Oracle® Communications Diameter Signaling Router

Equipment Identity Register User Guide

Release 9.1.0.0.0
G16658-01
December 2024

Oracle Communications Diameter Signaling Router Equipment Identity Register User Guide, Release 9.1.0.0.0

G16658-01

Contents

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

This section introduces the documentation updates for Release 9.1.0.0.0

Release 9.1.0.0.0 - G16658-01, December 2024

There are no updates for this release.

1
Introduction

This chapter provides a brief description of the Equipment Identity Register (EIR) feature for Oracle Communications Diameter Signaling Router (DSR). The chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Oracle for assistance.

1.1 Overview

This manual describes the EIR feature for DSR. EIR is used to reduce the number of Global System for Mobile (GSM) handset thefts by providing a mechanism to assist network operators in preventing stolen or disallowed handsets from accessing the network. This control is accomplished by comparing the International Mobile Equipment Identity (IMEI) that is provided during handset registration to a set of three lists provided by the network operator:

- Black - Mobile Stations (MS) on the Blacklist are denied access to the network
- White - MS's on the Whitelist are allowed access to the network
- Gray - MS's on the Graylist are allowed on the network, but may be tracked

Additionally, the operator can perform IMSI (International Mobile Subscriber Identity) based screening. The operator can allow the black listed IMEI based on the IMSI by provisioning the IMSI along with IMEI.

EIR is an optional feature on DSR and can be enabled and disabled administratively.

2
Feature Description

This chapter provides a functional description of the EIR feature, including network perspectives, assumptions and limitations, and a database overview. EIR is implemented on both vSTP and diameter networks.

2.1 Equipment Identity Register Overview

A handset theft problem exists in GSM networks in many countries. A person obtains a legitimate subscription to a network, and then obtains a legitimate IMSI, MSISDN, and SIM card. The person initially buys an inexpensive handset and then steals a better handset from another subscriber. After the handset is stolen, the thief replaces the SIM card with a legitimate SIM card. Because the SIM card and subscriber information contained on the SIM card (IMSI, MSISDN) are legitimate, the phone will operate and the network operator cannot determine that the subscriber is using a stolen handset. In addition to individual handset theft, organized groups stealing entire shipments of mobile handsets from warehouses and sell these handsets on the Black Market.

The Equipment Identity Register (EIR) is a network entity used in GSM networks that stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). The IMEI is used to identify the actual handset and is not dependent upon the International Mobile Subscriber Identity (IMSI), Mobile Station ISDN Number (MSISDN), or the Subscriber Identity Module (SIM). The IMSI, MSISDN, and SIM are all subscriber-specific and move with the subscriber when purchasing a new handset. The IMEI is handset-specific.

The EIR feature can be used to reduce the number of GSM handset thefts by providing a mechanism that allows network operators to prevent stolen or disallowed handsets from accessing the network. This control is accomplished by comparing the IMEI that is provided during handset registration to the following set of lists provided by the network operator:

- Black - Mobile Stations (MS) on the Blacklist are denied access to the network
- Gray - MSs on the Graylist are allowed on the network, but may be tracked
- White - MSs on the Whitelist are allowed access to the network

The Oracle Communications User Data Repository (UDR) stores the Whitelist, Graylist, and Blacklist of IMEI numbers. When a subscriber roams to a new MSC or VLR location, the handset attempts registration with the MSC or VLR. Before the MSC registers the subscriber with the VLR, it may send a query to DSR for EIR status of the handset. DSR returns a response indicating whether the IMEI is allowed, disallowed, or not valid. If the IMEI is allowed, the MSC completes registration; otherwise, registration is rejected.

EIR may also contain associations between individual IMEIs and IMSIs. This can provide a further level of screening by directly associating a particular IMEI with a particular IMSI. This association is used in the following way:

- If an IMEI is found on a Blacklist, an additional check of the IMSI could then be made.
- If the IMSI from the handset matches the IMSI provisioned with the IMEI, this would override the Blacklist condition and allow registration to continue. This could be used to

protect against mistaken Blacklist entries in the database, or to prevent unauthorized "handset sharing."

The IMSI Range Logic Support feature includes an IMSI range check logic before an IMEI lookup in the database. This feature helps to allow a specific set of subscribers on basis of IMSI.

2.2 EIR Call Flows

A call can follow and SS7/Sigtran or Diameter call flow.

2.2.1 SS7/Sigtran EIR Call Flow

When a handset roams into a new MSC or VLR area, it attempts a registration procedure with the VLR. In a network without the EIR function, this procedure results in the VLR sending a location update message to the HLR providing the HLR with the current MSC location of the Mobile Station (MS) or handset. When the EIR function is deployed in a network, this registration procedure is interrupted to validate the IMEI of the MS or handset attempting to register before completing the registration procedure and updating the HLR.

