

IMS Authorization Service Configuration Mode Commands

The IMS Authorization Service Configuration Mode enables to configure IP Multimedia Subsystem (IMS) authorization services to manage policy control functions and Gx interface support.

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

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.

- p-cscf discovery, on page 1
- p-cscf table, on page 3
- policy-control, on page 5
- qos-update-timeout, on page 6
- reauth-trigger, on page 7
- signaling-flag, on page 9
- signaling-flow, on page 10
- traffic-policy, on page 11

p-cscf discovery

This command defines the method of Proxy-Call Session Control Function (P-CSCF) discovery to be used.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus |
msisdn-modulus | round-robin } ] | diameter-configured }
[ default | no ] p-cscf discovery
```

default

Sets the P-CSCF discovery to default parameter.

no

Removes/deletes configured parameters for P-CSCF discovery.

table { 1 | 2 }

Specifies that which P-CSCF table is to be used to obtain the primary and secondary P-CSCF addresses. Total 2 tables can be configured for P-CSCF discovery.

algorithm { ip-address-modulus | msisdn-modulus | round-robin }

Specifies the algorithm to select the row from the P-CSCF table to be used for P-CSCF discovery.

- **ip-address-modulus**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- **msisdn-modulus**: This algorithm divides the MSISDN value, in binary without the leading "+", of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin way. If no algorithm is specified this is the default behavior.

Default: **round-robin**

diameter-configured

This option enables the table number and algorithm specified by the **diameter host-select table** configuration in Policy Control Configuration mode.

Usage Guidelines

Use this command to configure the table and row selection methods to select IP address/host address for P-CSCF discovery.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with IP address for P-CSCF discovery.

```
p-cscf discovery table 1 algorithm round-robin
```

p-cscf table

This command adds/appends rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

In releases prior to 18:

p-cscf table { 1 | 2 } row-precedence *precedence_value* **{ address** *ipv4_address* **| ipv6-address** *ipv6_address* **} [secondary { address** *ipv4_address* **| ipv6-address** *ipv6_address* **}] [weight** *value* **]**
no p-cscf table { 1 | 2 } row-precedence *precedence_value*

In 18 and later releases:

p-cscf table { 1 | 2 } row-precedence *precedence_value* **{ ipv4-address** *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } [secondary { ipv4-address** *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } [weight** *value* **]**
no p-cscf table { 1 | 2 } row-precedence *precedence_value*

no

Removes/deletes configured row with precedence in specified table for P-CSCF discovery address.

{ 1 | 2 }

Specifies which P-CSCF table is to be used to add/append the primary and secondary P-CSCF addresses. Two tables can be configured for P-CSCF discovery address.

row-precedence *precedence_value*

This keyword adds/appends the row with the specified row-precedence to the P-CSCF address table.

In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128, and a maximum of 128 rows can be added to a table.

In release 8.0, *precedence_value* must be an integer from 1 through 100, and a maximum of 16 rows can be added to a table.

secondary

Specifies the secondary IPv4/IPv6 address to be entered in P-CSCF table rows.

address *ip_address*

Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv4 address.

Important This keyword is available only in releases prior to 18. In 18 and later releases, this keyword is concealed and is replaced with **ipv4-address** to support the PDN type v4v6 request for VoLTE setup.

ip_address must be entered in IPv4 dotted-decimal notation.

ipv4-address *ipv4_address*

Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv4 address.

ipv4_address must be entered in IPv4 dotted-decimal notation.

Important This keyword is available in 18 and later releases to support the PDN type v4v6 request for VoLTE setup.

In releases prior to 18, the P-CSCF configuration accepts only one primary and one secondary P-CSCF IP addresses – both IPv4 and IPv6 addresses per row in the P-CSCF address table. Two IP addresses are not sufficient enough to address the requirement with PDN type v4v6 request for VoLTE setup. Hence, in release 18, the P-CSCF configuration has been enhanced to allow users to configure a maximum of two IPv4 addresses (primary/secondary) and two IPv6 addresses (primary/secondary) per P-CSCF table row.

ipv6-address *ipv6_address*

Specifies the primary and/or secondary IPv6 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv6 address.

ipv6_address must be entered in IPv6 colon-separated-hexadecimal notation.

In releases prior to 18, the P-CSCF configuration accepts only one primary and one secondary P-CSCF IP addresses – both IPv4 and IPv6 addresses per row in the P-CSCF address table. Two IP addresses are not sufficient enough to address the requirement with PDN type v4v6 request for VoLTE setup. Hence, in release 18, the P-CSCF configuration has been enhanced to allow users to configure a maximum of two IPv4 addresses (primary/secondary) and two IPv6 addresses (primary/secondary) per P-CSCF table row.

weight *value*

This keyword designates weight to a row-precedence relative to other row-precedences configured under this table, Default value is 1. *value* must be an integer from 1 through 10.

Within the IMS Authorization configuration, the P-CSCF address is selected based on round robin fashion. This feature allows the customer to perform P-CSCF selection based on weight factor.

With this CLI option, the user can configure and add weight (in the scale of 1 to 10) to each row, and the rows are selected based on weighted round-robin. That is, the row with higher weight parameter is selected more number of times than the row with less number of weights.

Usage Guidelines

Use this command to add rows with primary and/or secondary IP addresses for P-CSCF discovery. The row is added with the specified row-precedence.

In releases prior to 17.0, IMSA will select the servers if requested server address type and selected row server-address type are the same. Otherwise, it will return NULL. In 17.0 and later releases, P-CSCF server selection algorithm is modified such that the P-CSCF server selection happens based on UE-requested server-type.

The operator can add/remove rows to the table that is not currently selected by the **diameter host-select table** command in Policy Control Configuration Mode.

In releases prior to 18, the look-up and forwarding of P-CSCF server information from P-CSCF table to the session manager were performed by IMS Authorization (IMSA) server only during the setup. In 18 and later releases, whenever IMSA receives a Modify Bearer request with P-CSCF Address request indication, then the list of P-CSCF IP addresses are sent to the session manager through Modify Bearer Response message.

This look-up and forwarding functionality works even when the call is with the Local Policy (LP) engine during the time the Modify Bearer Request is triggered.

Example

The following command adds a row in **table 2** with primary IP address *209.165.200.228*, secondary IP address as *209.165.200.232*, and row-precedence value as *20* for P-CSCF discovery.

