No more passwords:
time to solve the proliferation of username/password

Contents

ebook

technology Decisions

IT leadership & innovation

www.technologydecisions.com.au

From the editor ...

Welcome to this special *Technology Decisions* eBook on Single Sign On (SSO) and password security.

It seems hardly a month goes by where we aren't shocked by media reports of substantial security breaches and data theft somewhere in the world, often affecting some of the biggest company names on the planet. There are many reasons why hackers are able to gain access to those companies' systems, but poor password security is often a factor.

With staff typically having access to many different IT systems via a variety of devices, both company supplied and personal, keeping on top of multiple passwords and permissions can be both a nightmare logistically and a nightmare from a security perspective.

But in addition to the security considerations, there are also efficiency and productivity concerns. The time taken to accomplish multiple, separate log-ins and the time taken for IT staff to resolve lost, stolen and forgotten passwords is not trivial. It can add up to substantial loss of productivity and therefore dollars.

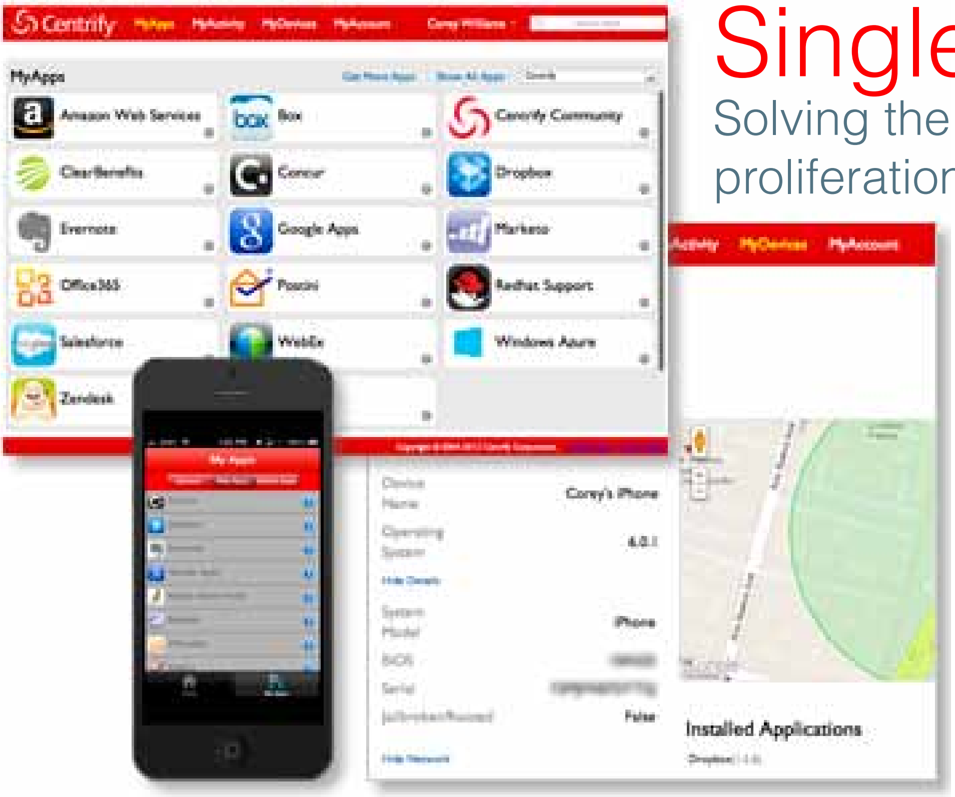
Fortunately, there are options to resolve these issues. Single Sign On and password management systems offer effective and secure ways to overcome the security and productivity concerns, boosting business resilience and efficiency.

The articles in this eBook will give you a comprehensive understanding of the pros and cons of SSO systems and password managers, helping you to make the right decisions about the best courses of action to take for your organisation.

IT security concerns us all, both personally and professionally, and it is incumbent on technology decision-makers within all organisations to ensure that their systems and the data they hold are protected by robust, reliable and accountable security strategies. SSO and password management are vital ingredients in those strategies.

