Software

Moving Single Sign-on (SSO) Beyond Convenience

Written by Todd Peterson, IAM evangelist, Dell Software

Introduction

For years, single sign-on (SSO) has been the poster child for identity and access management (IAM). Giving people the most convenient possible access to what they need is highly visible, yields measurable results, and is easy for everyone to understand. We all know that there are IAM requirements that are critical, which can't be solved through SSO – access governance, provisioning and privileged account management to name just a few. SSO is so visible for a reason; it's right in front of you.

Things are constantly changing. The growing complexity and diversity of the environment and the rigidity "traditional" IAM solutions introduce are the high-level challenges facing every organization's IAM program. Unfortunately IAM solutions are usually designed for a point-in-time and static state environment. SSO is no different. Yesterday's SSO solution may not address today's—or tomorrow's—access needs.

This brief white paper will discuss the objectives and benefits of SSO and how evolving application environments—including software as a service (SaaS) and cloud-delivered applications—demand a flexible and comprehensive approach to user access.

SSO: a primer

Single sign-on has been around a long time. What a vendor or integrator defines as SSO can vary widely. SSO falls into the following general categories:

- **Password synchronization (or same sign-on)** – Putting technology in place to ensure that all passwords everywhere are the same. This approach requires individual logins to each application or system a user needs to access but ensures that the password entered each time is the same regardless of the system being accessed.
- **Password replay (sometimes called enterprise SSO or form-fill)** – Putting technology in place that securely stores passwords across the range of systems and applications to be accessed, and fills in the password for the user under the covers when access is requested.

The right approach is to select an SSO strategy and technology that addresses the broadest range of access needs in the best way for each.

- **True SSO** – Creating an environment where a single login and the credential created with that login can be extended to additional systems and applications. Active Directory (AD) bridge technologies are classic examples of true SSO, as they enable an AD credential to be used to authenticated Unix, Linux, and Mac OS systems as well as applications, such as SAP, that are equipped to accept AD credentials. Microsoft has created an environment optimized for true SSO for applications such as SharePoint and Office 365.
- **Federation** – trusting the authentication request from an entity that is outside of the control of the organization hosting the application or data. Federation can be implemented internally (for example across domains or lines of business) or externally (for example to a partner or third-party service provider).
- **Web SSO** – technologies that provide a single login (could be same sign-on, true SSO, federated, password replay or any combination) for applications that are accessed via the web regardless of the hosting environment (internally owned and controlled, accessed in a federated approach, SaaS, etc.)

No one approach is ideal for all access needs. Consequently many organization adopt a blended approach to SSO with a variety of solutions, whichever is best for each access need, or deciding on the most important access needs and limiting SSO to just the solution ideal for those needs.

Access in today's world

Today's organization typically has a highly diverse user population—users that are solely on premises, users that are entirely remote, users that are accessing applications both on premises and remotely, and partners and customers that require access and are entirely outside of IT's control. In addition, the mix of applications being accessed is evolving. Where previously all applications were internally owned and hosted, today's application mix includes commercial off-the-shelf applications accessed both through fat clients as well as through more modern browser-based methods, including internally developed applications and applications that are entirely outside of the control of IT such as Salesforce.com, Google Apps, Office 365 and other SaaS applications.

With this expanding web of access needs, application types and accessing parties, a few underlying IAM principles remain constant:

- The organization needs the assurance that access is appropriate regardless of who is accessing the resources or how they are doing it.
- The organization needs to grant access efficiently via automation or streamlined processes, relieving IT of as much of the user-access burden as possible.
- The organization needs to preserve end-user satisfaction by making access easy and intuitive.
- The organization needs to know that technologies implemented today to achieve the above do not place a barrier in the path to tomorrow's user populations and access and security needs.

As more and more applications move to web-based access methods, the need for a unified SSO approach that covers all the browser-based options is becoming increasingly critical but even harder to achieve. Newer web-based access scenarios often require unique support depending on the application being accessed. Consequently addressing the "access need of the day" may result in one type of solution for one type of application and an entirely different solution for the next.

But there is a better way. Rather than choosing solutions in silos depending on what needs to be accessed and in what manner, the right approach is to select an SSO strategy and technology that addresses the broadest range of access needs in the best way for each without requiring settling for the "lowest common denominator," which sacrifices security and control in the interest of convenience. In other words, the wisest approach is to implement the most secure access possible for each application but all contained in the same solution, an approach that seems to be counter to the traditional way many have learned to approach single sign-on.

