# HSS Peer Service Configuration Mode Commands

**Command Modes**

The HSS Peer Service Configuration Mode is used to create and manage the Home Subscriber Server (HSS) Peer Service.

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Important** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

# auth-request

Configures the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
auth-request num-auth-vectors num
default auth-request num-auth-vectors
```

### num-auth-vectors *num*

Specifies the number of vectors the MME/SGSN is requesting from the HSS as an integer.

*num* prior to Release 16, the valid range is 1 through 3. Default = 1.

*num* beginning with Release 16, the valid range is 1 through 5. Default = 1.

**Usage Guidelines**

Use this command to configure the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

Receiving multiple vectors from the HSS for a given UE helps reduce the number of messages across the diameter connection plus provides the MME/SGSN with additional vectors for the UE in the event that the connection or the HSS id disabled.

**Related Commands:**

- To view the current number of requested vectors, execute the **show hss-peer-service service name** <*name*> command in the Exec mode.
- To set the minimum number (low watermark) of vectors to be maintained at all times, execute **min-unused-auth-vector** *min_num* command from the call control profile configuration mode. (SGSN only)
- For troubleshooting, check the number of free, used, or in-use vectors displayed in the output of the **show subscribers [ gprs-only | sgsn-only ] full** command. (SGSN only).

### Example

The following command sets the number of requested vectors to 2:

```
auth-request num-auth-vectors 2
```

# diameter hss-dictionary

Specifies the Diameter Credit Control dictionary for the HSS peer service.

## Product

MME

SGSN

## Privilege

Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

## Syntax Description

```
diameter hss-dictionary { custom1 | standard | standard-r9 } [
eir-dictionary { custom1 | custom2 | standard | standard-r9 } ]
default diameter hss-dictionary
```

### default

Sets the dictionary to default **standard-r9** for HSS peer service.

### custom1

Sets the Diameter dictionary to a customer-specific HSS Diameter dictionary. Default: Disabled

### standard

Sets the Diameter dictionary to the standard (3GPP release 8) HSS peer dictionary. Default: Disabled

### standard-r9

Sets the Diameter dictionary to the standard HSS peer dictionary for 3GPP release 9. Default: Enabled

### eir-dictionary { custom1 | custom2 | standard | standard-r9 }

Specifies that an Equipment Identity Register (EIR) dictionary is to be used in conjunction with the HSS Diameter dictionary.

**custom1**: Sets the EIR Diameter dictionary to a customer-specific EIR Diameter dictionary.

**custom2**: Sets 'custom2' as the EIR Diameter dictionary. **custom2** was created for use with the MME's S13 Additional IMEI Check feature.

**standard**: Sets the EIR Diameter dictionary to the standard HSS peer dictionary.

**standard-r9**: Sets the EIR Diameter dictionary to the standard HSS peer dictionary for release 9.

## Usage Guidelines

Use this command to select the Diameter dictionary and, optionally, the EIR end-point dictionary, for the HSS peer service.

### Example

The following command sets the Diameter dictionary to IETF RFC 4006 specific:

```
diameter hss-dictionary standard
```

The following command sets the special 'custom2' dictionary as the EIR dictionary:

```
diameter hss-dictionary standard eir-dictionary custom2
```

# diameter hss-endpoint

Associates a preconfigured Diameter origin endpoint with this HSS peer service.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
diameter hss-endpoint endpoint_name [ eir-endpoint eir_endpoint_name ] [
auc-endpoint auc_endpoint_name ]
no diameter hss-endpoint
```

### no

Removes previously associated Diameter origin endpoint from this HSS peer service.

### *endpoint_name*

Identifies a preconfigured Diameter endpoint specific to the HSS interface. The endpoint must be present in all Diameter messages and is the endpoint that originates the diameter message.

*endpoint_name* is a preconfigured Diameter endpoint name expressed as an alphanumeric string of 1 through 63 characters.

