



Eliminating Notes ID File Password Management: A Groundbreaking Alternative

White Paper

PistolStar, Inc.
PO Box 1226
Amherst, NH 03031 USA

Phone: 603.547.1200
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

© 2009 , PistolStar, Inc. All rights reserved.

Eliminating Notes ID File Password Management: A Groundbreaking Alternative

Table of Contents

Introduction	1.0
The Notes Client Authentication Challenge	1.1
Purpose and Overview	1.2
The Lotus Notes ID	2.0
Lotus Notes ID File: Securing End-Users' Key Pairs	2.1
Lotus Notes ID Password: Complexities and Problems	2.2
Notes ID Password Recovery	3.0
What Lotus Recommends for Recovering the Notes ID Password	3.1
Set-Up for Administrators	3.1.1
Obstacles and Drawbacks	3.1.2
Alternative Solutions Employed — Speed Notes ID Recovery But Jeopardize Security	3.2
PistolStar's Password Power Saves the Day	4.0
Improving the Whole Password Experience: Password Power's Benefits	4.1
<i>Eliminating Notes ID File Password Management: A Groundbreaking Alternative</i>	
Summary	5.0
Appendix A – System Requirements	6.0
Appendix B – Resources	7.0

1.0 Introduction

1.1 The Notes Client Authentication Challenge

Organizations utilizing Lotus Domino clients know all too well that their end-users are only allowed to authenticate against the Lotus Notes ID. As a result, a lost Notes ID file or forgotten password can create a nightmare for both the company's IT department and the end-user. The steps for recovering a Notes ID password are complicated, time-consuming and require Help Desk execution and end-user involvement. In the recommended scenario, the end-user initiates the recovery process for the Notes ID but must find three Domino administrators to generate recovery strings. This information is then used by the end-user to reset the password on their Notes ID. The result is excess work for IT and a drain on IT resources, as well as a large amount of downtime for the end-user.

To counteract the issues posed by having to reset the Notes ID password, end-users often maintain and provide administrators with a backup copy of their Notes ID file, saving a copy of the Notes ID password as backup in clear text. While this simplifies the Notes ID password recovery process, it seriously compromises the security of the Notes ID file and password, creating easier access for potential hackers.

The question is therefore raised: Can we somehow forego the Notes ID password? Being required to use a separate password for Lotus Notes, as well as for Domino Internet applications, Windows and LDAP directories (Microsoft Active Directory, Sun ONE LDAP, and Novell eDirectory) keeps the average end-user very busy trying to remember all their passwords. However, possessing multiple passwords does more than lead to lost or forgotten passwords and the need for password resets — problems also arise with password synchronization. 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 prevented. As a result, end-users are blocked from accessing certain applications, and administrators are called on to provide assistance, diminishing productivity and tying up IT resources.

With the ability to authenticate against the Domino HTTP password, Microsoft Active Directory or other LDAP directories, Notes Client end-users and administrators would be less concerned with the Notes ID file password and would no longer need to recover it when lost or forgotten. There would be no need for end-users to engage IT and wait indefinitely for password recovery, and there would be no concerns about password synchronization and quality. Most importantly, there would be no more worries about the vulnerability of Notes ID files and passwords and the security of the organization.

1.2 Purpose and Overview

This paper discusses the complexities and challenges of managing the Lotus Notes ID password. While the Lotus Notes ID serves a critical function that requires password-protection — each end-user has one for storing their public and private key (or key pair) — the Notes ID password is inherently plagued with issues related to password expiration and password resets requiring password recovery.

Recovering the Notes ID password is probably the most cumbersome, disrupt-

With the ability to authenticate against LDAP, Notes client users and administrators would be less concerned with the Notes ID file password and would no longer need to recover it when lost or forgotten.

tive and time-consuming challenge that IT administrators encounter. As a result, a large majority of organizations resort to using one of two shortcuts, neither of which maintains the necessary security of the Notes ID nor protects internal networks.