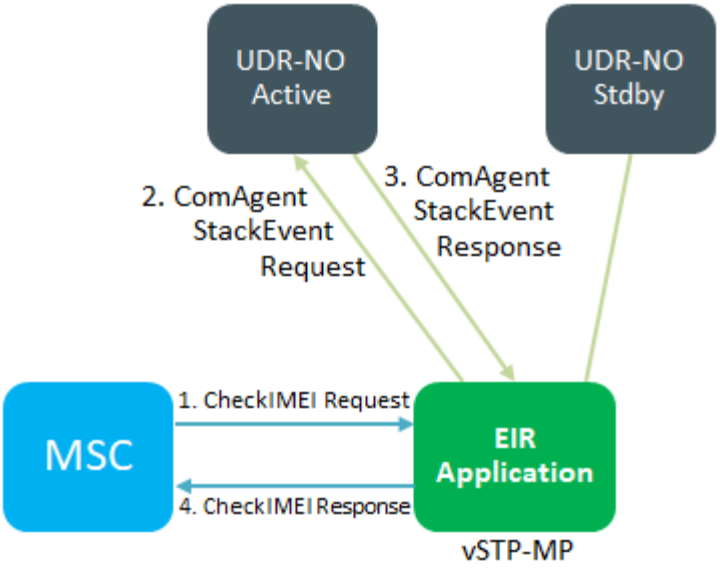
In the network with EIR, the MSC or VLR sends a MAP_CHECK_IMEI message to DSR requesting EIR processing before sending a location update to HLR. This message contains, at a minimum, the IMEI of the MS attempting registration. It may also contain the IMSI of the subscriber whose SIM card is currently being used in the MS or handset. Upon receipt of this message, EIR searches the Allowlist (Whitelist), Gray, and Block Lists (Black list) for a match on the IMEI. EIR then returns a response to the MSC. Depending upon the result of the search, the response contains either the equipment status of the MS or handset (whether the IMEI for the MS or handset is allowed or not based on its status in the Allowlist, Gray, or Block Lists), or a user error (invalid or unknown IMEI). The MSC then either continues the registration procedure (if the IMEI is allowed) or rejects it (if the IMEI is disallowed, invalid, or unknown).

If the IMSI is also included in the message, EIR attempts to match this IMSI to one provisioned with the IMEI before sending a response to the MSC. A match on IMSI overrides any Blocklist condition found based on the IMEI match alone and causes a response of MS allowed.

Figure 2-1 illustrates the steps for the vSTP EIR call flow process.

1. MSC sends a CheckIMEI request to vSTP-MP over SS7 links.
2. vSTP-MP queries the UDR NOAM for IMEI or IMSI DB. The query is sent to all UDR NOAMs in primary and secondary sites in a round robin manner. vSTP-MP uses the ComAgent StackEvent request to query the UDR database.
3. UDR NOAM looks up the IMEI or IMSI database and sends a response to the vSTP-MP. The response to vSTP-MP is then sent as a ComAgent StackEvent response.
4. EIR on vSTP-MP receives the response from UDR, applies the business logic on the received ComAgent StackEvent response, creates a SS7 CheckIMEI response message, and encodes it to send to MSC.

Figure 2-1 vSTP EIR Call Flow



The UDR information contains the list of IMEIs and an indication to the list where they are located. UDR contains two types of IMEIs:

- Individual IMEIs, see Table 2-1.
- Ranges of IMEIs, seeTable 2-2.

The Individual IMEIs are searched first, the IMEI entries in this list may also contain an association to an IMSI. If no individual IMEI match is found, IMEI ranges are searched.

EIR can support up to 100 million subscriber entries, including both individual IMEI and a range of IMEIs.

Table 2-1 Example of Individual IMEIs

IMEI	IMSI (optional)	White List	Gray List	Black List
12345678901234	495867256894125	No	No	Yes
234567890123456		No	Yes	No
49876523576823		No	Yes	Yes
68495868392048	495867565874236	Yes	Yes	No
29385572695759		Yes	Yes	Yes

As shown in Table 2-1, it is possible for a given IMEI to be on more than one list on the Allowlist, and also on the Gray and or Block List). The logic illustrated by Figure 2-1 is used to determine which answer to return in the CHECK_IMEI response, determined by which list or lists the IMEI is on. Table 2-2 also shows three possible EIR response types. The EIR response type is a system-wide EIR option that is configured by the user. The combination of the setting of the EIR response type, the list or lists in which the IMEI is located, and the optional IMSI check determines the response returned to the querying MSC.

