# RADIUS-based Web Authorization with Local Breakout - Basic

The following topics are discussed:



# Feature Description

## Overview

In earlier releases, the SaMOG Gateway supports the Web Authorization and Local Breakout features:

- The Web Authorization feature enables SaMOG to register the subscriber's non-SIM UEs by authenticating the subscriber through a web portal (using username and password). In the pre-authentication phase, SaMOG allocates the IP address to the UE. In the TAL/post-authentication phase, the P-GW allocates the IP address to the UE.
- The Local Breakout – Basic feature enables SaMOG to connect subscriber's UE directly to the Internet without employing a local or external P-GW. The UE's IP address is allocated using an IP pool configured locally (or provided by the AAA Server).

For more information on the Web Authorization and Local Breakout – Basic features, refer the *SaMOG Administration Guide*.

This feature integrates SaMOG as a gateway in deployment architectures where service providers (such as cable operators) can connect subscriber's non-SIM UEs to the Internet without an external P-GW, using policies and rules provided by the RADIUS-based AAA server. Gx and Gy interface's capabilities are not required on these networks. The subscribers of the non-SIM devices are authenticated using web authorization, and connected to the Internet Service Provider (ISP) using Local Breakout – Basic.

## License Requirements

The following licenses are required for RADIUS-based web authorization with LBO – Basic:

- SaMOG Local Breakout – Basic license
- SaMOG Web Authorization license
- Enhanced Charging Bundle (ECS) license
- (Optional) Application Detection and Control (ADC) license – To enable ADC related features

Contact your Cisco account representative for detailed information on specific licensing requirements.

# Relationship to Other Features

## Application Detection and Control (ADC)

This feature can support ADC functionalities when the ADC license is installed.

# How RADIUS-based Web Authorization with LBO Basic Works

# Architecture

## Web Authorization

### Pre-Authentication Phase

During the pre-authentication phase of web authorization, the Access-Accept message from the RADIUS-based AAA server contains the following attributes to enable SaMOG to assign IP address the UE and redirect the subscriber to the web portal:

- User-Name (UE MAC) – This is a mandatory attribute.
- SN1-Rulebase (Rulebase name in Starent VSA) – SaMOG redirects traffic to the web portal for subscriber authentication based on the configured rulebase, and its related ruledef and charging action. The rulebase can also be configured under the APN profile for SaMOG to use when the AAA Server does not share the rulebase. When both the rulebases exist, SaMOG will use the rulebase provided by the AAA Server.
- SN1-VPN-Name (Context name in the Starent VSA) – SaMOG allocates IPv4 or IPv6 address to the UE based on the IP pool configured for the context. The context can also be configured locally under the APN profile for SaMOG to use when the AAA Server does not share the context name.
- Framed-Pool (Pool name) – To indicate IPv4 and IPv6 pools, the AAA Server can send more than one IP pool name to SaMOG. SaMOG selects the pool configured under the context when the AAA Server does not share the pool name.
- Filter-ID (ACL name) – This attribute contains the allowed ACL for the UE.

### Post-Authentication Phase

After the pre-authentication phase, SaMOG awaits the IMSI or MN-NAI attribute from the AAA Server in the CoA message. This CoA message acts as the post-authentication trigger. On receiving the CoA message,

SaMOG removes the redirection rule and installs new rules from the CoA message. If the CoA message is not received within 5 minutes (timer expiry of 300 seconds), SaMOG disconnects the session.

## DSCP Marking

SaMOG supports DSCP marking in the web authorization post-authentication or direct TAL phase for uplink and downlink traffic. The QCI value is obtained in one of the following ways:

- The qci-qos-mapping table can be configured with the QCI value using the **qos default-bearer qci** *qci_value* under the APN Profile Configuration Mode. The QCI value can also be configured for the CGW service. Operator-defined DSCP marking, copy inner and copy outer options are supported.
- DSCP marking configured in the charging-action associated with a rulebase (using the Enhanced Charging Service). DSCP marking can be performed during pre-authentication and post-authentication phases.
- Default QCI value of 9.