The most typically used shortcut is to create a network drive shared only by administrators that stores each end-user's Notes ID. The other short cut is to store the original Notes ID 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. If the Notes ID dates back before the native password recovery came into play in Domino R5, the administrator may be able to set a new password for the end-user. This creates a security risk, as the administrator (current employee or not) knows the end-user's password and must communicate the new password to the end-user either verbally or in writing.

Saving the day for administrators and end-users alike, PistolStar's Password Power has a client-side plug-in capability that enables access to Lotus Notes applications via the Notes client by authenticating against LDAP (e.g. Microsoft Active Directory, Sun ONE LDAP, and Novell eDirectory), eliminating the need to maintain the Notes ID password and deal with the issues that accompany it.

Password Power assumes control of the Notes ID and automatically recovers the Notes ID password by simply resetting the end-user's password for Microsoft Active Directory, Sun ONE LDAP, or Novell eDirectory. The hassle and time sink of Notes ID recovery are eliminated because the end-user authenticates with this password. If they happen to forget it, a simple reset by the administrator immediately restores their access. Password Power also features a self-service component for the end-user in the form of a challenge/question and answer, which is accessible from any standard Web browser.

Providing end-users with secure access to all their applications with a single username and password is a lofty dream for any company. With Password Power, that dream becomes much more of a reality.

Password Power assumes control of the Notes ID and automatically recovers the Notes ID password by simply resetting the user's password for Microsoft Active Directory, Sun ONE LDAP or Novell eDirectory.

2.0 The Lotus Notes ID

2.1 Lotus Notes ID File: Securing End-Users' Key Pairs

As any IT administrator knows, the Lotus Notes ID is a significant part of the security of Lotus Notes and Domino. Each employee in an organization has one for containing their key pair — the public key and private key that are essential to Notes and Domino's Public Key Infrastructure (PKI). Based on the "Trust" model, the Lotus Notes ID certifies the employee for accessing the organization's network resources and establishes him or her as a trusted end-user.

Each key in the key pair can be used for encryption — an operation that requires the other key for successful decryption. While the public key is available and public, the private key is only available to the end-user. The Notes ID locks down both keys in the key pair. To ensure the security of the key pair, the Notes ID is password-protected, requiring end-users to authenticate against it when logging on to Lotus applications.

2.2 Lotus Notes ID Password: Complexities and Problems

By its nature and necessity, the password-protected Notes ID is extremely

secure. However, with that security, there comes a price — complexities with the Notes ID password that create problems for end-users and administrators that eventually slow productivity.

For starters, Lotus products don't handle the Notes ID well. End-users and administrators can't change the Notes ID password unless they know the current password that's on it. As a result, making password resets can become a major task if an end-user loses or forgets their password, as the administrator will have to first recover the password — a long and arduous process.

Another complexity with the Notes ID password is password expiration. 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 not only adds more tasks to the administrator's already heavy workload, but causes them difficulty with reconciling the different passwords as the separate policies may not be consistent with one another or, worse yet, even compatible.

When the Notes ID password is lost or forgotten, or when an end-user is automatically locked out when their password expires and prevents them from gaining any subsequent access to servers, the Notes ID password needs to be reset. If the end-user doesn't know their current password, then that password needs to be recovered by IT personnel. Notes ID recovery is a complicated and time-consuming process, which has led desperate IT departments to engage in alternative processes that are much faster but are inherently insecure, jeopardizing Notes IDs, exposing networks to corporate hackers, and increasing employees' risk of becoming victims of identity theft.

3.0 Notes ID Password Recovery

Whether an organization has several hundred or thousands of employees, performing password resets can be a frequent or even daily occurrence for administrators. When Notes ID password recovery is necessary, it could require more than one administrator as well as participation from the end-user. Numerous steps are involved in the process — some that are performed by the administrators and some by the end-user. Notes ID password recovery eats up valuable work time for several people, creating frustration and diminishing productivity.

The challenges administrators and end-users encounter during the Notes ID recovery process are many. Lotus recommends a set of procedures that safeguard the security of the Notes ID, but create other concerns for the administrators and cause disruptions for end-users.

