MN-NAI Support for Web Authorization Calls

This chapter describes MN-NAI support for web authorization calls in the following sections:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	ASR 5500
Feature Default	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *SaMOG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

MN-NAI based authentication is supported for Web Authorization calls.

Earlier, SaMOG only supported IMSI based pre-authentication to post-authentication transition. Now, MN-NAI based pre-authentication to post-authentication transition is also supported.

SaMOG now supports pre-Authentication to post-Authentication transition for DHCP and PMIPv6 triggered sessions. The output for the **show subscribers samog-only full** command is modified to show the pre and post-authentication phases for DHCP and PMIPv6 triggered calls. For DHCP and PMIPv6 triggered calls, the UE-MAC is displayed as Username in the output when the **show subscribers samog-only full** and **show subscribers samog-only all** commands are executed.

For DHCP and PMIPv6 triggered sessions, SaMOG directs a TAL setup towards a local P-GW when an incoming Accept-Accept request contains an IMSI or MN-NAI value as a user identity. If the Accept-Accept request does not contain any user identity, the SaMOG processes the request as a pre-authentication call.

How It Works

The MN-NAI Web Authorization Calls supports:

- MN-NAI in the CoA request.
- Pre-authentication phase for DHCP and PMIPv6 triggered sessions.

The above implementations are applicable for both LBO-Basic and LBO-Enhanced models.

LBO Enhanced (also called as LBO Heavy): Uses a local P-GW/GGSN service locally to offload traffic to the internet. The UE's IP address is allocated by a local P-GW/GGSN service.

LBO Basic (also called as LBO Lite): Does not use a local P-GW/GGSN service. Here, the SaMOG itself offloads data to the internet. The UE's IP address is allocated by an SaMOG service.

MN-NAI is also applicable for DHCP and PMIPv6 triggered sessions. The session establishment call flows for DHCP and PMIPv6 triggered sessions are discussed in the *Call Flows* section.

Note From Release 21.4 onwards, the existing call flows for DHCP and PMIPv6 triggered sessions are not supported.

For more information on DHCP and PMIPv6 triggered sessions, refer to *DHCP Trigger-based Session Creation* and *PMIPv6-based Session Creation* chapters in the *SaMOG Administration Guide* respectively.

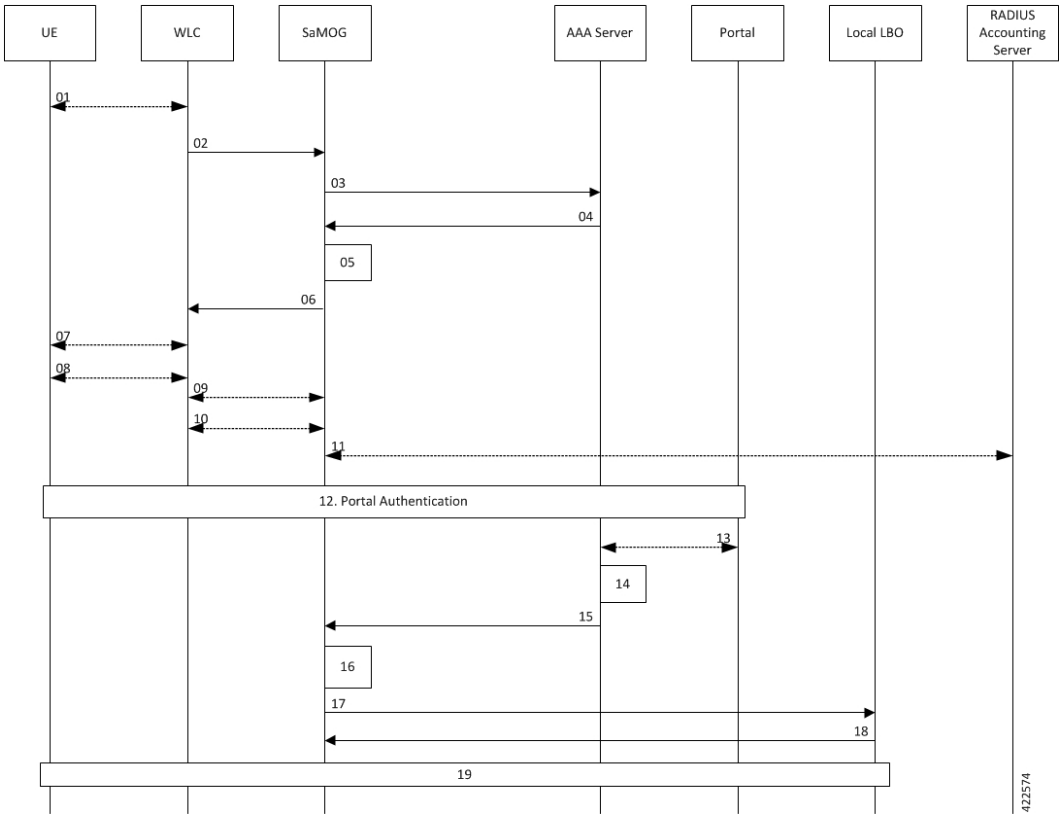
Call Flows

This section provides various call flows that illustrate the procedures used during DHCP and PMIPv6 triggered session establishment.