### eir-endpoint *eir_endpoint_name*

Identifies a preconfigured Diameter endpoint specific to the S13 or S13'  Equipment Identity Register (EIR) interface.

*eir_endpoint_name* must be an existing Diameter endpoint expressed as an alphanumeric string of 1 through 63 characters.

### auc-endpoint *auc_endpoint_name*

**auc-endpoint** Including this keyword option enables routing to an authentication center (AuC) as the endpoint in place of the hss-endpoint. If configured, all AIR messages are routed to this AuC-endpoint. If not configured, all AIR messages are sent to the configured HSS endpoint.

*auc_endpoint_name* Identifies the AuC endpoint and must be a unique endpoint name comprised of a string of 1 to 63 alphanumeric characters.

**Usage Guidelines**

Use this command to associated a Diameter origin endpoint to create a Diameter-based S6a or S6d (SGSN) interface association in this HSS peer service to provide AAA functionality to the EPS bearer context.

Optionally, use this command to associate a Diameter origin endpoint to create a Diameter-based S13 or S13' (SGSN) interface association in this HSS peer service to provide IMEI query capability between the MME and an EIR.

A second option, the **auc-endpoint** keyword, enables you to use this command to define an authentication center (AuC) as the routing endpoint in place of the hss-endpoint. If configured, all AIR messages are routed to this AuC endpoint. If not configured, all AIR messages are sent to the configured HSS endpoint.

**Important** The configuration of all endpoints is only valid when all necessary endpoint configuration has been completed. All endpoint listed above must also be defined as valid endpoints using the commands in the Diameter Endpoint configuration mode (refer to the *Diameter Endpoint Configuration Mode Commands* chapter in the *Command Line Interface Reference* manual) for more information on Diameter endpoint configuration parameters.

### Example

The following command associates the preconfigured Diameter endpoint *hss_1* with this HSS peer service for HSS interface support.

```
diameter hss-endpoint hss_1
```

The following command enables use of an authentication center (AuC1) in place of an HSS server (HSS1) as an endpoint for Diameter originated messages:

```
diameter hss-endpoint HSS1 auc-endpoint AuC1
```

# diameter suppress

Configures the MME to restrict the sending of the Notify-Request-Message to the HSS. By default, the Notify-Request-Message is sent to the HSS.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
[ no ] diameter suppress notify-request
```

**no**

Sets the command to the default value where the Notify-Request-Message is sent to the HSS.

**Usage Guidelines**

Use this command to restrict the MME from sending the Notify-Request-Message to the HSS. This can be used to control whether handover to non-3GPP access can occur.

# diameter update-dictionary-avps

Specifies which release of 3GPP TS 29.272 is to be used for the HSS peer service.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }
no diameter update-dictionary-avps
```

### no

Sets the command to the default value where Release 8 ('standard') dictionary is used for backward compatibility of previous releases.

### 3gpp-r10

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 10 of 3GPP 29.272.

### 3gpp-r11

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 11 of 3GPP 29.272.

Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile Station ISDN (A-MSISDN) flag of the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time a UE Attaches. For more information about supporting A-MSISDN, refer to the information for the **a-msisdn** command in the Call-Control Profile configuration mode.

### 3gpp-r9

Configures the MME/SGSN to signal Release 9 AVPs to HSS.

**Usage Guidelines**

Use this command to configure the 3GPP release that should be supported for this HSS peer service.

This command is only applicable for the 'standard' diameter dictionary as defined in the **diameter hss-dictionary** command.

