

# Emergency Call Support on the ePDG and P-GW

This feature provides emergency call support on the ePDG and P-GW.


- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- How it Works, on page 3
- Configuring AAA Failure Handling for S2b Emergency Calls, on page 9
- Configuring APN and S6b Authorization, on page 10
- Monitoring and Troubleshooting, on page 11


## Feature Summary and Revision History

| | |
|---|---|
| Applicable Product(s) or Functional Area | P-GW<br>SAEGW |
| Applicable Platform(s) | • ASR 5500<br>• VPC-DI<br>• VPC-SI |
| Feature Default | Enabled - Always On |
| Related Changes in This Release | Not applicable |
| Related Documentation | • *P-GW Administration Guide*<br>• *SAEGW Administration Guide* |

### Revision History

| Revision Details | Release |
|---|---|
| This release supports new emergency calls from S2b Interface.<br>**Important**<br>This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative. | 21.20 |
| First introduced | 21.1 |

# Feature Description

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction.

### Supported Functionality

3GPP Release 13 Emergency Call Support on the ePDG and P-GW includes the following functionality:

- Emergency call establishment over untrusted Wi-Fi for the P-GW. The P-GW includes the new **Emergency-Indication** AVP over the AAA S6b interface only during Emergency PDN connection establishment.
- Lawful Intercept is supported for Emergency PDNs over the S2b interface.
- Various Create Session Request message IEs have been modified to support all four different behaviors of emergency bearer establishment.
- Intra- and Inter-chassis recovery are supported for emergency call over the S2b interface.
- Network initiated dedicated bearer creation is supported for emergency calls over the S2b interface.
- The maximum APN restriction is ignored for emergency APN.
- Multiple PDNs are supported for emergency calls over the S2b interface.
- Context replacement for emergency calls over the S2b interface without IMSI with same IMEI is supported.
- P-GW emergency related statistics and bulkstats are available.
- Graceful shutdown of S2b emergency calls is supported.

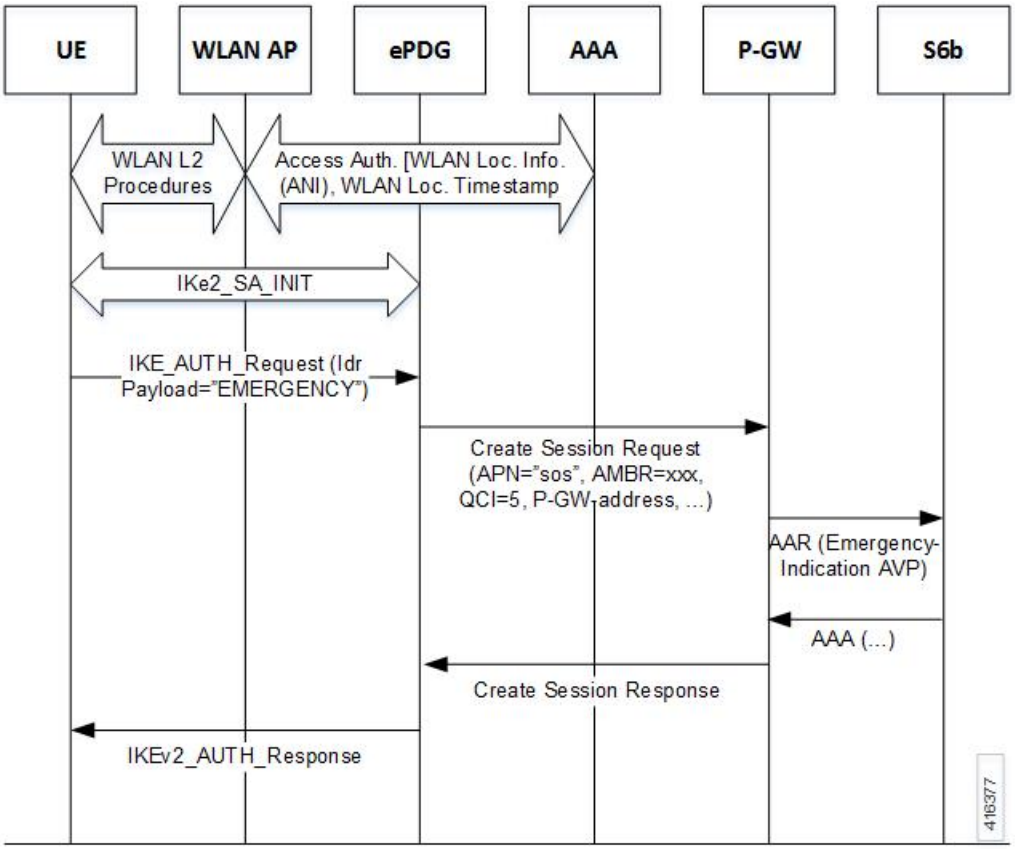
**Previous Behavior:** Emergency calls were not supported for the S2b interface. Also, handoff between the s2b interface and LTE was not supported for emergency calls.

