THE ESSENTIAL GUIDE TO

Managing Access to SaaS Applications

By Sean Deuby

IT professionals are grappling with not one, but three revolutions at the same time. First, cloud computing provides easy and dynamic access to information technology. Next, the ecosystem of cloud-based SaaS applications has exploded thanks to cloud computing. Finally, this SaaS ecosystem has helped power an even bigger boom of consumer-friendly mobile devices and apps that access SaaS.

This Essential Guide examines the opportunities and challenges of empowering, yet controlling, user access to SaaS applications. Specifically, identity management as a service promises to simplify secure access to and management of SaaS applications while reducing password sprawl. We also review how mobile computing has added to

Windows IT Pro

SPONSORED BY

Centrify®

the complexity of managing access to both corporate data and SaaS, and ways to evaluate the options available on the market.

Cloud Computing Is an Enabling Technology

Cloud computing is a revolution that's affecting many aspects of our lives, even if it may not appear to be. If you ask people who aren't in the technology business to describe cloud computing, most of them won't be able to do so. But they will likely be able to tell you, in great detail, about their favorite apps on their smartphone, or the latest episode of a show that's only available on a streaming video service like Netflix. These new innovations are possible thanks to cloud computing.

Cloud computing is the capability to provide on-demand computing resources via a subscription service. This service can be quickly scaled up or down, depending on your requirements and how much you're willing to pay. As the examples demonstrate, what's most important about cloud computing is that it enables other business models that are transforming our world. In his blog "Cloud Computing Predictions for 2014: Cloud Joins the Formal IT Portfolio," James Staten of Forrester Research states, "In 2013 enterprises got real about cloud computing. In 2014 we will integrate it into our existing IT portfolios—whether IT likes it or not."

Software as a Service Has Democratized Computing

One of the cloud computing business models that's transforming it is SaaS. Cloud computing enables a company to create a service (e.g., a way to share files between individuals) using a Platform as a Service (PaaS) cloud computing provider. Because it's built to work as a web service, and because many cloud computing service providers have a global presence, this SaaS application is available on very simple computers, often with nothing more than a web browser, nearly anywhere in the world. SaaS has democratized computing, making it easy for anyone with a credit card or purchase order to gain access to powerful resources previously undreamed of.

The SaaS model, however, has been a headache for information technology (IT) departments. IT is tasked with providing secure computing resources for a business, but SaaS's agility and ease of use has sidestepped IT. In a phenomenon known as "Shadow IT," employees bypass traditional IT and get their resources from SaaS applications directly – each requiring their own user id and password (Figure 1). This might be good for users getting their jobs done, but it also causes problems—especially security and governance problems. For example, when a general user starts using a SaaS app, data security isn't usually high on their list of concerns. And since there are often no central management dashboards that show which users are using how much of what resources, it's difficult to even discover what SaaS applications are being used.

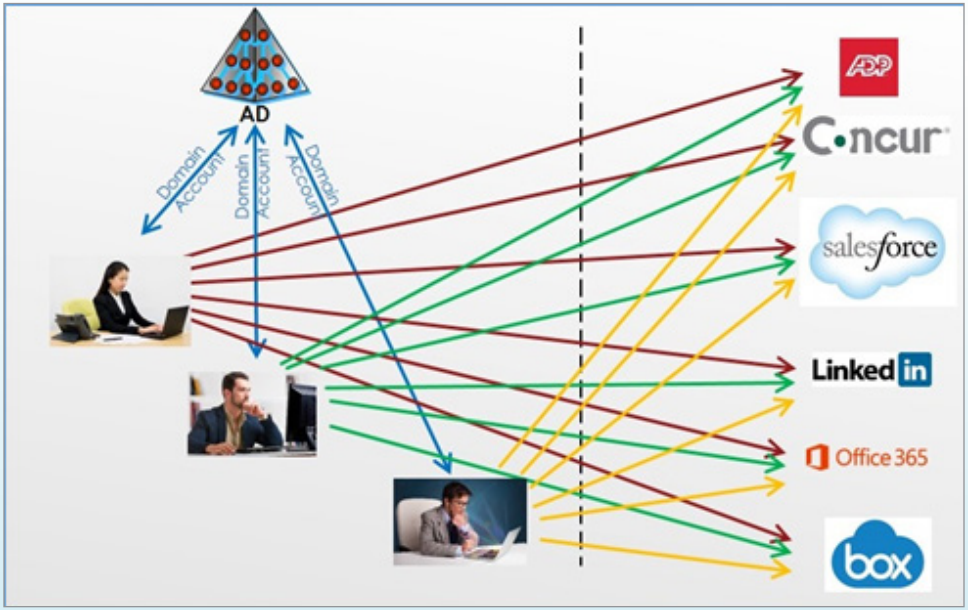

Figure 1: Unmanaged corporate users require separate SaaS accounts

Despite the management and security shortcomings that are part of most consumer SaaS apps, leveraging cloud computing can have significant advantages for business IT departments, if done correctly.

