Web Authorization Session Logout

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	SaMOG
Applicable Platform(s)	ASR 5500 vPC-SI vPC-DI
Default Setting	Enabled (depending on the response from the AAA Server)
Related CDETS ID(s)	CSCvc67377
Related Changes in This Release	Not Applicable
Related Documentation	SaMOG Administration Guide Command Line Interface Reference Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Overview

The SaMOG Gateway supports the Web Authorization feature that enables SaMOG to register the subscriber's non-SIM UEs by authenticating the subscriber through a web portal (using username and password). On successful authentication, the AAA server stores the subscriber profile (APN, IMSI, QoS) from the HLR/HSS for the subscriber's device, and SaMOG establishes the network connection for the UE.

The Web Authorization feature has two phases:

- Pre-Authentication Phase – SaMOG allocates the IP address for the UE locally, and redirects the UE traffic to a web portal for subscriber authentication.
- Post-Authentication/Transparent Auto Logon (TAL) phase – P-GW allocates the IP address to the UE.

During transition between the two phases, the subscriber session disconnects. The Web Authorization feature can also be configured where the transition between the pre-authentication and post-authentication phases are achieved without session disconnection (optimized Web Authorization feature).

Refer the *Web Authorization* and *Optimized Web Authorization* sections in the *SaMOG Administration Guide* for more information on these features.

The Web Authorization Session Logout feature provides additional functionality to the Web Authorization feature. In release 21.1 and earlier, when the subscriber logs out of the portal or exhausts the quota, SaMOG clears the subscriber session on receiving a trigger from the P-GW or PCRF.

In Release 21.2 and later, SaMOG does not clear the subscriber session when the subscriber logs out of the portal or exhausts the quota. The subscriber session is instead moved from the post-authentication phase to the pre-authentication phase, and retained until the subscriber logs back in, or the timeout period (configurable) expires. This functionality enables operators to provide session stickiness for subscribers by retaining the subscriber’s Wi-Fi network connection.

License Requirements

The Web Authorization Session Logout feature requires the following licenses:

- SaMOG General license
- SaMOG Web Authorization feature license (to configure web authorization)
- SaMOG Local Breakout feature license (to configure a local P-GW)

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

How Web Authorization Session Logout Works

Architecture

When the subscriber logs out from the web portal or exhausts the quota, the AAA Server initiates a subscription change request to SaMOG. The AAA Server does not include the APN subscription, vIMSI, or NAI information for the session (portal redirection rulebase, ACL name, IP pool name and Gi context names are optionally shared). On receiving the subscription change request without the user identity information, SaMOG verifies if the subscriber session is in post-authentication phase. SaMOG then switches the session back to the pre-authentication phase by initiating an address transfer from the local P-GW (through the VPN manager) to SaMOG, and installing the redirection rules and ACLs. CDRs used during the post-authentication phase are released when the session moves to the pre-authentication phase. New CDRs are used if the session moves back to the post-authentication phase.

The subscriber session will be retained in the pre-authentication phase until the subscriber re-authenticates through the web portal, or the session in the pre-authentication phase timeout period expires. The timeout period can be configured using the **disconnect preauth-wait-time** command under the MRME Configuration Mode.

Limitations

Architectural Limitations

- This feature is currently not support on GTPv1 and PMIPv6 towards P-GW.
- Only AAA Diameter-based authentication is supported. AAA Radius-based authentication is currently not supported.
- Inter-chassis session recovery (ICSR) is currently not supported with this feature.

Flows

Post-authentication to Pre-authentication

The figure below shows the detailed flow for the subscriber session moving from the post-authentication phase to the pre-authentication phase. The table that follows the figure describes each step in the flow.

