Using Microsoft Active Directory in the Domino World

White Paper
Using Microsoft Active Directory in the Domino World

Overview:
Companies utilizing IBM Lotus technology can obtain the ability to authenticate with Microsoft Active Directory to access Domino Internet applications and Notes clients as well as Windows. This capability is also available for companies with other directories installed, such as Novell eDirectory and Sun ONE.

Table of Contents

Introduction 1.0
   The Familiar Scenario 1.1
   Purpose and Overview 1.2

The Problem: The Password Management Challenge for Lotus Domino/Notes Shops 2.0
   Administrators Bear the Burden 2.1
   End-Users Feel the Pain Too 2.2
   Management Has Heightened Concerns 2.3

Microsoft Active Directory: Another Account to Maintain or the Answer to Simplifying End-User Account Management 3.0
   Active Directory Can Consolidate Passwords in Windows-Based Organizations 3.1
   Standardizing on Active Directory: Potential Issues to Consider 3.2

The Solutions: Configuring Active Directory as the Central Authentication Point for Domino Applications and the Notes Client 4.0
   Centralizing Password Management 4.1
      Enabling Best Practices 4.2
      Delivering Benefits to Administrators, End-Users & Senior Management 4.3
      Addressing Potential Issues with Standardizing on Active Directory 4.4

Summary 5.0

Appendix A – System Requirements 6.0
Appendix B – Password Controls 7.0
Appendix C – Active Directory Resources 8.0
Appendix D – PistolStar Resources 9.0
1.0 Introduction

1.1 The Familiar Scenario
If you’re a Domino system administrator, this is very likely a typical scenario in your day: An end-user telephones the Help Desk because they have forgotten or misplaced a password and are locked out of their computer. To address this issue, you start a virtual session in Microsoft Windows or Active Directory. However, only part of the problem is resolved, as the password the end-user forgot/lost is also their Notes ID password, which necessitates recruiting at least one other administrator who can generate the recovery information and relies on the cooperation of the end-user to complete the recovery process.

In most organizations employing Lotus technology, administrators find there are too many account directories and passwords to manage, as each end-user has at least three separate sets of credentials (usernames and passwords) — one each for the Windows workgroup or domain, the Domino Web server and the Notes ID file. Properly managing each of the many accounts requires several tasks, from creating new accounts in several places for every new employee to resetting passwords and synchronizing password quality rules. It is these tasks and not the complex troubleshooting that are generally the most time-intensive for administrators.

Password management is also the bane of the end-users. With so many separate passwords for accessing critical areas of the organization, there’s not only difficulty remembering them all, but recalling which password to use for each application. Remembering passwords becomes even more of a challenge when you consider that passwords generally need to be changed every 30-60 days. Therefore, the likelihood an end-user will forget or lose a password is very high, necessitating a call to the Help Desk for a password reset. According to research conducted by Gartner Inc., 30-45% of all Help Desk calls are for password resets and related end-user identification issues.

Often, a password reset requires a password change in several places, and the new passwords need to be synchronized with others. While password resets are expected as a frequent or even daily occurrence for administrators, when Notes ID password reset/recovery is necessary, Help Desk operations are seriously stalled. Notes ID password recovery — and password resets in general — eat up valuable work time for several people, creating frustration and diminishing productivity all around. Loss of employee time and productivity, not to mention security cost implications, present concerns for senior management.

1.2 Purpose and Overview
With the emergence of Microsoft Active Directory, a significant technology for Windows-centric computer environments, administrators have found they have yet another account to manage. The addition of alternative directories, such as Novell eDirectory and Sun ONE directory server, can also pose account management issues and add to administrators’ workloads.

Nonetheless, it is possible to leverage Microsoft Active Directory, or other LDAP directories, for resolving password management issues instead of having the technology add to the account administration burden of the IT staff. The password authentication process can be reduced almost entirely to Active Directory operations, further distributing the power of this dynamic technology.

