MRME Service Configuration Mode Commands

Command Modes

The MRME Service Configuration Mode provides commands to enable a trusted WLAN network to provide access to the Evolved Packet Core (EPC) using a AAA peer functionality.

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mrme-service)#`

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

aaa

This command allows you to control the range of EAP-payload size, or restrict the Framed-MTU AVP from being forwarded in the Auth-Request message to the AAA server.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mrme-service)#`

Syntax Description

aaa send framed-mtu *eap_payload_size*
no aaa send framed-mtu

no

Disables SaMOG from forwarding Framed-MTU AVP in the Auth-Request message to the AAA server.

eap_payload_size

Specifies the EAP payload limit for the AAA server to use during the Auth-Response on the link between the NAS and the peer.

twan_profile_name must be an integer from 64 through 1500.

Usage Guidelines This command enables SaMOG to support EAP TLS and EAP TTLS-based authentication. Use this command to control the range of EAP-payload size, or restrict the Framed-MTU AVP from being forwarded in the Auth-Request to the AAA server.

Example

The following command sets the EAP payload size to 1000:

```
aaa send framed-mtu 1000
```

associate

This command associates one or more TWAN profile with this MRME service.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mrme-service)#`

Syntax Description **[no] associate twan-profile** *twan_profile_name*

no

Removes the association of the TWAN profile with the MRME service.

twan_profile_name

Specifies the twan profile to associate with the MRME service.

twan_profile_name must be an integer from 1 through 64.

Usage Guidelines

Use this command to associate one or more TWAN profile with the MRME service. Once a TWAN profile is associated with the MRME service, SaMOG uses the Radius clients and access type for the clients configured under the TWAN Profile while processing the Radius messages from WLC.

For more information on configuring the Radius clients and access type, refer the *TWAN Profile Configuration Mode Commands* section.

Example

The following command associates the TWAN profile *twan1* with this MRME service.

```
associate twan-profile twan1
```

attribute

This command allows you to include SSID and Calling-Stationd-Id AVP values as part of DER messages over STa Interfaces.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > **context** *context_name* > **mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

Syntax Description

```
attribute sta { anid { called-station-id | ssid | ssid-wlan-prefix |
wlan-string } | calling-station-id { imsi | ue-mac } }
default attribute sta { anid | calling-station-id }
```

default

Sets the configuration to its default value.

Default calling-station-id: imsi

Default anid: wlan-string

anid { called-station-id | ssid | ssid-wlan-prefix | wlan-string }

Specifies to include the information from the ANID AVP in the DER message.

called-station-id: Include the called station ID from the WLC/AP in the ANID AVP.

ssid: Include the SSID information from the ANID AVP.

ssid-wlan-prefix: Include the SSID WLAN prefix information from the ANID AVP.

wlan-string: Include the WLAN string information from the ANID AVP.

calling-station-id { imsi | ue-mac }

Specifies to include the calling station ID in the DER message.

imsi: Include the IMSI information.

ue-mac: Include the UE MAC information.

Usage Guidelines

Use this command to include the received SSID and Calling-Station-Id values in the ANID/ Calling-Station-Id AVP as part of DER messages over STa Interfaces.

Example

The following command includes ue-mac information from the calling-station-id in the DER message.

```
attribute sta calling-station-id ue-mac
```

bind

This command allows you to configure an IPv4 and/or IPv6 address to be used as the connection point for establishing SaMOG sessions to handle authentication and accounting messages.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

Syntax Description

Release 19 and later:

```
bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address
 ipv6_address [ ipv4-address ipv4_address ] }[ auth-port auth_port_number ] [
acct-port acct_port_number ] [ max-subscribers max_subscriber_number ]
no bind { ipv4-address [ ipv6-address ] | ipv6-address [ ipv4-address ]
}
```

Release 18 and earlier:

bind address *ipv4_address* **[auth-port** *auth_port_number* **] [acct-port** *acct_port_number* **] [max-subscribers** *max_subscriber_number* **]**
no bind

no

Removes a previously configured binding.

address *ipv4_address*

Important This option is obsolete from Release 19 onwards.

Specifies the IP address of an interface to be used as the connection point for establishing SaMOG sessions.

ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

Important To define more than one NAS IP address per context, in Global Configuration Mode, use the **aaa large-configuration** command.

ipv4-address *ipv4_address* [ipv6-address *ipv6_address*] | ipv6-address *ipv6_address* [ipv4-address *ipv4_address*]

Important In this release, the configuration of the IPv6 bind address is supported as lab quality only.

Specifies the IPv4 or IPv6 address to be used as the connection point between the WLC and the SaMOG gateway for the RADIUS interface. You can optionally bind a secondary IPv4 address (if the primary bind address is an IPv6 address) or IPv6 address (if the primary bind address is an IPv4 address) to the MRME service.

