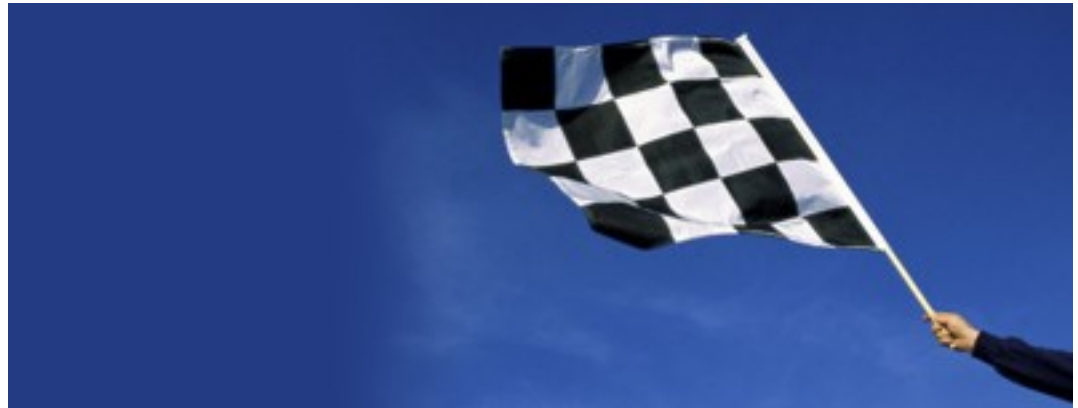


GO SSO!

**SAML SSO for
Lotus Domino**



Problem:

The password management process in most companies where IBM Lotus applications are employed can be extremely complex, as end-users typically have numerous passwords for accessing Lotus Notes and Domino HTTP sessions, as well as Microsoft Windows. Administrators are required to perform password resets in several places when an end-user forgets a password, synchronize several sets of password quality rules that may or may not overlap, and create and disable accounts in multiple places when someone joins or leaves the organization.

Solution:

Password Power integrates Domino authentication with Microsoft Active Directory and the highly secure SAML authentication protocol to enable single sign-on to all Domino HTTP sessions, including Lotus iNotes, Sametime, Quickr and Domino Web applications.

Password Power removes the need for administrators to manage separate passwords for Domino HTTP servers by enabling end-users to authenticate one time and then access additional applications or Websites without further prompting for a username and password.

The Domino SSO Plug-in is SAML Enabled:

What is SAML? Security Assertion Markup Language (SAML) is an XML-based authentication protocol which provides SSO between unrelated systems. An online Identity Provider creates a digitally signed token, which in turn leverages a single identity for access to specified systems, enabling SSO to internal applications or across the internet.

System Requirements:

- IBM Lotus Domino 6 or higher, IBM Lotus Sametime 7.5 or higher, IBM Lotus Quickr 6.5 or higher
- Microsoft Windows Server 2000, 2003 and 2008
- Internet Explorer 5.0 or higher, Mozilla Firefox 1.5 or higher

SAML FAQs:

- Can SAML eliminate the need for multiple identities? **Yes**
- Can SAML provide you with SSO across all internal applications? **Yes**
- Is SAML installed server-side only? **Yes**
- Is SAML platform neutral? **Yes**
- Does Password Power support the latest version of SAML (v.2.0)? **Yes**

Also enabled in the Domino SSO Plug-in:

- Enrollment-based
- Cross-domain
- Cookie-based
- SPNEGO-based
- NTLM-based
- Kerberos-based
- Smart Card-based
- SAML-based

Principal Features and Benefits:

- No Domino HTTP Password
- Full integration with Microsoft Active Directory
- Login prompts eliminated for Domino, Sametime and Quickr
- No passwords transmitted over the network
- No more Help Desk calls regarding lost or forgotten passwords
- Access to critical business applications is secured and simplified

Easy Deployment:

- Server-side solution
- No client-side software required
- No end-user training
- Seamless integration with Active Directory (no schema changes)

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

603.547.1200
salesteam@pistolstar.com

www.pistolstar.com