In this paper, we will discuss the password management challenge experienced by administrators and end-users in Windows-based Lotus shops, but present a novel solution: Enabling end-users to use Active Directory as the central authentication point for accessing Domino applications and the Notes client. With this capability, organizations can remove the need to maintain and use separate passwords for those applications. As a result, passwords become less of a “management” process.
2.0 The Problem: The Password Management Challenge for Lotus Domino/Notes Shops

2.1 Administrators Bear the Burden

Passwords play a critical role in maintaining the security of an organization, however password management is just one responsibility among the many handled by IT security teams. Unfortunately, because their end-users have at least three primary passwords — one each for Windows or their directory/network domain, the Domino Web server, and the Notes ID file — administrators in Lotus environments can find password management a greater challenge.

Managing Multiple Accounts

For administrators, properly managing each of the many accounts that each end-user possesses requires the following responsibilities:

- Creating a new account in several places each time there’s a new employee;
- Removing (or disabling) these accounts when an employee leaves the organization;
- Resetting passwords in several places when an employee/end-user forgets their password(s); and
- Synchronizing the diverse sets of password quality rules of the many accounts, which may or may not overlap.

These responsibilities multiply with every new account assigned to each Domino/Notes end-user. And the more accounts each end-user has with corresponding passwords, the greater the chances a password will be forgotten. If passwords are jotted on notes attached to the end-user’s computer or somewhere in their cubicle, then loss or theft of the passwords is also possible, creating another matter entirely that can impact the organization’s security.

Resetting Passwords

When an end-user has forgotten a password, it needs to be reset, but if they’ve forgotten (or lost) one password, they’ve likely forgotten all passwords. As a result, passwords need to be reset in several places. The Notes ID file password is one password that may need to be reset, or in its unique case, “recovered,” as the Notes ID file password is securely locked and end-users attempting to access Notes are only allowed to authenticate against the Notes ID.

Recovering the Notes ID Password

The steps for recovering a Notes ID password are complicated, time-consuming and require both Help Desk execution and end-user involvement. These procedures safeguard the security of the Notes ID, but create other concerns for the administrators.

Notes ID recovery information is located at the root-level certifier ID. IT personnel must specify which administrators can generate the recovery information and how many administrators are required to unlock a Notes ID password. A mail-in database is created for receiving and storing backup Notes ID passwords from the end-users, along with a database document for correct mail routing.

At least two and generally three administrators are required to locate the Notes ID password recovery information and send it the end-user. The administrators who have been recruited need to get a copy of the locked Notes ID on their local machine, open the Domino Administrator client and extract their ID recovery information. The information is a seemingly random, 16-character string. From the three administrators selected, the end-user must receive the strings of recovery information and enter them in the dialog box.

When the end-user receives and opens the email with the recovery information, it’s up to them to manually “accept” this information as it’s not done automatically. They must also enter their new/current Notes ID password, which completes the process by automatically sending a new backup copy of the Notes ID password to the mail-in database.

Engaging end-users in this process is a major hurdle for the administrators and cannot be enforced.
Plus, tracking down whether or not the end-user has accepted the recovery information is a manual process, since the email containing the backup Notes ID is the only evidence the end-users received and accepted the recovery information. Unfortunately, it’s sent to a standard Notes database that does not have tracking tools or views present.

Synchronizing Numerous Sets of Password Quality Rules
Possessing multiple passwords does more than lead to lost or forgotten passwords and the need for password resets — problems also arise with password synchronization. For example, changes made to the Windows password often do not synch with the Notes ID password. Also, since Windows and the Notes ID have different policies for password quality — setting minimum complexity requirements that do not correspond with one another — password synchronization is often hindered. As a result, administrators are called on to provide assistance to end-users who are blocked from accessing certain applications due to password synching issues.

Policies regarding password expiration of the Notes ID password also create complexity. Configured through password policy management, the Notes ID password expires after a designated period of time. Therefore, end-users who haven’t changed their Notes ID password prior to the expiration will be locked out of Lotus applications.

