



Password Power 8 Lotus Notes Plug-In

Tech Brief



Pour plus d'information
www.cooperteam.fr

Password Power 8 Lotus Notes ID Plug-In

Summary

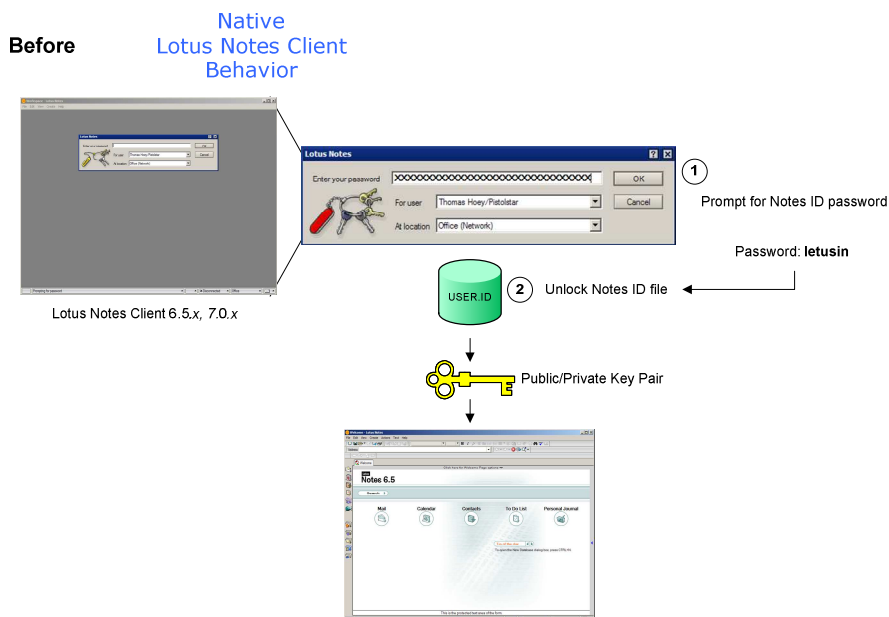
The Password Power Notes ID Plug-In provides authentication redirection utilizing the network directory or LDAP password for accessing the Lotus Notes client, bypassing the need to recover the Notes ID password if it is lost or forgotten.

Normally, end-user authentication for the Notes client is accomplished by entering the Notes ID password to unlock the Notes ID file, which contains the public and private key pair that allows access to the Notes client. Because the key pair is essential to Notes' Public Key Infrastructure (PKI), the steps required to recover the Notes ID password are complicated and time-consuming. The end-user must initiate the Notes ID recovery process and then typically has to find three Lotus 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.

With PistolStar's Password Power Notes ID Plug-In, a successful authentication to Microsoft Active Directory, Novell eDirectory, Lotus Domino LDAP, Tivoli Directory Server or Sun ONE LDAP grants access to the Lotus Notes client. This effectively eliminates the headache of manual Notes ID password recovery by allowing a reset of the LDAP password to restore access to Lotus Notes. Password synchronization between LDAP and the Notes ID file is also performed for times when the LDAP server is unreachable.

The following provides a step-by-step explanation on how the Notes ID Plug-In works and corresponds with the steps outlined in Figure 1 below.

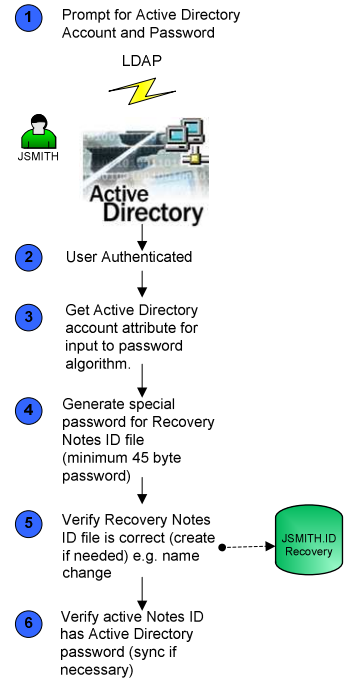
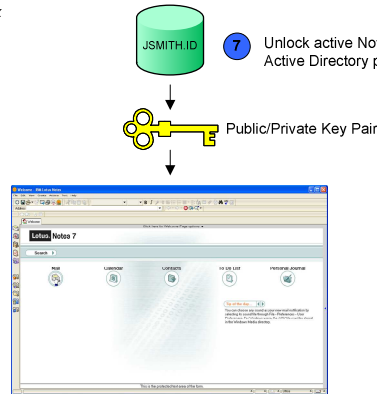
Figure 1.



After Password Power 8 (optional single sign-on)



Lotus Notes Client 6.5.x, 7.0.x



Encryption

The Active Directory or LDAP password is stored “in memory” in the Microsoft Windows registry. Either the 3DES or AES encryption algorithm is used, depending on the version of Password Power in use. 3DES, which has a 168 bit key, is only used by earlier versions of Password Power. The advanced encryption standard (AES), which has a key of at least 256 bits, is used by more recent versions of Password Power.

