



SAML-based Single Sign-On for Lotus Domino

Tech Brief

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

Phone: 603.547.1200
Fax: 617.674.2727
E-mail: sales@pistolstar.com
Website: www.pistolstar.com

SAML-based Single Sign-on for Lotus Domino

Summary

The Password Power 8 Plug-in for Lotus Domino Single Sign-on (SSO) is SAML-enabled for all versions allowing end-users to achieve SSO to web applications both hosted by the company or any business partner. SAML SSO is one of eight options Password Power provides for achieving SSO and reducing the incidence of forgotten passwords.

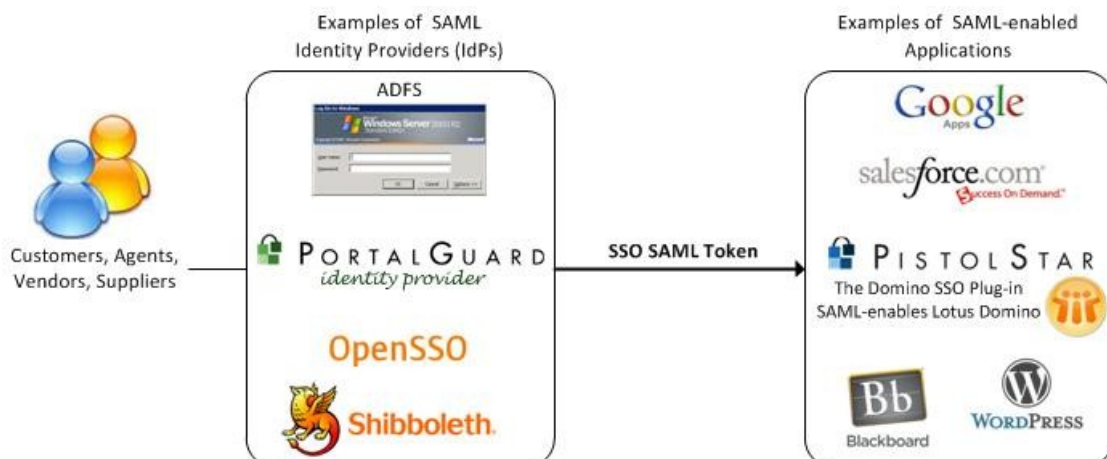
For the intranet, SSO is something that has been in high demand and supported by Password Power 8 for years, but with the emerging drive for extranet support and move to cloud services, Web-based SSO is now the focus. External users, from customers, to partners, to vendors and even suppliers, all want seamless access to hosted web-based applications while eliminating password prompts. Administrators want to utilize databases, such as SQL, that do not require licenses for external users and get out of the credential management business.

So how can a trust be established between distinct environments to allow SSO? SAML SSO with the Plug-in for Domino SSO provides a more efficient way to access hosted applications and removes the need to manage external users' credentials.

Originally developed by OASIS Security Services Technical Committee, Security Assertion Markup Language (SAML) is leading the way in providing seamless Web SSO as an open, widely implemented, industry standard protocol. SAML is an XML-based authentication protocol that passes assertions between hosted web applications. Once the end-user requests access to a hosted resource, an online identity provider creates a SAML token containing the end-user's identity assertions. Once those assertions are validated by the hosted resource the end-user is granted access without any further password prompts.

When using SAML, Web SSO can be achieved and the end-user will no longer be prompted for multiple passwords for hosted applications. As a result, administrative and IT costs associated with performing password resets in several places, synchronizing numerous sets of password quality rules that may or may not overlap and creating and disabling accounts will be greatly reduced.

To provide federated access to specified environments, a trust can easily be established between the organization and its suppliers, customers, vendors, etc. A positive impact can be realized by increasing usability for these business partners and displaying a concern for their requirements and desire for seamless access.



The following provides a step-by-step explanation on how SAML SSO with the Password Power Plug-in for Domino SSO works and corresponds with the steps outlined in Figure 1.1 and 1.2 on pages 4 and 5.

How it Works

HTTP Post Binding Method (Figure 1)

(Step 1) The end-user clicks on a Domino link requesting a protected resource. Their request is redirected to the Identity Provider (IdP). *(Step 2)* The IdP ensures the user has authenticated with it, then builds a SAML token containing identity assertions for the user.

(Step 3) An HTML response is then sent from the IdP to the end-user. It contains a form with the encoded SAML token and original Domino URL as encoded data fields. The form is typically coded to auto-submit to the Domino server. *(Step 4)* The HTML form, containing the SAML token, is POSTed to the Domino server. *(Step 5)* The Domino plug-in parses out the SAML token, verifies its digital signature and extracts the identity assertions/claims.