**New Behavior:** Emergency calls are now supported on the S2b interface and handover is also supported for emergency calls from the S2b interface to LTE and vice-versa for "authenticated imsi" only.

# How it Works

The ePDG sends a Create Session Request (CSReq) message to the P-GW. The P-GW deduces the emergency related policies to apply from the Access Point Name (APN) received in the CSReq message. For emergency attached User Equipment (UE), if the International Mobile Station Identifier (IMSI) cannot be authenticated or the UE has not provided it, then the International Mobile Equipment Identifier (IMEI) is used as UE identifier.

***Figure 1: Call Flow: 3GPP R13 Emergency Call Support on the ePDG and P-GW***




The P-GW sends the **Emergency-Indication** AVP over the s6b interface so that the 3GPP AAA server only applies specific policies for emergency services. For an unauthenticated UE, the 3GPP AAA server does not update the Home Subscriber Server (HSS) with the identity of the P-GW. For an authenticated UE, this indication is sent together with the "PDN GW currently in use for emergency services" message, which comprises the PDN GW address and the indication that the PDN connection is for emergency services to the HSS, which stores it as part of the UE context for emergency services.

Support is available for all four different behaviors of emergency bearer establishment:

- Valid UEs only.
- Only UEs that are authenticated are allowed.
- IMSI required, authentication optional.
- All UEs are allowed.

This section describes the new Attribute Value Pair (AVP) and modified Information Elements that support the feature.

### Emergency-Indication AVP

A new **Emergency-Indication** AVP is defined in the Authentication and Authorization Request to signal a request to establish a PDN connection for emergency services.

### Information Elements

This section describes other important elements in a Create Session Request that have been modified to work properly with the feature.

***Table 1: Information Elements in a Create Session Request***

| Information Elements | P | Condition/Comment | IE Type | Ins. |
|---|---|---|---|---|
| IMSI | C | The IMSI is included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, except for the case:<br>If the UE is emergency attached and the UE is UICCless.<br>The IMSI shall be included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, but not used as an identifier.<br>- If UE is emergency attached but IMSI is not authenticated.<br>The IMSI is included in the message on the S2a/S2b interface. | IMSI | 0 |