RADIUS Triggered - Web Authorization Call/Session Establishment

The figure below shows the detailed session establishment flow for a RADIUS triggered session. The table that follows the figure describes each step in the flow.

Figure 1: RADIUS Triggered Session Establishment Call Flow



Step	Description
01	UE sends 802.1x association request to AP/WLC with the SSID/Open-SSID information that it wishes to associate with.
02	WLC sends Access Request to SaMOG as the SSID on WLC is configured with MAC based authentication and the SaMOG is configured as RADIUS Server. Here, the EAP payload will not be present.
03	On SaMOG, SSID based policy is applied. If applicable operator policy allows Non-EAP based authentication, SaMOG fetches the AAA authentication server information from the policy and forwards Access-Request to AAA.
04	AAA sends Access-Accept request to SaMOG. The AAA server also sends a Session-Timeout AVP with a small value to allow web authentication.

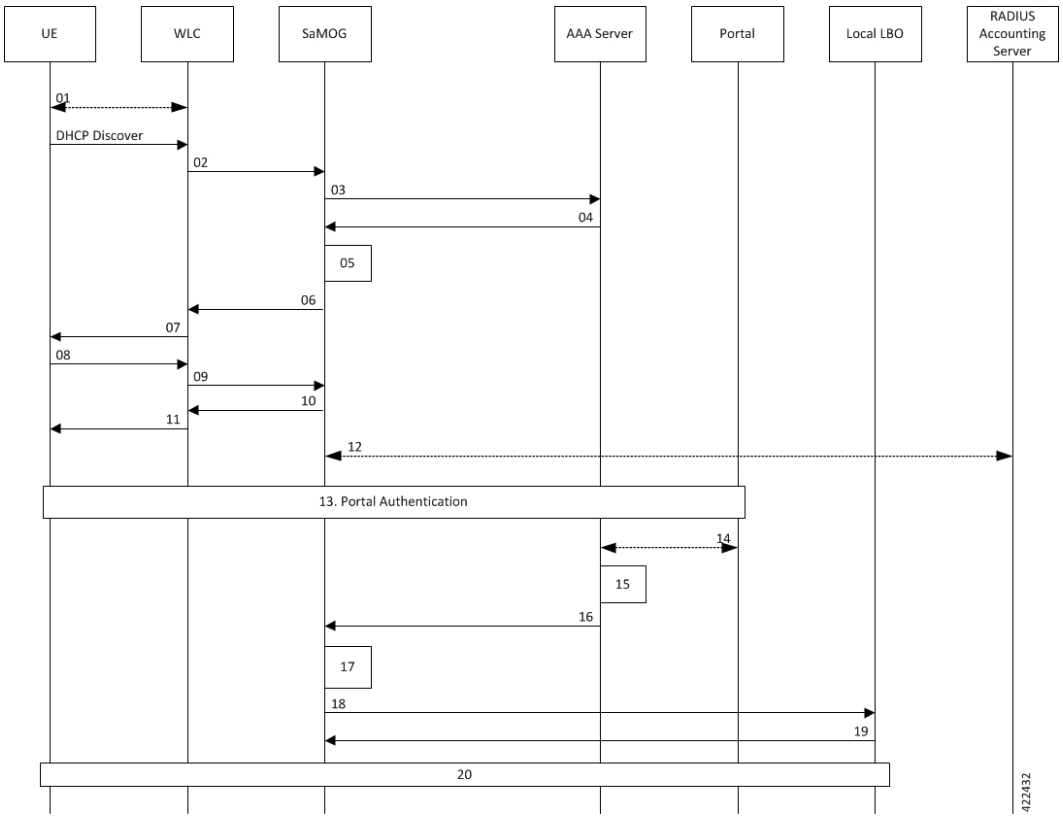
Step	Description
05	SaMOG triggers the following procedures before sending an Access-Accept message to WLC: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules. The local P-GW assigns an IPv4 address and forwards it to the SaMOG Gateway.
06	SaMOG sends Access-Accept to WLC.
07	WLC sends 802.1x association response to UE. MAC based authentication between UE and AP/WLC is now complete.
08	UE performs L3 Attach procedures by initiating DHCP/IPv6-ND messages to WLC for fetching the IP Address or the IPv6-prefix.
09	WLC initiates EoGRE/PMIPv6 procedures towards SaMOG for L3 Attach.
10	Accounting is enabled on WLC and SaMOG is configured as an accounting server on the WLC.
11	SaMOG forwards an accounting start request towards AAA. AAA then associates the UE MAC Address and UE IP Address. AAA sends a Accounting Start Response, which will be forwarded by SaMOG towards WLC.
12	Web-based authentication takes place between UE and Portal Server.
13	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details
14	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
15	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.
16	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile, SaMOG looks for IMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses.