Table 2-2 Logic for IMEIs in Multiple Lists

Presence in List			EIR Response Type		
White	Gray	Black	Type 1	Type 2	Type 3
X			in White List	in White List	in White List
X	X		in Gray List	in Gray List	in Gray List
X	X	X	in Black List	in Black List	in Black List
X		X	in Black List	in Black list	in Black List
	X		in Gray List	in Gray List	Unknown
	X	X	in Black List	in Black List	Unknown
		X	in Black List	in Black List	Unknown
			in White List	Unknown	Unknown

Example Scenarios

Example One

1. A CHECK_IMEI is received with IMEI = 49876523576823, no IMSI in message.
2. An individual IMEI match is found, see Table 2-1, entry
3. Indicating the IMEI is on the Gray and Block Lists.
   The EIR Response Type is set to Type 3 and an IMSI is not present.
4. Table 2-2 indicates the required response is Unknown.
5. EIR formulates a CHECK_IMEI error response with Error = 7 Unknown Equipment

Example Two
Example 2 is the same as Example 1, except that the setting of the EIR Response Type is re-provisioned by the operator to Type 2.

1. A CHECK_IMEI is received with IMEI = 49876523576823, no IMSI in message.
2. An individual IMEI match is found (Table 2-1, entry
3. Indicating the IMEI is on the Gray and Block Lists.
   The EIR Response Type is set to Type 2, and an IMSI is not present.
4. Table 2-2 indicates the required response is Blocklisted.
5. EIR formulates a CHECK_IMEI response with Equipment Status = 1 Blocklist.

Example Three

1. A CHECK_IMEI is received with IMEI = 12345678901234, and IMSI = 495867256894125.
2. An individual IMEI match is found, see Table 2-1, entry.
3. Indicating the IMEI is on the Blocklist.
4. The EIR Response Type is set to Type 1.
5. Table 2-2 indicates that the normally required response would be Blocklisted, however, because an IMSI is present in the message, and the IMEI is on the Blocklist, the IMSI is compared to the IMSI entry in the database for this IMEI.
6. In this case, the IMSI in the RTDB matches the IMSI in the query, thus the Blocklist condition is cancelled.
7. EIR formulates a CHECK_IMEI response with Equipment Status = 0 Allowlist.

Example Four

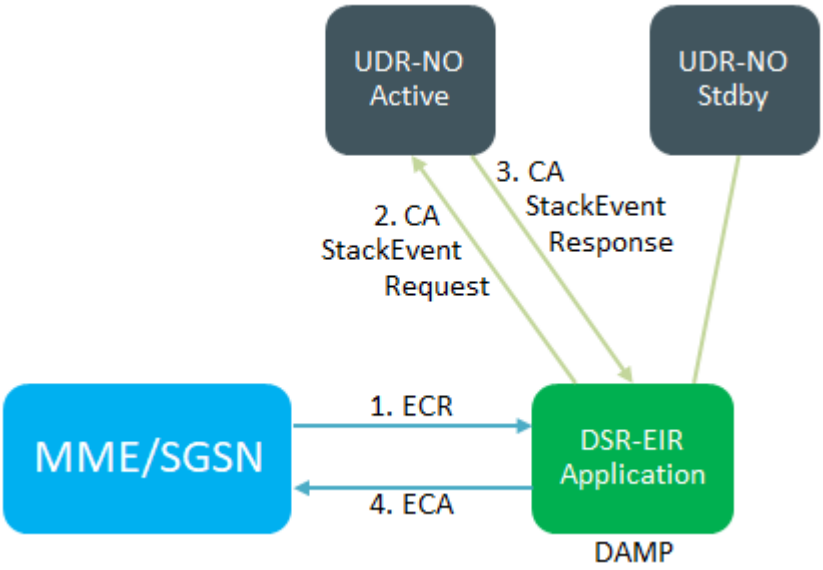
1. A CHECK_IMEI is received with IMEI = 12345678901234, and IMSI = 495867256894126.
2. An individual IMEI match is found (Table 2-1 entry 1), indicating the IMEI is on the Blocklist.
3. The EIR Response Type is set to Type 1.
4. Table 2-2 indicates that the normally required response would be Blocklisted, however; because an IMSI is present in the message, and the IMEI is on the Blocklist, the IMSI is compared to the IMSI entry in the RTDB for this IMEI.
5. In this case, the IMSI in the RTDB does not match the IMSI in the query, the Blocklist condition is maintained.
6. EIR formulates a CHECK_IMEI response with Equipment Status = 1 Blocklist.

2.2.2 Diameter EIR Call Flow

Figure 2-2 illustrates the steps of the diameter EIR call flow process.

1. MME/SGSN sends the ECR message to DAMP over S13/S13' interface links.
2. DAMP queries the UDR active and standby NOAMs in a round-robin manner for IMEI data. DAMP uses the ComAgent StackEvent request for querying the UDR DB.
3. UDR NOAM looks up the IMEI DB and sends a response to the DAMP. The response to DAMP is sent as a ComAgent StackEvent response.
4. EIR on DAMP receives the response from UDR; applies the business logic on received ComAgent StackEvent response; creates an ECA message; and encodes it to send to MME.

Figure 2-2 Diameter EIR Call Flow



2.3 EIR List Determination

The EIR list determination algorithm is the same for both SS7/Sigtran and Diameter.

Whitelist Processing

Indicates the IMEI is valid and registration should be allowed for this MS/UE (User equipment).