3.1 What Lotus Recommends for Recovering the Notes ID Password

Here is a brief overview of the steps for Notes ID recovery as outlined in the Notes 6.5.1 Administrator Help Guide:

3.1.1 Setup for Administrators:

1. Add Notes ID recovery information to the root-level certifier ID using the

Password Power enables end-users and IT to diminish down time and increase productivity, and provides administrators with security best practices" for meeting the corporate objectives of senior management.

Domino Administrator client. At this point, it must be specified which administrators can generate the recovery information and how many administrators are required to unlock a Notes ID.

2. Create mail-in database for receiving and storing backup Notes IDs from the end-users
3. Create mail-in database document for correct mail routing

Once an administrator completes step #1, all end-users created in organizations with new installations of Notes will automatically have the recovery information in their Notes IDs. But, with the large majority of organizations with Notes installations, the end-users have already been created and have their Notes IDs, therefore the administrator must email the recovery information to all the existing end-users.

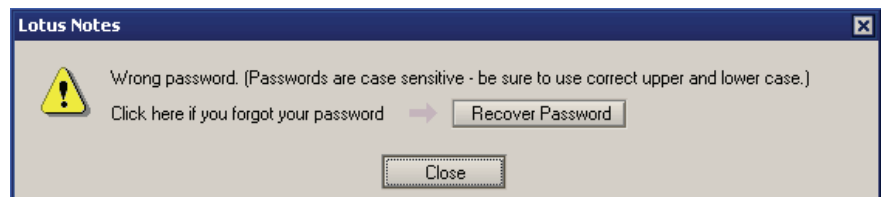
When the end-user receives and opens the email with the recovery information, it's then up to them to manually accept this information as it's not done automatically. They must also enter their current Notes ID password, which completes the process by automatically sending a new backup copy of the Notes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

3.1.2 Obstacles and Drawbacks

Engaging end-users in this process is a major hurdle for the administrators and cannot be enforced. Plus, tracking down which end-users have or haven't 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.

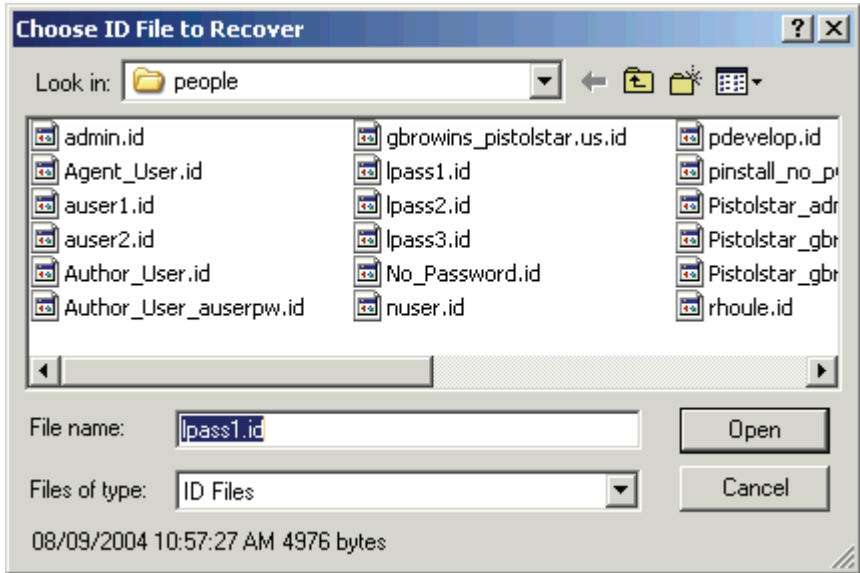
On the occasions when an end-user enters an incorrect Notes ID password, a dialog box appears indicating the end-user can click a "Recover Password" button if they've forgotten their password (see dialog box 1 below).

Password Power secures the authentication process while dramatically reducing the number of Help Desk calls regarding password resets, enabling administrators to allocate fewer resources for managing passwords.



Dialog Box 1.

Once they click that button, another dialog box appears in which they must choose which ID to recover (see dialog box 2 below). This is where the process can become problematic for the end-user.



Dialog Box 2.

