

2.3 MEUPS Database

The MEUPS system contains a single MSSQL 2005 database which serves many purposes. Below are the key areas of the MEUPS database and a brief description of their purpose.

- **User Information** – Stores user information such as first and last name, company and telephone number. Used to synchronize with accounts stores such as Active Directory.
- **Application Information** – Stores application information such as URL, Roles and Security to be used with custom claims.
- **Workflow Information** – Workflows, or authorization requests, allow users to request changes to their authorizations through a formalized approval process. These requests are modified via user-initiated actions as well as a Windows service which monitors the status of the requests. The Windows service monitors active requests for timeouts and takes the appropriate action by using the MLL object.
- **Directory Information** – Stores directory information such as system name and used to synchronize user account information.
- **Custom Claims Transforms Information** – Stores information to be used to creating custom claims for applications.
- **Audit Information** – Every time a user record is updated, the prior version is retained in a designated audit table. All authorization activity (GRANTS and REVOKEs) is also retained in another designated audit table. Database views are available that enable easy report authoring against this data. Note there is no purge policy in effect—all audit data will be kept indefinitely.

The database allows access using **Integrated Windows Authentication** and **SQL Authentication**. A single database role was created for data interaction named *MEUPS_Users*. This database role is granted execute permissions to all externally accessible stored procedures and granted view access to all externally accessible views. Stored Procedures beginning with '_' are not intended for external access. For security reasons, the *MEUPS_Users* role does not have schema or other database type access other than access listed above.

MEUPS uses database mail as a mechanism to communicate with MEUPS users. *DatabaseMailUserRole* role is allowed to send email using the mail profile defined for MEUPS. This profile sets the production STMP server for mail delivery and response email address for every outbound email and should be updated/changed as needed. For security purposed no external access is allowed to send email.

MEUPS has a single .NET Integrated stored procedure named *_SendSyncMsg*. The procedure initiates synchronization with external accounts stores configured in the *ActiveDirectory* table. This procedure is configured with PERMISSION_SET = UNSAFE for security reasons:

MEUPS incorporates programmatic standards for both naming and error handling. MEUPS uses Pascal casing as the default naming standard as defined with the first word being a verb. All internal

