User authentication data directory - CustomerID

Last reviewed: 2017-08-22

Ubisecure CustomerID supports two directory services for storing user authentication data:

- **Ubisecure Directory** is the default repository for user authentication related data.
- **Microsoft Active Directory** is an optional repository for user authentication related data.

> **NOTE: Microsoft Active Directory** usage for storing user authentication related data will be deprecated in future versions. This is because we will be moving to using an SQL database as the storage for all data and migrations from **Microsoft Active Directory** will be more problematic than migrations from **Ubisecure Directory**.

If you use Active Directory for storing the user authentication related data, Ubisecure Directory is still used for storing some of the configuration data concerning Ubisecure CustomerID.
Ubisecure Directory is a shared repository with Ubisecure SSO. Microsoft Active Directory is an optional user authentication data repository.

Ubisecure Directory

Ubisecure Directory is the name of the Ubisecure CustomerID's internal user authentication data repository. By default, Ubisecure CustomerID uses Ubisecure Directory as its main configuration and user authentication data repository. However, user authentication data can optionally be stored also in Microsoft Active Directory.

If Ubisecure Directory contains the user authentication data, it is called the main repository. If the user authentication data is located in an external directory (AD), that directory is called the main repository. The main repository contains multiple kinds of objects: Users, Organizations, Roles, Mandates and Groups each having a special meaning.

The repository contains the following main branches:

- The `eIDM Groups` branch contains Ubisecure CustomerID internal groups and it has no organization structure. It specifically contains a special group, the `eIDMUser` group, which is needed by users in order to login to the Ubisecure CustomerID system.
- The `eIDM Users` branch contains all users and the organization structure of the Ubisecure CustomerID system. The `eIDM Users` branch also contains all virtual organizations and roles.
- The `eIDM Mandates` branch contains mandate data that holds information about the roles contained in each mandate.
- The `eIDM Services` branch contains the web agent that Ubisecure CustomerID uses.

The following figure provides a high-level description of the main repository structure.

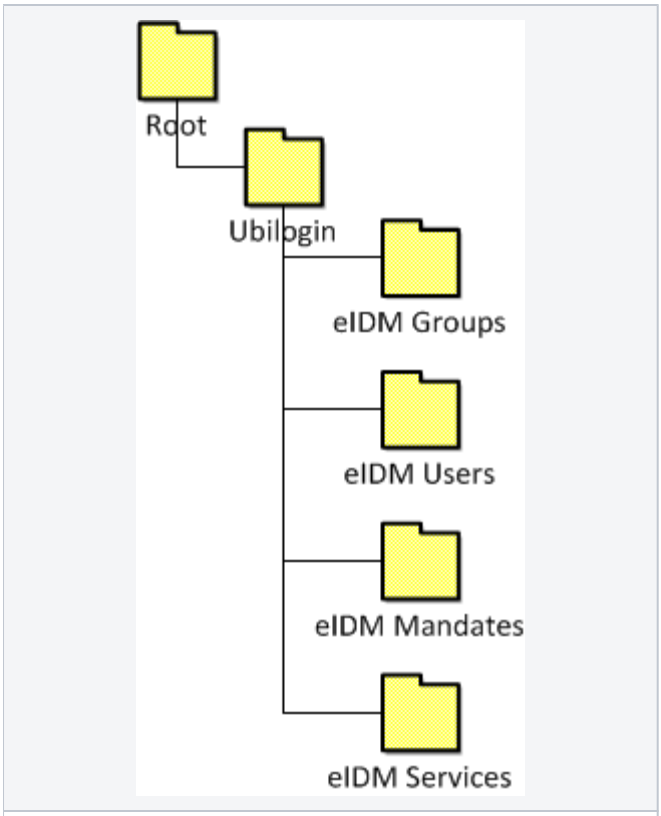

Figure 2. The high-level UbisecureCustomerIDmain repository structure

Active Directory

NOTE: Microsoft Active Directory usage for storing user authentication related data will be deprecated in future versions. This is because we will be moving to using an SQL database as the storage for all data and migrations from **Microsoft Active Directory** will be more problematic than migrations from **Ubisecure Directory**.

If Active Directory is not used as the main user authentication data repository, no special considerations are required. Instead, Ubisecure Directory (AD LDS or OpenLDAP) is used as the main user authentication data repository. It is a design decision during the implementation project to determine the optimal location of the user authentication data. Factors which influence this decision include the existence of legacy applications, licensing for AD users and other business and/or legal constraints. These decisions must be made at the initial stages of the project.

For example, the storage of social security numbers of external users in a company internal database may cause unwanted administrative overhead because of mandatory data reporting legislation.

Ubisecure CustomerID Database

Ubisecure CustomerID contains an internal database for all Ubisecure CustomerID data storage needs. The database is used, for example, to hold the workflow state, custom attributes and in conjunction with user approvals to hold information about the user and the approver.
The database also contains some duplicate data to the main repository because it facilitates faster lookups concerning that data.
The database contains multiple tables, which are described in the following table.

TABLE	DESCRIPTION
`CIDTAPPROVALREQUESTS`	This table holds approval requests related to assignment requests. One assignment request can contain multiple approval requests.
`CIDTASSIGNMENTREQUESTS`	This table holds assignment requests.
`CIDTASSIGNMENTS`	This table holds information about the roles or mandates related to assignment requests. One assignment request can in principle contain multiple roles/mandates but in practise it contains a single role.
`CIDTDATABASEVERSION`	This table contains the version number of the Ubisecure CustomerID database schema.

CIDTFEDERATIONIDENTITIES	This table contains federation identities.
CIDTFEDERATIONPARTNERS	This table contains federation partners.
CIDTMANDATEROLEDELEGATIONS	This table contains mandate role delegations.
CIDTMANDATEROLES	This table contains mandate roles.
CIDTMANDATES	This table contains mandates.
CIDTMANDATETEMPLATEROLES	This table contains mandate template roles.
CIDTMANDATETEMPLATES	This table contains mandate templates.
CIDTORGANIZATIONCUSTOMATTRIBUTES	This table holds untyped and multivalued organization custom attributes.
CIDTORGANIZATIONS	Database organization object, which links the database to the organization object in the main repository. This table also holds a copy of the built-in organization attributes.
CIDTROLES	Database role object, which links the database to the role object in the main repository.
CIDTUSERCUSTOMATTRIBUTES	This table holds untyped and multivalued user custom attributes.
CIDTUSERS	Database user object, which links the database to the user object in the main repository. It also contains built-in and typed user attributes.
CIDTPENDINGEMAILS	This table is used when user changes his or her email address and the new email address must be confirmed before it is taken into use.
CIDTPENDINGMOBILES	This table is used when the user changes his or her mobile number and the new mobile number must be confirmed before it is taken into use.
CIDTREGISTRATIONS	This table holds information about the registrations.

Table 1. Tables in Ubisecure CustomerID Database

Assignment requests are used when roles or mandates are assigned to a user or a pending user and the action must be confirmed. An assignment request can contain multiple approval requests, which allows the creation of multi-tier approvals.

System automatically removes all workflow related entries from the database that were not processed in the configured time. This means that administrators can configure, for example, the amount of days a role invitation is valid; if the role invitation is not processed during this time, it will expire and be removed.