Figure 1: Post-Authentication to Pre-Authentication Call Flow

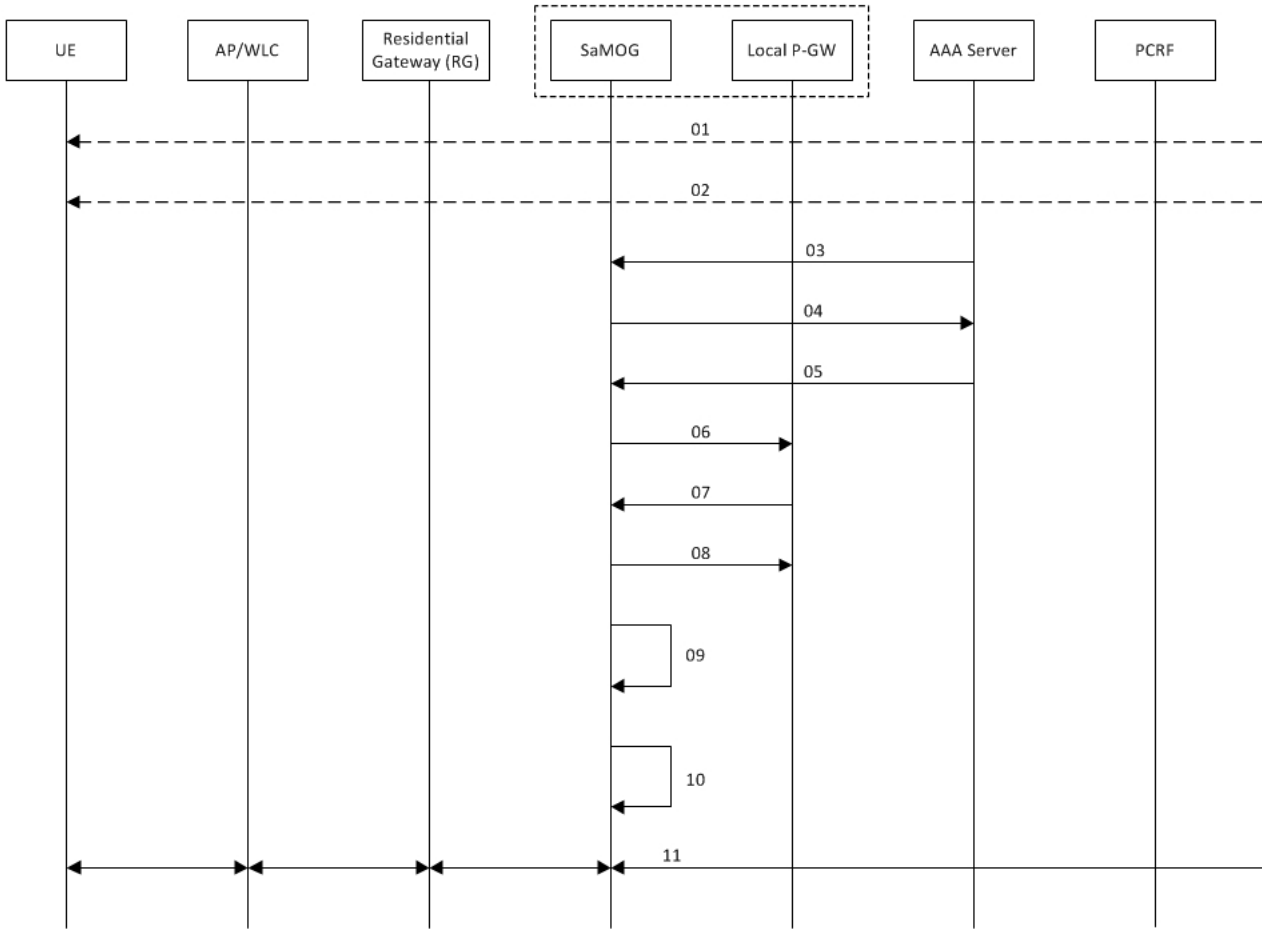

Table 1: Post-authentication to Pre-authentication

Step	Description
1	Subscriber session is established using web authorization.
2	Subscriber logs out from the portal, or exhausts the quota limit for the session.
3	The Diameter Server initiates an RAR message to SaMOG for the session.
4	SaMOG responds with an AAR message to the Diameter Server.
5	The Diameter Server initiates the AAA towards SaMOG where, • The Diameter Server does not share the user identity (no IMSI or NAI). • (optional) Parameters like the redirection rulename, ACL name, IP pool name (IPv4/IPv6) and Gi context name are included.

