Percipient
intelligent data engineering

UniConnect Data Security Overview

Data Security is defined as protecting data from destructive forces and from the unwanted actions of unauthorised users.

To that end, the UniConnect platform offers data security features not found in other data integration tools. It is designed for the protection of both data confidentiality and data availability. This means that the platform ensures that information is not accessible to unauthorized individuals, entities or functions, but is readily available upon demand by authorized entities.

No Copies

Importantly, the data queries processed by UniConnect are performed in memory, that is, they are not written to disk. There is therefore no duplication of the data, unlike traditional data discovery infrastructure which relies heavily on the data being staged before it can be queried. In the event of a system fault or system crash, the platform ensures that data is re-retrived from the source rather than a local cache.

Authentication and Authorization

In addition, the Uniconnect platform has inbuilt features to support only authenticated and authorised access. These controls take place at three levels:

- Access is restricted by users
- The functional authorization of the underlying platforms is maintained, which can be specific to database tables
- The admin user interface is supportive of audit protocols

Model A

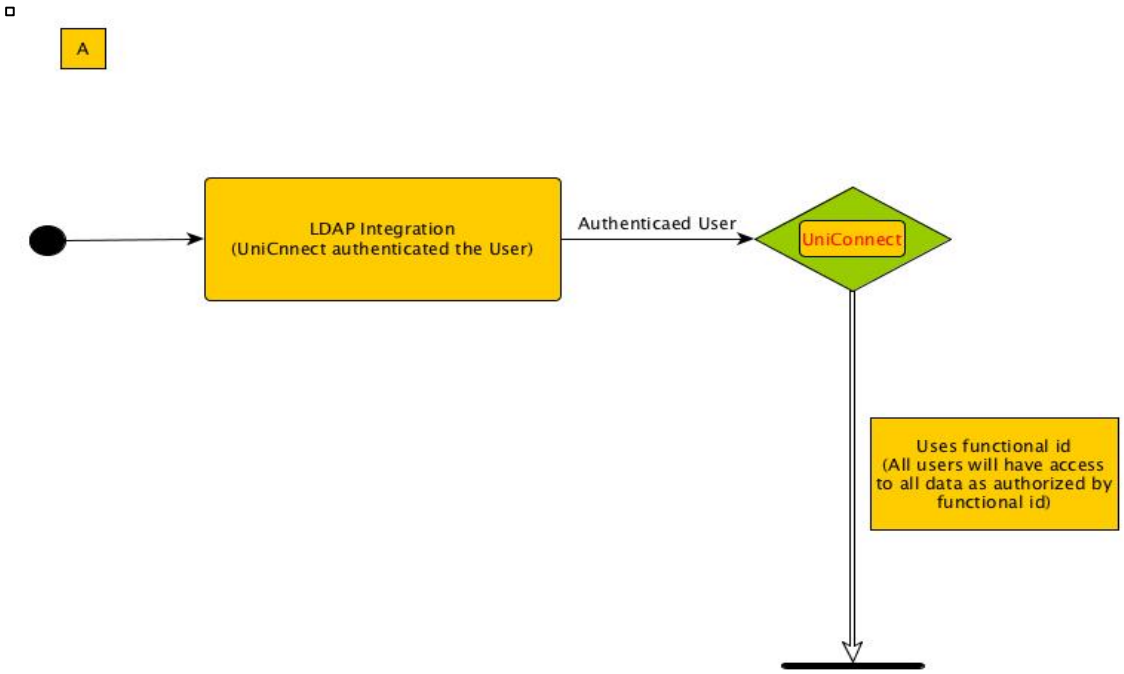
LDAP is a well-defined enterprise standard for *authentication*. Business computer networks use an LDAP server to organise information into hierarchies. To access the information, users must log into the server via an authentication (ie identity verification) process.

In most analytic environments, administrators typically integrate an enterprise's systems or databases with their existing LDAP server. This enables them to use the server as the master source of user data, and ensures that the LDAP protocol is maintained.