If the EIR Global Response configuration option is set (with the `eirgrsp` parameter) to a value other than `off`, the IMEI is treated as being on the list indicated by the EIR Global Response option, regardless of the actual status of the IMEI. No list logic processing is performed on the IMEI.

If the EIR Global Response option is set to `off`, the individual IMEIs are searched first.

If no match is found, the range IMEIs are searched next. If the IMEI is found only on the Whitelist after either search, the list logic processing is complete, and the Whitelist status of the IMEI is sent to the MSC.

Blacklist Processing

Indicates the IMEI is invalid and registration should not be allowed for this MS/UE (User equipment).

If the IMEI is found on the Blacklist after either search, list logic processing continues based on the EIR response type, set by the `eirrsptype` parameter of the `chg-gsmopts` command. If the EIR response type is type 3, and the IMEI is not also found on the Whitelist, the status of the IMEI is unknown.

If the IMEI is also found on the Whitelist, or if the EIR response type is either type 1 or 2, the value of the IMSI Check option, set with the `eirimsichk` parameter of the `chg-gsmopts` command, is checked. If the IMSI check option is `on`, and the IMSI is present in the message, the RTDB is searched for the IMSI. If there is a match for the IMSI, the status of the IMEI is determined to be “White with Override.” If there is no match for the IMSI, the status of the IMEI is determined to be “Black with IMSI Match Failed.” If the value of the IMSI Check option is `off`, the status of the IMEI is determined to be "on the Blacklist".

Graylist Processing

Indicates the IMEI is questionable. Registration should be allowed, but the MS/UE should be tracked.

If the IMEI is found on the Graylist after either search, list logic processing continues based on the EIR response type. If the EIR response type is type 3, and the IMEI is not also found on the White List, the status of the IMEI is unknown.

If the IMEI is also found on the Whitelist, or if the EIR response type is either type 1 or 2, the status of the IMEI is determined to be on the Graylist.

2.4 EIR Protocol

Messages for Local Subsystems

The message arrives at the EIR subsystem as Rt-on-SSN or Rt-on-GT. If the message arrives as Rt-on-SSN, it must contain either the DSR true point code or the EIR capability point code in the DPC field of the message, and the DSR EIR subsystem number in the Called Party Subsystem field of the message. If the EIR query has DSR capability point code for the DPC, then DSR processes the message, but it is not able to divert this message in the event of subsystem failure.

If a message arrives at the EIR subsystem as Rt-on-GT, it should also contain a service selector that translates to the EIR subsystem. These messages also contain one of the DSR

capability point codes in the DPC field. DSR also processes the message if it has the DSR true point code for the DPC, but it is not able to divert these messages in the event of subsystem failure.

SCCP Management to Support EIR

vSTP does not support a mated subsystem, hence, in case of SSN failure or a routing failure, messages are not routed to the mated node.

vSTP-MP can receive messages from a network with a CdPA routing indicator of route-on-gt and DPC is TPC in these situations:

- If a message has the subsystem (SSN) present and the SSN value is from EIR, then the message is sent for EIR processing.
- If message does not have the SSN or the SSN is not from EIR, then the SCCP layer performs normal GTT routing.

> **Note:**
>
> The SSN status management and network management messages, for example, SSP and UPU, do not support EIR; however, if the remote node sends an SST message, then SCCP handles the message.

2.4.1 Check_IMEI Message Handling

When the CHECK_IMEI message is received by the protocol, the IMSI (if active) and SVN are parsed from the MSU. Because different vendors place the IMSI information in different locations within the message, the decoder searches for the IMSI in multiple locations.

Once the required data is parsed, a lookup is performed in the RTDB to determine the response type for the IMEI/IMSI combination.

The appropriate response message is sent to the originating MSC.

Encoding Errors

When a response is generated, it is sent based on the CgPA information in the incoming message. However, some conditions may prevent DSR from generating the response. Most of the errors involve GTT on the CgPA; if the incoming data is Rt-on-SSN, the number of potential errors is much smaller.

Whenever an encoding error is detected, the response message is discarded.

Data Collection

See EIR Alarms and Measurements for a description of the measurements collected for the EIR feature.

2.5 EIR List Log File Serviceability

When the file system reaches 80% of its total capacity, a minor alarm is raised. A major alarm is raised at 90%. All of the files in this partition are managed from **Debug**, and then **Manage Logs & Backups**.

EIR log entries are delivered to and stored on the MPS using a best effort approach.

Logs are retained in these conditions:

- One million records can be logged in 24 hours
- An hourly synchronization takes place from the MP to the active SOAM
- The active SOAM synchronizes the log with the standby SOAM for backup
- The log is retained for 5 days on the SOAM

3
EIR Functionality

This chapter identifies requirements for EIR.