Step	Description
6	SaMOG receives the subscription change request without the user identity from the AAA Server. If the subscriber session is in the post-authentication phase, SaMOG initiates the process to move the session from post-authentication to pre-authentication phase. • If the AAA Server does not share the rulename, ACL name, IP pool name or context name, SaMOG takes these information from the Web authorization profile. • SaMOG transfers the user-allocated IP address (IPv4, IPv6, or IPv4v6) from the P-GW to SaMOG through the VPN manager. • SaMOG also initiates an ECS session creation with the redirection rulebase and ACLs. • On receiving the address allocation request, the VPN manager initiates an abort request to the P-GW.
7	On receiving the abort request from the VPN manager, P-GW sends a Delete Bearer Request (DBR) to SaMOG.
8	SaMOG responds to the DBR and cleans up the EGTPC/GTPU interfaces. The session, however, is not deleted.
9	The VPN manager provides the addresses requested by SaMOG. SaMOG initiates a FLOW creation for the IPs, and receives the downlink traffic from the ISP for the UE addresses.
10	SaMOG switches the session from post-authentication to pre-authentication on receiving the FLOW creation success notification from the NPU manager.
11	The subscriber is now redirected to the web portal for authorization. Once the subscriber successfully authenticates their identity, pre-authentication to post-authentication procedures are initiated. The AAA Server sends a re-authorization trigger to move the UE back to the post-authentication phase and provide the subscriber with access to the Internet.

Configuring Web Authorization Session Logout

Configuring the Pre-Authentication Wait Timer

Use the following configuration to configure the timeout for the subscriber's session after the session moves from the post-authentication phase to the pre-authentication phase:

```
config
   context context_name
      mrme-service service_name
         disconnect preauth-wait-time minutes
         end
```

Notes:

- Use the **default disconnect preauth-wait-time** command to restore the configuration to its default value.
- **Default:** 5 minutes

- *minutes* must be an integer from 1 through 60.

Monitoring and Troubleshooting Web Authorization Session Logout

Show Command(s) and/or Outputs

show samog-service statistics

The following fields are available to the output of the **show subscribers samog-service statistics** command in support of this feature:

```
MRME Service Stats:
Non-EAP Session Stats:
    Post-to-Pre:
        Attempted:    1               Success:        1
        Failure:    0
```

*Table 2: **show subscribers samog-service statistics** Command Output Descriptions*

Field	Description
MRME Service Stats:	
Non-EAP Session Stats:	
Post-to-Pre:	
Attempted	Total number of non-EAP sessions attempted to move from post to pre-authentication phase.
Success	Total number of non-EAP sessions successfully moved from post to pre-authentication phase.
Failure	Total number of non-EAP sessions that failed to be moved from post to pre-authentication phase.

show subscribers samog-only full

The following fields are available to the output of the **show subscribers samog-only full** command in support of this feature:

```
Web Authorization:    Yes
    Web authorization phase: Pre-Auth
     Post-pre switch: 1
```

*Table 3: **show subscribers samog-only full** Command Output Descriptions*

Field	Description
Web Authorization	Indicates if the web authorization is enabled for the subscriber.

Field	Description
Web authorization phase	Indicates the current web authorization phase for the subscriber session.
Post-pre switch	Total number of times the subscriber session was switched from post-authentication to pre-authentication phase.

Bulk Statistics

The following bulk statistics in the SaMOG schema support this feature:

Variable	Description	Data Type
mrme-non-eap-post-to-preauth-call-attempted	**Description:** Total number of non-EAP sessions attempted to move from post to pre-authentication phase. **Triggers:** Increments whenever a non-EAP session moves from post to pre-authentication phase is attempted. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-non-eap-post-to-preauth-call-success	**Description:** Total number of non-EAP sessions successfully moved from post to pre-authentication phase. **Triggers:** Increments whenever a non-EAP session successfully moved from post to pre- authorization phase. **Availability:** Per SaMOG Service **Type:** Counter	Int32
mrme-non-eap-post-to-preauth-call-failure	**Description:** Total number of non-EAP sessions that failed to be moved from post to pre-authentication phase due to internal errors, missing pre- authorization phase configurations, missing ACL, IP address pool, rulebase, and so on. **Triggers:** Increments whenever a non-EAP session fails to be created. **Availability:** Per SaMOG Service **Type:** Counter	Int32