process is the same for customers bringing their own Virtual Desktop infrastructure with the exception of prioritizing DaaS traffic back to Evolve's network

Cloud Connect configured as the default gateway of the local area network

In this topology, EvolveIP provides a managed Cloud Connect device. All onsite traffic uses the Cloud Connect as the default gateway bypassing any other layer 3 devices.

Local Operating System Deployment

- The Cloud Connect device is configured to prioritize traffic to EvolveIP voice services. (Completed by EvolveIP)
- Switches should be configured to trust DSCP values from end user machines and the Cloud Connect (Completed by customer unless the customer has contracted for a managed on-site switches)
  - A template for Cisco switches is available
- End users machine should be configured to tag UC-1 traffic as EF (Completed by Customer)
 - Instructions to do this on Windows machines is available

Virtual Desktop using Evolve IP Desktop as a Service Solution

- The Cloud Connect device is configured to guarantee bandwidth to EvolveIP DaaS servers. (Completed by EvolveIP)
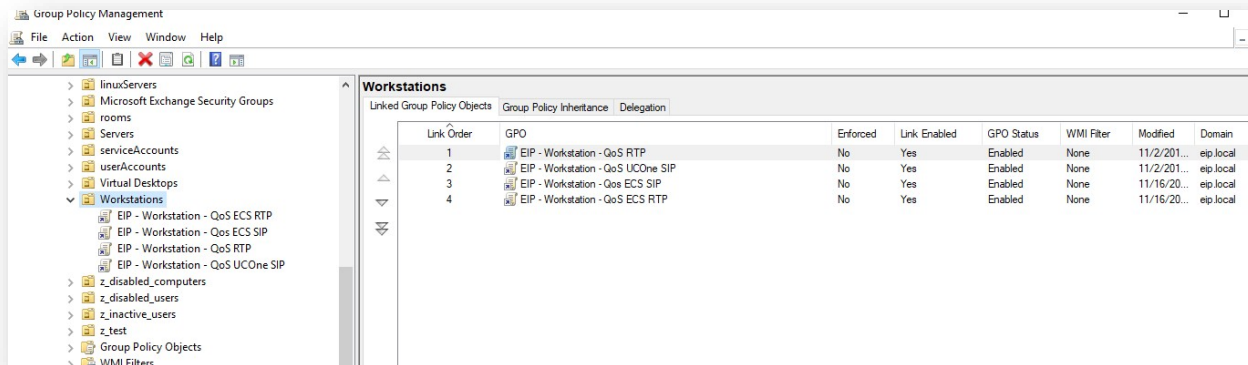
Configuration of QoS Policy for Windows

The following settings assume that the network supports and honors DSCP values for QoS.

### Domain Group Policy Objects
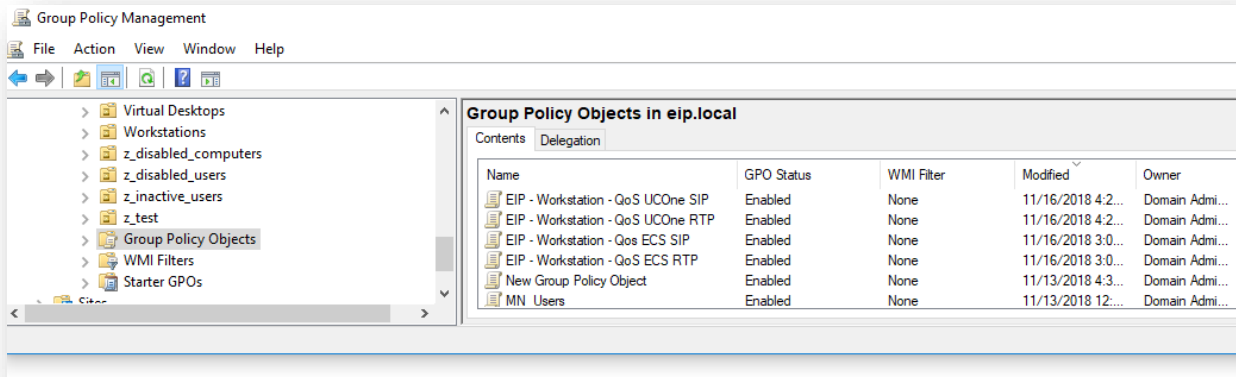
Domain Workstation Group Policy

UC-One or Communicator Softphone Applications

To configure:

1. Open Group Policy Management MMC
2. Expand the treeview for User Configuration\Windows Settings\Policy-base QoS\
3. Right-click on the "Policy-based QoS" object and select "Create new policy..."
4. Create one policy for SIP, per below image **(Application name) Communicator.exe**
5. Create another policy for RTP, per below image **(Application name) Communicator.exe**
6. Restart UC-One
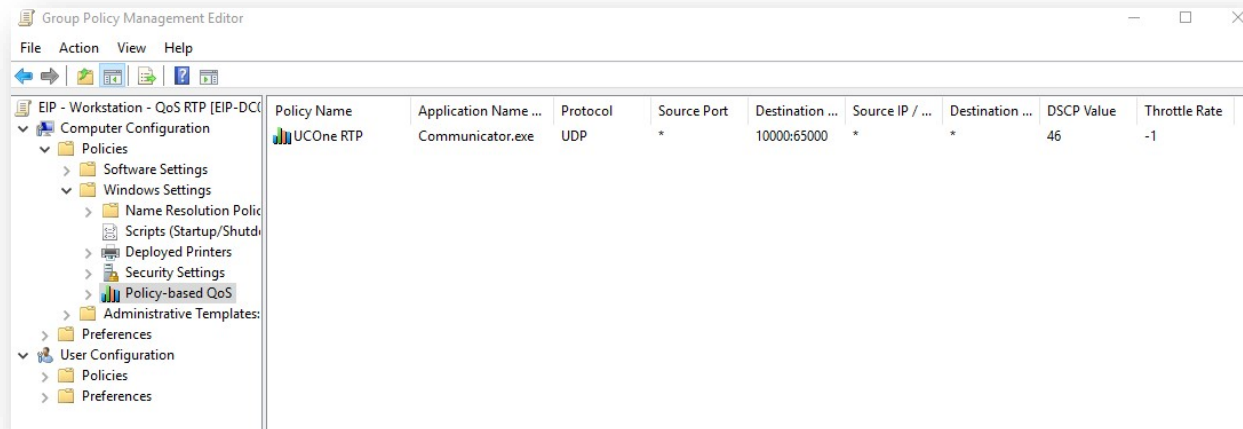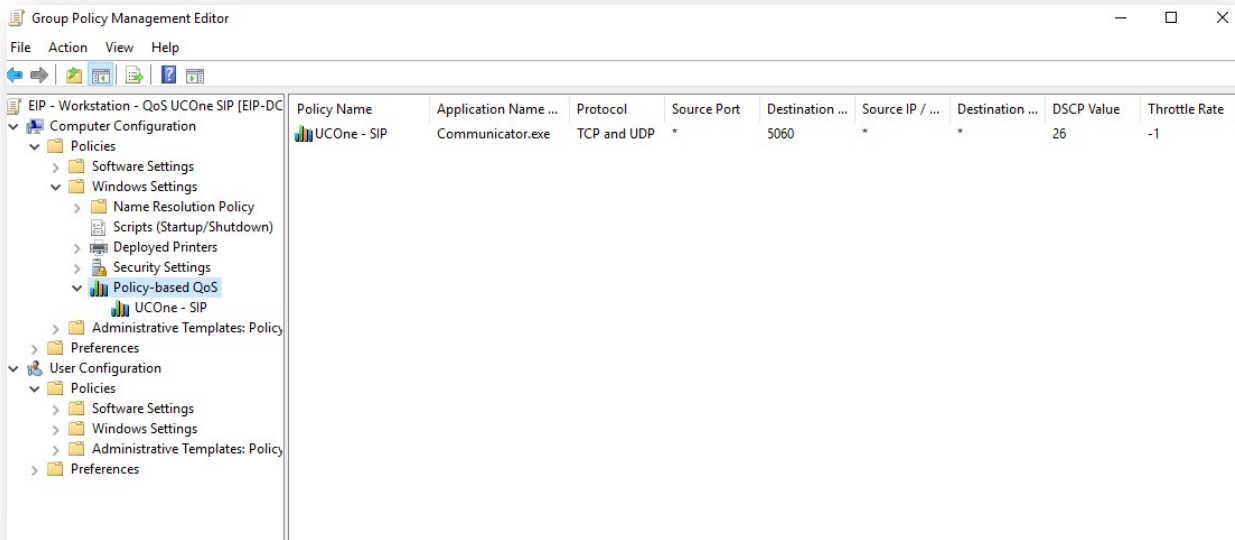
Windows Registry Configuration to Tag UC-One Traffic