The file picker in this dialog box does default to the Notes ID the end-user is trying to unlock, but the administrators may need to procure a backup copy for them from the mail-in database. The end-user must obtain this ID on a disc or network drive since they are locked out of their mail, then find it in the file picker. This process is a big hurdle for the end-user. The biggest obstacle is yet to come, however.

The next step for the end-user is to enter the ID recovery information from the required number of administrators. A dialog box finally pops up (see dialog box 3 below) with the list of administrators from whom they must obtain the recovery information.

PistolStar's Password Power Plug-Ins offer benefits for end-users, IT personnel and senior management alike.



Dialog Box 3.

But, how does the end-user contact the administrators when they're locked out of email and they can't open Notes to access a corporate directory that

might be stored somewhere in a Domino database? Usually, they end up making a phone call to the Help Desk or enlisting a co-worker to help them contact the administrators and get the recovery information. Either way, they've already involved another person and the process is just getting started.

Next, the administrators who have been drawn into the process 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 (in this case), the end-user must receive the strings of recovery information and enter them in the dialog box (dialog box 3 above). The recovery information strings generally look like the following examples:

703fe2794631b6b0

727b8bcf1440a8dc

86a41447ee7c3d2f

How the end-user actually receives this information from the administrators is another question, since (again) they are locked out of email. The process likely devolves to insecure transmissions such as writing it on scrap paper, copying it to a text file the end-user accesses over the network, or relaying it over the phone. The later mode of transmission could result in further problems if the end-user records an incorrect or transposed character.

3.2 Alternative Solutions Employed — Speed Notes ID Recovery But Jeopardize Security

Because of the time-intensiveness of the Lotus-recommended process for Notes ID recovery and the havoc it causes for administrators and end-users, the majority of organizations with Notes installations have resorted to employing one of two alternative processes. While these processes have provided some relief by simplifying and short-cutting Notes ID recovery, they are very insecure solutions and thus place end-users' Notes IDs in jeopardy.

The more commonly used alternative is to create a network drive shared only by administrators that stores a copy of end-users' Notes IDs. In this scenario, all Notes IDs have the same password or a default, user-specific password (e.g. their employee ID number). In itself, allowing end-users to share the same password is an obvious breach of security. However, because an end-user's Notes ID is where their private key is stored, and because the private key identifies the end-user and validates them for others on the network and in the organization, this approach greatly exposes the security of the entire organization and places it at risk for hacking, information theft, and corporate sabotage. The Notes ID file name usually matches the end-user's name, therefore, a hacker could use known facts about the end-user to guess their Notes ID file password and access protected files.

The second alternative to Notes ID recovery used by organizations is to store the last Notes ID password of each end-user in clear text, which is not encrypted. This approach makes it easy to recover the Notes ID, however, as with the other alternative, the security of the organization comes into question. Any end-user can easily access another's public key, and if they are able to just as easily procure the private key, then they can tap into any files the other end-user has secured or misrepresent themselves as the other end-user.

PistolStar serves Global 2000 companies and organizations across multiple vertical industries including automotive, chemicals, consumer products, finance/banking, government, healthcare, manufacturing, advertising and media, communications, pharmaceuticals and retail.

While organizations have been relieved to discover these shortcuts, they have been concerned with its security drawbacks and the potential consequences. Organizations with Notes installations have continued to seek simplified yet secure solutions to maintaining and recovering the Notes ID, and have not found one available until now.

4.0 PistolStar's Password Power Offers Ground-breaking Alternative

Developed by former Iris software engineers, PistolStar's Password Power provides capabilities that eliminate the need for maintaining the Notes ID password and dealing with the issues surrounding Notes ID recovery.

Password Power enables authentication against LDAP (e.g. Domino, Microsoft Active Directory, Sun ONE LDAP, and Novell eDirectory) for accessing Lotus Notes, iNotes, Domino Internet applications, Sametime Connect, and Windows operating systems. It removes the need for separate passwords for these applications and the Notes ID files by configuring LDAP or HTTP as the central password authentication point.

By leveraging LDAP or HTTP, Password Power provides unparalleled flexibility for easily accessing multiple platforms, servers and applications. Password Power reduces the number of times an end-user must supply log-on information during a Windows session to a single instance, and it can automatically update other passwords, such as the AS400 password, when a password is changed in Windows.