(Step 6) Optionally, the claims from the SAML token are used to look up the username in the Domino Directory and find their Person Document. *(Step 7)* The Domino plug-in then returns the user's authenticated name to the Domino HTTP server and suppresses any authentication attempts by Domino itself. *(Step 8)* The user now receives a Domino session for the remainder of their browser session (e.g. LTPA token).

Artifact-based Authentication (Figure 2)

(Step 1) The end-user clicks on a Domino link requesting a protected resource. *(Step 2)* Their request is redirected to the IdP. The redirect contains an artifact/identifier generated by the Domino plug-in which represents a SAML request.

(Step 3) The IdP contacts the Domino server directly and, through an <ArtifactResolve> message, requests the actual SAML request generated by the Domino plug-in. *(Step 4)* Via an <ArtifactResponse> message, the Domino plug-in sends back its SAML request. *(Step 5)* The IdP ensures the user has authenticated with it, generates a SAML response containing identity assertions for the user and redirects the user's browser back to Domino. The redirect contains the IdP's own artifact/reference which represents its SAML response.

(Step 6) Domino sends an <ArtifactResolve> message directly to the IdP, requesting the SAML response for the end-user. *(Step 7)* The IdP responds with an <ArtifactResponse> message containing the SAML token for the end-user.

(Step 8) Optionally, claims from the SAML token are used to look up the username in the Domino Directory and find their Person Document. *(Step 9)* The Domino plug-in then returns the user's authenticated name to the Domino HTTP server and suppresses any authentication attempts by Domino itself. *(Step 10)* The user now receives a Domino session for the remainder of their browser session (e.g. LTPA token).

Deployment

Implementation of Password Power SAML SSO for Domino is seamless and requires no changes to Active Directory/LDAP schema. A server-side software installation (single DLL implemented as a DSAPI filter) is required on each Domino server for which SSO via SAML is desired. Notes.ini variables control how the Plug-in operates and any logging goes directly to the Domino server console/log.nsf. The HTTP task only needs to be restarted to put the changes into effect.

Additional client-side software is not required. All major Web browsers, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari, are capable of performing SAML authentication to Web servers.

System Requirements

The Password Power Plug-in for Domino is a server-side solution which supports Lotus Domino R6/7/8/8.5.x on 32 or 64-bit versions of Microsoft Windows Server 2003, 2008 and 2008 R2.

SAML Identity Provider Options

Active Directory Federation Services (ADFS) 2.0

ADFS 2.0 maintains security while allowing end-users to access applications inside and outside organizational boundaries, such as cloud-based applications. IT staff can now enable SSO for the end-user without requiring a separate set of credentials.

Information:

<http://www.microsoft.com/windowsserver2008/en/us/ad-fs-2-overview.aspx>

Downloads:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=118c3588-9070-426a-b655-6cec0a92c10b&displaylang=en>

Oracle OpenSSO

The Open Web SSO Project (OpenSSO) provides SSO as a form of security within a network that provides a foundation for access to applications, which are based on disparate identity repositories. OpenSSO is based on Sun Java™ System Access Manager offered by Sun Microsystems.

Information:

<http://opensso.dev.java.net>

Downloads:

<http://opensso.dev.java.net/public/use/index.html>

References

OASIS SAML Executive Overview

<http://www.pistolstar.com/Executive>

OASIS SAML Technical Overview

<http://www.pistolstar.com/Technical>

Figure 1

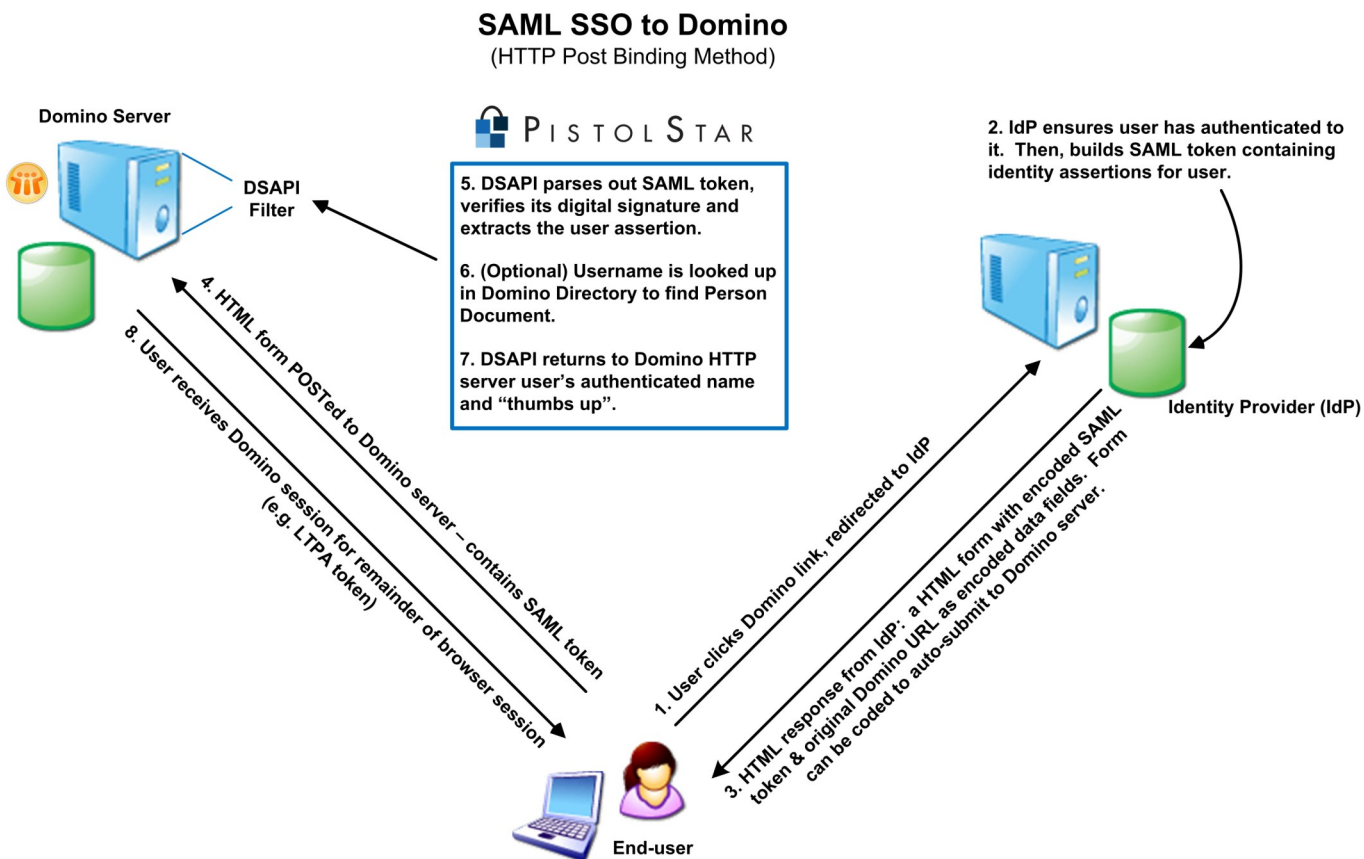


Figure 2 on Next Page

Figure 2

PISTOL STAR SAML SSO to Domino (HTTP Artifact Binding)

SAML Requestor

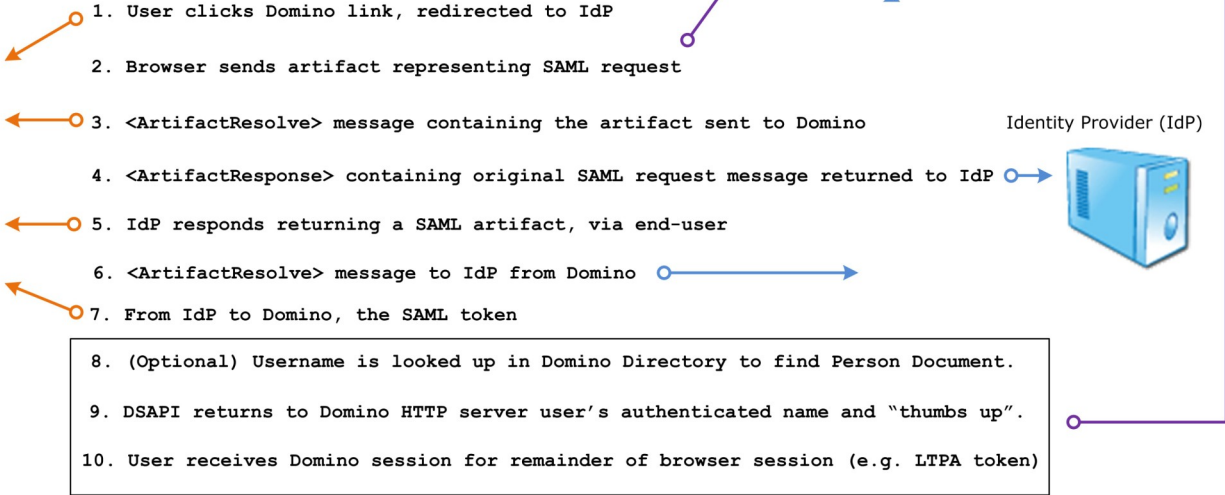
User Agent

End-user

SAML Responder

Domino Server
DSAPI Filter

Identity Provider (IdP)



###