**One Identity Manager Architecture**

One Identity Manager Overview

One Identity Manager Architecture

**One Identity Manager Architecture**

**Figure 1: Overview of One Identity Manager Components**



One Identity Manager consists of the following components:

**Database**

The database represents the One Identity Manager kernel. It fulfills the main tasks, which are managing data and calculating inheritance. Object properties can be inherited along the hierarchical structures, such as, departments, cost centers, location or business roles. In the case of data management, the database maps the managed target systems, ERP structures as well as the compliance rules and access permissions.

The database is separated into two logical parts, payload and metadata. The payload contains all the information required to maintaining data, such as information about employees, user accounts, groups, memberships and operating data, approval workflows, attestation, recertification and compliance rules.

The metadata contains descriptions for the payload, such as, scripts for formatting rules and value templates or specific interaction. One Identity Manager’s entire system configuration, all the front-end control settings and the queues for asynchronous processing of data and processes are also part of the metadata.

Recalculation of inheritance is started by the database trigger logic. The triggers queue processing tasks in a task list called the "DBQueue".

The DBQueue Processor processes these tasks and recalculates inheritance of the respective database objects. The table "Jobqueue" is used for storing processing tasks that are run from the object layer.

The database systems SQL Server® or Oracle® Database can be implemented.

**Server Service**

One Identity Manager uses so called 'processes' for mapping business processes. A process consists of process steps, which represent processing tasks and are joined by predecessor / successor relations. This functionality allows flexibility when linking up actions and sequences on object events. Processes are modeled using process templates. A process generator (Jobgenerator) is responsible for converting script templates in processes and process steps into a concrete process in the ’Job queue’.

The server service "One Identity Manager Service" ensures distribution in the network of data managed in the One Identity Manager database. The One Identity Manager Service performs data synchronization between the database and any connected target systems and executes actions at the database and file level. The One Identity Manager Service retrieves process steps from the JobQueue. Process steps are executed by process components. One Identity Manager Service also creates an instance of the required process component and passes the parameters to the process step. Decision logic monitors the execution of the process steps and determines how processing should continue depending on the results of the executed process components. The One Identity Manager Service enables parallel processing of process steps because it can create several instances of process components.

The One Identity Manager Service is the only One Identity Manager component authorized to make changes in the target system.

**Application Server**

Clients connect to an application server storing business logic. The application server provides a connection pool for accessing the database and ensures a secure connection to the database. Clients send their queries to the application server, which processes the objects, for example, by determining values using templates and sending the results back to the clients. The data from the application is sent to the database when an object is saved.

Clients can alternatively work without external application servers, by keeping the object layer themselves and accessing the database layer directly. In this case, only the part of the object layer required for the acquisition process is mapped in the clients.

**Web Server**

There is an application running on a web server based on a web page render engine for implemented browser-based user interfaces. Users use a web browser to access the website that has been dynamically set up and customized for them. Data exchange between database and web server can take place directly or through the application server.

**Front-Ends**

There are different front-ends for different tasks. For example, a different front-end is used to configure One Identity Manager as that for managing employee data. The contents to be displayed and the extent to which it can be altered is determined in conjunction with the access rights of the respective user through the object layer.

Available front-end solutions are client and browser based.

**Figure 2: Overview of One Identity Manager Components without Application Server**



This sample application consists of two components:

Android™ OpenID Connect application

.NET OAuth2 protected Web Application Programming Interface (API).

The sample Android™ application contains a package called openidconnect which can be used in a standard Android™ project to authenticate users, using the OpenID® Connect Code Flow.

The sample Web API contains a .NET Open Web Interface (OWIN) middleware called CAMBearerTokenAuthentication which can be used in a standard .NET Web API project to authenticate the Android™ application, using the Access Tokens obtained from Dell™ One Identity Cloud Access Manager.

The Web API validates the Access Token by using it to call the Cloud Access Manager User Info Endpoint. The validation is performed using the provided OWIN middleware, which will cache the User Info responses. The OWIN middleware will also verify that the Access Token was scoped for itself by checking that the User Info response contains at least one of its scopes. The claims returned from the User Info Endpoint are used by the Web API to identify the user and control their access.

The OWIN authentication middleware is registered and configured using:

Assessment & Roadmap Review and Planning

User Provisioning Automation of user management and access to systems within an organization

Change Management Automation and support for development, rollout and maintenance of system components from current state to future state.0

Role LifeCycle Management Modeling and implementation of Roles within an organization

Access Management & Control Real-time enforcement of application security using identity-based, attribute based and policy based access controls and provisioned entitlements

Governance Implementation of a controls based framework and a robust governance program

Audit & Compliance Support for laws, regulation and policies defined within an organization for Business and IT Development

Validate your current state

Highlight your constraints

Identify your crucial success factors

Define your desired future state & first win

Develop your blueprint

Deliver a step by step roadmap:

Costs Timelines Milestones Business Justification

Dell Software’s solutions for access management include:

• Identity Manager

• Quick Connect

• Virtual Directory Server

• Active Roles

• Privileged Password Manager

• Privileged Session Manager

• Authentication Services

• Enterprise Single Sign-on

• Cloud Access Manager

• Defender

Dell Software’s solutions for federation include:

• Cloud Access Manager

• Quick Connect

• Virtual Directory Server

Dell Software’s solutions for auditing and reporting include:

• Identity Manager

• Change Auditor

• InTrust