SaaS gives companies the ability to use applications to solve their business needs quickly while sidestepping all the traditional application deployment overhead. Companies no longer need to worry about scoping requirements; selecting, buying, installing, and integrating hardware; monitoring and maintaining applications; or managing each application's end-of-life. These activities are all outsourced to the company providing the applications as a web service.

Mobile Devices Enable Truly Personal Computing

Another aspect of SaaS that isn't always obvious is that it (along with hardware advances) has powered the "bring your own device" (BYOD) mobile revolution. Most mobile apps have a small client on the device that communicates over a cellular or Wi-Fi network to a SaaS backend that does all the work. How useful is a smartphone without network access, document sharing, or social media apps? As anyone who has tried using an out-of-range smartphone knows, it's just a shadow of its full capability.

Mobile computing and its associated apps have revolutionized the way we live and work. Entire industries have collapsed—and others have risen—from the impact of this truly personal computing. But mobile devices have created yet another set of problems for IT. The popular phrase "consumerization of IT" has both overt and subtle meanings, especially in this mobile context. Overtly it means that easy-to-use IT solutions are now literally in the hands of the consumer. But if you're in IT, you realize there's another meaning, too: *Just because you can, doesn't mean you should*. IT pros know there are many ways you can get things done with technology, but a lot of them aren't appropriate, scalable, manageable, or secure enough for the workplace. Users who find IT-like capabilities on their mobile devices, however, generally don't think, "Should I be putting potentially sensitive corporate data on my unlocked personal device?" If it makes their jobs easier, they will use it. Dropbox is perhaps the best example of this. The service's convenient file sharing has enabled

easy collaboration and sharing of large files, but all corporate data on Dropbox is outside corporate control.

Figure 2 shows how employee-owned mobile access to corporate SaaS applications further complicates IT oversight of these applications:

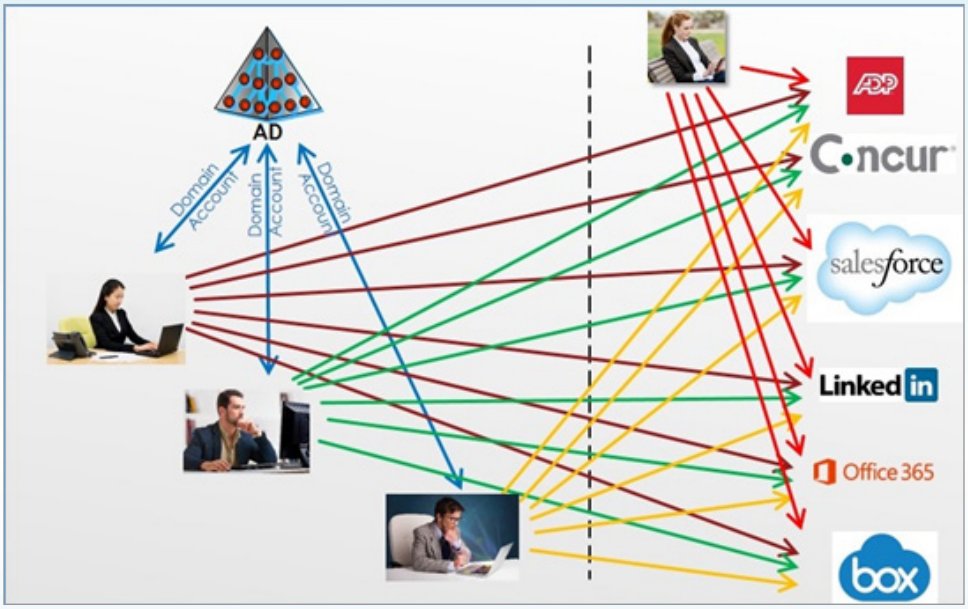

Figure 2: Mobile users complicate SaaS security even more

Internet Single Sign-On Simplifies SaaS Access

Integrating these technologies into mainstream IT is one of the big challenges for 2014 and beyond. Perhaps counterintuitively, a method for managing access to SaaS applications that's quickly gaining popularity is itself a SaaS application: Identity management as a Service (IDaaS).