3.1 Global Response

The Equipment Identity Register (EIR) provides an EirOptions table to configure the global response type (eirGlobalResp). If this option is set to `on`, then a checkIMEI response is sent to the MSC. By default, the eirGlobalResp option within EIR is set to `off`. If you leave it off, this order determines the equipment status.

1. IMSI range screening.
2. IMEI and IMEI range screening.
3. SV screening where the last two digits of IMEI are used for the software version.
4. IMSI exact match.

The attribute or parameter follows these rules for its name:

- Common parameters for SS7 and Diameter have an "eir" prefix.
- Diameter-specific parameters have a "diameter" prefix.
- Specific parameters have an "ss7" prefix.

The EIR attributes/parameter included in EIR are listed in Table 3-1.

Table 3-1 Attribute/Parameter Mapping

Attribute/Parameter Name	Description	Default Value	Valid Values or Range
ss7DefMapVer	Map version to decode message	V3	V1, V2, V3
eirDefMcc	E212 default mobile country code.	None	XXX (X = 0-9, A-F,a-f)
eirDefMnc	E212 default mobile network code.	None	XX or XXX (X = 0-9, A-F,a-f)
eirDefImsiResp	EIR default IMSI response. **Note**: When IMSI lookup is successful, this parameter defines the IMSI override lookup response.	Whitelist	Whitelist, Blacklist, Graylist, Unknown
eirGlobalResp	EIR Global Response status.	Off	Off, Whitelist, Blacklist, Graylist, Unknown

Table 3-1 (Cont.) Attribute/Parameter Mapping

Attribute/Parameter Name	Description	Default Value	Valid Values or Range
eirDefResp	EIR default response status (used when UDR connectivity is down). **Note**: If this parameter is set to `on`, then the IMSI response is used; otherwise, equipment status is set based on the IMEI lookup.	Whitelist	Whitelist, Blacklist, Graylist, Unknown
eirImsiChk	EIR IMSI Check status. This parameter is not valid for IMEI ranges.	false	true, false
eirRespType	EIR Response Type.	Type1	Type1, Type2, Type3
eirImsiScrn	EIR IMSI range screening. Search IMSI in IMSI range table.	true	true, false
diameterCongErr	Value in the 'result code' AVP of the response send, at the time of Congestion.	3004	3004, 5006
diameterVendorId	S13 local Vendor ID. All the outgoing messages that require Vendor ID in VENDOR_SPECIFIC_APPLICATION_ID will use this configured value. Currently only 10415 is supported.	10415	10415
diameterProductName	Product Name. It contains the vendor-assigned name for the product. All the outgoing messages that require Product name AVP will use this configured value.	DSR	DSR

3.2 IMSI Screening

The following table contains the options for screening the IMSI. The IMSI range table is used to search for matching IMSI before checking the IMEI in the UDR database.

Table 3-2 IMSI Range

Field	Description	Range	Comments
startAddr	Start of IMSI digits	15 digits	The IMSI prefix begins with 0 and must be 15 digits to be accepted. This field is the key field.

Table 3-2 (Cont.) IMSI Range

Field	Description	Range	Comments
endAddr	End of IMSI digits	15 digits	The IMSI prefix begins with 0 and must be 15 digits to be accepted.
equipmentStatus	Equipment status	White list, Black list, Gray list, Unknown	

The IMSI range supports POST, DELETE, and PUT operations to create, delete, and update the IMSI range. To manage IMSI screening, follow these rules:

- If IMSI is present in the configured IMSI ranges, send the corresponding configured equipment status in Check_IMEI response or ECA message.
- If IMSI is not present in the configured ranges, proceed further and send the IMEI lookup query to UDR and get the configured IMEI data.
- A maximum of 100000 entries is allowed in the EirImsiRange table.
- Assume IMSI is in international format.
- All 15 digits are used for lookup.
- If the length of the IMSI in the message is less than 15, then 0s are added to the beginning of the IMSI number to make 15 digits.

Create IMSI Range
To create the IMSI range, follow this procedure.

1. Create a file with this content.

```
$ cat imsiaddr.txt
{
   "startAddr": "070200000000000",
   "equipmentStatus": "Blacklist",
   "endAddr": "070200000000000"
}
```

> **Note:**
>
> If IMSI is less than 15 digits, add zero(s) until it becomes 15 digits.

2. Use that file to provision the IMSI range using any REST-based client.

3.3 Equipment Identity Database

The database schema used in UDR includes:

- Bulk upload of data for provisioning is supported.
- IMEI is validated to 15 digits when provisioning. Upto 10 IMSI can be associated with 1 IMEI.
- The database supports a 100000 IMSI range to support white listing special subscribers.
- It is also possible to provision the Software Version (SV) against the IMEI.

- The SV is two digits, if it is not provisioned. The default value of 99 is stored against the IMEI.

> **Note:**
>
> BCD and HEX values in the IMEI and SV are not supported.

