

IPSG RADIUS Server Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Server Configuration Mode is used to create and configure IPSG RADIUS Server/eWAG services in the current context. This mode enables configuring the system to receive RADIUS accounting requests as if it is a RADIUS accounting server, and reply after accessing those requests for subscriber information.

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Important The commands or keywords/variables that are available are dependent 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.

- accounting-context, on page 2
- associate sgtp-service, on page 2
- bind, on page 3
- connection authorization, on page 6
- gtp max-contexts-per-imsi, on page 7
- gtp peer-ip-address, on page 8
- ip, on page 9
- map ue-mac-to-imei, on page 12
- overlapping-ip-address, on page 12
- plmn id, on page 13
- profile, on page 14
- radius accounting, on page 15

- radius dictionary, on page 19
- respond-to-non-existing-session, on page 20
- sess-replacement, on page 21
- setup-timeout, on page 22
- w-apn, on page 23

accounting-context

This command allows you to specify the GTPP accounting context.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

accounting-context *context_name*
no accounting-context

no

If previously configured, removes the accounting context configuration.

context_name

Specifies name of the GTPP accounting context.

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

Usage Guidelines

Use this command to specify the GTPP accounting context.

Example

The following command specifies to use the GTPP accounting context *context12* for the eWAG service:

accounting-context *context12*

associate sgtp-service

This command allows you to associate an SGTP service with the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

associate sgtp-service *sgtp_service_name* **[context** *sgtp_context_name* **]**
no associate sgtp-service

no

If previously configured, removes the service association from the configuration.

sgtp-service *sgtp_service_name*

Specifies name of the SGTP service to associate with this service.

sgtp_service_name must be the name of an SGTP service, and must be an alphanumeric string of 1 through 63 characters in length.

context *sgtp_context_name*

Specifies name of the context in which the SGTP service is configured.

sgtp_context_name must be the name of the context, and must be an alphanumeric string of 1 through 63 characters in length.

If a context is not specified, the current context is used.

Usage Guidelines

Use this command to associate an SGTP service with the IPSG service. This enables the GTP functionality for eWAG supporting GTP-C (GTP Control Plane) messaging and GTP-U (GTP User Data Plane) messaging between eWAG and GGSN over the Gn' interface.

Important Any change to this configuration will result in restart of the eWAG service.

Example

The following command associates an SGTP service named *service1*, configured in the context named *context2*, with the IPSG service:

associate sgtp-service *service1* **context** *context2*

bind

This command allows you to bind the current IPSG/eWAG service to a logical AAA interface, and specify the number of subscriber sessions allowed.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
bind accounting-proxy address ipv4_address [ max-subscribers max_sessions |
port port_number | source-context source_context ]
bind address ipv4_address [ disconnect-message [ src-port source_port_number ]
 | max-subscribers max_sessions | port port_number | source-context source_context
 ]+
bind authentication-proxy address ipv4_address [ acct-port port_number |
auth-port port_number | max-subscribers max_sessions | source-context
source_context ]
no bind
```

no

If previously configured, removes the binding for the service.

bind accounting-proxy address *ipv4_address* [max-subscribers *max_sessions* | port *port_number* | source-context *source_context*]

- **accounting-proxy address** *ipv4_address* : Specifies the IP address of the interface where accounting proxy requests are received by this service in IPv4 dotted-decimal notation.
- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.
- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

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

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

bind address *ipv4_address* [disconnect-message [src-port *source_port_number*] | max-subscribers *max_sessions* | port *port_number* | source-context *source_context*]+

- **address** *ipv4_address* : Specifies the IP address of the interface where accounting requests are received by this service in IPv4 dotted-decimal notation.
- **disconnect-message [src-port** *source_port_number* **]**: Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

  src-port *source_port_number*: Specifies the port number to which the disconnect message must be sent.

  source_port_number must be an integer from 1 through 65535.
- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.
- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

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

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

bind authentication-proxy address *ipv4_address* [acct-port *port_number* | auth-port *port_number* | max-subscribers *max_sessions* | source-context *source_context*]

- **authentication-proxy address** *ipv4_address* : Specifies the IP address of the interface where authentication proxy requests are received by this service in IPv4 dotted-decimal notation.



Important Enabling authentication proxy also enables accounting proxy.

- **acct-port** *port_number*: Specifies the port number of the interface where accounting proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1813
- **auth-port** *port_number*: Specifies the port number of the interface where authentication proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1812

- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

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

  This keyword should be configured if the source of the RADIUS requests is in a different context then the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

- +: Indicates that more than one of the preceding options may be specified in a single command.

Usage Guidelines

Use this command to bind the IPSG RADIUS Server/eWAG service to a logical AAA interface and specify the number of allowed subscriber sessions. If the AAA interface is not located in this context, configure the **source-context** parameter.

Use the accounting and authentication proxy settings to enable RADIUS proxy server functionality on the IPSG. These commands are used when the NAS providing the RADIUS request messages is incapable of sending them to two separate devices. The IPSG in RADIUS Server mode proxies the RADIUS request and response messages while performing the user identification task in order to provide services to the session.

Example

The following command binds the service to a AAA interface with and IP address of *209.165.200.228* located in the source context named *aaa_ingress*:

```
bind address 209.165.200.228 source-context aaa_ingress
```

connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests received by the current IPSG service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
connection authorization [ encrypted ] password password
no connection authorization
```

no

Deletes the RADIUS authorization from the current IPSG RADIUS Server service.

[encrypted] password *password*

- **encrypted**: Specifies that the RADIUS authorization password is encrypted.
- **password** *password*: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In StarOS 12.2 and later releases, *password* with encryption must be an alphanumeric string of 1 through 132 characters, and without encryption an alphanumeric string of 1 through 63 characters.

  In StarOS 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

The IPSG RADIUS server service does not terminate RADIUS user authentication so the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests sent to this service. The password is encrypted, and the password used in this example is "*secret*".

```
connection authorization encrypted password secret
```

gtp max-contexts-per-imsi

This command allows you to configure multiple primary contexts having the same IMSI number.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

gtp max-contexts-per-imsi *max_value* **min-nsapi** *min_nsapi_value*
default gtp max-contexts-per-imsi

default

Configures this command to disable use of multiple primary contexts. Only one PDP context per user is allowed.

max-contexts-per-imsi: 1

min-nsapi: 15

max-contexts-per-imsi *max_value*

Specifies the limit for the maximum number of contexts per IMSI.

max_value must be an integer from 1 through 11.

min-nsapi *min_nsapi_value*

Specifies the range of NSAPI values to be assigned to different PDP context of the same subscriber.

*min_nsapi_value*must be an integer from 5 through 15.

Usage Guidelines

Use this command to configure the maximum number of contexts per IMSI, and the range of NSAPI values to be assigned to different PDP context.

Example

The following command configures the maximum contexts per IMSI to 5 and specify the range of values NSAPI valie to 7.

```
gtp max-contexts-per-imsi 5 min-nsapi 7
```

gtp peer-ip-address

This command allows you to configure GGSN IP address under the eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

gtp peer-ip-address *ipv4_address*
no gtp peer-ip-address

no

Deletes the configuration, if previously configured.

gtp peer-ip-address *ipv4_address*

Specifies the GGSN IP address.

ipv4_address

Usage Guidelines

Use this command to configure the GGSN IP address under the eWAG service.