Model A is appropriate where such LDAP servers exist and LDAP integration is needed.

While LDAP directories are helpful for user-based authentication, they do not restrict what an authenticated user can access. To add an additional layer of security, the UniConnect platform also uses internally a Functional ID for each data source. This means that UniConnect maintains the functional *authorization* (ie access control) of the underlying system or database, which can extend to the specific schema or tables within the database.

Figure A



This security approach is equivalent to that used by such BI and visualisation tools as Websphere, Weblogic, and Cognos.

Model B

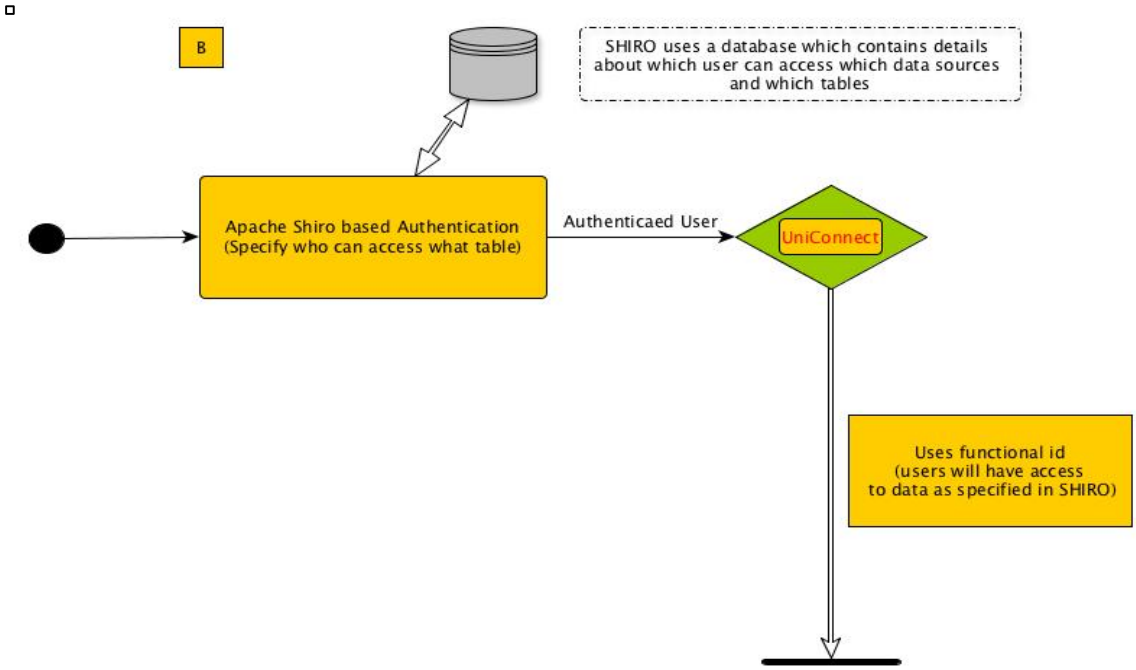
The UniConnect platform offers an even more fine-grained user authentication and authorization, if required. This approach does not use LDAP protocols. Instead, **Model B** uses a powerful, industry-proven and easy-to-use open source security framework called Apache Shiro.

Shiro supports a database capable of storing authorization details ie who can access what. Unlike traditional security paradigms, the "who" here is the currently executing user, which

can be a person, a role, a permission-holder or even a computer process. The authentication process is a single method call, and user identities can be based on one or more "realms" ie data specific operations.

The "what" can be fine-grained instance-level access to individual resources, including a table or a functionality (but not to the level of a row). Shiro can support any data model for access control.

Figure B



In both the above models, all passwords are encrypted using private and public keys.

Finally, the UniConnect platform's Admin Interface enables users to keep track of the queries made, query owners, the data sources queried, and all finished, failed or erroneous queries. This is in line with most audit protocols.