



Oracle Identity Manager (OIM) is a user provisioning system. It defines properties for how users and groups get authorized to access compute and content resources across the enterprise. Identity Management technologies that are present in virtually all IT environments are designed to provision and de-provision users, manage normal user login activity, and may grant single sign-on to multiple systems and applications. However, in general these technologies don't detect or secure privileged identities.

Enterprise Random Password Manager (ERPM) works with all provisioning systems and can consume the configuration settings as input to its privileged identity management access control system with very little effort. ERPM can also manage the internal privileged identities used by user provisioning systems such as OIM. As an Oracle Platinum Partner, Lieberman Software Corporation works with its clients and Oracle to ensure all OIM/ERPM integrations are seamless when deployed in the client environment.

Oracle Internet Directory (OID) is a directory service compatible with LDAP, but uses Oracle database structures to store its internal tables. ERPM integrates with OID out-of-the-box. This integration can be useful when integrating OIM with ERPM.

ERPM also has a separate mechanism to import system data from LDAP directories, which would include OID. Since OIM now supports a LDAP identity repository for managing users, roles and role assignments, Lieberman Software can leverage this content and format as it would with any other LDAP.

For tighter integration with OIM, the Generic Technology Connector (GTC) can be used. The GTC supports simple integrations to custom-built applications or other systems, like ERPM, that rely on simpler data exchange formats such as comma-separated fields. GTC provisioning automates account creation from the OIM server to ERPM using the data from the OIM repository.

With the above said, there are four unique ways in which ERPM integrates with OIM and OID:

- Bulk importing of OIM/OID IT Resources into ERPM as **Managed Systems**
- **Delegation Rights:** Auto-provisioning of groups and their associated roles/rights in OIM/OID to groups within ERPM with similar rights
- **Web Application Authentication:** Default authenticated user access to ERPM against OID/OIM
- **OIM/OID Password Management and Discovery**

Managed Systems

In order to change passwords on systems, ERPM needs to know about the systems. System discovery and organization is handled through the use of logical managed groups of systems called systems lists.

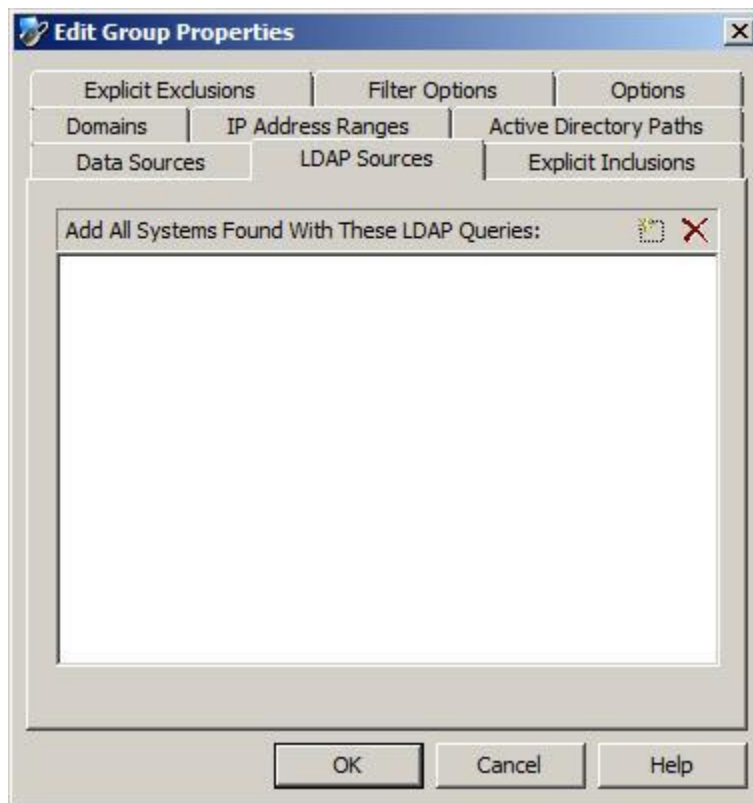


There are two basic approaches to managing system lists. One approach is to configure the system list once by explicitly adding systems to the list from using the various discovery features and then update that system list manually when the network topology changes. The second, and preferred approach, is to define an inclusion set based on inclusion ranges and then dynamically build the list of systems in that group from those ranges. Both methods have very compelling use cases.

The second approach works very well when network configuration is more dynamic; systems are being added and removed from the network on a regular basis. By providing the solution with criteria such as an OID/LDAP query, database query, IP range to scan, or other methods, ERPM will simply re-scan those criteria on a regular basis and automatically add or remove systems from the systems list automatically which in turn, automatically updates any jobs associated with those systems lists.

Additional system lists may be created to represent different logical groupings of systems. Typical uses include creating multiple systems lists designed to match the network configuration in OID. Systems can be members of as many system lists as is required without affecting licensing. System lists can be used to separate systems based on system type, physical location, OU membership, domain, or almost any other metric.