Corporate IT can gain some control over shadow IT by enticing users back into the corporate fold with an Internet single sign-on (SSO) solution, which allows users to access SaaS applications without being prompted for user IDs or passwords. Internet SSO is appealing to both users and IT. It's appealing to users because keeping track of accounts for numerous SaaS applications is frustrating and a serious time drain; being able to use SaaS applications without signing on each time is worth some IT

governance. Internet SSO is appealing to IT because it brings back some control and visibility to SaaS usage that was previously lacking.

The Identity Bridge

The component that connects an enterprise's on-premises computing infrastructure with cloud services is known as an identity bridge. An identity bridge contains three major elements (Figure 3):

- A **provisioning element** that manages populating SaaS applications with accounts of authorized users
- An **authentication element** that authenticates these users to the application
- A **data element** (not shown) that provides the means to pass business data from the company to the SaaS application so that it can make authorization decisions

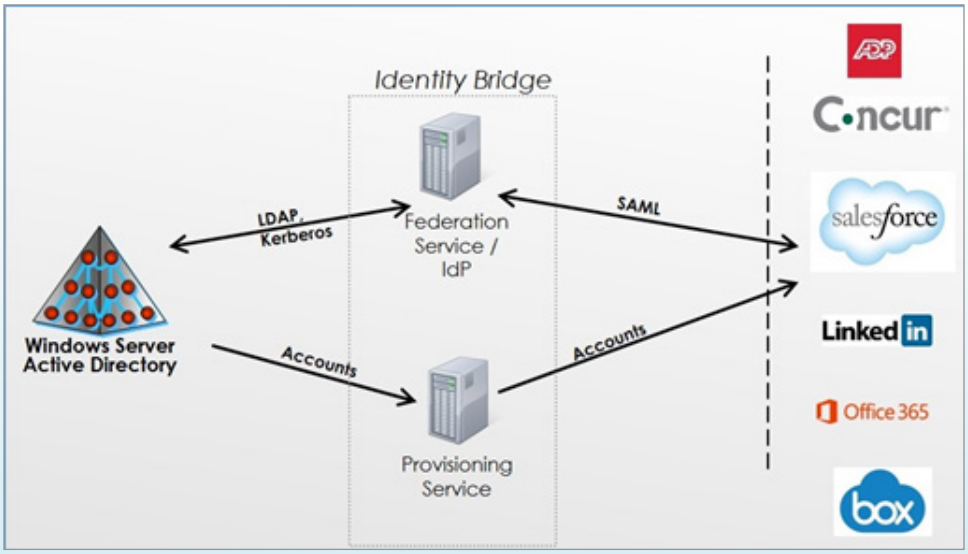

Figure 3: A simple identity bridge

The Provisioning Element

Managing accounts for SaaS applications involves a lot of CRUD—that is, a lot of Create, Read, Update, and Delete operations. This is com-

monly known as provisioning. You need to manage the full account lifecycle—you can't forget the "D" part. If you don't delete or disable accounts, unauthorized users (e.g., a terminated employee) might still have access to corporate data and services. Accounts can be provisioned, updated, or de-provisioned by a variety of methods of varying sophistication, including comma-delimited files, Microsoft Excel worksheets, just-in-time Security Assertion Markup Language (SAML) provisioning, directory synchronization, and the System for Cross-domain Identity Management (SCIM) identity provisioning protocol.

The Authentication Element

Authentication for a SaaS application can be accomplished one of two ways: entering a user ID and password (either manually or automatically) or using identity federation. The former method is pretty well known (and increasingly reviled). The latter method is well established and has superior security.

Federated authentication uses an identity provider (typically Active Directory) that is trusted by the SaaS application to verify the identity of a user attempting to log on to the SaaS application. The SaaS application passes the authentication request back to the identity provider. Once the identity provider authenticates the user, it provides a token back to the SaaS application containing useful information such as the user's email address and group membership. No passwords are included in this token. The SaaS application knows the token is really from the identity provider because it's been digitally signed for authenticity.

Unfortunately, only about 7 percent of the approximately 25,000 SaaS applications on the Internet support federation at this time. Typically, they're the largest SaaS applications. The rest require a user ID and password, a process known as form fill. However, in the case of SSO/IDaaS solutions, even these latter applications that don't support federation can be managed by IT, thanks to SSO applications that manage unique passwords for each SaaS app, without the user ever needing to know what those passwords are. Since the user doesn't have to remember dozens of

username and password combinations, IT can create unique credentials for each app used, easing access for users, and mitigating the risk of data theft if a SaaS application backend is hacked or compromised.