When an end-user logs in, Password Power serves as a gatekeeper for the Notes ID. Password Power also automatically provides Notes ID password recovery by simply resetting the end-user's directory password (e.g. Microsoft Active Directory, Sun ONE LDAP, and Novell eDirectory). The issues and time consumption with Notes ID recovery are eliminated because the end-user authenticates with their directory password. If they forget their directory password, a simple reset by the administrator immediately restores their access.

Password Power resolves any concerns that might arise when standardizing on a different, single directory in a Domino environment. For example, Password Power effectively handles the mapping of usernames from Windows to Domino as well as the Domino authentication to LDAP. Password synchronization between LDAP and the Domino user accounts and Notes ID file is also facilitated. By utilizing a directory as the central password authority, Password Power also simplifies the coordination of disparate password policies.

4.1 Improving the Whole Password Experience: Password Power's Benefits

Together, administrators and end-users reap an abundance of benefits from the capabilities offered by Password Power:

- Use just one set of credentials provides access to multiple applications. Single sign-on can be optionally enabled, allowing end-users to supply log-on information only one time during a Windows session;
- Password synchronization – and the issues that accompany it – is no longer necessary as synching is automatically facilitated between LDAP and the Domino user account and Notes ID file;

The issues and time consumption with Notes ID recovery are eliminated because the end-user authenticates with their directory password.

- Notes ID password recovery becomes the simple process of resetting the password for Microsoft Active Directory, Sun ONE LDAP, or Novell eDirectory — performed in a fraction of the time with improved security and less cost;
- Administrators can avoid any concerns regarding different passwords on multiple Notes ID files on multiple machines;
- Notes ID password expiration becomes a thing of the past, as it's not required when end-users are performing single directory authentication;
- Password policy management is no longer needed, as Password Power automatically transfers Windows password policy rules to other passwords and simplifies the coordination of disparate password policies; and
- Mapping of usernames is smoothly and effectively managed from Windows to Domino as well as the Domino authentication to the single directory.

Of course, the biggest benefit of all from Password Power is reduced administrative overhead. Password synchronization and password policy management are no longer necessary, and, most of all, Notes ID password recovery becomes a simple process performed in minutes with improved security and less cost. End-users will never again be “forgetting” passwords because there is really only one password they need — their Windows password, or their LDAP password, or their HTTP password. Using the Notes ID password becomes a thing of the past.

End-users will never again be “forgetting” their passwords because there is really only one password they need — their Windows password, LDAP password or HTTP password.

5.0 Summary

Organizations with Notes installations find managing the Notes ID file and maintaining or recovering the Notes ID password to be a formidable ordeal. The Notes ID file is fraught with administration issues and time-consuming and complicated tasks, particularly with recovery of the Notes ID password. Most companies have abandoned the Lotus-recommended solution for Notes ID recovery in favor of simpler and quicker processes. Consequently, these alternative processes compromise the security of the Notes ID and put organizations at risk for corporate hacking, theft and sabotage.

Fortunately, there is now a tool that allows organizations to remove the time-intensive maintenance and recovery tasks for the Notes ID, reducing administrators’ workloads, increasing productivity, and freeing IT resources for resolving more critical issues. PistolStar’s Password Power makes this possible by enabling authentication against directories such as LDAP for accessing Windows and Lotus applications. End-users also benefit from Password Power as it allows them to have only one password to remember and to log in only once, realizing time-savings and increased productivity on their end as well.

The upshot of all this is — whichever way you are performing Notes ID recovery, it is very likely the wrong way for ensuring the productivity and security of your organization. With PistolStar’s Password Power, you gain the ability to do it the right way.

6.0 Appendix A

Systems Requirements

Password Power is a client-side and optional server solution that integrates seamlessly with IBM Lotus technology 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

Resources

[“The Myths & Realities of Lotus Notes and Domino 8.5 Security”](#) PistolStar White Paper, January 2009.

[“Using Active Directory in the Domino World.”](#) PistolStar White Paper, October 2005.

###