

Password Management Issues In Notes/Domino Environments



an Osterman Research white paper
sponsored by

P I S T O L S T A R[®]
Password Power Plug-ins

Why You Should Read This White Paper

Password management in Lotus Notes/Domino environments can be difficult for both end users and IT staff. Since users of the Lotus Notes client typically authenticate against the Lotus Notes ID using a password, a lost or forgotten Notes ID password creates a headache for individuals and the IT staff that must help recover it, since the steps that IT must go through to securely recover the ID password can be complicated and time-consuming when using the built-in functionality of Notes. While there are faster alternatives available, these alternatives can increase the risk to network security.

Password management in Lotus Notes/Domino environments can be difficult for both end users and IT staff. Since users of the Lotus Notes client are allowed only to authenticate against the Lotus Notes ID, a lost or forgotten Notes ID password creates a nightmare for individuals and the IT staff that must help recover it.

The problem is exacerbated by the increasing number of enterprise-wide systems that are being deployed, each of which has its own password management methodology and unique set of problems. The result is placing an increased burden on help desk staff that must assist users in recovering passwords securely and with the confidence that they are doing so only for valid users of these systems. A minimum of one out of six help desk calls is related simply to password resets – some estimate the figure to be as high as 30%.

In addition to the increased workload for help desk and other IT staff, users who need to recover a password are effectively locked out of the systems they need to access while their password is being recovered, significantly and negatively impacting their productivity.

What is needed, therefore, is a method that allows users to recover their Notes ID password or other login information, to do so in a secure manner, to generate a password that is of sufficiently high quality and to do so without a call to a help desk or other IT staff members. This document discusses the problem in more detail and looks briefly at a solution to the problem offered by PistolStar.

Pain Points in Password Management

In order to more fully understand the problem with Notes ID management, Osterman Research undertook a primary market research study specifically for this white paper. We spoke with organizations of various sizes across a range of industries, focusing our research on individuals who are involved in the support and management of Lotus Notes/Domino environments for their organizations.

Notes ID Password Recovery is Not Too Time-Consuming...

Our research found that when a user loses their Notes ID password, three out of five organizations can recover it with 15 minutes of work or less. However, about one in four organizations requires up to 30 minutes of work to recover the ID password, while one in eight organizations must invest more than 30 minutes of work to recover a single password. Consequently, the recovery process can represent a fairly significant investment of IT staff time, not to mention that it is a disruptive task that prevents IT staff from working on more productive activities.

...but the Total Elapsed Time Can Be Significant

However, the total elapsed time to recover a Notes ID password can be significantly longer. We found that for one in six organizations, the total start-to-finish time for recovering an ID password is more than one hour and, in some cases, can be more than four hours. Another one-quarter of organizations would require up to one hour for the recovery, while the balance can do so in 30 minutes or less. What this means is that when users lose their Notes ID password, they are effectively prevented from doing any productive work while they wait for their password to be recovered. If we assume that an employee earns \$65,000 annually, each hour spent waiting for an ID password to be recovered means that the organization loses more than \$31.00 in productivity for that employee.*

For one in six organizations, the total start-to-finish time for recovering a Notes ID is more than one hour and, in some cases, can be more than four hours.

Although the elapsed time to recover a Notes ID password is significant, if a user loses his or her ID password on a weekend or holiday, the amount of time to recover it can be significantly longer. Our research found that nearly three out of five organizations would require more than one hour to recover an ID password outside of normal work hours, and that more than one in five organizations would require more than 24 hours to effect the recovery.

Losing Notes ID Passwords is Common and Expensive

Our research discovered that during a typical month, there are 17 requests per 1,000 users to recover a Notes ID password or a password for another enterprise system. While this may not seem to be a significant number at first glance, what this means is that during any given year about 20% of users will lose one or more passwords that IT must help them recover. Further, our research found that IT organizations estimate the cost of a single password reset to be slightly more than \$20 per incident. This means that for an

organization of 5,000 users, the cost to IT of just resetting passwords is in excess of \$20,000 annually.