- UDR is able to respond with an error INVALID_KEY_VALUE when IMEI is provisioned with any value other than numeric digits.
- UDR is able to respond with an error INVALID _KEY_VALUE over the provisioning interface when it detects that IMEI being provisioned is not correct in length.
- UDR allows provisioning of the type of Black listing against the IMEI (within the main subscriber profile) and SV as shown in Table 3-3.

Table 3-3 UDR Attributes

Attribute	White List	Gray List	Black List	SV
Allowed Values	TRUE/FALSE	TRUE/FALSE	TRUE/FALSE	00 to 99 Decimal only
Default Values	TRUE	FALSE	FALSE	99

3.4 EIR Logging

Logs are written in each STP MP's and DAMP's file management area located at /var/TKLC/db/ filemgmt/Eir_logs/. The file name is comprised of "File creation date and time"-"File close date and time"_"MP host name". A sample EIR log file name would be EIR_28052018.070425-28052018.120427_so1mp1__logs.

vSTP EIR logs an entry when:

- Equipment status is found to be blacklisted or graylisted
- Equipment status is blacklisted, but allowed due to IMSI overide
- In error scenario, like the UDR connection is not available and the configured default response in error (EIR options table) is black or gray.

A configurable flag is provided in EirOptions table in case logging is needed for the whitelisted devices. Default value of the flag will be `off`.

vSTP EIR Logging

In case of vSTP EIR, Logs will be written in a file in csv format on each STP-MP file management area.

If IMSI is not present or EIR not able to decode IMSI in the message then IMSI field will be kept blank in the Eir logs.

The logs provides in csv format and include the following information:

- Date and time of the message
- The IMEI digits and the OPC from the CHECK_IMEI message.
- IMEI SV, if available

- The IMSI digits from the CHECK_IMEI message (if present)
- SCCP CgPA Digits from the source of query
- Device Status - Whether the IMEI was Whitelisted, Graylisted, or Blacklisted
- Reason - Blacklisted, but allowed due to IMSI override or IMEI Range Match

Diameter EIR Logging

In case of Diameter EIR, Logs will be written in a file in csv format on each STP-MP file management area.

If IMSI is not present or EIR not able to decode IMSI in the message then IMSI field will be kept blank in the Eir logs.

The logs provides in csv format and include the following information:

- Date and time of the message
- The IMEI digits from the ECR message
- IMEI SV, if available
- The IMSI digits from the ECR message (if present)
- Origin-host and origin-realm of the ECR message
- Device Status - Whether the IMEI was Whitelisted, Graylisted, or Blacklisted
- Reason - Blacklisted, but allowed due to IMSI override or IMEI Range Match

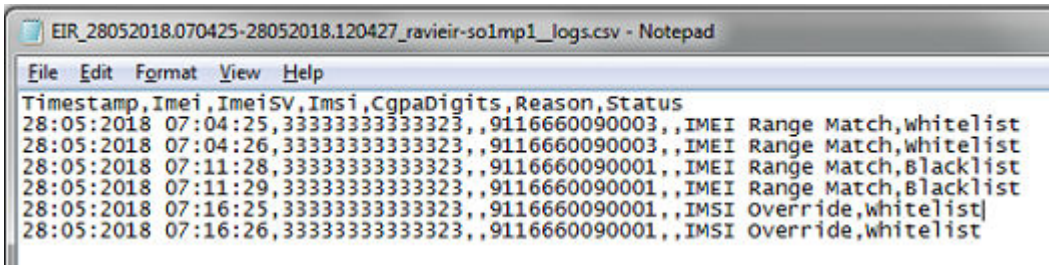
The MP copies the log file to the SOAM every hour to /var/TKLC/db/filemgmt/export/Eir_Log/Deir.

The MP copies the log file to the SOAM every hour to /var/TKLC/db/filemgmt/ export/Eir_Log/Vstp.

For example, if an MP server receives entry ID 1234 on July 15, 2003, at exactly 4:36 PM from a Service Module card provisioned at address 192.168.120.1 indicating that Blacklisted subscriber 9195551212 using handset 12345678901234 was detected, this entry is created:

```
20030715163600,192.168.61.1,1234,9195551212,12345678901234,0
```

Figure 3-1 Sample Log File



3.5 EIR Interface

EIR supports both SS7 and Diameter interfaces through the MAP_CHECK_IMEI request and response messages on the SS7 interface; and the Equipment Check Request and Answer

messages on the S13 and S13' Diameter interfaces. For more details on the supported interfaces, refer to 3GPP Specification document for 3GPP Interfaces.

4
EIR Configuration

This chapter provides procedures to configure the connection required for EIR to access the database on UDR NOAM using Application administration.

4.1 EIR Configuration Procedure

Use this procedure to set up EIR.