Further, policies for Notes ID password expiration are configured separately from the Windows password, requiring administrators go to multiple locations to designate password expiration and complexity. This causes difficulty with reconciling the different passwords as the separate policies may not be consistent with one another or, worse yet, even compatible.

Experiencing Loss of Productivity and a Drain on Resources
All the tasks and issues presented above add significantly to the administrator’s already heavy workload, diminishing their ability to operate efficiently and accomplish even the most important tasks in a timely manner. Since password resets and related issues are responsible for a large percentage of the calls received at the Help Desk, the IT department’s costs for those calls can be draining. As it is, end-users average 21 Help Desk calls per year, each costing $10 - $30. Therefore, organizations with 2,000 or more employees can spend over $350,000 annually just on Help Desk calls.

The consequences of the multiple password management scenario are larger than one might believe. Administrators alone see their productivity drop and valuable IT resources are consumed, but other parties in the organization are also impacted.

2.2 End-Users Feel the Pain Too
Password management has also become a tremendous challenge to end-users, as corporate IT systems now include multiple platforms, different servers for various purposes, as well as the numerous software applications. In Lotus Domino/Notes environments, end-users have separate passwords to manage each day for Windows, Domino and the Notes ID file, and they encounter numerous prompts for these passwords.

For end-users, dealing with multiple passwords and password prompts delays access to critical applications and prevents them from working at an optimum level of efficiency.

When they’ve forgotten a password and require a password reset, end-users can experience substantial downtime while they call the Help Desk and wait for an administrator to perform the reset.

As mentioned, the task of Notes ID file password recovery also involves the end-user; there are several steps in the process that must be performed by the end-user, in addition to those steps taken by the administrators. Lotus’ recommended scenario is that the end-user initiate the recovery process for the Notes ID file password by finding the three Domino administrators who can generate the recovery strings. This recovery information is then applied by the end-user to reset the password on their Notes ID.

Hours can go by while the end-user waits for the administrators to generate and send the recovery...
strings — again, a large amount of downtime for the end-user, who cannot otherwise access their Lotus applications. This downtime translates to lost productivity as they are unable to proceed with their projects and perform the tasks required of them to get their job done.

2.3 Management has Heightened Concerns
To resolve the dilemma of managing multiple passwords, end-users and administrators have undertaken various measures and short-cuts. For example, to remember their passwords, end-users will often write them down and post them in full view of anyone coming near their desk or cubicle. To expedite the Notes ID file password recovery process, administrators will create a network drive shared only by administrators that stores each end-user’s Notes ID file password, or they may store the original Notes ID file password in a Notes database. In either case, the last Notes ID password of each end-user is stored in clear text, which is usually not encrypted.

Use of these practices can ultimately impact the security of the organization’s network, as they allow unauthorized individuals or internal hackers to obtain or access passwords very easily. The prospect that sensitive files can be compromised is of utmost concern to the organization’s senior management, as is the other ramifications of the multiple password scenario.

Downtime experienced by the end-users and administrators means lost time. Consequently, deadlines are not being met, and progress comes to a halt. Fielding a disproportionate number of Help Desk calls for password resets means IT is expending more time and resources in one area and not in other, possibly more critical, areas.

Always focused on their organization’s bottom line, senior managers are naturally concerned about the impact that lost time, resources and end-user/administrator productivity can have. Finding a solution that stems this impact is a top priority.

3.0 Microsoft Active Directory: Another Account to Maintain or the Answer to Simplifying User Account Management?

3.1 Active Directory Can Consolidate Passwords in Windows-Based Organizations
Employed properly, it is possible for end-users and administrators to use Microsoft Active Directory to consolidate passwords and simplify user account management. To configure Active Directory as the central authentication point for Lotus Domino/Notes products, you first want to ensure Active Directory is installed and working correctly for Windows end-user authentication. Information on how to do this is available through the resources identified in Appendix C.

