



Password Power 8 Plug-In for Lotus Domino Single Sign-On via Kerberos

Tech Brief

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

Phone: 603.547.1200
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

Password Power 8 Lotus Domino SSO via Kerberos Plug-In

Summary

The Password Power 8 Plug-In for Lotus Domino Single Sign-On (SSO) via Kerberos allows end-users connecting to Domino to achieve SSO to all Domino HTTP servers using the Kerberos authentication protocol*. Kerberos is one of three options Password Power now provides for achieving SSO to Domino HTTP, the other options being proprietary SSO tokens and via login to a portal such as Microsoft SharePoint.

End-users in most companies where IBM Lotus applications are employed typically have numerous password prompts, including those for accessing Microsoft Windows and Domino HTTP sessions (i.e. Lotus Domino Web Access (“iNotes”), Sametime, Quickr (QuickPlace), and Domino Web applications). As a result, the password management process for administrators becomes extremely complex, requiring them to perform password resets in several places when end-users forget their passwords, synchronize numerous 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.

The Plug-In for Domino SSO via Kerberos removes the need for administrators to manage separate passwords for Domino HTTP servers by making it possible for end-users to authenticate one time and then access additional applications or Websites without further prompting for a username and password.

Originally developed at and used by the Massachusetts Institute of Technology (MIT), Kerberos has become the foundation for authentication in Windows operating systems since Microsoft implemented it as the default authentication mechanism in Windows 2000. Kerberos requires connectivity to a central Key Distribution Center (KDC), which, in Windows, is any Microsoft Active Directory domain controller. End-users authenticate to the KDC, requesting encrypted *service tickets* for the specific service they wish to use (e.g. Web servers). Only the service and the KDC can decrypt the service ticket to get the end-user’s authentication information. The service trusts the credentials in the service ticket because it knows the ticket could only be created by the KDC and thus recognizes the end-user must have been authenticated by the KDC in order to receive the ticket.

Using Kerberos authentication, there are no passwords sent over the network and the end-user and server are mutually authenticated, preventing server attacks and malicious programs that try to impersonate the server to get the end-user’s private information. Kerberos authentication also enables end-users on Windows 2000, XP and Vista to just logon to a Windows domain at the start of their workday, as it provides further integration with Windows and Active Directory. Therefore, when the end-user wants to access a server for which they use Kerberos authentication, their browser retrieves the service ticket from the KDC and sends it to the server automatically.

The following provides a step-by-step explanation on how the Plug-In for Domino SSO via Kerberos works and corresponds with the steps outlined in Figure 1 on page 5.

How It Works

Authentication: Requesting a Resource

With the Plug-In for Domino SSO via Kerberos, the end-user begins Domino single sign-on by launching a browser from their client desktop and requesting a resource from the Domino server named mail.ad.pistolstar.com (**Step One**). The Password Power Domino Server API (DSAPI) filter on the Domino server sends a response to the browser that the end-user is not yet authorized and needs to be authenticated with the “Negotiate” protocol (**Step Two**).

Encrypted Service Ticket

The browser then interfaces with the security subsystem on the client machine to request a Kerberos service ticket for the Domino server (e.g. `HTTP\mail.ad.pistolstar.com`) from the Active Directory domain controller, which is acting as the KDC (**Step Three**). The KDC responds with a service ticket after validating the end-user’s credentials (done automatically if the user has logged in with an Active Directory domain account), looking up the end-user’s account with the requested service name and encrypting the ticket using the service account’s credentials (**Step Four**).

Service Tickets Validated

With the service ticket in its possession, the browser makes another request for the resource from the Domino Server (**Step Five**). The DSAPI filter parses out the service ticket and attempts to validate it. If successful, the end-user’s Kerberos (Active Directory) name is extracted from the ticket (e.g. jsmith@ad.pistolstar.com) (**Step Six**). Another option for this step is to use the Kerberos name in full or in part to lookup the end-user’s full hierarchical name in the Domino Directory (**Step Seven**).

Single Sign-On to Domino Achieved via Kerberos

The DSAPI filter then signals Domino that the end-user has been authenticated successfully, sending it the end-user’s authenticated name (**Step Eight**). Domino thus provides the end-user with access to the requested resource, along with a HTTP session token (e.g. Domino LTPA token), which is set in the end-user’s browser. The session token allows the end-user to avoid repeated or full Kerberos authentication while they are using the Domino HTTP cache, which dramatically increases the server’s response time (**Step Nine**).

Deployment

Installation of the Password Power Plug-In for Domino SSO via Kerberos is seamless and requires no changes to the Active Directory/LDAP schema. A server-side software installation (single DLL implemented as a DSAPI filter) is required on each Domino, Lotus Sametime and/or Lotus Quickr server for which browser single sign-on functionality via Kerberos 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 (i.e. the Password Power Web SSO Plug-In) is not required as Internet Explorer and Mozilla Firefox have built-in support for Kerberos authentication to Web browsers. However, some minor modifications to the browser settings may be necessary on the client machines to enable Kerberos/Negotiate authentication.

