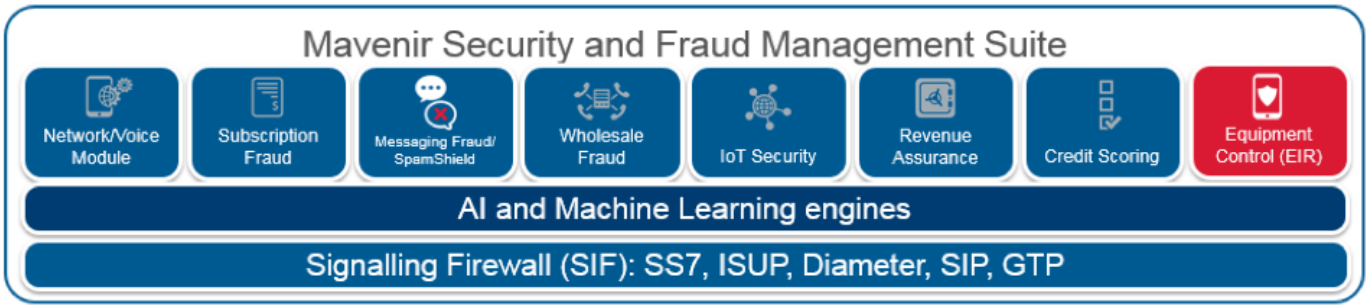
Mavenir's Equipment Identity Register (EIR) allows operators to control access to mobile networks, deterring device theft and fraud

Equipment Identity Register (EIR)



EQUIPMENT CONTROL WITH EQUIPMENT IDENTITY REGISTER (EIR)

Phone theft is a common issue today. The rise of smartphones places mobile devices at the center of people's personal and social life and the device contains numbers, messages, photos and videos that may not be backed up. Theft of the device means precious personal data is lost or, even worse, left open to abuse.

In addition, the deployment of pre-paid services where subscribers are anonymous and untraceable means that there is a ready market for stolen devices.

It is a significant initiative for an operator to actively fight theft of mobile devices, before risking becoming the victim of negative publicity. Reducing phone theft also reduces other frauds because stolen phones are widely used by those perpetrating scams.

The best tactic for reducing theft is to make theft a worthless activity. If it is widely understood that a stolen device will immediately be blocked then this reduces the value of the stolen device and lowers the incentive to theft.

Mavenir's EIR, the leading EIR platform and ranked number 1 worldwide, is the best tool for blocking stolen devices. Use of Mavenir EIR allows a mobile device to be blocked on the home network and potentially on all networks, regardless of the SIM card inside the device. Deploying an EIR allows prevention of the use of stolen mobile phones, which in turn, allows the operator to protect revenue and investment.

Key Benefits unique to the Mavenir EIR

In addition to blocking stolen devices, Mavenir's EIR performs a host of other valuable functions for the operator to retain subscribers, improve customer experience, increase brand awareness and maximize revenues. Additional services enabled by the Mavenir EIR with its built-in Device Tracker functionality includes:

- Locking subsidized mobile devices to SIM cards, ensuring tariff plans are adhered to.
- Locking SIM cards to particular devices.
- Detect and send SMS welcome messages to roaming subscribers.
- Expose mobile equipment make and model to external service applications, for example to enable optimal transcoding or ringtones types for the handset.
- Provide fraud and market reports about subscribers and mobile devices used.
- Automatically detect changes to mobile numbers, equipment and SIM cards, for fraudulent monitoring by detecting high SIM card swap rates.
- Enable intelligent marketing campaigns, for instance to particular handset types.
- SMS notifications sent to inbound roamers and particular SIM/device combinations.

Fighting fraud with Mavenir EIR

Mavenir's EIR is the world leading EIR system having been on the market since 1992, and has been deployed in over 100 networks throughout the world, and integrated with every major network infrastructure vendor's equipment.

Standards compliant EIR:

- 3GPP 22.016 compliant
- Support for CheckIMEI GSM Phase 1, Phase 2, Phase 2+ and 3G (including UMTS and W-CDMA) operations
- Support for ME-Identity-Check-Request over S13 and S13' interfaces for LTE networks.
- Black list, white list, grey list – Black list defines all handsets, which are to be barred. White list defines all handsets that may be used, acting as an "allow-filter", and grey list defines handsets that are "suspect" but allowed to operate on the network
- IMEIDB interface – Mavenir EIR provides a direct interface to the IMEIDB via SFTP. Mavenir EIR also provides an interface to the AMTA IMEI Clearinghouse (regional black list database used by the Australian operator community). Note: AMTA functionality is only available for the standalone EIR.
- IMEI+IMSI blocking using cloned handsets functionality

Support for user data convergence (UDC)

- Support for two options for networks with the layered UDC architecture:
- Monolithic (standalone) EIR: a "classic" EIR architecture where EIR stores equipment data in an embedded database and searches equipment lists held in memory. Provides an LDAP interface with Ericsson CUDB for retrieving MSISDN information.
- EIR Front-End: a "layered" EIR architecture where equipment data is held in an operator central database and provisioning is done centrally through a Provisioning Gateway.
- Flexible deployment options
- Support for standard COTS server deployments using commodity IT hardware.
- Support for virtualization using VMware.

High performance

- High per-node performance, N+1 scalability – Operators can add capacity by simply adding additional high capacity EIR nodes. EIRs synchronize information and are managed via a common management interface. This allows Mavenir EIR to affordably scale capacity with minimal disruption. N+1 scalability also provides increased service availability removing singe points of failure and allowing maintenance to be performed with no service downtime

- Geographic redundancy – Multiple Mavenir EIRs can be deployed within the same network at separate locations with lists synchronized automatically across EIRs. This supports a disaster recovery strategy, as well as potentially reducing backhaul connectivity costs between locations.
- MEI's stored as ranges, saving on database memory requirements (embedded database only)