Step	Description
17	es SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the IMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
18	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of end user.
19	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

DHCP-triggered Web Authorization Call/Session Establishment

The following figure illustrates a detailed session establishment flow for a DHCP triggered session.

Figure 2: DHCP-triggered Session Establishment Call Flow



Step	Description
01	The UE communicates with the WLC over the 802.11 link for WiFi association and data transmission.
02	The WLC receives the control (DHCP, ARP, etc.) and data packets from the UE and forwards them over the EoGRE tunnel to the SaMOG gateway.

Step	Description
03	On receiving the DHCP Request or DHCP Discover message sent by the UE from the WLC over the EoGRE tunnel, the SaMOG gateway acts as the RADIUS client and sends a RADIUS Access-Request to the AAA server to obtain the subscriber information based on the UE MAC address (received in L2 DHCP packet).
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message without an IMSI or MN-NAI value in the MAC@realm format. These values are received using CS-AV pair attributes similar to DHCP/Radius Accounting triggered sessions.
05	SaMOG triggers the following procedures: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules. The local P-GW assigns an IPv4 address and forwards it to the SaMOG gateway.
06	The SaMOG gateway in turn forwards the IPv4 address in the DHCP Offer/Reply message to the AP over the EoGRE tunnel.
07	The WLC forwards the DHCP offer with the allocated IP address towards the UE.
08	UE sends a DHCP request towards the WLC.
09	WLC forwards the DHCP request towards SaMOG.
10	SaMOG provides a DHCP acknowledgment.
11	The DHCP acknowledgment is forwarded to the UE.
12	SaMOG sends a RADIUS Accounting Request to the RADIUS accounting server and receives the corresponding response.
13	Web-based authentication takes place between UE and Portal Server.
14	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details.
15	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
16	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.

Step	Description
17	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile, SaMOG looks for vIMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses. SaMOG retains the allocated IP addresses and stops the webauth_preauth_timer.
18	SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the vIMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
19	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of end user.
20	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

PMIPv6-triggered Web Authorization Call/Session Establishment

The following figure illustrates a detailed session establishment flow for a PMIPv6-based session.