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{2C4BB6B3-6997-4C68-901E-
A6576B2B5777}User\Software\Policies\Microsoft\Windows\QoS]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{2C4BB6B3-6997-4C68-901E-
A6576B2B5777}User\Software\Policies\Microsoft\Windows\QoS\UC-One RTP]
"Version"="1.0"
"Application Name"="c:\\Program Files (x86)\\Evolve IP\\UC-One\\Communicator.exe"
"Protocol"="UDP"
"Local Port"="*"
"Local IP"="*"
"Local IP Prefix Length"="*"
"Remote Port"="10000:65000"
"Remote IP"="*"
"Remote  IP  Prefix  Length"="*"
"DSCP Value"="46"
"Throttle  Rate"="-1"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{2C4BB6B3-6997-4C68-901E-
A6576B2B5777}User\Software\Policies\Microsoft\Windows\QoS\UC-One SIP]
"Version"="1.0"
"Application Name"="c:\\Program Files (x86)\\Evolve IP\\UC-One\\Communicator.exe"
"Protocol"="*"
"Local Port"="*"
"Local IP"="*"
"Local IP Prefix Length"="*"
"Remote Port"="5060"
"Remote IP"="*"
"Remote  IP  Prefix  Length"="*"
"DSCP Value"="26"
"Throttle  Rate"="-1"
```

Evolve Contact Suite Softphone Applications

To configure:

1. Open Group Policy Management MMC
2. Expand the treeview for Computer Configuration\Windows Settings\Policy-base QoS\
3. Right-click on the "Policy-based QoS" object and select "Create new policy..."
4. Create one policy for SIP, per below image **(Application name) EvolveContactAgent.exe**