### Example

After a command is issued to support the AVPs as defined by the various releases of the 3GPP 29.272 spec, use the following command to disable the support:

```
no diameter update-dictionary-avps
```

# dynamic-destination-realm

Enables the MME to construct the destination realm using the MCC and MNC of foreign subscribers.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
[ default | no ] dynamic-destination-realm
```

### default

Returns the configuration to the default setting, where the MME uses the configured peer realm as the destination realm.

### no

Disables the dynamic destination realm configuration. This provides the same behavior as the **default** keyword.

**Usage Guidelines**

This command configures the MME to derive the EPC Home Network Realm/Domain based on the user's IMSI (MNC and MCC values) and use it as the Destination Realm in all diameter messages.

For a foreign subscriber, the MME does not know the HSS nodes in all the foreign PLMNs. In this case the MME routes S6a/S6d requests directed to foreign PLMNs via a Diameter Routing Agent (DRA) using only the destination realm. The DRA in turn routes the request to the correct HSS based on the destination realm. In order to accomplish this, the MME needs to dynamically construct requests to the DRA/HSS with a Destination Realm representing the foreign PLMN of the UE.

Refer to *Configuring Dynamic Destination Realm Construction for Foreign Subscribers* in Chapter 2 of the *MME Administration Guide* for more information about configuring this feature.

### Example

The following command configures the MME to derive the desination realm for foreign subscribers based on the user's IMSI (MNC/MCC).

```
dynamic-destination-realm
```

# end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines**

Use this command to return to the Exec mode.

# exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
exit
```

**Usage Guidelines**

Use this command to return to the parent configuration mode.

# failure-handling

Configures failure handling behavior in the event of a failure with the HSS peer service. It also defines the action on various error codes on the Diameter interface during authentication or session activities.

**Product**

MME

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
failure-handling { authentication-information-request |
check-identity-request| notify-request | purge-ue-request |
update-location-request } { diameter-result-code start_error_code [ to
end_error_code ] | request-timeout } action { continue | retry-and-terminate
 | terminate }
no failure-handling { authentication-information-request |
check-identity-request | notify-request | purge-ue-request |
update-location-request } diameter-result-code start_error_code [ to
end_error_code ]
default failure-handling { authentication-information-request |
check-identity-request | notify-request | purge-ue-request |
update-location-request } request-timeout
```

### no

Removes the preconfigured failure handling procedures for calls in an HSS peer service.

### default

Sets the default action for failure handling procedure for calls in an HSS peer service.

For default actions on Diameter result/error codes see the *Usage* section below.

### authentication-information-request

Configures the MME-HSS service to handle the failures in an Auth-Information-Request message.

Configures the SGSN-HSS service to handle the failures in an Auth-Information-Request message.

### check-identity-request

Configures the MME-HSS service to handle the failures in a Check-Identity-Information-Request message.

Configures the SGSN-HSS service to handle the failures in a Check-Identity-Information-Request message.

### notify-request

Configures the MME-HSS service to handle the failures in a Notify-Request message.

This option is not supported on SGSN.

### purge-ue-request

Configures the MME-HSS service to handle the failures in a Purge-UE-Request message.

Configures the SGSN-HSS service to handle the failures in a Purge-UE-Request message.

### update-location-request

Configures the HSS peer service to handle the failures in an Update-Location-Request message.

### diameter-result-code *start_error_code* [to *end_error_code*]

Configures the HSS peer service to handle the failures for various request message having specific single or range of Diameter result codes in a request message.

*start_error_code* specifies an individual error code for Diameter protocol as an integer from 3000 through 5999. This will be the starting of code if a range of error codes is specified with the optional keyword **to** *end_error_code*.

**to** *end_error_code* is used to specify a range of error codes to handle by this command. *end_error_code* specifies the end error code for Diameter protocol as an integer from 3000 through 5999.

### request-timeout

Configures the HSS peer service to handle the failures for various request messages if response to that message is not received before timeout duration exhausted.

### action { continue | retry-and-terminate | terminate }

Specifies the action to be taken on failure of any message as a policy for failure handling.

- **continue**: This option works differently for each system.

  For the SGSN: On receipt of any error for MICR session request, the SGSN allows the HSS peer service to continue with the session procedure without any interruption. For all other request/message types, the SGSN behaves as it would if configured for the **retry-and-terminate** option.

  For the MME: The MME does not support this option and if **continue** is included in the command, the MME behaves as it would if configured for the **retry-and-terminate** option.

  For 12.0 and earlier releases the **continue** option in failure handling *on SGSN* for IMEI procedures has the same behavior as that of the **retry-and-terminate** option.

  **Important** For releases after 14.0, the **continue** option for IMEI procedure *on SGSN* can be configured in case of timeout and error responses requests from HSS so that the requests will be re-tried on a second peer (if configured) and the call is continued. The configuration of **continue** option for IMEI procedure is as follows:

```
configure
 context <name>
 hss-peer-service <name>
 failure-handling check-identity-request request-timeout action continue

 failure-handling check-identity-request diameter-result-code <range1>
to <range2> action continue
 failure-handling check-identity-request diameter-result-code <range1>
action continue
 exit
 exit
 exit
```

- **retry-and-terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) occurs, the system retries sending the request (AIR/ULR/NOR/PUR/MICR) to another peer that is configured in the same endpoint. If no response is received for AIR or ULR from the second peer, then the system allows the HSS peer service to terminate the session.
- **terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) is met, the system allows the HSS peer service to immediately terminate the session (AIR/ULR/MICR) without any further action.

## Usage Guidelines

Use this command to configure the failure handling behavior in the event of a communication failure with the HSS peer service.

The following are the default actions for Diameter result codes:

- For all protocol error codes 3000 to 3999, the default action is terminate. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999, the default action is continue.
- For transient error codes 4002, 4003, and 4181, the default action is retry.
- For error code 4001, the default action is terminate.
- For permanent error codes 5000 to 5999, the default action is terminate

### Example

The following command will allow HSS peer service to continue if any failure in Auth-Information-Request message occurred with Diameter error code *3050*:

```
failure-handling authentication-information-request diameter-result-code
 3050 action continue
```

# request timeout

Configures the application request timeout between the HSS peer service and HSS node. The MME/SGSN waits for this duration before retransmitting the request to corresponding HSS node.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
request timeout dur
[ no | default ] request timeout
```

### no

Disables the configured application request timeout value.

### default

Sets the application request time out duration to default value of 300 seconds.

### *dur*

Specifies the application request timeout duration (in seconds) as an integer from 1 through 300. The MME/SGSN will wait for this duration before retrying the request with corresponding HSS. Default: 20

**Usage Guidelines**

Use this command to set the waiting period for HSS peer service in seconds after which the request is deemed to have failed or system will resend the request.

### Example

The following example configures the application request timeout duration to 20 seconds:

```
default request timeout
```

# zone-code-format

Configures how the MME must interpret the received zone-code values from the HSS.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**configure > context** *context_name* **> hss-peer-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
zone-code-format  { ascii-string }
[ default ] zone-code-format
```

### default

Returns the command to the default setting, where the MME interprets the zone-code as an octet string.

### ascii-string

Configures the MME to interpret the zone-code as an ascii string. This option is provided to maintain backward compatibility.

When configured as ascii-string, the MME interprets the received zone-code as an ASCII string (coded in hexadecimal representation) and converts it byte by byte to an integer value. For example, if the HSS sends the zone-code value as 3032, the MME converts this to 02 (ASCII value of 0 in Hex is 0x30, ASCII value of 2 in Hex is 0x32). With this configuration, the MME accepted zone-codes only within the range of 0 to 99.

**Usage Guidelines**

This new command specifies the format of the zone-code value received from HSS to MME. The MME uses this configuration to interpret and convert the received zone-code value to an integer value and validate it against the list of allowed zone-code configured for the zone-code restriction feature.

By default, the MME interprets the received zone-code value from HSS as a octet-string (2 bytes) which is coded in full hexadecimal representation. The MME converts the entire 2 byte octet string coded in hexadecimal to integer value and it uses the same for validation for zone-code restriction feature. For example, if the HSS sends the zone-code value as 3032, MME converts this to 12338 (which is the equivalent of 0x3032).

### Example

The following command configures the HSS Peer Service to interpret the zone-code received from the HSS as an ASCII string.

```
zone-code-format ascii-string
```