Figure 3: PMIPv6-triggered Session Establishment Call Flow

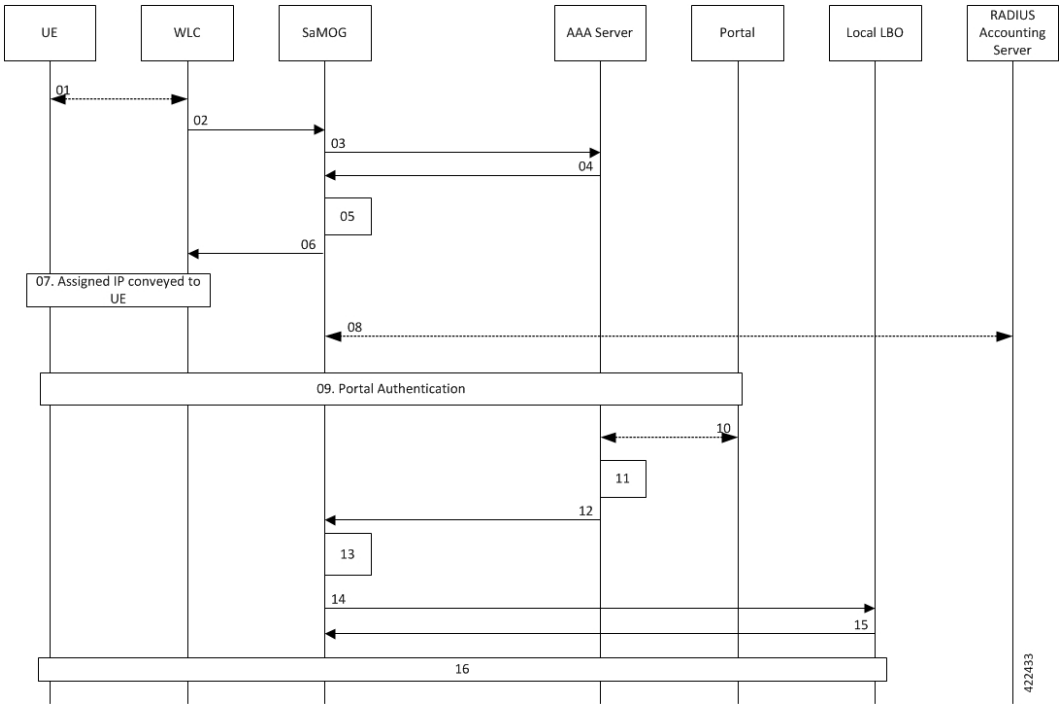


Table 1: PMIPv6-triggered Session Establishment Call Flow Descriptions

Steps	Description
01	UE performs 802.11 association with the WLC.
02	WLC forms a PMIPv6 Proxy Binding Update (PBU) and sends it to SaMOG. The message has the following parameter: UE MAC address in the Username part of NAI, or NAI can be only UE MAC (MAC@realm or MAC).
03	SaMOG caches the PBU message and maps its contents to the Radius Access-Request message towards the AAA server.
04	AAA server determines that the UE MAC is not authenticated and sends an Access-Accept message without an IMSI and MN-NAI value in the MAC@realm format. These values are received using CS-AV pair attributes similar to DHCP/Radius Accounting triggered sessions.
05	SaMOG triggers the following procedures: • Allocate IP address from the local pool. • Initiate the Web-Auth and Pre-Auth timer. • Install L4/L7 Redirect Rules.
06	SaMOG completes the session creation by sending the PBA message to the WLC.
07	UE attempts to access the HTTP page and the HTTP packet reaches the local gateway through SaMOG.
08	SaMOG sends a RADIUS Accounting Request to the RADIUS accounting server and receives the corresponding response.
09	Web-based authentication takes place between UE and Portal Server.
10	After the user is authenticated, portal server fetches MSISDN, IMSI or MN-NAI information of the user. Portal sends CoA request (user-name, IMSI or MSISDN, UE IP Address) towards AAA. AAA associates the UE MAC Address and UE IP Address with the IMSI, MSISDN or MN-NAI value. It sends MAP request towards HSS to fetch the UE subscription details.
11	AAA associates the UE MAC address, UE Subscription with the IMSI, MSISDN or MN-NAI value of the subscriber.
12	Further to this, AAA will be able to provide UE subscription details to SaMOG for a MAC based look-up. AAA caches this information as per operator policy, so that UE need not be redirected to the portal server every time.

Steps	Description
13	SaMOG processes the received RADIUS CoA based on locally configured web-authentication APN-profile. SaMOG looks for IMSI or MN-NAI value in CoA. If IMSI or MN-NAI is part of CoA packet, SaMOG removes the L4-Redirection rules, and also removes the DL NPU flow for the allocated IP addresses. SaMOG retains the allocated IP addresses, and stops the webauth_preauth_timer.
14	SaMOG initiates a GTPv2 CSReq for static IP address allocation with a.b.c.d and p:q:r:s::/64 for provided the vIMSI or MN-NAI value towards Local LBO based on received subscriber profile or locally configured APN-profile in case subscriber-profile is not received as part of RADIUS CoA.
15	SaMOG receives a GTPv2 CSResp from Local LBO with the allocated IP addresses of the end user.
16	SaMOG forwards the packet through the Local LBO; through the GTP-U Tunnel.

Limitations

SaMOG does not support RADIUS Accounting Triggered sessions for Web Authentication. This is under development and intended for future use. In Release 21.4, only TAL (post-authentication phase) is supported for RADIUS Accounting triggered sessions.

Monitoring and Troubleshooting

This section provides information on the show commands available to support the MN-NAI Support for Web Authorization Calls.

Show Command(s) and/or Outputs

show subscribers samog-only full

The following new fields are added to the output of this command for DHCP and PMIPv6 session triggers during the pre-authentication phase:

- DHCP Trigger
  - Web authorization phase
  - IP pool name
  - IPv6 pool name
  - IP context name
  - Rulebase name
  - Access-list Name

- Post-pre switch

- PMIPv6 Trigger
  - Web authorization phase
  - IP pool name
  - IPv6 pool name
  - IP context name
  - Rulebase name
  - Access-list Name
  - Post-pre switch