



Password Power 8 Lotus Domino Plug-In

Tech Brief



For more information:
www.cooperteam.com/uk

Password Power 8 Lotus Domino ID Plug-In

Summary

The Password Power 8 Domino Single Sign-On (SSO) Plug-In allows end-users connecting to Lotus Domino via a browser to authenticate with their network directory or LDAP password for access to all Domino Web applications as well as Microsoft Windows.

In most companies where IBM Lotus applications are employed, end-users typically have at least 3-4 separate usernames and passwords for Windows, their LDAP directory, and Lotus Domino Web applications. As a result, system administrators face a number of mundane tasks related to password management, such as resetting passwords in several places because end-users forget their passwords, synchronizing several sets of password quality rules that may or may not overlap, and creating and disabling accounts in multiple places when someone joins or leaves the organization.

The Domino SSO Plug-In removes the need for administrators to manage separate passwords for Domino Web applications by configuring LDAP as the end-user's central password authentication point. Passwords for Microsoft Active Directory, Novell eDirectory, Sun ONE LDAP, Lotus Domino LDAP, IBM Tivoli Directory Server, and OpenLDAP can be used to achieve single sign-on access to all Domino HTTP sessions, including Lotus iNotes, Sametime, QuickPlace, and Domino Web applications.

The following provides a step-by-step explanation on how the Domino SSO Plug-In works and corresponds with the steps outlined in Figure 1 on page 4.

How It Works

Authentication

With the Domino SSO Plug-In, browser-based Domino single sign-on begins at the Windows desktop, where the end-user enters their network or LDAP username and password (e.g. Microsoft Active Directory) (**Step One**). After successful authentication is achieved, Password Power's Network Provider stores the network/LDAP password, which is encrypted with the advanced encryption standard (AES). AES-encrypted passwords have a key of at least 256 bits and are used by recent versions of Password Power.

Once the end-user launches their browser (**Step Two**), the Domino SSO Plug-In loads and executes the Single Sign-On (SSO) Toolbar (**Step Three**). The Toolbar then reads the Domino Server List stored in SSO.ini, which controls which servers are accessed via single sign-on (**Step Four**).

Encrypted In-Memory Tokens

The Domino SSO Plug-In creates a token for each Domino server that contains the encrypted credentials for logging into these servers — the network username and password, the network domain, the full Lotus Notes name (optional) and a timestamp of when the cookie was created (**Step Five**). The tokens are session tokens, as opposed to being non-session or permanent tokens stored on the hard drive. They reside in the memory of the browser and are destroyed when the browser is shut down.

Copies of the token are then sent by the browser to the server for which it was created (e.g. *mail.acme.com*). Therefore, when the end-user wants to access their mail file on the Domino server, the browser presents the corresponding token to the Domino HTTP server (the network) (**Step Six**). The HTTP server receives and interprets the token using a DSAPI (Domino Server API) filter. The DSAPI filter overrides the normal authentication process and verifies the credentials provided in the token against the configured network/LDAP directory (e.g. Microsoft Active Directory) (**Step Seven**).

Username Mapping

The Domino SSO Plug-In resolves any of the issues that might arise when standardizing on a network directory/LDAP in a Domino environment. The Domino SSO Plug-In effectively handles the mapping of usernames from Windows and LDAP to Domino as well as the Domino authentication to LDAP. Password synchronization between LDAP and the Domino user accounts is also facilitated. By using the network directory/LDAP as the central password authority, the Domino SSO Plug-In also simplifies the coordination of disparate password policies.

After the Domino SSO Plug-In DSAPI filter successfully validates the network credentials, a configurable **key field** value is pulled from the end-user's network account (**Step Eight**). The key field could be the end-user's employee ID, email address, or full distinguished name. The key field name is stored in the Domino server's notes.ini file. The key field value must both exist and be unique for each end-user.

Achieving Single Sign-On to Domino via Browser

The key value (for example, *greg@acme.com*) is used to look up the Person document in the Domino Directory. The Domino view used for this lookup is also configurable. From the Person document, the full canonical Notes name is extracted and then presented to Domino with a successful return code. Single sign-on is then achieved (**Step Nine**). The end-user now has access to all their Domino Web applications after logging on just one time.

After successful authentication, the Domino server creates its own session for the end-user and provides the Domino session cookie back to the end-user's browser. Once the end-user has this Domino session cookie, the DSAPI filter is no longer called, thus leveraging the Domino HTTP cache for efficient access.

Deployment

The Password Power Domino SSO 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, a 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

What do you call it?

It is not out of the ordinary for the general population to assign different names to the same thing. Such is the case among Lotus Domino and Notes users when referring to Domino Internet. From working with our customers, we have found it is also called Domino HTTP, Domino LDAP, iNotes and perhaps other names we have not discovered yet. Each user has his/her own term for Domino Internet. So, what do you call it?