Jonathan Nally
Editor
Technology Decisions

ebook
technology Decisions
IT leadership & innovation
www.technologydecisions.com.au



Single Sign On

Solving the password proliferation problem

Stephen Withers

Having multiple passwords combined with numerous redundant sign-on processes poses both a security risk and a productivity loss for business. A single sign on system is the answer.

The use of cloud-based applications such as Salesforce CRM, Concur travel and expense management and WebEx conferencing has become commonplace in many organisations. Requiring employees to sign on individually to each system they use presents several problems, all of which are avoided by using single sign on (SSO).

Efficiency and convenience

Having to repeatedly sign on to various systems is irritating at best, and can be downright frustrating as it gets between people and their work. Imagine how much more convenient it would be if signing on to a computer or other device automatically gave you access to all the systems you were entitled to use.

That should also reduce the number of password resets required, as users only need to remember one password at a time. While many organisations have automated that function to take the load from helpdesk staff, the productivity impact on users is not merely the time it takes to perform the reset itself - the interruption to the flow of work causes a loss of focus, and it can take longer to pick up the thread again than it did to reset the password.

In addition, the more convenient it is to use officially sanctioned applications (eg, because they come under the SSO umbrella), the less likely people are to use unapproved software in an attempt to complete tasks more easily.

Security

The more times during a day that someone needs to enter a password, the more likely they are to pick one that's as simple as possible to type. But unless they are inclined towards security, they'll typically select one that barely meets the mandatory minimum length, and that requires as little use of the shift key as possible.

They will often use that same password on different systems as most of us find it impractical to remember more than a handful of passwords (password management software can be useful - see Is a password manager right for you?), so an intruder who is able to determine a person's credentials in one place (eg, via the recent Heartbleed vulnerability) will try using them in others.

But if the point of SSO is that you use one username and password, doesn't that mean it suffers from the same drawback? On the face of it, once you've discovered a user's credentials you can get into all the connected systems. The difference is that with SSO those credentials aren't stored on all of those systems. Rather, the SSO system testifies to all the others about the user's identity. But there is an element of putting all the eggs into one basket, so it is important to ensure that the SSO system is a stronger basket.

Another side to this issue is that SSO reduces the opportunity to steal passwords. SAML (Security Assertion Markup Language) based approaches mean that passwords do not travel between systems, so passwords cannot be 'sniffed' locally or remotely as they traverse networks, and there is nothing to steal from the remote systems.

The centralised nature of SSO provides an opportunity to implement two-factor authentication in a context-sensitive way. You might decide, for example, that the password alone is sufficient for login attempts originating from organisation-owned devices that are on the premises, that the second factor is mandatory when logging in from outside Australia and required intermittently for locations inside our borders.

Identity

Why do we sign on to systems? It's basically a way of establishing who we are. Not absolute proof of identity, admittedly, as people have been known to walk away from computers without signing out, to peek when their colleagues are typing their passwords or to deliberately share credentials including devices used for two-factor authentication.

Most organisations of any size already have a mechanism based on Active Directory or LDAP for controlling access to particular systems according to a person's job. Depending on the organisation, all employees may need an email account and limited access to the HR system so they can lodge holiday requests. Managers will need a higher level of access to the HR system to approve or reject those requests, and probably to the ERP system to keep tabs on any expenditure for which they are held responsible.

An SSO should interoperate with these identity and provisioning systems to minimise the administrative effort required, so that access to cloud-based systems is controlled in the same way as it is for internal systems.

In addition to simplifying things when a person joins or leaves the organisation or has a change of responsibilities, integration between an SSO system and Active Directory (or similar) makes it easier to demonstrate compliance with policies concerning access rights.

So why isn't selecting an SSO system simple?

Universality

It might sound obvious, but you only want one SSO system in your organisation, otherwise it's going to cost you more, be harder to manage and probably won't deliver the full benefits to users.