When the qci-qos-mapping definition and configuration for DSCP marking under the charging-action exist, SaMOG will prefer the configuration for DSCP marking under the charging-action.

The following decision table provides various combinations of QCI configurations in the network, and the QCI value selection by SaMOG:

| QCI received from AAA Server | QCI configured under APN profile | Charing action enabled with DSCP configuration | DSCP Marking (QCI value for the qci-qos-mapping table) |
|---|---|---|---|
| Yes | No | No | Value provided by the AAA Server |
| Yes | Yes | No | Value provided by the AAA Server |
| No | Yes | No | Value configured under the APN profile |
| No | No | No | Default QCI value of 9 |
| Yes | No | Yes | Value configured under Charging Action |
| No | Yes | Yes | Value configured under Charging Action |
| Yes | Yes | Yes | Value configured under Charging Action |
| No | No | Yes | Value configured under Charging Action |

## SaMOG as an Accounting Client

SaMOG can perform the functionalities of an accounting client when access points do not have this capability. Use the **accounting mode radius-diameter** command under the Call Control Profile Configuration Mode to enable SaMOG to act as an accounting client. When enabled, SaMOG supports WLAN attributes like calling-station-id and called-station-id in the RADIUS accounting messages.

# Flows

The figure below shows the detailed RADIUS-based web authorization flow with LBO – basic. The table that follows the figure describes each step in the flow.