However, the IT cost of resetting passwords is just the tip of the iceberg. For example, if we very conservatively estimate that the elapsed time to recover a Notes ID password or to reset another system's password is just 45 minutes, then the cost of lost productivity for an organization of 5,000 users is nearly \$24,000 annually. In other words, the typical organization will conservatively spend nearly \$9 per user per year in labor cost and lost productivity simply to recover Notes ID and other passwords.

Security Risks

The discussion above focuses on just the mechanics and the costs associated with password resets. However, there is a dramatically higher cost associated with these resets, namely password security.

In the typical Notes/Domino environment, password security is often inadequate. Notes IDs are often stored on a local server along with their associated passwords, creating a serious security risk.

In the typical Notes/Domino environment, password security is often inadequate. Anecdotal evidence suggests Notes IDs are often stored on a local server along with their associated passwords, creating a notable security risk by providing potential hackers a focal point for attack. Add to this the growing number of passwords that the typical user must manage – our research for this white paper found that the typical user manages a median of five passwords, although in some organizations the figure is much higher. When users have too many passwords to manage, they often write them down on paper or in a file on a local hard drive or file server that is often easily accessible, potentially making all their system passwords vulnerable.

Another quite serious problem is authenticating users who call into a help desk to reset a Notes ID or other password, a problem that is particularly serious for organizations with geographically separated users. For example, a hacker can call into a help desk and attempt to gain access to a password under false pretenses. Validating users over the phone is, at best, difficult and fraught with security risks.

A Solution to the Problem

Because of these problems, what is needed is a Notes ID password management system that has the following characteristics:

- **Strong security** to prevent unauthorized parties from gaining access to Notes ID or other passwords. Ideally, such a system would authenticate users against a corporate directory so that a user's new password could be generated based on specific attributes about that user contained in the directory.
- **End user self service** so that users who lose their Notes ID password can reset it without the help of IT staff or the help desk. This can dramatically reduce the downtime associated with an inability to access enterprise systems, while freeing IT and help desk staff for more important tasks.
- **Minimal training requirements** so that users can employ familiar procedures when resetting their Notes ID passwords without disrupting their normal workflow.

What is needed is a Notes ID and password management system that has strong security, end user self service and minimal training requirements.

Our research found that there is strong demand for such a capability. For example, when asked about the desirability of a system with these attributes, two-thirds of organizations indicated that it would be desirable or very desirable to have this capability. Further, when asked about the desirability of having Notes IDs managed from a central directory (e.g., Active Directory), nearly two-thirds of organizations indicated that this would be desirable or very desirable.

PistolStar's Password Power Offers a Better Way

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 directories (e.g., Domino, Microsoft Active Directory, SunONE 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 AS/400 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. The issues and time consumption associated 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 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.

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 using a directory as the central password authority, Password Power also simplifies the coordination of disparate password policies.

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.

- Notes ID password recovery becomes the simple process of resetting the password for Microsoft Active Directory, SunONE LDAP, or Novell eDirectory — performed in a fraction of the time with improved security and lower 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, since it is 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.
- Mapping of usernames is smoothly and effectively managed from Windows to Domino, as well as the Domino authentication to the single directory.

The biggest benefit from Password Power is reduced administrative overhead. End-users will never again 'forget' passwords because there is really only one password they need — their Windows password, or their LDAP password, or their HTTP password.

Of course, the biggest benefit from Password Power is reduced administrative overhead. End-users will never again 'forget' 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.

Summary

Password management is a time-consuming and expensive activity that consumes IT resources and makes users less productive while they wait for IT to reset their Notes ID and other passwords. Further, the whole process is less secure than it should be in many cases, since help desk or other IT staff often are never really sure that they have adequately authenticated valid users of corporate systems. What is needed, therefore, is a system that allows end users to reset their own passwords when needed, to generate a strong password based on directory information that already exists and to do so independently of IT. PistolStar's Password Power is such a system, offering a variety of benefits to IT and end users alike.

*Data was not collected on system password recovery times other than Lotus Notes

© 2005 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.