1. From an active UDR NOAM, add DAMP to UDR.
   a. Log into UDR as the admin and navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and click **Insert**.
   b. Specify the DAMP server XSI IP address as a client.
   c. Select the UDR server group from `Available Local Server Groups` that needs to communicate with the DAMP.
   d. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** and verify the connections are set to **InService**.
   e. Verify the **Routed Services Status** is set to `Normal` by navigating to **Communication Agent**, and then **Maintenance**, and then **Routed Services Status** and then:
      - For Diameter, verify the **DRADbSvc** status is `Normal`.
      - For SS7, verify the **STPDbSvc** status is `Normal`.
2. From an active UDR NOAM, add vSTP MP to UDR.
   a. Log into UDR as the admin and navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and click **Insert**.
   b. Specify the vSTP MP server XSI IP address as a client.
   c. Select the UDR server group from `Available Local Server Groups` that needs to communicate with the vSTP MP.
   d. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** and verify the connections are set to **InService**.
   e. Verify the **Routed Services Status** is set to `Normal` by navigating to **Communication Agent**, and then **Maintenance**, and then **Routed Services Status** and then:
      - For Diameter, verify the **DRADbSvc** status is `Normal`.
      - For SS7, verify the **STPDbSvc** status is `Normal`.
3. From an active DSR NOAM, add UDR to DSR NOAM.
   a. Navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and click **Insert**.
   b. Specify the UDR NO server XSI IP address as a server.
   c. Select the DAMP server group in `Local SG` that needs to communication with UDR.
   d. Add the standby server to the DR NOAM.

e. Set the Connection Groups by navigating to**Communication Agent**, and then **Configuration**, and then **Remote Servers** and then:

- For Diameter, click **Edit**.
- For SS7, select the **STPSvcGroup** and click **Edit**.

f. Add all available UDR NO servers.

4. From an active UDR SOAM, ensure ComAgent connection are InService.

a. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status**.

b. Make sure the ComAgent connection is set to **InService**.

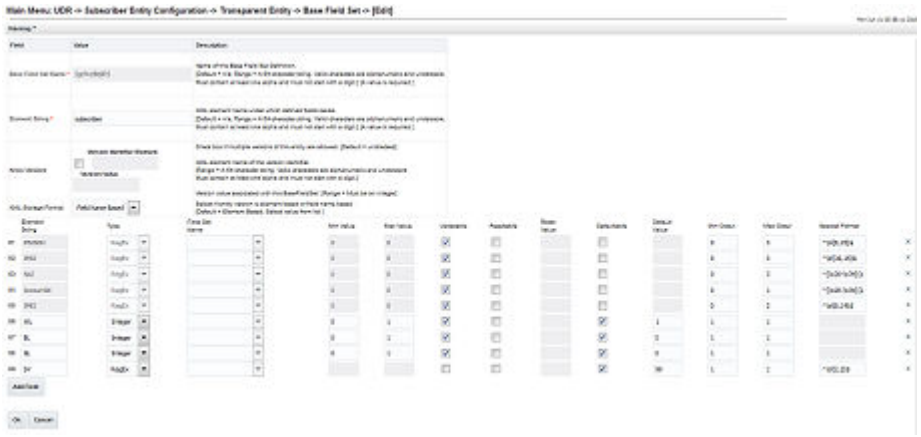
5. From an active NOAM, add subscribers in UDR.

a. Add the required fields for the EIR subscriber profile according to

List	Field name	Type	Value Range	Default Value
White List	WL	INT	0-1	1
Gray List	GL	INT	0-1	0
Black List	BL	INT	0-1	0
Software Version	SV	INT	0-1	99

The EIR profile fields should look similar to Figure 4-1.

Figure 4-1 EIR Subscriber Screen



Note:

You can also enable EIR feature with the help of **enableEIRSec** loader:

i. Login to Active NOAM Server console and run the **enableEIRSec** loader.

ii. Enable EIRSec with following steps:

i. Go to the path `/usr/TKLC/udr/prod/maint/loaders/upgrade`

ii. Run the **enableEIRSec** script.

b. Navigate to **UDR**, and then **Configuration**, and then **Provisioning Options** and mark the **Allow SOAP Connections** and **Allow REST Connections** checkboxes.

c. Click **Apply**.

d. Navigate to **UDR**, and then **Configuration**, and then **Provisioning Connections** and type the provisioning client's IP address for the White list.

6. From an active SOAM, add entries to the EirImsiRange table.

   Refer to IMSI Screening.

7. From an active SOAM, set the EIR admin state to `Enabled`.

   Navigate to **Diameter**, and then **Maintenance**, and then **Application**, click **Enable**.
   For SS7, run the `applicationAdmin Eir Enabled` command.

   ```
   applicationAdmin Eir Enabled
   ```

8. For Diameter only, from an active SOAM, add S13 application ID in DSR.

   Navigate to **Diameter**, and then **Configuration**, and then **Application IDs**, click **Insert** and add the S13 interface application ID.

9. For Diameter only, from an active SOAM, add an application route table in DSR for EIR.

   Navigate to **Diameter**, and then **Configuration**, and then **Application Route Tables** and insert the new ART or add a rule in an existing ART.