*Figure 1: RADIUS-based Web Authorization with LBO – Basic Call Flow*

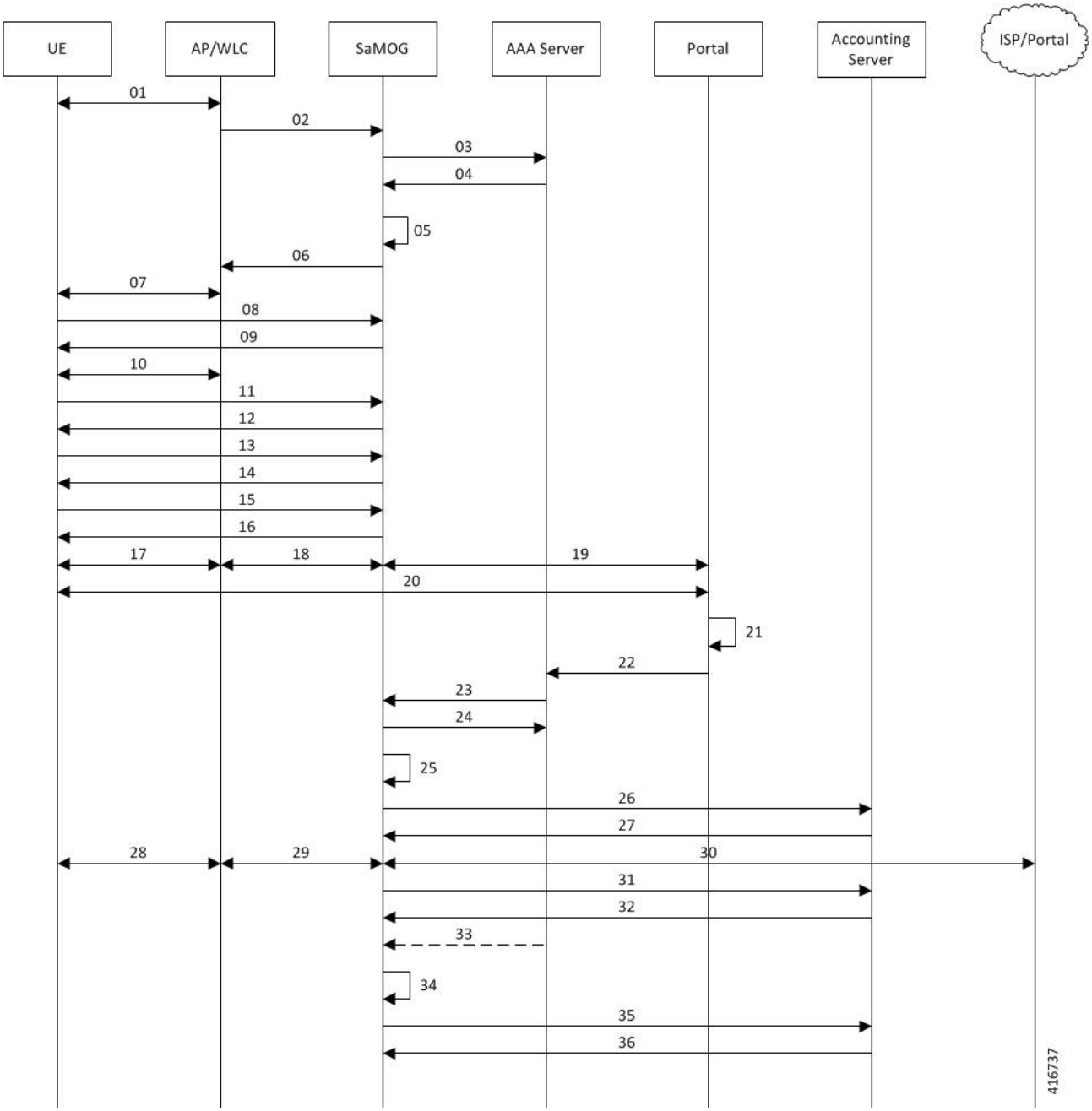


*Table 1: RADIUS-based Web Authorization with LBO – Basic*

| Step | Description |
|---|---|
| 01 | UE sends 802.1x association request to AP/WLC with the SSID/Open-SSID information that it wishes to associate with. |

| Step | Description |
|---|---|
| 02 | On the WLC, the SSID is configured with MAC-based authentication, and SaMOG as the RADIUS Server.<br>The WLC sends an Access-Request (user-name=UE-MAC, called-station-id=AP-MAC:SSID, Calling-Station-Id=UE-MAC) message to SaMOG without the EAP payload. |
| 03 | On SaMOG, an SSID-based policy is applied.<br>If applicable, the operator policy allows Non-EAP based authentication. SaMOG fetches the AAA authentication server information from the policy. SaMOG initiates the authentication process by sending the Access-Request message received from the AP/WLC to the AAA server. |
| 04 | On the AAA Server, a MAC-based session lookup takes place as the user session is not found. Since the AAA Server is configured to allow user sessions, it sends an Access-Accept message to SaMOG. The subscription details will not be available on the AAA Server at this point. So the AAA Server sends only the user-name AVP in Access-Accept message.<br>Optionally, the AAA server can provide the Filter-Id AVP and SN1-Rulebase AVPs for redirection along with SN1-IP-Pool-Name, SN1-VPN-Name, SN1-Primary/Secondary-DNS-Server, Framed-IPv6-Pool, SN1-IPv6-Primary/Secondary/DNS parameters. |
| 05 | Since the AAA Server does not provide the APN, SaMOG fetches the default web authorization APN profile associated to the operator policy. This APN profile is configured for IP address allocation and traffic redirection (if rulebase is not provided by the AAA Server).<br>SaMOG performs the following procedures before sending the Access-Accept message to WLC:<br>• Reserves IP Address (a.b.c.d and p:q:r:s::/64) from the local IP/IPv6 pool for UE.<br>• Installs L4/L7 redirection rules to redirect the user traffic to the web portal and installs downlink NPU flow for the allocated ip-address and ipv6-prefix.<br>• Initiates webauth_preauth_timer with a timeout value of 5 minutes. Post-authorization phase will be triggered within this timer. |
| 06 | SaMOG forwards the RADIUS Access-Accept message to the AP/WLC. |
| 07 | The WLC/AP sends an 802.1x association response to the UE. MAC-based authentication between the UE and AP/WLC is complete. |
| 08 | UE initiates an L3 attach procedure by sending a DHCP-Discover. SaMOG receives the same through the EoGRE tunnel. |
| 09 | SaMOG sends the allocated IPv4 address, default gateway address, and the lease duration through the DHCP-Offer message to the UE. |
| 10 | SaMOG sends DHCP-Request with a request IP as received in DHCP-Offer. SaMOG responds with a DHCP-Reply confirming the allotment of IP address. |
| 11 | UE sends the ARP-Request message to resolve the MAC address of the default gateway. |