| Information Elements | P | Condition/Comment | IE Type | Ins. |
|---|---|---|---|---|
| MSISDN | C | For an E-UTRAN Initial Attach and a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN the IE is included when used on the S11 interface, if provided in the subscription data from the HSS. For a PDP Context Activation procedure and a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN the IE is included when used on the S4 interface, if provided in the subscription data from the HSS.<br>The IE is included for the case of a UE Requested PDN Connectivity, if the MME has it stored for that UE. It is included when used on the S5/S8 interfaces if provided by the MME/SGSN.<br>The ePDG includes this IE on the S2b interface during an Attach with GTP on S2b , UE initiated Connectivity to Additional PDN with GTP on S2b and a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, Initial Attach for emergency session (GTP on S2b), if provided by the HSS/AAA.<br>The TWAN includes this IE on the S2a interface during an Initial Attach in WLAN on GTP S2a, UE initiated Connectivity to Additional PDN with GTP on S2a and a Handover to TWAN with GTP on S2a, if provided by the HSS/AAA. | MSISDN | 0 |
| ME Identity (MEI) | C | The MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface:<br>- If the UE is emergency attached and the UE is UICCless.<br>- If the UE is emergency attached and the IMSI is not authenticated.<br>For all other cases the MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface if it is available. | MEI | 0 |
| | CO | The TWAN/ePDG shall include the ME Identity (MEI) IE on the S2a/S2b interface, if it is available. | | |
| Serving Network | C | This IE is included on the S4/S11, S5/S8 and S2b interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN, a UE requested PDN connectivity, an Attach with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b and an Initial Attach for emergency session (GTP on S2b). | Serving Network | 0 |

| Information Elements | P | Condition/Comment | IE Type | Ins. |
|---|---|---|---|---|
| Indication Flags | C | This IE shall be included if any one of the applicable flags is set to 1.<br>Applicable flags are:<br>- Unauthenticated IMSI: This flag is set to 1 on the S4/S11 and S5/S8 interfaces if the IMSI present in the message is not authenticated and is for an emergency attached UE. | Indication | 0 |
| Selection Mode | C | This IE is included on the S4/S11 and S5/S8 interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN and a UE requested PDN connectivity<br>This IE is included on the S2b interface for an Initial Attach with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b and an Initial Attach for emergency session (GTP on S2b)<br>The IE indicates whether a subscribed APN or a non-subscribed APN chosen by the UE/MME/SGSN/ePDG/TWAN was selected.<br>This IE is included on the S2a interface for an Initial Attach in WLAN on GTP S2a, a Handover to TWAN with GTP on S2a and a UE initiated Connectivity to Additional PDN with GTP on S2a. The value is set to "MS or network provided APN, subscription verified". | Selection Mode | 0 |
| | CO | When available, this IE is sent by the MME/SGSN on the S11/S4 interface during TAU/RAU/HO with S-GW relocation. | | |
| UE Local IP Address | CO | The ePDG includes this IE on the S2b interface during an Initial Attach for emergency session (GTP on S2b). Otherwise the ePDG shall include this IE on the S2b interface based on local policy. | IP Address | 0 |
| UE PDP Port | CO | The ePDG includes this IE on the S2b interface if NAT is detected and the UE Local IP Address is present. | Port Number | 0 |
| WLAN Location Information | CO | This IE is included on the S2b interface if the WLAN Location Information is available. | TWAN Identifier | 1 |
| WLAN Location Timestamp | CO | This IE is included on the S2b interface, if the WLAN Location Timestamp is available. | TWAN Identifier Timestamp | 0 |

### Emergency Handover Support

When a subscriber makes an emergency call over WLAN, user equipment (UE) adds *sos* to the *NAI* to indicate that this is an emergency attach to ePDG. ePDG informs P-GW about this emergency attach in create session request. When the caller moves away from WLAN into LTE coverage or vice versa, the call gets handed over without being dropped.

P-GW supports following emergency call handovers:

- **Handover of Emergency Calls from LTE to Wi-Fi(S2b)** : Handovers of emergency calls from LTE to Wi-Fi (S2b) for authenticated UE is supported. While the UE moves from LTE to untrusted Wi-Fi, LTE triggers an Authentication Authorization Request (AAR) to the S6b server with the AVP *Emergency-Indication* sent in that Authentication and Authorization Request (AAR). Also, an STR is sent when a Wi-Fi (S2b) call is cleared.:

  1. The ePDG sends Create Session Request to the P-GW.
  2. If the UE requested P-CSCF in the IKE Config request, P-CSCF is requested.
  3. Downlink packets are sent on LTE access. The ePDG includes the IP address that is received within the IKE message from the UE in the PAA (PDN Address Allocation) in the GTPv2 Create Session Request.
  4. The P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
  5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
  6. 3GPP AAA sends AAA to the P-GW.
  7. The Policy and Charging Rules Function (PCRF) acknowledges IP-CAN Session Modification with a Credit Control Answer (CCA).
  8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
  9. ePDG sends Create Bearer Response message.
  10. P-GW sends the Delete Bearer Request message.
  11. The S-GW sends Delete Bearer Response message to the P-GW.

- **Handover of Emergency Calls from Wi-Fi(S2b) to LTE** : Handover of Emergency Calls from Wi-Fi (s2b) to LTE for authenticated UE is supported. Since an emergency call in LTE does not have S6b interface authorization enabled, handover of emergency calls from untrusted Wi-Fi to LTE triggers a Session Termination Request (STR) to the S6b server:

  1. The MME selects the P-GW from the MME Emergency Configuration Data and sends a Create Session Request.
  2. The S-GW sends a Create Session Request.
  3. P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR), if Gx authentication is enabled or P-GW applies the local policy and does not query PCRF if local policy is configured. P-GW sends Session Termination Request to S6b server and P-GW provides IPv6 Prefix and/or IPv4 address in PAA.

**Note** If the MME indicates Piggyback support, then, the P-GW piggybacks the Create Bearer Request message to the Create Session Response message.

4. The MME sends a Modify Bearer Request message to the S-GW.
5. The S-GW processes each message independently. The S-GW forwards the Create Bearer Response to the P-GW(without piggybacking).

- **Emergency PDN Handover with HO=0**: Handovers from LTE to Wi-Fi is supported:

1. The ePDG sends Create Session Request to the P-GW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.

**Note** Downlink packets are dropped at the P-GW while the session is being handed over to WLAN.

2. P-GW checks for an LTE session.
3. If there is an LTE session, the P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
4. 3GPP AAA sends AAA to the P-GW.
5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
6. The PCRF acknowledges of IP-CAN Session Modification with a Credit Control Answer (CCA) message. This message includes the Policy and Charging rules. The P-GW enforces and triggers for events that must be reported by the P-GW.
7. If Online flag is enabled and if P-GW does not have quota for the WLAN rating group, or if Online Charging Server (OCS) has not sent a 4011 for the WLAN rating group previously, then the P-GW sends a CCR-u to the OCS reporting the usage.
8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
9. After the P-GW sends the Create Session Response, the P-GW sends an interim Accounting Request (ACR) to the OFCS.
10. The OFCS responds with an ACA to the P-GW.
11. P-GW sends the Delete Bearer Request to the S-GW.
12. The S-GW sends Delete Bearer Response to the P-GW.

# Configuring AAA Failure Handling for S2b Emergency Calls

Emergency calls over the S2b interface should not be rejected due to a failure from the S6b server. To ensure this, failure handling must be configured in the APN which is used for emergency calls .

Handling is configured in the **aaa group** so that emergency calls continue regardless of failures as indicated by the result code.

**To configure AAA failure handling for S2b emergency calls:**

```
configure
  context ingress_context_name
    aaa group default
      diameter authentication failure-handling authorization-request
result-code 3000 to 5999 action continue
       diameter authentication failure-handling authorization-request
request-timeout action continue
          end
```

Note the following assumptions:

- If an IP-CAN Session Modification Request triggered by the PCRF removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signaling, then the PCEF starts a configurable emergency inactivity timer. When the configured period of time expires, the P-GW initiates an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session
- If the Gx/S6b interface returns a Virtual APN, which is not configured as an emergency APN, then the call is rejected with the cause code "APN_DENIED_NO_SUBSCRIPTION