This command replaces the hidden mode command **[no] ggsn-ip-address** *ipv4_address*

Example

The following command configures the GGSN IP address *209.165.200.228* under the current eWAG service.

```
gtp peer-ip-address 209.165.200.228
```

ip

This command enables you to configure IP parameters for the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
ip { gnp-qos-dscp | qos-dscp } qci { { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6 |
 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } { af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be
 | ef | pt } } +
default ip { gnp-qos-dscp | qos-dscp }
no ip { gnp-qos-dscp | qos-dscp } qci { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6
| 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } +
```

default

Configures this command, for specified option, with default setting for all QoS Class Identifier (QCI) values.

- QCI-based DSCP map:
  - **qci 1**: **ef**
  - **qci 2**: **ef**
  - **qci 3**: **af11**
  - **qci 4**: **af11**
  - **qci 5**: **ef**
  - **qci 6**: **ef**
  - **qci 7**: **af21**
  - **qci 8**: **af21**

- **qci 9**: **be**

- ARP-based DSCP map for interactive class:
  - **qci 5 allocation-retention-priority 1**: **ef**
  - **qci 5 allocation-retention-priority 2**: **ef**
  - **qci 5 allocation-retention-priority 3**: **ef**
  - **qci 6 allocation-retention-priority 1**: **ef**
  - **qci 6 allocation-retention-priority 2**: **ef**
  - **qci 6 allocation-retention-priority 3**: **ef**
  - **qci 7 allocation-retention-priority 1**: **af21**
  - **qci 7 allocation-retention-priority 2**: **af21**
  - **qci 7 allocation-retention-priority 3**: **af21**
  - **qci 8 allocation-retention-priority 1**: **af21**
  - **qci 8 allocation-retention-priority 2**: **af21**
  - **qci 8 allocation-retention-priority 3**: **af21**

no

Resets configured value for specified QCI with its default setting.

gnp-qos-dscp

Specifies, for uplink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qos-dscp

Specifies, for downlink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qci { 1 | 2 | 3 | 4 | 9 }

Specifies the QCI attribute of QoS.

- **1**: QCI 1 attribute of QoS
- **2**: QCI 2 attribute of QoS
- **3**: QCI 3 attribute of QoS
- **4**: QCI 4 attribute of QoS
- **9**: QCI 9 attribute of QoS

qci { 5 | 6 | 7 | 8 } allocation-retention-priority { 1 | 2 | 3 }

Specifies the QCI attribute of QoS with ARP.

- **5**: QCI 5 attribute of QoS
- **6**: QCI 6 attribute of QoS
- **7**: QCI 7 attribute of QoS
- **8**: QCI 8 attribute of QoS

allocation-retention-priority { 1 | 2 | 3 }: Specifies the ARP.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | pt

Specifies the Per-Hop Forwarding Behavior (PHB) to use.

- **af11**: Assured Forwarding 11 PHB
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best Effort Forwarding PHB
- **ef**: Expedited Forwarding PHB
- **pt**: Pass Through (do not modify the ToS)

Usage Guidelines

Use this command to configure IP parameters for the eWAG service.

Example

The following command specifies to configure the DiffServ Code Point marking to be used for sending packets specifying QCI as 1 and Assured Forwarding 11 PHB:

```
ip gnp-qos-dscp qci 1 af11
```

map ue-mac-to-imei

This command allows you to map the UE MAC received in the Calling-Station-Id RADIUS attribute to IMEIsV in order to forward it in the GTP CPC message to the GGSN.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

`[ default | no ] map ue-mac-to-imei`

default

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

Default: Mapping is disabled.

no

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

Usage Guidelines

Use this command to enable or disable mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

overlapping-ip-address

This command allows you to enable or disable overlapping of IP addresses which enables multiple users to use the same IP address.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

`[ default | no ] overlapping-ip-address`

default

If previously configured, disables IPSG support of overlapping IP addresses.

Using overlapping IP addresses is disabled by default.

no

If previously configured, disables IPSG support of overlapping IP addresses.

Usage Guidelines

Use this command to enable or disable overlapping IP addresses for subscribers on different networks that are independent of each other.

Example

The following command enables IPSG overlapping of IP addresses:

```
overlapping-ip-address
```

plmn id

This command allows you to configure Public Land Mobile Network (PLMN) identifier for the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

plmn id mcc *mcc_number* **mnc** *mnc_number*
no plmn id

no

If previously configured, deletes the PLMN ID configuration.

mcc *mcc_number*

Specifies the mobile country code (MCC) part of the PLMN identifier for the eWAG service.

mcc_number must be a three-digit number ranging from 200 to 999.

mnc *mnc_number*

Specifies the mobile network code (MNC) part of the PLMN identifier for the eWAG service.

mnc_number must be a two- or three-digit number ranging from 00 to 999.

Usage Guidelines Use this command to configure the location-specific mobile network identifiers included in the Routing Area Identity (RAI) field of the PDP Create Request messages sent to the GGSN.

Important Any change to this configuration will result in restart of the eWAG service.

Example

The following command configures the PLMN identifier for the eWAG service as MCC *333* and MNC *99*:

```
plmn id mcc 333 mnc 99
```

profile

This command allows you to configure the IPSG/eWAG service to use APN or subscriber profile.

Important In release 14.0, eWAG service uses only the APN profile. In release 15.0, ReWAG uses the APN profile and DeWAG uses the subscriber profile. Whereas, the IPSG service uses both APN and subscriber profiles.

Product eWAG

IPSG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
profile { APN [ default-apn apn_name ] | subscriber }
default profile
```

default

Configures this command with its default setting.

Default: **APN**

APN

Specifies to use APN profile for the service.

default-apn *apn_name*

Important This option is supported only for the eWAG service.

Specifies the default APN to be used for the eWAG service.

apn_name must be the name of an APN, it must be an alphanumeric string of 1 through 62 characters in length, and can consist only of the alphabetic characters (A–Z and a–z), digits (0–9), dot (.), and the hyphen (-).

subscriber

Important This option is supported only for the IPSG RADIUS Server service, and in release 15.0 for DeWAG service. For the DeWAG service, this command must be configured with the **subscriber** option. This is because DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Specifies to use subscriber profile for the service.

Usage Guidelines

Use this command to set the service to support APN profiles (supporting Gx through the enabling of **ims-auth-service**) or for basic subscriber profile lookup.

For the DeWAG service, this command must be configured with the **subscriber** option. This is because DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Example

The following command specifies to use the subscriber profile:

```
profile subscriber
```

radius accounting

This command allows you to specify the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

radius accounting { client { *ipv4_address* | *ipv4_address/mask* } [encrypted] key *key* [acct-onoff [aaa-context *aaa_context_name*] [aaa-group *aaa_server_group_name*] [clear-sessions] +] [dictionary *dictionary*] [disconnect-message [release-on-acct-stop *acct_stop_wait_timeout*] [dest-port *destination_port_number*] + | interim create-new-call | validate-client-ip }
no radius accounting { client { *ipv4_address* | *ipv4_address/mask* } | interim create-new-call | validate-client-ip }
default radius accounting { interim create-new-call | validate-client-ip }

no

If previously configured, removes the specified configuration.

ipv4_address* | *ipv4_address/mask

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

ipv4_address/*ipv4_address/mask* must be in IPv4 dotted-decimal notation.

A maximum of 16 IP addresses can be configured.

[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.

  In StarOS 12.2 and later releases, *key* with encryption must be an alphanumeric string of 1 through 236 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that *key* is case sensitive.

  In StarOS 12.1 and earlier releases, *key* must be an alphanumeric string of 1 through 127 characters and is case sensitive.

acct-onoff [aaa-context *aaa_context_name*] [aaa-group *aaa_server_group_name*] [clear-sessions] +

Important In release 12.3 and earlier releases, this option is applicable only to the IPSG Proxy Mode.

Important In release 14.0 and later releases, this option is applicable to the IPSG Proxy and Server Modes.

Specifies to proxy accounting On/Off messages to AAA server.

- **aaa-context** *aaa_context_name*: Specifies the context to find AAA server groups. If not specified, by default, the AAA context will be the source context.

  aaa_context_name must be the name of a AAA context, and must be an alphanumeric string of 1 through 79 characters.

- **aaa-group** *aaa_server_group_name*: Specifies the AAA server group. If not specified, by default, the AAA server group will be *default*.

  aaa_server_group_name must be the name of AAA server group, and must be an alphanumeric string of 1 through 63 characters.