It is usually important that the system handles cloud (SaaS) and on-premises applications, and also mobile apps, so make sure the SSO system you are considering provides broad support. In particular, if you are using any SaaS applications that require the entry of a username and password via a web form, ask potential SSO providers whether they offer a mechanism to securely store or access these credentials for delivery as required to such programs.

On the mobile side, SSO is often handled by an app that automatically handles sign-on to web applications. Some device vendors provide an API that makes it easy for developers to support SSO in their apps.

Mobility

Apart from the mobile-related issues discussed above under universality, there's a particular issue around mobility in that SSO intersects with mobile device management (MDM).

One of the basic tasks of an MDM system is to provision certificates such as those required for Wi-Fi or VPN access. Mobile SSO also requires certificates, so it is important an SSO system can leave provisioning them to whichever MDM system is in use or handle the job itself where necessary. Having this capability also opens the door to using what is primarily an SSO system as your MDM tool, if the system provides the additional features either as a standard part of the product or as one or more optional extras.

Broad support

BYOD has largely been the rule as far as smartphones are concerned (depending on your industry, the idea of a company-issued phone might be completely alien), and in many occupations there is a growing expectation that some out-of-hours work will be involved. So an SSO system should work on any operating system staff are likely to use - at a minimum, Windows, OS X, iOS and Android, and in some segments support for Linux might be expected.

> *SSO means your employees don't need to remember multiple passwords and aren't required to log in each time they use a different system or application.*

Security

If an SSO system unnecessarily duplicates the functions of an existing Active Directory or similar infrastructure, it increases the attack surface whether the additional server is on premises or in the cloud. Ensuring that the SSO system obtains the information from Active Directory (and so on) as and when it is needed provides better security, a simplified architecture and lower cost.

Policy

What happens when you don't use Active Directory or similar (eg, a relatively young organisation may have made a deliberate decision to go 'all cloud', completely avoiding all on-premises servers) or you need to manage users who are excluded from Active Directory (eg, contractors)? In such situations it is a big advantage if the SSO system incorporates its own facilities for defining and applying policies.

Administration

Close integration with Active Directory can also make life simpler for administrators. Since the right to access a particular resource (eg, an application) is determined by the security group(s) the user belongs to, administrators are starting off in familiar territory. The benefits of that familiarity can be maximised if the SSO system provides plugins so that administrators can control some or all of its functions from within Active Directory tools.

And if those familiar tools can be used to manage all of the computers and mobile devices present within the organisation, regardless of their operating systems, the complexity of the administrative environment is reduced. Less complexity means less training and fewer errors.

Summary

SSO means your employees don't need to remember multiple passwords and aren't required to log in each time they use a different system or application. The organisation benefits from improved security, better auditability, simplified onboarding and offboarding, and increased productivity.

But not all SSO systems are created equal. Before adopting a particular system, make sure that it covers all the functional bases (eg, support for mobile apps as well as browser-based access from PCs and support for the platforms used or likely to be used within the organisation), works alongside existing systems such as Active Directory and MDM, avoids unnecessary duplication of security-critical data and - to the extent possible - provides administrators with familiar tools.

Is a password manager right for you?

Dylan Bushell-Embling

Organisations need to weigh up all the pros and cons of password managers to decide if they meet their needs, or whether SSO is a better option.

Passwords have frustrated enterprise security experts for many years. Despite repeated warnings, too many users have the same password across multiple applications and websites. With best-practice guidelines also stipulating the use of complex passwords with a mixture of character types, it's hard to blame them, as the average human brain can struggle to store multiple strong passwords at once.

The security of a password-based login system hinges entirely on the strength of the password used. Besides repeating passwords, end users often use simple passwords that are easily guessable. Or they will leave their passwords where others can find and read them, for example on sticky notes near their computer.

Password managers are an attempt to solve this problem. Password managers can take many forms, but in essence they are designed to serve as a database to store and organise passwords and other codes.