4.2 Configuring EIR Application

The **EIR** > **Configuration** folder contains the tables used to configure the EIR application. EIR application provides a mechanism that will allow the network operators to prevent stolen or disallowed handsets from accessing the network. The pages allow you to view the following information and perform the following actions:

4.2.1 Options

The Equipment Identity Register (EIR) Options are those configuration values that govern the overall EIR functionality for VSTP and Diameter.

The Options can only be updated and cannot be created or deleted.

Select the **EIR**, and then **Configuration**, and then **Options** page. The page displays the elements on the **Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 4-1 Options Elements

Element	Description	Data Input Notes

Table 4-1 (Cont.) Options Elements

Element	Description	Data Input Notes
Diameter Cong Err	If the incoming messages running on DEIR exceed or connection capacity on DEIR is not able to process the messages, DAMP fails in processing messages and it shall discard the messages and respond with the configured value in the result code.	{'default': 3004}
Diameter Product Name	This parameter is the vendor assigned name for the product. Currently only DSR is supported.	{'default': DSR}
Diameter Vendor Id	S13 local Vendor ID. All the outgoing messages that require Vendor ID in VENDOR_SPECIFIC_APPLICATION_ID will use this configured value. Currently only 10415 is supported, The CEA message will have 10415 in the response.	{'default': 10415}
Eir Def Imsi Resp	Equipment Identity Register (EIR) 'default' IMSI response.	{'default' : Whitelist}
Eir Def Mcc		E212 'default' mobile country code. It should support any 3 digits hexa-decimal number or None.
Eir Def Mnc	E212 'default' mobile network code. It should support any 2 or 3 digits hexa-decimal number or None.	
Eir Def Resp In Err	Default Equipment Identity Register (EIR) Response status when EIR application is in Degraded state. EIR can be in degraded state due to connectivity to Offboard UDR is down or Congested.	{'default' : Whitelist}
Eir Global Resp	Equipment Identity Register (EIR) Global Response status.	{'default' : Off}
Eir Imsi Chk	Equipment Identity Register (EIR) IMSI Check status. This parameter is not valid for IMSI range.	
Eir Imsi Scrn	Specifies the use of Equipment Identity Register (EIR) IMSI screening status. This option specifies whether the IMSI Screening shall be done before the IMEI check.	{'default' : true}
Eir Log White List	Specifies whether the white list logging for Diameter Equipment Identity Register (EIR) shall be on. This option has a 'default' of OFF.	{'default' : false}

Table 4-1 (Cont.) Options Elements

Element	Description	Data Input Notes
Eir Resp Type	Equipment Identity Register (EIR) Response Type.	{'default' : Type1}
Eir Software Version Screening	Specifies whether the Software version screening for Equipment Identity Register (EIR) shall be on. This option has a 'default' of OFF.	{'default' : false}
SS7 Def Map Ver	Default MAP version.	{'default' : V3}

You can perform edit task on **EIR**>**Configuration**>**Options** page.

Editing an Options

Use this procedure to change the field values for a selected Options. (The **Options Name** field cannot be changed.):

1. Select the **Options** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

4.2.2 IMSI Ranges

IMSI addresses are used to configure an equipment status for an IMSI range. An IMSI range is a combination of start address and end address. IMSI addresses can be used to bypass the IMEI check for certain IMSI ranges as defined by the operator.

Select the **EIR**, and then **Configuration**, and then **IMSI Ranges** page. The page displays the elements on the **IMSI Ranges** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 4-2 IMSI Ranges Elements

Element	Description	Data Input Notes
Start Address	Start IMSI address for the IMSI range. This is used to uniquely identify an IMSI range record.	Default = n/a; Range = Valid characters are numeric only of length 15.
Equipement Status	Equipment status.	Default = n/a; Range = Blacklist, Graylist, Unknown, Whitelist
End Address	End IMSI address for the IMSI range.	Default = n/a; Range = Valid characters are numeric only of length 15.

You can perform add, edit, or delete tasks on **EIRConfigurationIMSI Ranges** page.

Adding a IMSI Range

Perform the following steps to configure a new IMSI Range:

1. Click **Insert**.

> **Note:**
>
> The new IMSI Range must have a name that is unique across all IMSI Ranges at the SOAM. In addition, the IMSI Range's IP Port combination must also be unique across all IMSI Ranges configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a IMSI Range

Use this procedure to change the field values for a selected IMSI Range. (The **IMSI Range Name** field cannot be changed.):

1. Select the **IMSI Range** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a IMSI Range

Use the following procedure to delete a IMSI Range.

> **Note:**
>
> You cannot delete a IMSI Range if it is part of the configuration of one or more Linksets.

1. Select the **IMSI Range** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5
EIR Alarms and Measurements

Alarms and Events

New alarms and events have been added to the Alarms and KPIs reference guide. See the EIR sections.

Measurements

New measurements have been added to the Measurements reference guide. See the EIR section.