| Step | Description |
|---|---|
| 12 | SaMOG sends ARP-Reply message to the UE with the virtual MAC address that is configured in the APN profile. |
| 13 | For IPv6/Dual stack, the UE sends a Router Solicitation to obtain the IPv6 address/prefix. |
| 14 | SaMOG responds to the UE with a Router Advertisement containing the IPv6 prefix. |
| 15 | UE sends a Neighbor Solicitation to determine the link-layer address of SaMOG. |
| 16 | SaMOG sends a Neighbor Advertisement to the UE with its link-layer address. The UE may also send a DHCPv6-Info-Request to obtain the DNS server addresses at this stage. If received, SaMOG sends a DHCPv6-Info-Reply with the DNS server addresses configured under the APN profile. |
| 17 | UE initiates data packets. |
| 18 | SaMOG receives the data packets from the UE through the EoGRE tunnel. |
| 19 | SaMOG redirects the traffic to a web portal as per the redirection rules installed (Step 5).<br>If L4 rules are applied, SaMOG changes the destination address to the IP address of the portal, and forwards the packets.<br>If L7 rules are applied, SaMOG redirects the packets to the IP address of the portal without modifying the destination address. |
| 20 | UE provides the subscriber's credentials for authorization. |
| 21 | Web-based authorization takes place between the UE and the portal server. |
| 22 | Portal server indicates the successful authentication status with the AAA server. |
| 23 | Post successful authentication, the AAA server triggers post-authorization phase by sending a CoA with the IMSI/MN-NAI and new rulebase in the SN1-Rulebase AVP. If CoA doesn't contain IMSI/MN-NAI identifier, SaMOG will not consider the CoA as a post-authorization trigger. |
| 24 | SaMOG sends CoA-Acknowledgement to the AAA Server. |
| 25 | SaMOG removes the redirection rules and installs the new rulebase received in the CoA message. SaMOG will offload the traffic locally with certain ECS capabilities. |
| 26 | SaMOG sends an Accounting-Request (Acct-Status-Type: Start) to the accounting server, if SaMOG has been configured to act as the Accounting client. |
| 27 | The Accounting Server sends an Accounting-Response to SaMOG. |
| 28 | UE initiates data packets. |
| 29 | SaMOG receives the data packets through the EoGRE tunnel. |
| 30 | SaMOG locally offloads the traffic to ISP without any redirection. SaMOG enforces any ECS capabilities like DSCP marking, rate limiting, MSS overwriting, and so on. |

| Step | Description |
|---|---|
| 31 | When the accounting interim conditions (volume/interval) configured under the AAA group are met, SaMOG sends an Accounting-Request (Acct-Status-Type: Interim) to the Accounting Server. |
| 32 | The Accounting Server sends an Accounting-Response to SaMOG. |
| 33 | (Optional) The AAA Server could send more CoA messages to SaMOG to install new rules. |
| 34 | SaMOG installs the new rules received in the CoA message. |
| 35 | Upon UE detach, SaMOG sends an Accounting-Request (Acct-Status-Type: Stop) message to the Accounting Server. |
| 36 | The Accounting Server sends an Accounting-Response message to SaMOG. |