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. Examples of other typically used deployment software include Microsoft SMS, BMC Marimba, Altiris Deployment Solution and Numara Deploy.

System Requirements

The Password Power Domino SSO 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 #253

“Deploying Password Power 8 to Thousands of Clients Automatically Without End-User Intervention”

PistolStar TechNote #254

“The Advantage of Authentication Redirection Over Password Synchronization”

PistolStar TechNote #255

“Achieving Single Sign-On for Your Organization’s End-Users “

PistolStar TechNote #256

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

PistolStar TechNote #257

“Username Mapping with Authentication Redirection”

PistolStar White Paper

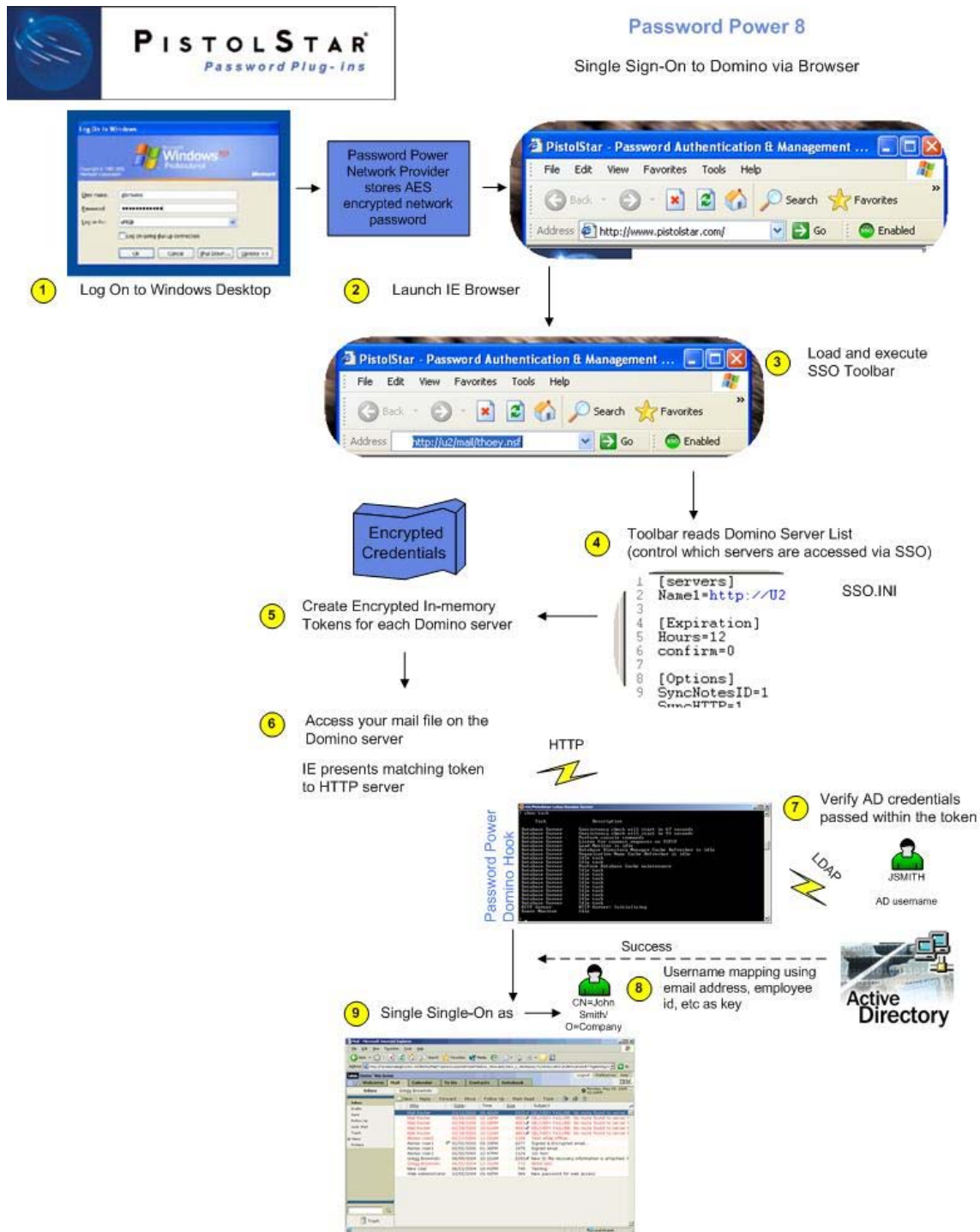
“The Realities of Single Sign-On”

PistolStar White Paper

“Using Microsoft Active Directory in the Domino World”

Figure 1 on page 4.

FIGURE 1.



Copyright 2007 PistolStar, Inc. No information contained in this document may be shared without explicit written approval from PistolStar, Inc.

###