The second bind address can be bond in the same command or separate commands. When the second bind address is provided, the MRME service restarts and existing sessions are lost for the other bind address.

ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

ipv6_address must be an IPv6 address expressed in colon (or double-colon) notation.

auth-port *auth_port_number*

Specifies the authentication port number of the interface where authentication requests are received. The system binds the default authentication port to 1812.

In addition to the authentication port, the accounting port and maximum subscriber limit can also be configured optionally.

auth_port_number must be an integer from 1 through 65535.

acct-port *acct_port_number*

Specified the accounting port number of the interface where accounting requests are received. The system binds the default accounting port to 1813.

In addition to the accounting port, the maximum subscriber limit can also be configured optionally.

acct_port_number must be an integer from 1 through 65535.

max-subscribers *max_subscriber_number*

Specifies the maximum number of subscriber sessions allowed.

max_subscriber_number must be an integer from 0 through 4,000,000.

Usage Guidelines

Use this command to configure the IPv4 address to be used as the connection point for establishing SAMOG sessions for handling authentication and accounting messages.

Example

Release 19 and later: The following command binds the MRME service with the IPv6 address of 192.168.1.254 and a secondary IPv6 address of 7777::101:1 with an accounting port number of 58 and maximum subscriber limit of 1000.

```
bind ipv4-address 192.168.1.254 ipv6-address 7777::101:1 acct-port 58
max-subscribers 1000
```

Release 18 and earlier: The following command binds the service with an IP address of 196.10.2.3 with an accounting port number of 58 and maximum subscriber limit of 1000.

```
 bind address 196.10.2.3 acct-port 58 max-subscribers 1000
```

disconnect

This command allows you to specify the delay duration before which the call is disconnected.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

Syntax Description

```
disconnect { delay-time seconds | preauth-wait-time minutes | wait-time seconds
 }
default disconnect { delay-time | preauth-wait-time | wait-time }
```

default

Configures this command to its default setting.

delay-time default: 30 seconds

preauth-wait-time default: 5 minutes

wait-time default: 10 seconds

delay-time *seconds*

Specifies to configure the timer to retain the session on receiving an Accounting Stop, and for roaming scenarios, session continuity on receiving an Accounting Start.

seconds must be an integer from 1 through 60.

preauth-wait-time *minutes*

Specifies the maximum time (in minutes) to wait in the web authorization pre-authorization phase after which the subscriber's session is cleared, if the post-authorization trigger is not received.

minutes must be an integer from 1 through 60.

wait-time *seconds*

Specifies to configure the timer to wait for accounting start message from the new WLC after processing the accounting stop message from the old WLC.

seconds must be an integer of 10 through 300.

Usage Guidelines

Specifies to configure the timer to wait for accounting stop message after triggering a Disconnect Request Message to WLC for an SaMOG session.

Example

The following command sets the disconnect wait time to 60 seconds.

```
disconnect wait-time 60
```

The following command sets the pre-authorization wait time to 10 minutes:

```
disconnect preauth-wait-time 10
```

dns-P-GW

This command allows you to configure the source context in which the DNS client is configured, or enable/disable P-GW selection based on topology and load-balancing of P-GWs, based on weights from DNS.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > **context** *context_name* > **mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

Syntax Description

dns-pgw { context *context_name* **| selection { topology [weight] | weight } }**
{ default | no } dns-pgw { context | selection { topology [weight] | weight } }

default

Returns the command to its default value.

default dns-pgw context: MRME will fetch the dns-client configuration from the current context.

default dns-pgw selection topology: MRME will perform P-GW selection based on the topology.

no

If previously configured, removes the dns-pgw configuration.

context *context_name*

Specifies to configure the source context in which the DNS client is configured.

context_name must be an alphanumeric string of 1 through 79 characters.

selection { topology [weight] | weight }

Specifies to enable/disable P-GW selection based on topology and load-balancing of P-GWs based on weights from DNS.

Usage Guidelines

Use this command to configure the source context in which the DNS client is configured, or enable/disable P-GW selection based on topology and load-balancing of P-GWs, based on weights from DNS.

In case of topology-based selection, when the DNS procedure outputs a list of P-GW host names for the APN FQDN, MRME performs the longest suffix match and selects the P-GW which is topologically closest to the MRME/subscriber. In case of weight-based selection, if there are multiple entries with the same priority in the list of P-GW host names for the APN FQDN in the output from the DNS procedure, calls are distributed to the P-GWs according to the weight field in RRs. The weight field specifies a relative weight for entries with the same priority.