- **clear-sessions**: Specifies to clear eWAG or IPSG sessions on receiving accounting On/Off messages.
- **+**: Indicates that more than one of the preceding options may be specified in a single command.

dictionary *dictionary*

Specifies the dictionary to use.



Important In this release, eWAG supports only the **starent-vsa1** dictionary.

dictionary can be one of the following.

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835.
custom*X*	These are customized dictionaries. For information on custom dictionaries, please your Cisco account representative. *X* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, a 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type This dictionary is the master-set of all of the attributes in all of the dictionaries su by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary incorporates additional Starent Networks VSAs by using a two-byte VSA Type This dictionary is the master-set of all of the attributes in all of the -835 dictiona supported by the system.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Star Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary a one-byte wide VSA Type field in order to support certain RADIUS applicatio one-byte limit allows support for only 256 VSAs (0–255). This is the default dic **Important** In StarOS 12.0 and later releases, no new attributes can be added to the **starent-** dictionary. If there are new attributes to be added, you can only add them to the dictionary. For more information, please contact your Cisco account representat

Dictionary	Description
starent-vsa1-835	This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Sta Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default diction

Important For information on the specific dictionary to use for your deployment contact your Cisco account representative.

disconnect-message [release-on-acct-stop *acct_stop_wait_timeout*] [dest-port *destination_port_number*]

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

- **release-on-acct-stop** *acct_stop_wait_timeout*: Specifies to wait for the accounting stop request after sending the Packet of Disconnect (PoD) to the client for the specified time. This keyword is disabled by default.

  acct_stop_wait_timeout must be an integer from 10 through 300 seconds. This indicates the time to wait to clear the call in case IPSG does not receive any accounting stop for the subscriber after sending the PoD.

  This keyword is configured on a per RADIUS accounting client basis and not for the entire service.

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

  destination_port_number must be an integer from 1 through 65535.

interim create-new-call

Important This option does not apply to the IPSG Proxy Mode.

Specifies to create a new session upon receipt of a RADIUS interim message.

Default: Disabled

validate-client-ip

Specifies to enable the ipsgmgr to validate RADIUS accounting messages from different configured RADIUS client IP address, and forward requests to the session manager.

Default: The RADIUS client IPs are validated.

Usage Guidelines

Use this command to configure the communication parameters for the RADIUS client from which RADIUS accounting requests are received.

Example

The following command configures the service to communicate with a RADIUS client with an IP address of *209.165.200.228* and an encrypted shared secret of *key1234*:

```
radius accounting client 209.165.200.228 encrypted key key1234
```

radius dictionary

This command allows you to specify the RADIUS dictionary for the current IPSG/eWAG service.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

radius dictionary *dictionary_name*
default radius dictionary

default

Specifies to use the default dictionary.

Default: **starent-vsa1**

dictionary *dictionary_name*

Specifies the dictionary to use.



Important In 15.0 and later releases, for DeWAG use the **starent** dictionary.

dictionary_name must be one of the following.

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835.

Dictionary	Description
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please co your Cisco account representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type fiel This dictionary is the master-set of all of the attributes in all of the dictionaries suppo by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary an incorporates additional Starent Networks VSAs by using a two-byte VSA Type fiel This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default dictio
starent-vsa1-835	This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Sta Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default dictio

Important For information on the specific dictionary to use for your deployment contact your Cisco account representative.

Usage Guidelines Use this command to specify the RADIUS dictionary to use for the IPSG RADIUS Server/eWAG service.

Example

The following command specifies to use the *custom10* RADIUS dictionary:

```
radius dictionary custom10
```

respond-to-non-existing-session

Configures the IPSG service to respond to Radius Accounting-Stop messages even if a session does not exist.

Product IPSG

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

`[ default | no ] respond-to-non-existing-session`

default

Configures this command with its default setting.

Default: Disabled. IPSG service drops packets containing the Radius Accounting-Stop message if the session does not exist.

no

If previously enabled, disables the configuration.