```
p-cscf table 2 row-precedence 20 address 209.165.200.228 secondary
209.165.200.232
```

policy-control

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to configure Diameter authorization and policy control parameter for IMS authorization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy-control

no

Disables the pre-configured policy control parameters for IMS authorization in this IMS authorization service.

use-pcscf-config-from-imsa

Specifies to use the P-CSCF configuration from IMSA in Local Policy.

Usage Guidelines

Use this command to enter the Policy Control Configuration Mode to configure the policy control parameters for Diameter authorization and charging policy in IMS Authorization Service.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsa-dpca)#

Policy Control configuration commands are described in the *Policy Control Configuration Mode Commands* chapter.

qos-update-timeout

This command is obsolete in release 11.0 and later releases. This command sets the Quality of Service update timeout for a subscriber in IMS authorization service.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-imsa-service)#

Syntax Description

qos-update-timeout *timeout_duration*
no qos-update-timeout

no

Disables the pre-configured QoS update timeout parameter in this IMS authorization service.

timeout_duration

Specifies the duration of timeout in seconds as an integer from 0 through 3600.

Default: 60

Usage Guidelines

Use this command to set the maximum time to wait for a subscriber to initiate the update QoS procedure in IMS authorization service.

Example

The following command sets the QoS update timeout to *90* seconds.

qos-update-timeout 90

reauth-trigger

This command specifies the trigger events to initiate re-authorization for a subscriber in IMS authorization service.



Important This command now moved to Policy Control Config mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default ] reauth-trigger { all | { an-gw-change | bearer-loss |
bearer-recovery | plmn-change | policy-failure | qos-change | rat-change
 | sgsn-change | tft-change | tft-delete } + }
```

Default

Sets the pre-configured Re-authorization trigger to default value.

all

Sets the IMS authorization service to initiate re-authorization process for a subscriber on all events listed in this command.

an-gw-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber whose access network gateway changed.

bearer-loss

Sets the IMS authorization service to initiate re-authorization process for a subscriber on loss of bearer or service.

bearer-recovery

Sets the IMS authorization service to initiate re-authorization process for a subscriber when a bearer or service recovered after loss of bearer or service.

default-bearer-qos-change

Sets the IMS authorization service to initiate re-authorization process when QoS is changed and DEFAULT_EPS_BEARER_QOS_CHANGE event triggered for the default EPS bearer context of a subscriber in LTE network.

plmn-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Public Land Mobile Network (PLMN) of subscriber.

policy-failure

Sets the IMS authorization service to initiate re-authorization process for a subscriber on failure of credit and charging policy for subscriber.

qos-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Quality of Service level/rating of subscriber.

rat-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Radio Access Type (RAT) of subscriber node.

sgsn-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in SGSN for subscriber node.

tft-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Traffic Flow Template (TFT) of subscriber session.

tft-delete

Sets the IMS authorization service to initiate re-authorization process for a subscriber when Traffic Flow Template (TFT) of subscriber session is deleted by a system administrative user.