Example

This command will configure the source context in which the DNS client is configured to "mrmectx".

```
dns-P-GW context mrmectx
```

fqdn

This command allows you to configure the MRME fully qualified domain name (FQDN) to match the longest suffix during dynamic allocation.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mrme-service)#`

Syntax Description

`fqdn` *`fqdn_name`*
`{ default | no } fqdn`

default

Returns the command to the default setting of "null".

no

Removes the configured FQDN from the MRME service configuration.

fqdn_name

Specifies the MRME FQDN name that will be used for the longest suffix match during dynamic allocation.

fqdn_name must be an alphanumeric string of 1 to 255 characters.

Usage Guidelines

Use this command to configure the MRME FQDN under MRME service to match the longest suffix during dynamic allocation.

Example

The following command sets an MRME FQDN value of "topon.eth.mrme.north.blore.3gppnetwork.org".

`fqdn topon.eth.mrme.north.blore.3gppnetwork.org`

pgw-selection

This command provides P-GW selection related parameters for this MRME service.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mrme-service)#`

Syntax Description

`[ no ] pgw-selection { fallback pgw-id | local-configuration-preferred }`

no

Removes the configuration.

local-configuration-preferred

Specifies the SaMOG Gateway to perform P-GW selection based on local configuration.

When this keyword is enabled,

- In the case of dynamic P-GW selection from the AAA server (APN FQDN based selection), the SaMOG Gateway first tries to establish session with the locally configured P-GWs. If the locally configured P-GWs are not reachable, APN FQDN resolution is performed, and SaMOG Gateway tries to establish session with the resolved IP addresses.
- In the case of static P-GW selection from the AAA server (IP address or P-GW FQDN), SaMOG tries to establish session with the AAA server provided P-GW address (IP address or resolved P-GW FQDN). If the AAA server provided P-GW addresses are not reachable, session setup fails.

fallback pgw-id

Specifies the SaMOG Gateway to trigger fall back to locally configured P-GW addresses (or DNS resolved P-GW addresses using APN FQDN) when session establishment with AAA provided P-GW address or DNS provided P-GW address for P-GW FQDN fails.

Usage Guidelines

Use this command to enable SaMOG Gateway to perform P-GW selection based on local configuration.

When the **local-configuration-preferred** keyword is enabled, SaMOG first uses the locally configured P-GW addresses to fall-back to. When the locally configured P-GW addresses are not reachable, SaMOG then uses APN FQDN based P-GW address resolution.

When the **local-configuration-preferred** keyword is not enabled, SaMOG first uses APN FQDN based P-GW address resolution to fall-back to. When the P-GW address resolved using APN FQDN is not reachable, SaMOG then uses the locally configured P-GW addresses.

When session establishment with AAA provided P-GW address or DNS provided P-GW address for P-GW FQDN fails, fall-back is triggered when the **fallback pgw-id** keyword is enabled.

Example

The following command enables the SaMOG Gateway to use locally configured P-GW addresses first for P-GW resolution:

```
pgw-selection local-configuration-preferred
```

radius

This command allows you to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

Important From release 16.0 onwards, this command has been deprecated. Instead, use the **radius** command described under the *TWAN Profile Configuration Mode Commands* section.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > **context** *context_name* > **mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

Syntax Description

radius client *ipv4_address*[**/***mask*] **{ [encrypted] key** *key* **[[disconnect-message [dest-port** *port_number* **]] [acct-onoff { [aaa-context** *aaa_context_name* **] [aaa-group** *aaa_group_name* **] [clear-sessions] }] }**
no radius client *ipv4_address*[**/***mask*]

no

Removes a previously configured RADIUS client.

ipv4_address[/mask]

Specifies the IP address, and optional subnet mask of the RADIUS client from which RADIUS accounting and authentication requests are received.

ipv4_address[/mask] must be an IPv4 address expressed in dotted-decimal notation.

[encrypted] key *key*

- **encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.
- **key** *key*: Specifies the shared key between the RADIUS client and this service.

  key with encryption must be an alphanumeric string of 1 through 288 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that *key* is case sensitive.

disconnect-message [dest-port *port_number*]

Specifies to send RADIUS disconnect messages to the configured RADIUS accounting client in call failure scenarios.

- **dest-port** *port_number* : Specifies a port number to which the disconnect message must be sent.

  port_number must be an integer from 1 through 65535.

acct-onoff { [aaa-context *context_name*] [aaa-group *group_name*] [clear-sessions] }

Important The **acct-onff** keyword is currently not supported in this release.

Usage Guidelines Use this command to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

Example

The following command configures the service to communicate with a RADIUS client with an IP address of 190.21.33.40 and an encrypted shared secret of key1234Ax3Z, and clear the session when accounting on/off messages are received:

```
 radius client 190.21.33.40 encrypted key 123 4Ax3Z acct-onoff
clear-sessions
```

setup-timeout

This command is currently not supported in this release.