**To configure failure handling template for Gx failure (PCRF down)**:

```
configure
  failure-handling-template gx_template
   msg-type any failure-type diabase-error action continue local-fallback

       end
```

**Following example shows failure handling template configuration for Gx failure (PCRF return ErrorCode):**

```
configure
  failure-handling-template gx_template
     msg-type credit-control-initial failure-type diameter result-code
3000 to 5999 action continue local-fallback
       msg-type credit-control-update failure-type diameter result-code
 3000 to 5999 action continue local-fallback
           end
```

**Following example shows failure handling template configuration for Gx delayed response:**

```
configure
  failure-handling-template gx_template
    msg-type credit-control-initial failure-type resp-timeout action
continue
       msg-type credit-control-update failure-type resp-timeout action
```

```
continue
          end
```

**To configure local policy for Gx failure (PCRF down or PCRF return ErrorCode):**

```
configure
        local-policy-service service_name
          ruledef  ruledef_name
             condition priority  priority  { variable { eq | ge | gt | le |
 lt | match | ne | nomatch } regex | string_value | int_value | set }
            end
```

```
configure
  local-policy-service service_name
    actiondef   actiondef_name
      action priority  priorityaction_name arguments
        end
```

```
configure
  local-policy-service service_name
    eventbase   eventbase_name
      rule priority  priority   [ event list_of_events ] ruledef
ruledef_name actiondef actiondef_name [ continue ]
        end
```

```
configure
  contextcontect_name
    ims-auth-service   service_name
      [ no ] policy-control
        associate failure-handling-template gx_template
          associate local-policy-service  service_name
            end
```

# Configuring APN and S6b Authorization

### Configuring APN to attach emergency PDN on LTE

For emergency PDN handover with S6b Gx, configure APN mode to attach emergency PDN on LTE.

```
configure
  context context_name
    apn apn_name
      emergency-apn
      end
```

### Enabling S6b Authorization

Following is the sample configuration to enable S6b authorization:

```
configure
```

```
context context_name
  pgw-service service_name
    apn apn_name
      authorize-with-hss [ egtp[gn-gp-enabled] [ s2b [gn-gp-enabled]
 [ s5-s8 [gn-gp-enabled | gn-gp-enabled]] [ report-ipv6-addr ]| lma [
s6b-aaa-group aaa-group-name | report-ipv6-addr ] | report-ipv6-addr ]
[ default | no ] authorize-with-hss
       end
```

# Enabling S2b Interface eGTP Service

Use the following configuration to enable S2b Interface eGTP service:

```
configure
  context context_name
    egtp-service service_name
      interface-type { interface-cgw-egress | interface-epdg-egress |
interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn |
 interface-sgw-egress | interface-sgw-ingress }
      end
```

Following the example configuration to enable S2b Interface eGTP service:

```
configure
       context EPC2
        egtp-service PGW21EGTP
         interface-type | interface-pgw-ingress [ s2b ] [ s2a ]
                          end
```

# Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature

# Show Commands and Output

This section provides information regarding show commands and their outputs in support of the feature.

## show apn

```
pdp type:  ipv4 and ipv6
apn type:  emergency
ehrpd access: N/A
absolute timeout :  0           idle timeout :  0
emergency inactivity timeout :  1000
idle-timeout-activity ignore-downlink:   Disabled
…..
```

# show pgw- service-statistics-all

```
pgw# show pgw-service statistics all
PGW Node Level Statistics:
VPN Name: local
Total bearers active:
  Default bearers:    5                                  Dedicated bearers:  5
    Normal bearers:   2                                  UE-initiated:  0
    Emergency bearers (Auth-IMSI): 1                     Network-initiated: 5
    Emergency bearers (Unauth-IMSI):1                    Normal bearers:   2
    Emergency bearers (Only IMEI): 1                     Emergency bearers (Auth-IMSI):  1
    Emergency bearers (Unauth-IMSI):1

    Emergency bearers (Only IMEI): 1
```