# Configuring RADIUS-based Web Authorization with LBO – Basic

## Configuring Local Breakout – Basic

The following is a sample configuration to enable Local Breakout – Basic:

```
lte-policy
    subscriber-map smap
      precedence 1 match-criteria all operator-policy-name oppolicywebauthdia

  operator-policy name oppolicywebauthdia
    associate call-control-profile cc-profwebauthdia
    apn webauth-apn-profile apnprfwebauth

  call-control-profile cc-profwebauthdia
    accounting context aaa aaa-group accounting1
    authenticate context aaa aaa-group STawebauth auth-method eap non-eap
#exit

apn-profile apnprfwebauth
    ip access-group acl-lbo-flow in
    ip access-group acl-lbo-flow out
    ip address pool name lbo-pool-1
    active-charging rulebase rb_lite
    ip context-name lbo-gi
    local-offload
    twan default-gateway 12.0.0.10/8
    accounting mode gtpp
    associate accounting-policy acctpolicy4g
    accounting context aaa gtpp group gtpp4g
  #exit

  context lbo-gi
    ip access-list acl-lbo-flow
      redirect css service acs1 any
    #exit
    ipv6 access-list acl-lbo-flow
      redirect css service acs1 any
    #exit
```

```
    ip pool lbo-pool-1 12.0.0.0 255.255.255.252 public 0 policy allow-static-allocation
subscriber-gw-address 12.0.0.2
    ipv6 pool pool_ipv6 prefix 1:2:3:5:5:6:7:9/48 public 0 policy allow-static-allocation
    interface ISP
      ip address 192.168.200.1 255.255.255.0
      ipv6 address bbbb::1/64 secondary
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp group default
    #exit
```

# Configuring DSCP Marking by SaMOG

The following is a sample configuration for SaMOG to mark DSCP values:

```
config
    qci-qos-mapping qci_qos_map_name
        qci qci_value_1 downlink encaps-header copy-inner
        qci qci_value_1 uplink encaps-header copy-inner
        qci qci_value_1 downlink encaps-header copy-outer
        qci qci_value_1 uplink encaps-header copy-outer
        qci qci_value_2 downlink encaps-header dscp-marking value1
        qci qci_value_2 uplink encaps-header dscp-marking value2
end

config
    apn-profile profile-name
      associate qci-qos-mapping qci_qos_map_name
        end

config
    context context_name
        cgw-service service_name
          associate qci-qos-mapping qci_qos_map_name
            end
```

**Important** The DSCP marking configuration under the APN Profile Configuration Mode takes priority over the DSCP marking configuration under the CGW Service Configuration Mode.

# Configuring DSCP Marking by ECS

The following is a sample configuration for the AAA server to send a rulebase in the Access-Accept/CoA message. The APN profile can also be configured with the rulebase with DSCP marking as **ef** (expedite forwarding) in both uplink and downlink traffic:

```
rulebase rulebase_name
   action priority action_priority ruledef ruledef_name charging-action charging_action_name


ruledef ruledef_name
    ip any-match = TRUE

charging-action charging_action_name
    content-id id
```

```
    ip tos ef uplink
    ip tos ef downlink
```

# Configuring SaMOG to act as the RADIUS Accounting Client

The following is a sample configuration to enable SaMOG to act as the RADIUS accounting client:

```
call-control-profile call_control_profile_name
    accounting mode radius-diameter
    associate accounting-policy accounting_policy_name
    accounting context aaa aaa-group aaa_group_name
    authenticate context aaa aaa-group aaa_group_name auth-type radius auth-method eap
non-eap
    exit

aaa group accounting_policy_name
    radius attribute nas-ip-address address ip_address
    radius dictionary custom71
    radius accounting server ip_address key key port port_number
    radius accounting interim interval interim_interval
    radius accounting interim volume total interim_volume
    exit

    policy accounting accounting_policy_name
        cc profile 2 interval interval
        cc profile 2 volume total total
        cc profile 8 interval interval
        cc profile 8 volume total total
    exit
```

# Monitoring and Troubleshooting

# RADIUS-based Web Authorization with LBO Basic Show Command(s) and/or Outputs

## show subscriber samog-only full

The following field is available in the output of the **show subscriber samog-only full** command in support of this feature:

```
CGW Subscriber Info:
---------------------
   QCI                 : 9
```

***Table 2: show subscriber samog-only full Command Output Descriptions***

| Field | Description |
|---|---|
| **CGW Subscriber Info** | |
| QCI | Subscriber's QCI value. |

**show subscriber samog-only full**