Password managers can come as desktop software, mobile applications, web-based services or over the cloud. Some come in the form of USB sticks that can be used on any computer. They are typically designed to automatically generate strong passwords when a new database entry is created.

From an end-user perspective, the most immediate advantage of the password manager is the need to remember only one strong password. They can still use different, effective passwords across every application and website that needs one.

In addition to storing passwords, many password managers on the market can act as a form-filler and serve as a protection against phishing by comparing the URL of the current site against the URL of the currently accessed site.

Password managers can also act as a protection against keylogging, as by using automated form entry or by copying and pasting the password, the user never need type in the password.

Beware the drawbacks

But there are also weaknesses inherent to password managers, the most obvious being that from a single point of intrusion, hackers can potentially gain access to a user's entire password library.

Some desktop password managers store their databases in an unencrypted form, meaning anybody gaining physical access to a computer can access and read them. Some use a master password to lock up the database, but the effectiveness of this approach then hinges on the strength of the master key.

Another consideration is the method the password manager uses to automatically generate the passwords. If the password manager users a weak random number generator, the password could potentially be guessed using brute force methods.

These weaknesses can be addressed using other technologies including two-factor authentication, advanced encryption techniques and security failsafes - such as a password manager that locks up after an incorrect master password is entered a certain number of times.

For enterprises, password managers can serve as an alternative to single sign on (SSO) systems. SSO systems typically use security authentication tokens to enable users to log in once and access a range of applications and systems. But the advantage of SSO is it can be configured to use other authentication methods beyond passwords, including smart cards or biometrics. Companies which are serious about security may want to consider adopting SSO instead.

Office 365 Single Sign-On

High availability without high complexity

Randy Franklin Smith

The move to Office 365 is a huge leap forward in productivity and savings. But failing to pair it with reliable SSO can send an organisation backwards.

A distinction is often made between 'enterprise' technologies that are appropriate only for large enterprises and those that are practical and valuable to small and medium businesses (SMBs) as well. SMBs often view this distinction differently to technology vendors. A great example is the effort and expense required to provide Single Sign-On (SSO) between on-premise networks and Office 365 (O365), and even more so to make it highly reliable.

Out of the box, O365 requires a separate user account and group administration. This requirement is an immediate step backward for end users, IT staff and the organisation as a whole. End users now need to remember or attempt to synchronise two passwords instead of one. End users must enter their credentials multiple times: once to access their workstation and on-premise servers and again to access O365. If they close their browsers, they must re-authenticate the next time they access the cloud.

IT staff must now provision not one Active Directory (AD) account for new hires but also an additional account in O365. With each department's information split between on-premise applications and the cloud, IT finds itself maintaining duplicate group memberships between the two environments. Redundant user accounts and groups have been repeatedly demonstrated not only to increase work and degrade user experience but also inevitably to create risk as entitlements become outdated and credentials fail to be revoked. Such problems were big issues more than a decade ago, before AD gained its current ubiquity and enabled organisations to centralise identity information within their networks.

Obviously, SSO with O365 is required for any organisation with on-premise IT, regardless of size, if the organisation plans to avoid these problems during its move to the cloud. Microsoft offers SSO between on-premise and O365 with Active Directory Federation Services (ADFS) a native component of Windows Server and the DirSync utility which provides synchronisation between AD and Office 365.

Out of reach

One of the benefits of O365 is the high availability that automatically comes with the cloud. Many organisations would never migrate to the cloud unless O365 could meet or exceed their current availability commitment. For other organisations, O365's availability is a key value proposition that motivates the switch.

Therefore, organisations need SSO and high availability. However, implementing a highly reliable SSO for O365 with ADFS is simply not an option for most organisations. High-availability ADFS relies on Network Load Balancing (NLB) clusters, which require cluster members to be on the same subnet. This key requirement for ADFS high availability creates several issues that make it impractical for all but the largest organisations. Even then, ADFS high availability is questionable.

But organisations that roll out a basic ADFS implementation create a perilous single point of failure that can render O365 inaccessible to users even when the O365 service is fully operational.

