

WHITEPAPER

LDAP Integration

Simplified Administration and Increased Security

Whitepaper
Accela, Inc.

March 2006

Reducing Administration While Increasing Security

Overview

Agencies and departments worldwide are constantly being faced with two seemingly conflicting pressures. The first pressure is to constantly reduce the costs of providing services, especially information services. The second is to counter the ever-present security threats that jeopardize information assets, over which they are custodians. Many organizations struggle to balance these responsibilities.

Occasionally, a technology arises that addresses both of these critical needs. The emergence, standardization, and subsequent adoption of the Lightweight Directory Access Protocol (LDAP) is one of these technologies. Smartly leveraging LDAP can put an organization on the path to providing improved service levels, greater security, and simplified use, all at reduced expense to tax payers.

LDAP

As distributed processing computer systems began to blossom, it became evident that users would need to keep track of usernames and passwords (their identities) on many different systems. While this task would soon become painful for users, security administrators were faced with an even bigger challenge—ensuring that only the appropriate people have access to sensitive data.

Proprietary systems soon emerged that allow disparate applications to leverage a central repository of user identity information. These systems broke the ground for standards to emerge. These standards started with x.500 in the late eighties and evolved into LDAP in 1995.

LDAP is a protocol for querying and modifying data in directory service; it is independent of the system storing and managing identity data. Many directory service vendors provide for LDAP access into their systems. These vendors include:

- Microsoft
- Novell
- Sun Microsystems
- Oracle
- Red Hat

Leveraging LDAP

Many computer systems and applications include security mechanisms that require users to authenticate themselves prior to use gaining access to functionality. Based on an authenticated identity, the system or application then allows a user to access specific data or perform certain actions.

The challenge for users is that they often have to remember unique usernames and passwords for each application they use. Security administrators need to account for every identity in every system to ensure that the right users are accessing the right systems. For many agencies, it is just not practical to manage this information in real-time so the task ends up being relegated to annual (or even less frequent) audits.

An LDAP accessible directory can serve as a shared repository for user identity information. For example, a user's identity (and password) in Microsoft Active Directory can be leveraged as the same identity for a permitting application. The user needs to track only one username and one password, making the system more secure.

If a user departs from an agency, the security administrator only needs suspend the user's account in Active Directory. The user's access is automatically suspended for all applications associated with that identity.

A Note About Single Sign On (SSO)

Another category of solutions that reduce complexity for IT organizations is known as Single Sign On, or simply SSO. When using an SSO solution, an end-user would authenticate once to their workstation, which would then pass that authentication to other applications and Web sites that the end-user utilizes.

These SSO solutions have their pros and cons, but it's important to note that LDAP integration does not equate to SSO. LDAP integration allows a single user name and password to be used by multiple systems, but does not automate the authentication to those systems.

LDAP and Accela Automation

Accela Automation is designed to provide the lowest possible total cost of ownership experience for agencies, while at the same time integrating with agency security policies. As such, Administrators can configure Accela Automation to leverage identities accessible via LDAP.

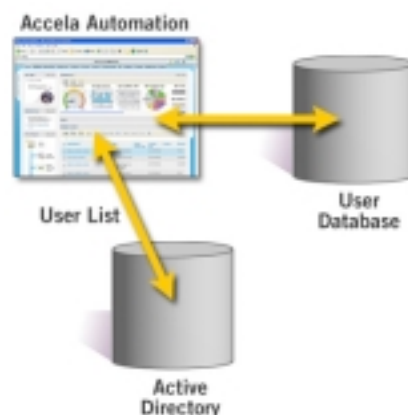


Figure 1

When configured to use an LDAP accessible directory, an administrator performs the following steps to add users (Active Directory is used in the example, but Accela Automation supports any LDAP accessible directory):

1. An administrator marks directory user groups whose users access Accela Automation.
2. A user import process runs automatically as a part of normal daily operations.
3. The daily Accela processes import the users into the Accela Automation user database and they remain linked to their corresponding entries in Active Directory.
4. An administrator assigns rights and privileges to the users as appropriate using the normal Accela Automation tools.

Once this process is complete, users in the Active Directory are linked to the users in Accela Automation.

Leveraging an LDAP directory offers many advantages:

- **Simplified process for adding users** – An administrator does not have to re-enter data about users that already exist in another system. New users that come into the Active Directory also automatically appear in Accela Automation (with no rights or privileges yet assigned).
- **Simplified user identity management** – Because identities link back to a shared repository, it is easy to determine which user is represented by the identity and thus what access rights they need.
- **Minimized productivity delay for new users** – A new user within the agency can have almost immediate access to all the systems they need to be productive.

Leveraging the Shared Identity

Once administrators establish an integrated identity for a user, the user authentication process leverages the user's shared identity.

Authentication occurs as follows:

1. Accela Automation users enter their Active Directory username and password when logging in.
2. Accela Automation forwards the username and password combination to the Active Directory via a secure (SSL encrypted) connection.
3. The Active Directory checks the username and password combination to see if they are correct.
4. The Active Directory responds to Accela Automation indicating whether or not the username and password combination is correct.
5. If the username and password combination is correct, Accela Automation grants the user access into the system. If the combination is not correct, access is denied.

This process greatly simplifies the experience for the end-user since they only have a single username and password to remember.

Benefits of Shared Identities

Shared identities offer benefits for many users at an agency.

For the Accela Automation administrator:

- Simplified process for adding users
- Simplified identity information management
- Minimized delay in productivity for new users

For the agency security administrator:

- Single point for password management
- Single point for security policy administration
- Automated de-provisioning for suspended users

For the end-user:

- Common username and password across all systems

Conclusion

Accela Automation's integration with standards-based shared identities delivers the vision of reduced administration while at the same time increasing security. For many agencies, all components needed for this solution are already in place - only minor configuration is necessary to reap the benefits of shared identities.