The wide world of web-based access

Web applications are multiplying and users expect access to these apps to become as mobile as they are. The options for achieving secure and convenient access are growing as well.

There is no single standard that exists across all web applications that can be leveraged to unify access and security. However there are a few approaches that can create the single, secure access strategy.

The following table represents the common authentication/access methods used by different types of web applications:

Application type	Authentication/login type
Commercial off-the-shelf applications with a web frontend	**Username/password**. Typically commercial off-the-shelf applications require use of the login method built into the application itself. The most secure approach to create SSO for these types of applications is to implement a form-fill solution that securely stores credentials and automates the login process. **SAML**. Other commercial off-the-shelf applications are equipped to accept SAML tokens for authentication. Because SAML is a more secure login method than form fill, SSO for these applications should leverage the more secure option. **WS Federation**. Yet other applications can authenticate via the WS Federation protocol for a login experience called Windows Integrated Authentication that closely mirrors the "true" SSO available for the Windows environment. Again, the ideal SSO solution will leverage the most secure method possible for these types of applications.
Home-grown web applications for employees	**HTTP header**. The vast majority of home-grown web applications for internal use are developed with an HTTP header as the login source. In order to create SSO for these types of applications, the ability to support HTTP headers is mandatory.
SharePoint	**Federation**. Regardless of the type of authentication built into applications meant to be accessed by third parties outside of the direct control of an organization, the need to provide federated access is paramount. The correct SSO solution for these types of applications should include the ability to act as both an Identity Provider (IdP), the entity providing the trusted identity, and as a Service Provider (SP), the entity consuming the trusted identity from an IdP.
Office 365	**WS Federation/Trust**. As a Microsoft offering, Office 365 uses the same authentication standards as SharePoint and is ideally treated when that standard is leveraged and optimized.
Salesforce.com and Google Apps	**SAML**. The most popular SaaS applications are also equipped to accept SAML tokens and the correct SSO choice for them would leverage SAML over less-secure options.
Other SaaS applications	**SAML**. Many SaaS applications accept SAML tokens and, making the ideal SSO choice obvious. **Username/password**. Other SaaS applications use other non-standard login methods. Similar to many commercial off-the-shelf applications, SSO for these types of applications is best achieved through form-fill scenario. Surprisingly, the majority of cloud and SaaS apps still opt for built-in security versus leveraging federation.

There are a few approaches that can create the single, secure access strategy.

The best option is to implement an SSO solution that provides all the Options. Only with this unified approach is convenience maximized right along with security and control.

The delicate balance between security and convenience becomes painfully obvious when one looks at the variety of ways that access can be achieved. Form-fill SSO works across pretty much every application type listed above, however it is not the best choice for everything. If an application can leverage SAML, it should be used. But implementing a SAML-only solution leaves applications that cannot leverage SAML out in the cold. Similarly, implementing a solution designed for only Windows Integrated Authentication (WS Federation/Trust) is ideal for SharePoint, Office 365 and the applications designed for that method, but does nothing for the rest of the web application world. And as soon as federation expands beyond the Microsoft-centric application world, additional solutions are required.

The best option is to implement an SSO solution that provides all the options listed above—form fill, HTTP headers, SAML, WS Federation/Trust, as well as federation as an IdP and as an SP. Only with this unified approach is convenience maximized right along with security and control.

What about remote users?

It is rare in today's world for all users in an organization to operate exclusively on premises, requiring access only from a desktop computer in the office. The explosion of mobility has created a world where users require access to their everyday applications from anywhere, and increasingly from whatever device they happen to have handy—corporate-owned and controlled laptops, borrowed or public computers, and a host of mobile devices such as cell phones and tablets. Yet this boon to productivity can be the bane of security. Along with the focus on ensuring that users—regardless of location and device—can get to the right applications when they need them, there is a vital requirement to ensure that only the right people are accessing those systems, and that they are only getting to what they are authorized to access.

The same trap exists for ensuring appropriate remote access that acts as an impediment to convenient access—namely the diversity of options can result in a disjointed mix of solutions and strategies. The right SSO solution for access to web applications will also take into account the idiosyncrasies of remote access and the enhanced security practices it demands. Along with a unified login experience that spans the widest range of options, the solution should also provide the security and control necessary to ensure appropriate access for remote and mobile users across the same wide range of application types. Leveraging role-based access control, the solution would present users with a consolidated view of the applications they are entitled to access, protected in a proxy scenario and accessed via any browser.