ERPM allows querying pre-configured LDAP compliant directories, such as Active Directory, Open LDAP, Oracle Internet Directory (OID), etc., to populate the systems list:





Edit LDAP System Search Path

LDAP Authentication Server: LSC

Subpath Under Root: cn=computers,dc=lsc,dc=ent

System Type

Windows Linux/Unix

Test

OK Cancel

Edit Group Properties

Explicit Exclusions | Filter Options | Options

Domains | IP Address Ranges | Active Directory Paths

Data Sources | LDAP Sources | Explicit Inclusions

Add All Systems Found With These LDAP Queries:

(LSC) cn=computers,dc=lsc,dc=ent

OK Cancel Help



Delegation Rights

A key goal of privileged identity management is to grant access to the identity only to authenticated requestors, in a timely manner, over a secure communication channel for a predetermined length of time and a documented purpose, using the least privilege required. ERPM provides a web interface to allow the remote recovery of passwords. Passwords for accounts that have been changed through ERPM can be displayed through the web application.

The web interface is an ASP web application that allows any user with the appropriate delegations the right to recover passwords for accounts managed by ERPM. There are a number of rights that can be delegated out to users of the web application. These rights apply to users, [global] groups, and/or roles (RBAC) and controls access to the features of the web interface as well as system and account information exposed through the web interface.

Access to specific managed lists of systems and accounts on those systems can be restricted based on specific users or groups using the delegation system. The delegation of recovery is done by granting **rights to the members of Windows groups, Windows users, Roles which can include users from Various LDAP directories including Active Directory, Open LDAP, OID, etc., or explicit users.**

With this in mind, when the user or a direct member of an OID/OIM group logs on, they will have access to the systems in their managed group(s). Access to those systems includes the right to look at stored passwords on those systems.

Once the delegation rules and the password recovery web console options are configured, a user will log into the website, which uses OID authentication, and based on the configuration options, the rights assigned to the user, and the systems and/or accounts the user has access to, these configuration options will determine the user's process for checking out a password. The delegation is set up by linking a delegated entity to a specific set of managed machines, or a specific vault.

Roles are used to grant permissions for users from disparate domains and directories. For example, a '*Password Recovery*' role may have been granted rights to login, view accounts, and recover passwords. In turn, this role contains users from different directories such as users from multiple active directories, eDirectory, OID, Open LDAP, etc.

Web Application Authentication

The web application settings are options that tell the website what operations to perform when a password is checked out or checked in. **ERPM allows default authenticated user access against OID/OIM.** This provides a means for any user who can authenticate against a central directory, such as Active Directory or OID, to gain access to the ERPM password recovery console based on the rights delegated to the user in AD/OID/LDAP/OIM. This provides an easy and global way to allow users to gain access to the website to use features such as the personal vault.

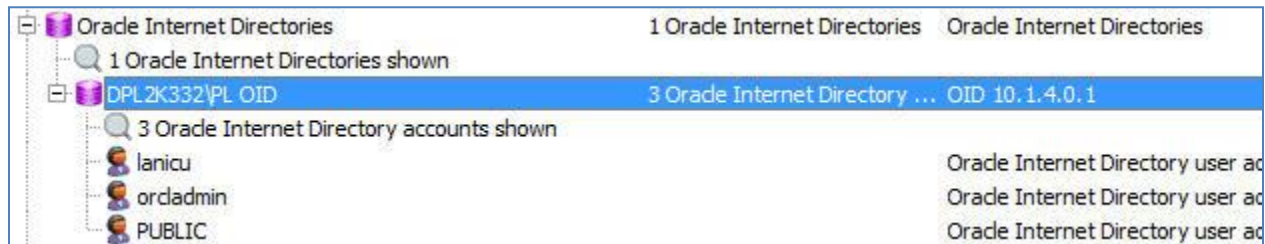


OID/OIM Password Management and Discovery

The primary goal of ERPM is to make password changes very easy. ERPM can manage passwords in any LDAP compliant directory. There are three directory node types available out-of-the-box:

- **Oracle Internet Directories**
- Novell eDirectory Databases
- IBM Tivoli Directories

The purpose of these three nodes is to identify default search and authentication settings appropriate to the three directory types. It is possible to add *any* directory type that is LDAP compatible to any of the three nodes.



Once a directory is added, ERPM can discover the accounts in the directory and manage those accounts; discovery is not necessary to take part in password management.

The structure of password change jobs are system based, rather than account based, which means it is very easy to change the same account on many systems at once with the same job. In most cases after jobs have been created, they will be set to run either once or indefinitely and will not require user interaction.

The first step in changing a password requires selection of the systems to be included in the job. Once the systems have been selected, the name of the account to be changed needs to be entered. **Accounts stored in directories such as Oracle Internet Directory, Tivoli Directory, eDirectory, OpenLDAP, and more can be scheduled to be changed regularly, with no manual intervention.**

After the account is selected, the new password settings are defined. The password for the account on all selected systems can be set to a static value or can be generated randomly in compliance with compatibility and complexity settings. Once the password settings are defined, the only remaining step is to set the schedule for the password update job, and to indicate if these credentials are used to run other applications or services. The scheduling option will dictate whether the job runs once, runs right away, runs at a later time, or runs on an ongoing basis.