The Data Element

A powerful aspect of federated identity is its ability to securely transmit a wide variety of data about a user to services that need this information. The data element, which is a part of the federation service, transmits this data in the form of claims inside security tokens. Claims carry pieces of information about the user. This is similar to the Active Directory security token inside the Kerberos ticket, because the AD security token contains data about the user's group membership. However, claims are a far more flexible means of passing data about the user. When you establish a federated trust between an enterprise and a SaaS application, you can choose claims the SaaS app requires and your identity infrastructure can provide. Typical claims for SaaS applications are email address/user principal name (e.g. name@company.com), group membership, manager's email address, or job role. In this way, the SaaS applications your employees use can securely receive a full set of information to provide rich functionality.

Types of Identity Bridges

There are two major types of identity bridges: on-premises identity bridges and cloud-based identity bridges. Each type has its own advantages and disadvantages.

On-Premises Identity Bridges

Probably the best-known example of an on-premises identity bridge is Microsoft's Active Directory Federation Services (AD FS) for federated authentication, combined with DirSync for identity provisioning. These tools are provided with Windows Server operating systems at no extra cost. Though these tools are free, they are solutions for a limited number of use cases.

DirSync (and its successor Azure Active Directory Sync) only synchronize your on-premises identities with Microsoft's Azure Active Directory (the identity platform for all of Microsoft Online Services). If you need to handle provisioning for SaaS vendors other than a Microsoft Online Services SaaS application like Office 365, and you choose not to use Azure Active Directory to access SaaS vendors, you must use the vendor's proprietary solution (Figure 4). This per-application provisioning method can quickly become very hard to manage as the number of SaaS applications used in a company keeps increasing.

AD FS is a standards-based federation service that can be used to establish federated connections to many SaaS applications. But AD FS is complex to deploy, and requires multiple servers in a high-availability configuration. Once in production, the product's complexity and support costs increase linearly as IT connects it to more SaaS applications.

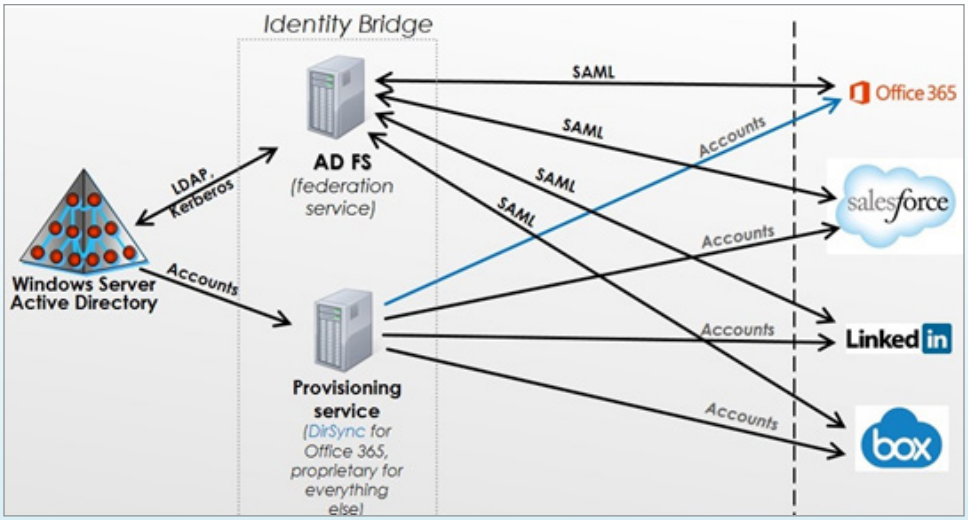

Figure 4: AD FS and provisioning services

Identity management as a service

Despite the challenges of deploying an on-premises identity bridge, the advantages of using on-premises identity stores far outweigh its drawbacks. IDaaS architecture (Figure 5) allows a company to use

its identity stores to authenticate users and control access to SaaS applications, while minimizing the complexity required to maintain the connections. The job of managing federated connections and provisioning identities for tens or hundreds of SaaS applications is moved out to a cloud service specifically designed for it. A typical IDaaS solution manages a portfolio of over 1,000 SaaS applications; establishing single sign on with one of these integrated applications requires very little effort on the part of the IDaaS customer. Instead of connecting to 100 SaaS applications, for instance, all IT needs to do is connect an identity bridge to the IDaaS service. And in most cases, the identity bridge is purpose-built for the IDaaS service and therefore very lightweight and simple to install and maintain.