But wait, I want more than just SSO!

While SSO is the primary objective discussed in this document there are a number of additional capabilities that, if combined with the SSO solution, can further the journey from simply providing convenient access to enhanced security and ultimately business agility. Examples of additional benefits include:

- Access control – while SSO is inherently an "access control" solution, the opportunity exists for the SSO solution to deliver enhanced access controls through role and rule-based approach that draws upon existing identity data and security policy in real time. In addition, the granularity of that access control can be expanded beyond the capabilities of simple SSO only.

- **Cloud-access provisioning** – combining the SSO functions with the ability to provision access further streamlines operations and enhances the value achieved through SSO itself.
- **Access auditing** – beyond being an access "portal" a good, comprehensive and universal SSO solution for web applications should also provide the ability to audit and report on the access events it enables.
- **Strong authentication** – many organizations require a deeper level of assurance of a user's identity when logging in remotely or to specified applications. The right SSO solution for web applications will easily plug into advanced authentication technologies such as multi-factor authentication through a one-time password (OTP) token.
- **Governance** – finally as security and compliance are the ultimate objective, any unified SSO solution for web applications should include the ability to plug into and be managed by an identity and access governance framework.

The Dell One Identity approach to SSO for web applications

The Dell One Identity family of IAM solutions enables organizations to achieve easier accountability and greater transparency by placing the business in control of those things that matter most. Dell One Identity solutions address the most pressing needs through:

- A broad, modular and integrated IAM portfolio
- Simpler solutions with rapid time to value
- Granular enforcement with enterprise business value

This approach holds doubly true for single sign-on to web applications.

Dell One Identity Cloud Access Manager meets users' needs for browser-based access to internal resources and cloud-based web applications while simultaneously enhancing security and IT efficiency. Beyond just SSO, Cloud Access Manager also provides just-in-time cloud provisioning, federation, authorization and auditing, for a wide array of application types and access scenarios.

Cloud Access Manager covers the entire range of application access types described in this paper including HTTP header, WS Federation/Trust, SAML, form fill, and federation as both an IdP and SP. Key capabilities of the solution include:

- **Centralized authentication, SSO and attribute retrieval** – connect multiple user directories and applications into a centralized authentication "hub" that enables a single login event (and password) to create a session spanning multiple web applications, hosted locally or by software-as-a-service (SaaS) vendors. Using a robust, rules-based engine, Cloud Access Manager can deliver additional data about users to protected applications, for personalization or fine-grained access control.
- **Policy-based access control** – ensure that users can access only the resources they are authorized to use, based on IT-defined user roles. Roles and role membership can be assigned dynamically based on policies evaluated in real time, using existing identity data. Rules-based access control can be applied down to sub-regions of a web application, for enabling more granular authorization.
- **Identity federation** – enable access scenarios that span security boundaries (cloud-based applications, multi-forest collaboration, heterogeneous platforms, partner extranets, etc.) without the need for redundant user passwords. With federation support in both Identity Provider and Service Provider roles, Cloud Access Manager easily facilitates user access to web applications, regardless of where the users and/or the apps are located.

Dell One Identity Cloud Access Manager meets users' needs for browser-based access to internal resources and cloud-based web applications while simultaneously enhancing security and IT efficiency.

- **Cloud access provisioning** – for federated SSO to cloud applications such as Salesforce.com, Google Apps or Office 365 to work, user accounts have to be provisioned at the cloud application. Cloud Access Manger centralizes access provisioning and SSO functions into a single tool, for greater IT efficiency. Just-in-time provisioning saves money by activating licenses only when access is actually used.
- **Workspace aggregation and remote access** – the Cloud Access Manager Application Portal simplifies how users find all the applications they need to get work done. Users find an easy-to-read, role-based collection of links to the applications to which they are entitled. Through the Cloud Access Manager proxy, users can access any application from any location via a web browser,
- **Access auditing** – Cloud Access Manager enables security professionals to leverage its role as a centralized authentication and access control solution for auditing and reporting on access events for compliance, repudiation and forensics purposes.

To see Cloud Access Manager for yourself and learn more about the Dell One Identity family of IAM solutions visit software.dell.com/products/cloud-access-manager.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL’S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.