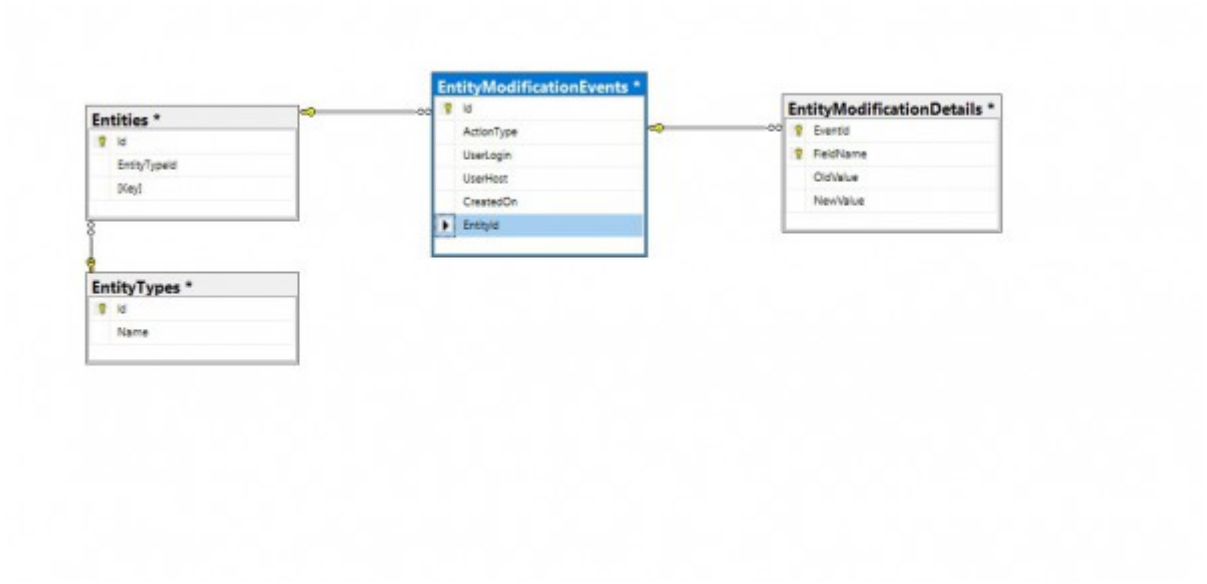
Audit trailing

An **audit trail** (also called audit log) is a security-relevant chronological set of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure or event. In PMA.core audit trailing is implemented as part of 21 CFR.11

How does it work?

PMA.core implements audit trailing as a middleware between the application and the connection to the SQL server database. This middleware captures all requests from the application to the database and, depending on the operation, creates records on a sub-schema of the database with all the required information to recreate them.

The sub-schema of the audit trail database can be seen in the table diagram bellow



- EntityTypes: All types known to audit trail i.e Root Directory, User, Form, FormData
- Entities: All specific entities that are available in PMA.core i.e. a specific Root Directory, specific user etc.
- EntityModificationEvents: This is the main table of audit trail that contains information about an entity that has changed on the PMA.core database. This contains the header information about the change.
- EntityModificationDetails: The detailed fields that was changed. This describes in detail a specific change in the *EntityModificationEvents* table with an one to many relationship(master/detail)

The **EntityModificationEvents** table in detail contains the following columns

- ActionType: The type of action this record represents, one of Create/Delete/Update
- UserLogin: The user that performed this action
- CreatedOn: The date and time the operation occured in the database
- EntityId: A foreign key to the *Entities* table for which the operation occured

The **EntityModificationDetails** is connected to the **EntityModificationEvents** and contains the

following columns:

- EventId: A foreign key to the **EntityModificationEvents** that this record describes in detail
- FieldName: The name of the database field that was changed. This is a field of the entity that was changed
- OldValue: The value before the change. This is null for Create operations
- NewValue: The value after the change. This is null for Delete operations

Consulting

The easiest way to consult the audit trail is via PMA.core's pre-defined audit trail views for the main entities of *Root Directories* and *Users*:

- Root directories
- Users

For more advanced use cases you can execute SQL Queries in the sub-schema of PMA.core database which was described in the previous paragraph.

Notes on storage requirements

Keeping an Audit trail of all changes happening in a live production PMA.core server can be quite space consuming. You can always check all storage requirements of PMA.core in the Diagnostics -> Installation Checks -> Storage Checks page

In that page you can check the total size of SQL database including the audit trail but also check other storages used such as the tile cache directory and the cloud cache

If the usage of Audit trail storage is getting large you can always backup the tables **EntityModificationEvents** and the **EntityModificationEvents** and safely delete all rows from these tables.