Usage Guidelines

Use this command to enable/disable the IPSG service to respond to Radius Accounting-Stop messages with a Radius Accounting-Response message for non-existing sessions.

sess-replacement

This command allows you to enable/disable the Session Replacement feature for eWAG and IPSG services.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

```
sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key
 [ with-diff-acct-sess-id ] }
{ default | no } sess-replacement
```

default

Configures this command with its default setting.

Default: Disabled.

no

If previously configured, deletes the configuration.

with-diff-acct-sess-id

Specifies to replace current session when a new session request comes with same IP address and same user name/IMSI but different accounting session ID.

with-diff-ip

Specifies to replace current session when a new session request comes with same user name/IMSI but different IP address.

with-diff-key [with-diff-acct-sess-id]

Specifies to replace current session when a new session request comes with same IP address but different user name/IMSI.

For IPSG, you can also use a combination of replacement options of different key and different account session ID.

Usage Guidelines Use this command to enable/disable the Session Replacement feature. By default, the Session Replacement feature is disabled.

Example

The following command enables session replacement specifying to replace the current session when a new session request comes with same user name/IMSI but different IP address:

```
sess-replacement with-diff-ip
```

setup-timeout

This command allows you to configure a timeout for session setup attempts for the current IPSG/eWAG service.

Product eWAG

IPSG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

setup-timeout *setup_timeout_seconds*
default setup-timeout

default

Configures this command with its default setting.

Default: 60 seconds

setup_timeout_seconds

Specifies the time period, in seconds, for which a session setup attempt is allowed to continue before being terminated.

setup_timeout_seconds must be an integer from 1 through 1000000.

Usage Guidelines

Use this command to configure a timeout for IPSG/eWAG session setup attempts.

Example

The following command configures the timeout for session setup attempts to *30* seconds:

```
setup-timeout 30
```

w-apn

This command allows you to configure the W-APNs that can be connected through DeWAG, and the default-gateway IP addresses to be used by the UEs for connecting to the W-APN network.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

w-apn *apn_name* **default-gw** *ipv4/ipv6_address/maskbits* **+**
no w-apn *apn_name*

no

If previously configured, removes the specified configuration.

apn-name *apn_name*

Specifies the APN name.

apn_name must be the name of an APN and must be a string of 1 to 62 characters in length consisting of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

This value is compared against the subscribed APN returned by the AAA server or locally configured APN in the subscriber-template configuration to find the default-gateway IP address to be used in DHCP signaling packets.

default-gw *ipv4/ipv6_address/maskbits*

Specifies the IP address of the default gateway to be used by UE for W-APN access.

You can configure a maximum of four default gateways per W-APN. Multiple default-gateways are possible as the APN can have different pools of different subnet with different default-gateway IP addresses.

ipv4/ipv6_address/maskbits must be an IPv4/IPv6 address and subnet-mask, for example 192.168.1.1/24.

This value should be in the same subnet as that of UE allocated IP address from GGSN for the W-APN. GGSN does not supply subnet-mask along with IP address. Therefore, the identification of whether GGSN-allocated IP address is in same subnet or not is done with the help of configured "/maskbits". This default-gateway value is sent to the UE as default-gateway IP address using "Router" option in DHCP-OFFER message. The maskbits is sent to the UE as subnet-mask using the "Subnet Mask" option in DHCP-OFFER message.

Usage Guidelines

Use this command to configure the list of W-APN names that can be connected through DeWAG and the default-gateway IP addresses to be used by UE for connecting to the W-APN network. During DHCP signaling the configured default-gateway value will be notified to UE as the router. This command also configures the subnet-mask to be used for the respective default-gateway IP address in order to find the network prefix of the default-gateway.

Note that DeWAG will be acting as 'default-gateway' for the UE in its connected network.



Important This command can be configured a maximum of four times to configure four different APNs and the corresponding default-gateways.

Example

The following command configures an APN named *apn123* with the default gateway IP address and mask *209.165.201.0/27*:

```
w-apn apn123 default-gw 209.165.201.0/27
```