3.2 Standardizing on Active Directory: Potential Issues to Consider
Configuring Active Directory can be easy with the right solution, however, as with any transition, there is a set of problems that could arise. Before a Windows/Domino/Notes organization attempts to standardize on Active Directory, the following should be considered:

1. Username mapping between Active Directory and Domino. For example, an end-user may be known as jsmith to Active Directory but John W Smith/Acme to Domino. If Active Directory is the central name authority, then signing onto Windows as jsmith must somehow tell Domino that this is the same end-user as John W Smith/Acme.
2. Re-directing Sametime, iNotes, Quickr, and Web application authentication from the Domino Directory to Active Directory.
3. Coordinating Active Directory with the usernames and passwords stored in Notes ID files, which are inherently separate and not part of any server-based directory.
4. Resolving the password synchronization problem. In other words, removing the need for an end-user to go to multiple places when making a password change. (This is different from the administrator’s password resets because password changes are the responsibility of the end-user.) Typically, an end-user who wants to change their password must go to Ctrl-Alt-Del within Windows, File/Tools/UserID in Notes, and their Person document (for the Web password) in the Domino Directory.
5. Resolving the single-sign-on (SSO) problem. In other words, removing the need for an end-user to retype their password multiple times when performing related operations. It is easier for an end-user to have only one password and to enter it only once, however, if an organization needs a high level of data security, they may want to maintain multiple passwords per person and require the end-user to re-enter the password when entering a new computing domain.

6. Simplifying the management of password policies. Organization password rules should be enforced consistently across computer systems, while making it easy to set and update these rules.

7. Minimizing apparent system changes for the end-user and reducing the need for retraining during the transition. Many system administration projects have been jeopardized when it became clear that end-users would need to be re-educated to perform everyday procedures.

These problems are illustrated by Figure #1, which shows the complexity of the overlapping directories, passwords, and sign-on schemes.

Though these obstacles would suggest that standardizing on Active Directory in a Domino environment is prohibitive, a solution exists that addresses and resolves them while enabling organizations to deliver simplified end-user access to their Domino applications.

4.0 The Solution: Configuring Active Directory as the Central Authentication Point for Domino Applications & the Notes Client

4.1 Centralizing Password Management
We have proof that end-users can centralize and simplify password management using Active Directory, and that proof is found in Password Power — PistolStar’s single sign-on and authentication redirection solution. With Password Power, end-users with organizations utilizing Lotus technology can authenticate with Microsoft Active Directory for accessing Windows, Domino servers and Notes clients. System access and account management are simplified, as Lotus end-users typically have separate passwords for Windows NT, 2000 or XP, Lotus Notes (including the Notes ID file), Lotus Domino Web applications, Lotus Sametime and Lotus Quickr.

By allowing end-users to authenticate against a central directory such as Active Directory, Password Power makes it possible for them to have only one password to remember or change, eliminating the downtime and lost
productivity associated with maintaining multiple passwords. When a password change is implemented, the Domino Web passwords and the Notes ID file password are automatically updated.

With Password Power, administrators and end-users are relieved of dealing with the daunting process of recovering the Notes ID file password. Password Power eliminates the need to perform Notes ID password recovery since end-users can use their Active Directory password to unlock and access the Notes ID password automatically.

Password Power also allows end-users to achieve single sign-on — they just enter their Active Directory password at the Windows login and they’re experiencing the convenience of smooth and instant access without repeated password prompts. With only one password in play, administrators’ account management tasks are streamlined, and they realize a dramatic reduction in Help Desk calls, as end-users no longer require them to perform password resets for forgotten passwords. With Password Power, if an end-user does forget their Active Directory password, answering the previously-created challenge question will give them immediate access to Notes and Domino. Because Password Power facilitates authentication with Active Directory, password synchronization of the Notes ID is no longer required.

4.2 Enabling Best Practices
As it provides authentication power, enabling Active Directory authentication to access Domino, Notes, Sametime and Quickr, as well as Windows, Password Power also incorporates best practices for maintaining and enhancing the security of corporate data.

Administrators can address specific problems and challenges, such as enabling secure access to corporate intranets and extranets, and protecting applications and content from illegal usage. They can also achieve security best practices through the ability to define password rules and numerous password preferences related to password quality, history, expiration, 3-strikes and last login.