System Requirements

The Password Power Plug-In for Domino is a server-side solution and supports Microsoft Windows XP and Vista client machines, Windows 2003 and 2008 Active Directory as KDC (MIT KDC not supported), and Lotus Domino R6/7/8/8.5 on Windows and AIX. Internet Explorer 5.0 or higher or Mozilla Firefox 1.5 or higher are required. End-users must log in using their Active Directory domain account. Machines on which Domino is running must be joined to the Active Directory domain and Domino should run as a service.

References

PistolStar TechNote #253

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

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”

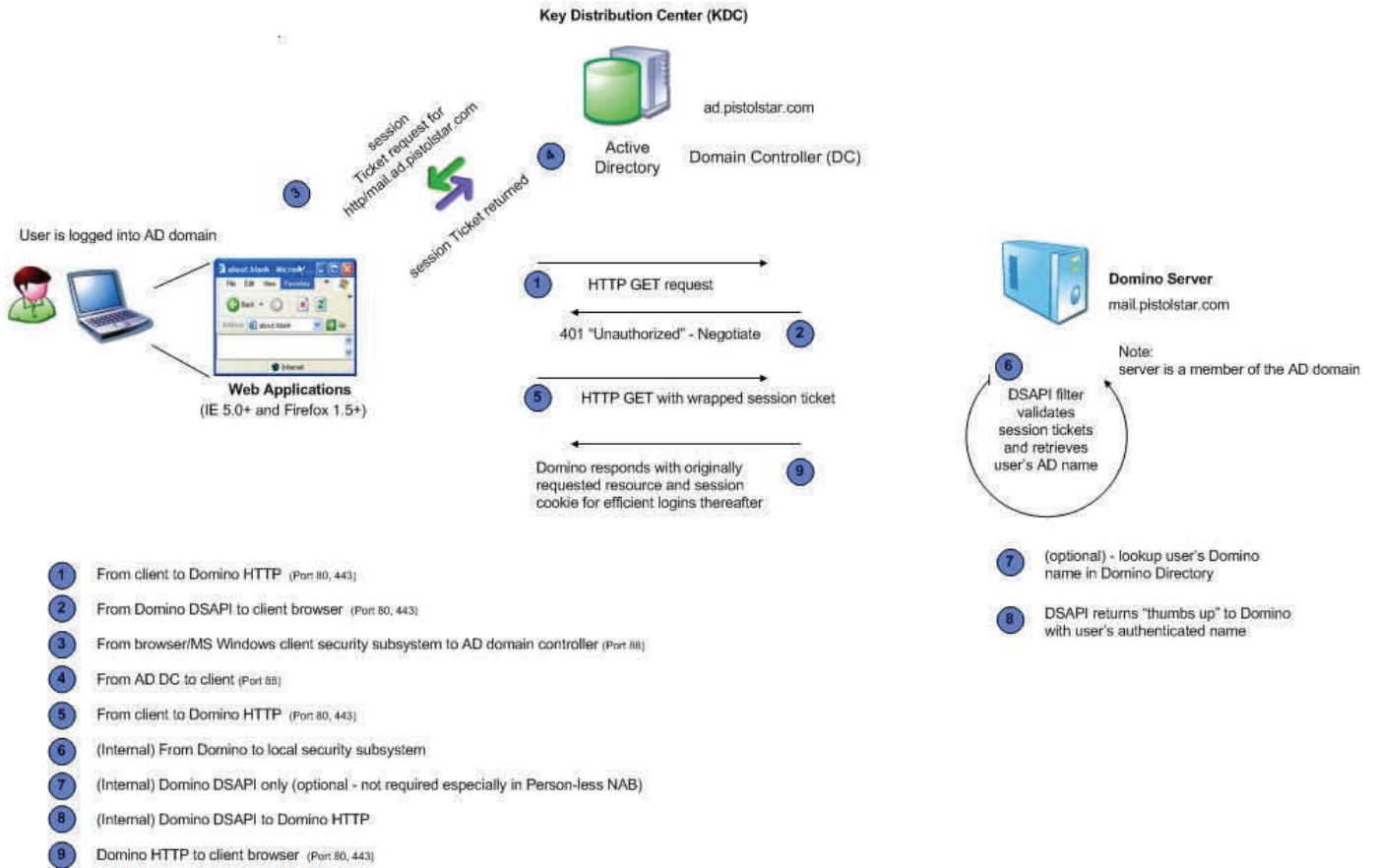
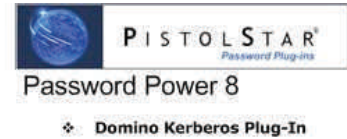
PistolStar White Paper

“Myths & Realities of Lotus Notes and Domino 8.5 Security”

Figure 1 on next page.

Figure 1.

Kerberos SSO to Domino HTTP



*Kerberos is a network authentication protocol that is designed to provide strong authentication to client/server applications by using secret-key cryptography. For a free implementation of the protocol and more information, go to http://web.mit.edu/Kerberos/#what_is

###