

IPSG RADIUS Snoop Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Snoop Configuration Mode is used to create and configure IPSG services within the current context. The IPSG RADIUS Snoop Mode configures the system to inspect RADIUS accounting requests on the way to the RADIUS accounting server and extract user information.

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

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

Entering the above command sequence results in the following prompt:

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

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.

- bind, on page 1
- connection authorization, on page 2
- profile, on page 3
- radius, on page 4
- sess-replacement, on page 6
- setup-timeout, on page 7

bind

This command allows you to configure the service to accept data on any interface configured in the context. Optionally, you can also configure the system to limit the number of sessions processed by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind [max-subscribers *max_sessions* **]**
no bind

no

If previously configured, deletes the binding configuration for the service.

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.

Usage Guidelines

Use this command to initiate the service and begin accepting data on any interface configured in the context.

Example

The following command prepares the system to receive subscriber sessions on any interface in the context and limits the sessions to *10000*:

```
bind max-subscribers 10000
```

connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests "snooped" by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

connection authorization [encrypted] password *password*
no connection authorization

no

Deletes the RADIUS connection authorization configuration from the current IPSG RADIUS snoop service.

[encrypted] password *password*

- **encrypted**: Specifies that the received 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

RADIUS accounting requests being examined by the IPSG RADIUS snoop service are destined for a RADIUS Accounting Server. Since the "snoop" service does not terminate user authentication, 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 "snooped" by this service. The password is encrypted, and the password used in this example is "*secret*".

```
connection authorization encrypted password secret
```

profile

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

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
profile { APN | subscriber }
default profile
```

default

Configures this command with its default setting.

APN

Specifies the service to support APN configuration required to enable Gx support.

subscriber

Specifies the service to support subscriber profile lookup.

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.

Example

The following command specifies to use the subscriber profile:

```
profile subscriber
```

radius

This command allows you to specify the RADIUS accounting servers where accounting requests are sent after being "inspected" by this service.

Product IPSG

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius { accounting server ipv4_address [ port port_number | source-context
context_name ] | dictionary { 3gpp2 | 3gpp2-835 | customXX | standard |
starent | starent-835 | starent-vsa1 | starent-vsa1-835 } }
[ no ] radius accounting server ipv4_address [ port port_number | source-context
 context_name ]
```

no

Removes the RADIUS accounting server identifier from this service.

radius accounting server *ipv4_address*

Specifies the IP address of a RADIUS accounting server where accounting requests are sent after being "snooped" by this service in IPv4 dotted-decimal notation.

Up to 16 addresses can be configured.

port *port_number*

Specifies the port number of the RADIUS Accounting Server where accounting requests are sent after being "snooped" by this service.

port_number must be an integer from 1 through 65535.

Default: 1813

source-context *context_name*

Specifies the source context where RADIUS accounting requests are received.

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

If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

dictionary { 3gpp2 | 3gpp2-835 | custom *XX* | standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }

Specifies what dictionary to use. The possible values are described in the following table:

Dictionary	Description
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please cont 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 RF
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorp additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionar master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and inco additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionar master-set of all of the attributes in all of the -835 dictionaries supported by the systen
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Net vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-by VSA Type field in order to support certain RADIUS applications. The one-byte limit a support for only 256 VSAs (0–255). This is the default dictionary.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent N vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-by VSA Type field in order to support certain RADIUS applications. The one-byte limit a support for only 256 VSAs (0–255). This is the default dictionary.

Usage Guidelines Use this command to specify the RADIUS Accounting Servers where accounting requests are sent after being snooped by this service.

Example

The following command specifies the IP address (*209.165.200.228*) of a RADIUS Accounting Server whose accounting requests are to be "snooped", and the source context (*aaa_ingress*) where the requests are received on the system:

```
radius accounting server 209.165.200.228 source-context aaa_ingress
```

sess-replacement

This command allows you to enable/disable session replacement.



Important This command is not supported in this release. The Session Replacement feature is under development for future use.

Product IPSG

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key
 }
{ 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

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

Usage Guidelines Use this command to enable/disable session replacement. By default, session replacement 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 the timeout value for IPSG session setup attempts.

Product IPSG

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
setup-timeout setup_timeout
default setup-timeout
```

setup_timeout

Specifies the period of time (in seconds) the IPSG session setup is allowed to continue before the setup attempt is terminated.

setup_timeout must be an integer from 1 through 1000000.

Default: 60

Usage Guidelines Use this command to prevent IPSG session setup attempts from continuing without termination.

Example

The following command configures the session setup timeout setting to *20* seconds:

```
setup-timeout 20
```