Password Power centralizes password policies related to password expiration, password quality, etc., to make certain that the policies of the three primary password sets are in line with one another. Otherwise, the password synchronization process will not occur or be broken, preventing immediate and streamlined access to all applications.

During the authentication process, Password Power automatically transfers the password security policies implemented by the administrator through Windows to the other passwords. This ensures the coordination of disparate password policies, particularly those of Windows and Notes.

Password Power responds to organizations’ corporate and regulatory compliance needs by supporting the system access management and data protection requirements of SOX, HIPAA, and Gramm-Leach-Bliley. Enabling authentication redirection to Active Directory provides Password Power with added strength and flexibility for maximizing these compliance-related capabilities:

• Facilitating and enforcing the use of stronger passwords;
• Ensuring employees only have access to systems and information required for their jobs;
• Guaranteeing accounts are disabled and access is completely revoked when employees leave company;
• Automating password reset processes to eliminate human error;
• Enforcing password policies that require passwords to be strong and changed regularly;
• Confirming unified password policies via accurate password synchronization
• Enabling strong authentication; and
• Protecting sensitive corporate and customer data through encryption.

4.3 Delivering Benefits to Administrators, End-Users and Senior Management
Password Power serves and benefits both end-users and IT administrators in several ways. For end-users, Password Power eliminates the frustration of remembering multiple passwords and greatly decreases the likelihood they will write down their password and become a target for internal network intruders.
Password Power also creates convenience for end-users by allowing them to perform their own password resets and to make changes to only one password in one place. By removing the need to engage IT to create a new password, Password Power also reduces end-users’ downtime, allowing them to be more productive.

For IT administrators, Password Power dramatically reduces the number of Help Desk calls regarding password resets, enabling them to allocate fewer resources for managing passwords.

Most importantly, by enabling end-users and IT to diminish downtime and increase productivity, and by incorporating security “best practices,” Password Power helps meet the corporate objectives of senior management. Ultimately, Password Power can positively impact an organization’s bottom line.

### 4.4 Addressing Issues of Standardizing on Active Directory

Along with the proper use of Active Directory, Password Power resolves the issues that can arise when standardizing on Active Directory in a Domino environment. Simply put, Password Power handles the following:

- Windows to Domino username mapping, either within Active Directory or by Password Power itself;
- Domino authentication to Active Directory;
- Password synchronization between Active Directory and Domino user accounts and Notes ID files;
- Single sign-on between Domino and Active Directory;
- Simplified coordination of disparate password policies as a result of using Active Directory as the central password authority. (Assuming you want single passwords within your organization.); and
- User retraining is minimized because Password Power operates transparently with little-to-no end-user participation required.

Figure #2 shows how Password Power can lead to an improved topology for Active Directory and Domino integration.

![Figure #2](image.png)

### 5.0 Summary

Administrators in organizations employing Lotus applications find they have too many accounts to manage, as their end-users have at least three separate passwords for accessing the systems they need to perform their job from day-to-day — Windows, the Domino Web server and the Notes ID file. Adding further to their workload are the frequent Help Desk calls to reset passwords and/or recover the Notes...
ID file password, since end-users clearly have more passwords than they can remember.

The emergence of Microsoft Active Directory, a significant technology for Windows-centric environments, has introduced another account to be managed as well as another password that needs to be remembered. However, the power of Active Directory can be leveraged to resolve the password management issues of administrators and end-users. By serving as the main authentication point for accessing Domino servers, Notes clients and Windows, Active Directory enables organizations to reduce the password authentication process, simplifying password management and removing the need for end-users to remember multiple passwords.

While there are potential issues to be considered when standardizing on Active Directory in a Lotus Domino/Notes environment, such as synchronizing diverse password quality rules, a solution exists that heads off these issues while it simplifies password authentication and management through the use of Active Directory. PistolStar’s Password Power makes it possible for end-users to have only password to remember or change, eliminating the downtime and lost productivity that administrators and end-users experience from maintaining multiple accounts and passwords.