Usage Guidelines

Use this command to set the triggers to initiate QoS re-authorization process for a subscriber in IMS authorization service.

Example

The following command sets the re-authorization trigger to **bearer-loss**, so that re-authorization of subscriber session is initiated on loss of bearer.

```
reauth-trigger bearer-loss
```

signaling-flag

This command specifies whether a request for a PDP context dedicated to signaling (for IMS sessions) should be granted or denied.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
signaling-flag { deny | permit }
default signaling-flag
```

default

Sets the signaling flag to default mode of deny.

deny

Denies the request for a signaling PDP context for IMS session and keeps signaling co-existed with other traffic on PDP contexts. Default: Enabled

permit

Permits the request for a signaling PDP context for IMS session and a separate signaling context activated. Default: Disabled

Usage Guidelines

Use this command to allow or deny the activation of a dedicated PDP context for signaling. The user equipment (UE) may indicate that the PDP context should be dedicated for IP multimedia (IM) signaling by setting the IP Multimedia Core Network (IM-CN) signaling flag in the Protocol Configuration Options (PCO).

The **deny** option causes the system to inform the UE that the PDP context will not be dedicated for IM signaling and signaling will co-exist with other traffic on PDP context.

The **permit** option is used to activate the signaling context for signal traffic and the other traffic uses other PDP context for traffic with the following destinations:

- Towards the DHCP and DNS servers for the IMS domain
- Towards the P-CSCF(s)

The UE is not trusted to follow these restrictions, and the system monitors and restricts the traffic from the dedicated PDP context. The **signaling-flow class-map** command is used to configure the restrictions.

Example

The following command denies the request for a signaling PDP context for IMS session.

```
default signaling-flag
```

signaling-flow

This command specifies the packet filters and policy servers for bandwidth control and singling context enforcement that define the traffic that is allowed through the dedicated signaling context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
signaling-flow permit server-address ipv4/ipv6_address [ server-port { port_num
 | range start_port to end_port } ] [ description STRING ]
no signaling-flow permit server-address ipv4/ipv6_address [ server-port {
port_num | range start_port to end_port } ]
```

no

Disables the signaling flow option configured with this command.

server-address *ipv4/ipv6_address*

The server address refers to the destination IP address in uplink packets, and the source IP address in downlink packets.

ipv4/ipv6_address is an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and can be used with a subnet mask.

A maximum of 16 signaling server addresses can be configured per IMS Authorization service.

server-port { *port_num* | range *start_port* to *end_port* }

Specifies the TCP/UDP port number(s) of the server to be used for communication.

port_num must be an integer from 1 through 65535.

range *start_port* **to** *end_port* provides the option to configure the range of ports on server for communication.

start_port must be an integer from 1 through 65535 but lesser than *end_port*, and *end_port* must be an integer from 1 through 65535 but greater than *start_port*.

description *STRING*

Specifies the customized description for configured signaling server as an alphanumeric string of 1 through 63 characters.

Usage Guidelines Traffic that matches any instance of the signaling-flow command will be forwarded via the signaling PDP context. In addition, the policy server gives policy gates to use for the signaling PDP context.

Example

The following command sets the packet filter server address to *209.165.200.228* with port number *1234* for packet filtering.

```
signaling-flow server-address 209.165.200.228 server-port 1234
```

traffic-policy

This command specifies the action on packets which do not match any policy gates in the general purpose PDP context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
traffic-policy general-pdp-context no-matching-gates direction { downlink
 | uplink } { forward | discard }
default traffic-policy general-pdp-context no-matching-gates direction {
 downlink | uplink }
```

default

Sets the default traffic policy for packets without any policy gate match in general purpose PDP context.

By default packets which do not have any matching policy gate are forwarded.

no-matching gates

Applies traffic policy for packets which do not match any policy gate.

direction { downlink | uplink }

Specifies the direction of traffic to apply this traffic policy in general PDP context.

downlink: Specifies the traffic from system to MN. Default is set to forward.

uplink: Specifies the traffic from MN to system. Default is set to forward.

forward

Forwards the packets which do not match any policy gates. Default: Enabled

discard

Discards the packets which do not match any policy gates. Default: Disabled

Usage Guidelines

This command provides configuration on traffic policy applied on packets which are not matching any policy gate in general PDP context. Packets can either be forwarded or discarded on the basis of operator's configuration.

This command needs to be configured once for downlink and once for uplink separately.

Example

The following command discards uplink packets which do not match any policy gate in general purpose PDP context.

```
traffic-policy general-pdp-context no-matching-gates direction uplink
discard
```