5. Create another policy for RTP, per below image **(Application name) EvolveContactAgent.exe**
6. Restart ECS Agent
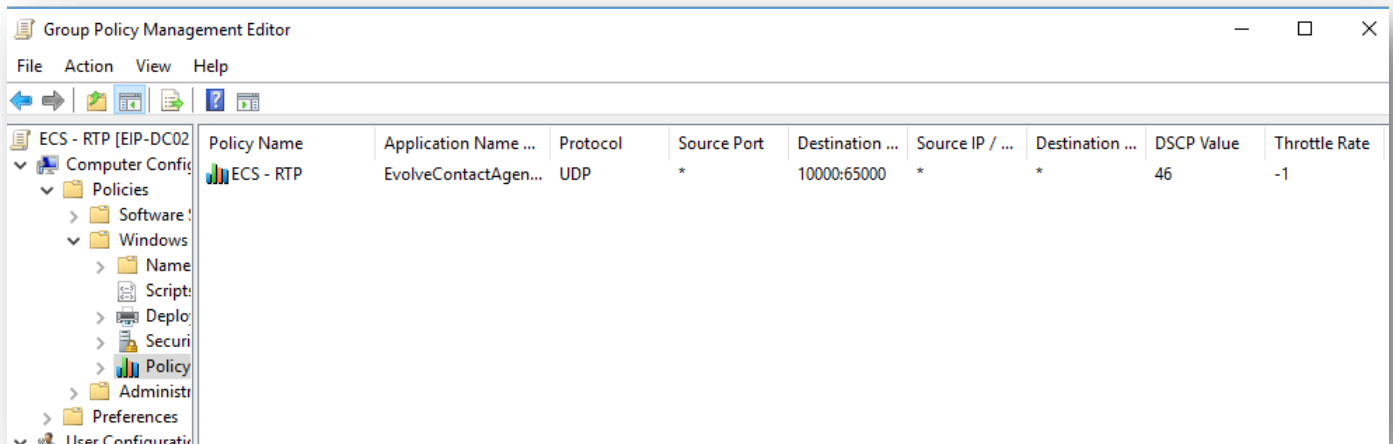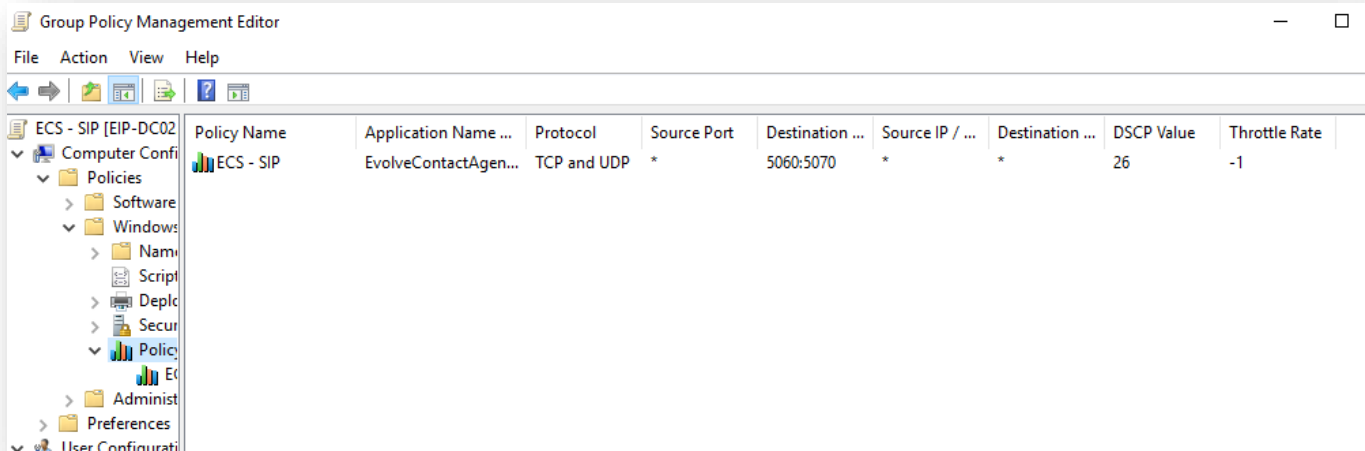
*The same steps should be applied for the ECS Supervisor with the application name **EvolveContactSupervisor.exe***

Appendix A: Cisco Configuration

I. Cisco Router QoS Configuration

ip access-list ext DaaS
permit ip any 207.195.238.0 0.0.0.127
permit ip any 64.27.43.0 0.0.0.63

ip access-list ext VOICE_PUBLIC
permit ip any 69.39.190.112 0.0.0.15
permit ip any 74.117.227.0 0.0.0.63
permit ip any 162.213.114.128 0.0.0.15
permit ip any 64.27.39.160 0.0.0.31
permit ip any 208.89.20.112 0.0.0.15
permit ip any 199.66.103.32 0.0.0.31
permit ip any 64.27.43.96 0.0.0.15

 Class-map match-any VOICE
   Match ip dscp 46
   Match access-group name VOICE_PUBLIC

 Class-map match-any DaaS
  Match access-group name DaaS

 policy-map VOICE
   class VOICE
   priority
     police cir percent 40
      conform-action transmit
      exceed-action drop
   class DaaS
     bandwith percent 50

interface "WAN interface"
service-policy output VOICE

II. Cisco ASA QoS Configuration

class-map VOICE
 match dscp ef

policy-map VOICE_POLICY
 class VOICE
   priority

service-policy VOICE_POLICY interface outside

III. Cisco Switch QoS Configuration

mls qos

interface "trunks and ports connecting to end users and cloud connect"

mls qos trust dscp
priority-queue out