



Password Power 8

Lotus Domino Single Sign-On Plug-In

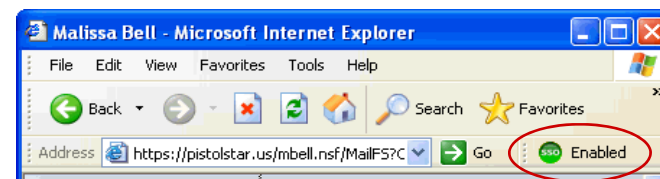
Access All Domino Web Applications Using Network Password

Browser-Based
Single Sign-On
Via
Microsoft
Active Directory

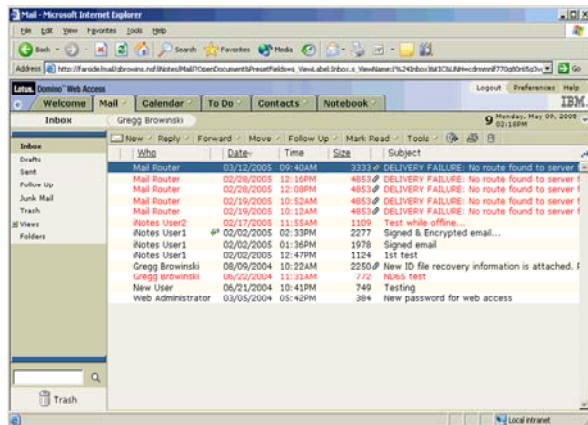
Remove Need to Manage Separate Passwords for Domino Web applications

- ◆ End mundane tasks such as resetting multiple passwords when users forget one and synchronizing several password quality rule sets
- ◆ Handle mapping of all user names
- ◆ Facilitate password synchronization between Active Directory and the Domino user accounts
- ◆ Simplify coordination of disparate password policies

Use password for Microsoft Active Directory or other network/LDAP directory for single sign-on access to all Domino HTTP sessions, including Lotus iNotes, Sametime, QuickPlace and Domino Web applications



Single Sign-On Toolbar is executed to read the Domino Server List stored in SSO.ini, which controls which servers are accessed via single sign-on.



Single sign-on is achieved once the full canonical Notes name is extracted from the Person document and presented to Domino.

One-Time Logon = Efficient Access to Multiple Applications

- ◆ Password Power Network Provider stores the AES-encrypted Active Directory password.
- ◆ Token created for each Domino server contains the encrypted credentials for logging into that server and is stored in the browser memory until browser is shut down.
- ◆ Server interprets token sent from browser by using a DSAPI filter, which overrides the normal authentication process and verifies the token's credentials against Active Directory.
- ◆ Configurable **key field** value from user's Active Directory account (e.g. user's email address) is used to look up Person document in the Domino Directory, which provides the full canonical Notes name to Domino.
- ◆ Domino server creates its own session for the user and sends the Domino session token back to the user's browser, providing single sign-on.

No Proprietary Database
Seamless Client Install – No Servers Required
No Schema Changes Required to Active Directory