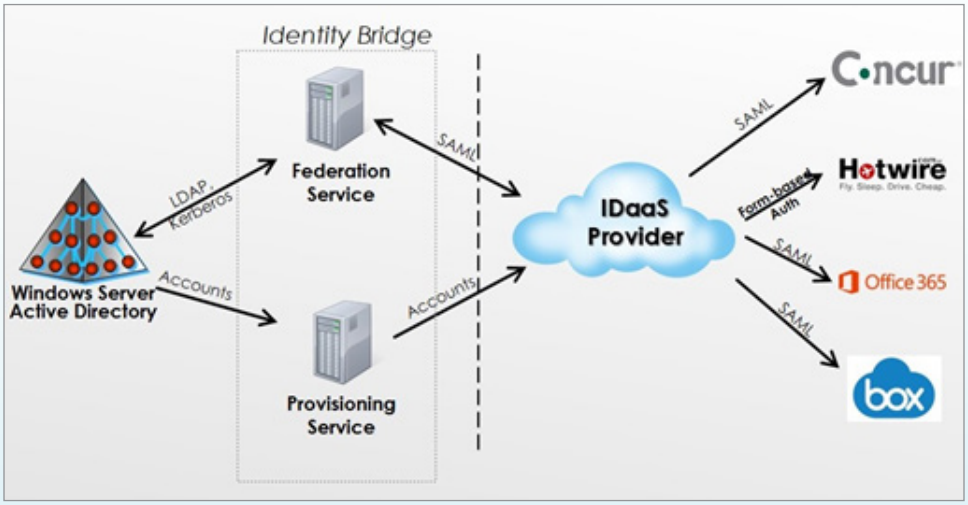

Figure 5: Identity management as a service outsourcing SaaS integration

Using an IDaaS solution also has a significant advantage compared to locally maintaining these connections, given that over 90% of SaaS applications don't yet support federation and must have a userid and password entered manually (a process known as form fill). This is because IDaaS solutions use a technique named password vaulting, in which customer user IDs and passwords are stored

in a secure manner in the cloud service. When a user attempts to log on to a SaaS application that only supports form fill, the IDaaS solution automatically populates the user ID and password fields, and essentially presses the Enter key. The result is that the user is seamlessly logged on.

Because it's a cloud service, IDaaS also has the agility to satisfy customer's needs for quick access to new applications. Provisioning access to a new SaaS application is a matter of hours compared to days or weeks doing with a general purpose on-premises bridge. And when an application is no longer needed, removal takes just minutes. IDaaS providers also are much more user friendly than a general purpose bridge. Instead of bookmarking or remembering the URL for every SaaS application they use, customers of the service typically access their authorized applications through a single, easy to remember portal. These portals are also mobile friendly, with a downloadable client or mobile-friendly version.

Since most, if not all, of the provisioned SaaS apps will likely be accessed via mobile devices, it makes sense to look for mobile device management and access policy in any full-featured IDaaS solution. Device posture can be a powerful part of any app access policy, but the device must be managed before policy can be applied. Passcode polices, encryption, and certificate management are all critical components for securing corporate data on devices used to access apps, and in cases where policy mandates multi-factor authentication, a managed mobile device can be an easy, but strong, second factor.

Vendor Evaluation Considerations

When considering an IDaaS solution, the first evaluation criterion is whether regulatory requirements allow you to use a cloud service like IDaaS. The second, which is much more nuanced, is how comfortable you are with the idea of putting your company's identity information in the cloud. If you only use SaaS applications that support federation, no passwords need be stored in the IDaaS service as the service

will pass the authentication request to your identity infrastructure. If you choose to use form fill-based applications (and most companies do), a password of some kind will be stored in the IDaaS service. (Note: it shouldn't be the same as the user's corporate passwords.)

If you have a highly complex on-premises identity infrastructure, look carefully at how well different vendor's solutions will integrate with your own. And have a good look at a vendor's deployment scenarios—not only to see if they meet your requirements, but also because they may open up new opportunities you didn't have before.

Centrify®

Single Sign-On for Office 365 ...and Beyond

Go beyond browser SSO to also give users unique mobile "zero sign-on" to Office 365... and their other SaaS apps as well.

Secure Browser Single Sign-on (SSO)

Mobile Zero Sign-on (ZSO)

Turnkey Active Directory Integration

User Self-Service with MyCentrify

Limited Time Offer: Save 80%

Get Centrify for Office 365 with SSO for only $8 per user per year.
Mobile device and application management included.