By centralizing password management through Active Directory, Password Power enables single sign-on and allows self-service password resets. When a password change occurs, the Domino Web and Notes ID file passwords are automatically updated, ensuring Notes password policies are in synch with Windows. Password Power also eliminates the need to perform the weighty task of recovering the Notes ID file password — a huge time-savings in itself.

In addition to resolving the issues experienced by administrators and meeting the needs of end-users, Password Power provides tremendous value for an organization’s senior managers by enabling password security best practices that help maintain the security of important data and ensure compliance with regulatory and corporate standards.

Further, Password Power addresses management’s concerns over the bottom-line impact that multiple passwords can inflict due to downtime and productivity loss from the steady stream of Help Desk calls. By providing a password authentication advantage via Active Directory, Password Power does even more — it removes the difficulties experienced by administrators and end-users and alleviates specific cost concerns felt by managers. Password Power demonstrates its merit, both as a password authentication powerhouse and as a solution that benefits an entire enterprise.

6.0 Appendix A

System Requirements – Password Power 8

Password Power is a client-side solution with an optional server component that integrates seamlessly and doesn’t require end-user setup. Password Power’s server-side capabilities support Microsoft Windows Server 2003 and 2008, Unix, Linux, Sun Solaris, IBM System i and IBM AIX 5.1 and higher, as well as Lotus Domino R5, 6, 7, 8, and 8.5. On the client side, Password Power supports Microsoft Windows XP and Vista, as well as Lotus Notes 6, 7, 8, and 8.5.

7.0 Appendix B

Password Controls

Each of the three general types of passwords referred to in white paper — for Windows accounts, for Notes ID files, and for Domino Internet accounts — has several options and system administrator controls, which are summarized below.

Overall control:

- Windows — Minimum length, minimum complexity (described below), password history, minimum age, and maximum age.
- Notes ID — Minimum complexity (described below), password history, maximum age.
- Domino Internet (HTTP) password (R5 server or earlier) -- No policies.
- Domino Internet (HTTP) password (ND6 server or later) -- Minimum length or minimum complexity, and maximum age.

Account lockout:
- Windows -- Set on Domain or Local policy.
- Notes Client -- No account lockout possible when accessing local databases with a valid local ID file.
  Domino HTTP -- Delete or change HTTP password, otherwise none.

Password complexity:
- Windows – Password does not contain all or part of the user's account name; is at least six characters in length; contains characters from three of the categories upper case, lower case, digits, non-alphanumeric. Complexity requirements are enforced upon password change or creation. (From msdn.microsoft.com/library/en-us/library/ms161959.aspx.)
- Notes Based on password strength, which is loosely related to password length, as shown in the table below. (From www-128.ibm.com/developerworks/lotus/library/ls-password_quality/)

<table>
<thead>
<tr>
<th>Password quality scale</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Password is optional</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>Allow any password</td>
<td>fish password (password quality scale 3) lightferret b 4D (password quality scale 6)</td>
</tr>
<tr>
<td>2-6</td>
<td>Allow a weak password, even though it might be guessed by trial and error.</td>
<td>pqlrtmrx wefourkings (password quality scale 8)</td>
</tr>
<tr>
<td>7-12</td>
<td>Require a password that is difficult to guess but might be vulnerable to an automated attack</td>
<td>4891spyONu lakestreampondriverocean stRem2pO() (password quality scale 13) stream8pond1river7lake2ocean (password quality scale 16)</td>
</tr>
<tr>
<td>13-16</td>
<td>Require a strong password, even though the user may have difficulty remembering it</td>
<td></td>
</tr>
</tbody>
</table>

8.0 Appendix C

Active Directory Resources

Microsoft Active Directory technology center

Best practices for Active Directory design and deployment

Best practices for Active Directory users and computers

Best practices for assigning permissions on Active Directory objects
Information on the PistolStar product set, including the products discussed here:
www.pistolstar.com/products.html

9.0 Appendix D

PistolStar Resources


###