The Notes ID password is *not* stored in the Notes ID file. It is used to derive a key that is used to encrypt the ID file. Password Power does not change how Notes encrypts or decrypts the Notes ID file.

How It Works

Authentication

When an end-user launches Lotus Notes, the Notes ID Plug-In uses the Notes Extension Manager to prompt for the end-user’s LDAP username and password, which in this explanation will be Microsoft Active Directory (**Step One**). The LDAP credentials are used to authenticate the end-user against the nearest Active Directory domain controller and are used to synchronize the Notes ID password (if necessary) for offline purposes (**Step Two**). This innovative technique we call authentication redirection allows the use of one password stored in one location — the LDAP directory — to access Lotus Notes, Lotus Domino Websites, and IBM and SAP applications.

Recovery Notes ID File

The Notes ID Plug-In retrieves a configurable key attribute from the user’s Active Directory account (**Step Three**). When the Notes ID Plug-In then creates a special password for the Recovery Notes ID File (**Step Four**), the key value is among the inputs that generate this password, which is 45-63 characters in length.

The Notes ID Plug-In verifies the Recovery Notes ID file is correct, and automatically creates it if one does not already exist (**Step Five**). The Recovery Notes ID File is simply a file copy of the end-user’s Notes ID file with the generated password from the previous step set as its password. Because the password on the Recovery ID is tied to the key field, the Recovery ID is effectively connected to the end-user’s Active Directory account. The end-user’s Notes ID is then synchronized with Active Directory, which is passed back to Notes, signaling that the end-user should not be further prompted.

In effect, no username mapping is performed as the end-user still uses the Notes ID to access Notes. Password Power functions as a layer between Notes ID management and the end-user, providing the end-user’s Notes ID password for accessing Lotus Notes.

Password Verification Via Synchronization

The Notes ID Plug-In then verifies that the active Notes ID has the Active Directory password, synchronizing if necessary (**Step Six**). The Notes ID Plug-In still utilizes the Notes ID but serves as the gatekeeper for it by providing password synchronization between Active Directory and the Notes ID file and (optionally) the end-user's HTTP password in the Lotus Domino Directory.

Unlocking the Notes ID with Active Directory

Once the previous steps have all been accomplished, the Notes ID Plug-In sends the password back to Notes, signaling that the end-user should not be prompted further for authentication (**Step Seven**). The end-user now has access to Lotus Notes.

If the end-user forgets their Active Directory password, a simple reset of the password immediately restores access. Reset can be accomplished by the administrator or by the end-user through a separate self-service password reset Plug-In offered by PistolStar. Because the Notes ID Plug-In enables the Notes ID password to be controlled from Active Directory, password resets in Active Directory immediately reset the password stored in the end-user's Notes ID the next time the end-user launches Notes, completely eliminating the need to use the Notes password recovery process.

The Notes ID Plug-In can also optionally place an end-user's updated Notes ID and associated Recovery ID in an enterprise Notes ID repository after a username or password change, which makes it available for disaster recovery purposes, but, most importantly, eliminates the need to store end-users' Notes ID and password in the open or have a common password for all Notes IDs in the repository.

By configuring an LDAP directory as the central password authentication point, the Notes ID Plug-In also simplifies the coordination of disparate password policies such as password quality, expiration, etc.

Deployment

The Password Power Notes ID Plug-In installation is seamless and requires no changes to the LDAP/Active Directory schema. To enable browser single sign-on functionality and Domino authentication against LDAP, server-side software installation (single DLL) is required on each Domino, Lotus Sametime and/or Lotus QuickPlace server. To use Password Power's password synchronization functionality, single server-side software installation of a mail-in database is required.

The Password Power client is also installed to every workstation and laptop that requires management. To simplify installation and enable customers to deploy it automatically without end-user intervention, the Password Power client uses a fully compliant MSI — Microsoft Installer, which leverages the Windows Installer service. All Windows versions supported by Password Power already employ Windows Installer to facilitate software installs. By using an MSI package, Password Power enables customers to perform a "silent install," whereby end-users experience no interruptions in their workday and are not required to take any actions.

System Requirements

The Password Power Lotus Notes ID Plug-In supports Microsoft Windows Vista, XP, 2003 and 2000, and passwords for the following LDAP Directories: Microsoft Active Directory, Novell eDirectory, Lotus Domino LDAP, Tivoli Directory Server and Sun ONE LDAP. No changes are required to the LDAP schema.

References

PistolStar TechNote #251

“Understanding the Integration of the Notes ID Password with Third-Party Identity Management Systems”

PistolStar TechNote #254

“The Advantage of Authentication Redirection Over Password Synchronization”

PistolStar TechNote #256

“Storage, Handling and Security of End-Users’ Passwords”

PistolStar TechNote #257

“Username Mapping with Authentication Redirection”

PistolStar White Paper

“Eliminating Notes ID File Password Management: A Ground-breaking Alternative”

###