In this discussion we will make two assumptions that apply to most organisations:

- The organisation has at least two physical sites (eg, offices, branches, data centres) that are connected by VPN or WAN.
- If one site fails for any reason, management requires that O365 remain available to: users at other sites that are still operational, telecommuters and users at the first site who can move to an alternative location.

Before researching NLB cluster requirements, you might assume that you could achieve high availability simply by leveraging the multiple sites that most organisations already have. Ideally, you would deploy an ADFS server at two or more sites in which domain controllers are present or could be added. Then again, if ADFS at the first site were unavailable for any reason, O365 would ideally automatically failover to the ADFS server at an alternative site; any user with internet access would be able to access any resources in O365 regardless of any individual physical site's status. If this capability were supported, highly available O365 with SSO would be in reach of any organisation with at least two offices with DSL-grade internet - even small organisations with just a handful of users. No special networking hardware, WAN services or power equipment would be required.

However, organisations cannot leverage existing physical sites in this way because ADFS clusters require NLB, which requires all members to be on the same IP subnet. Placing ADFS servers at different sites puts those servers on different subnets, thus breaking NLB and preventing ADFS clustering and highly available SSO to O365. And in case you are wondering, other manual cutover scenarios such as retargeting O365 to a completely different ADFS instance or simply turning off SSO are either unsupported or impractical.

The crux of the problem is twofold.

NLB does not protect against problems that affect the entire site. Such problems include power outages, internet connection failures and disasters such as fire and flood. Only the largest organisations house an enterprise data centre in a hardened physical building, in a region with low incidence for disaster and with redundant power systems, redundant internet connections entering the building from opposite sides of the block, fire suppression systems and all the other related technologies that are required for a single data centre to remain operative under any condition.

NLB does not permit the deployment of ADFS servers at different sites. This issue is vexing because if you have two locations connected by VPN with a domain controller at both locations, you have the makings for high availability. The more physically separate the two sites, the more independent their power, internet connectivity and physical disaster probability. Even two offices in the same region can usually use different internet providers and purchase inexpensive battery backup systems.

Organisations that roll out a basic ADFS implementation create a perilous single point of failure that can render O365 inaccessible to users even when the O365 service is fully operational.

The good news is that you can achieve highly available SSO for Office 365 without ADFS. There are vendors who provide solutions that completely eliminate the need for ADFS and DirSync, and which can easily leverage your existing sites to provide highly available SSO to O365, enabling your users to continue working regardless of what happens at different locations.

Eliminating the need for ADFS and DirSync

Solutions exist whereby SSO for O365 can be accomplished in just five minutes using a Microsoft-validated replacement for ADFS and DirSync. This involves simply registering with the appropriate cloud service solutions provider and performing a cloud proxy service install at each site using (optionally) existing Windows. The provider's system will then automatically configure O365 to use the service to authenticate your users.

Setting up an SSO service requires specialised knowledge and significant investments in high-availability, clustered servers. So it's important to choose a provider who can supply a Microsoft-validated service and who can offer an industry-leading, easy-to-deploy comprehensive solution for AD-based SSO, user provisioning and mobile management. Look for a provider who can support a wide range of software-as-a-service apps, so that your users have access to all your cloud-based applications.

Your vendor should also provide additional benefits, such as a secure browser SSO via a user portal, user self-service and one-click mobile access to SaaS apps.

resources
from our sponsor

Centrify®

Centrify provides unified identity services across data center, cloud and mobile environments that result in single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service(IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and mobile, and mobile device management.

www.centrify.com

+61 1300 795 789

Unified Identity Management for SaaS, Mobile and Macs

http://www.centrify.com/products/centrify-user-suite.asp

Unified Identity and Audit across Windows, Linux & UNIX

http://www.centrify.com/products/centrify-server-suite.asp

Request a Free Trial of Centrify Solutions

http://www.centrify.com/trial

another ebook from
www.technologydecisions.com.au

published by
wfm
WESTWICK-FARROW MEDIA