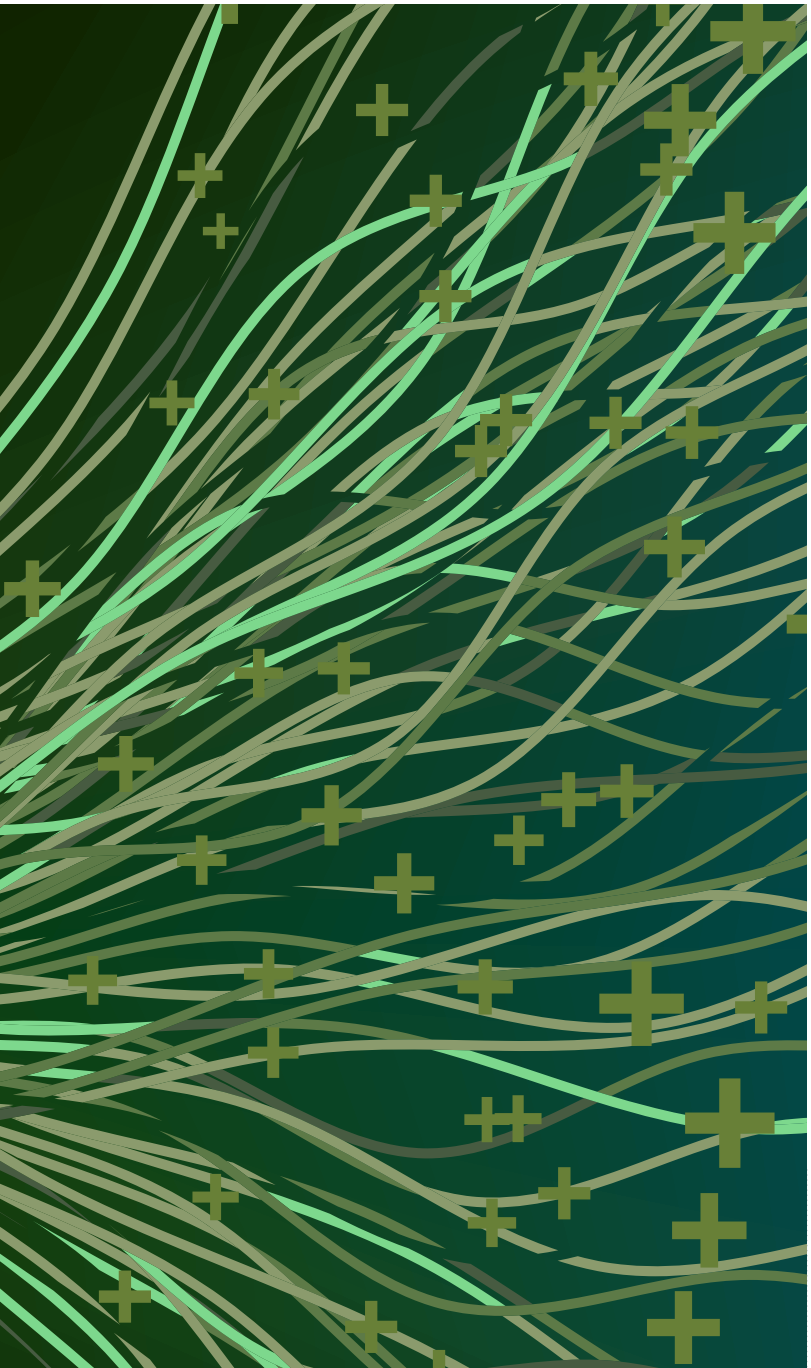
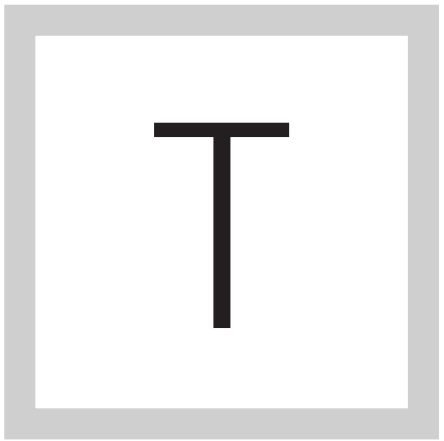


E-Guide

HOW MICROSOFT AZURE AD USERS CAN EMPLOY SSO

TechTarget | SearchSecurity



ECHNOLOGY JOURNALIST David Strom explains how to use Azure Active Directory and Azure Multifactor Authentication for hybrid cloud management.

HOW MICROSOFT AZURE AD USERS CAN EMPLOY SSO

David Strom

One of the ways you can secure data and applications in hybrid clouds is to employ Microsoft's Azure Active Directory and its single sign-on access control feature. Azure AD is a multitenancy cloud and identity management service, designed to enable employees to use a common identity across cloud services, and on premises software.

If you are already using the Azure cloud, setting up single sign-on (SSO) should be a simple matter. With SSO, you can enable role-based access to a range of Software as a Service (SaaS) applications, such as Microsoft Office 365 and Salesforce.com, by allowing employees to securely access multiple resources with a single login.

However, it is difficult to setup SSO access control. Many people get lost in the hall of mirrors that is the Azure setup process. (See the series of support documents on MSDN here.) Microsoft promises to do a better job integrating SSO access control into the Azure management portal, and to simplify, its control menus (sometime soon).

Eventually, Azure AD will be the control point for the Windows Store, according to the company. Still, Azure AD is mainly a developer's toolkit rather than a polished identity management service such as Okta or Ping Identity. Its main dashboard, shown in Fig. 1, is somewhat bare-bones compared to other SSO tools.

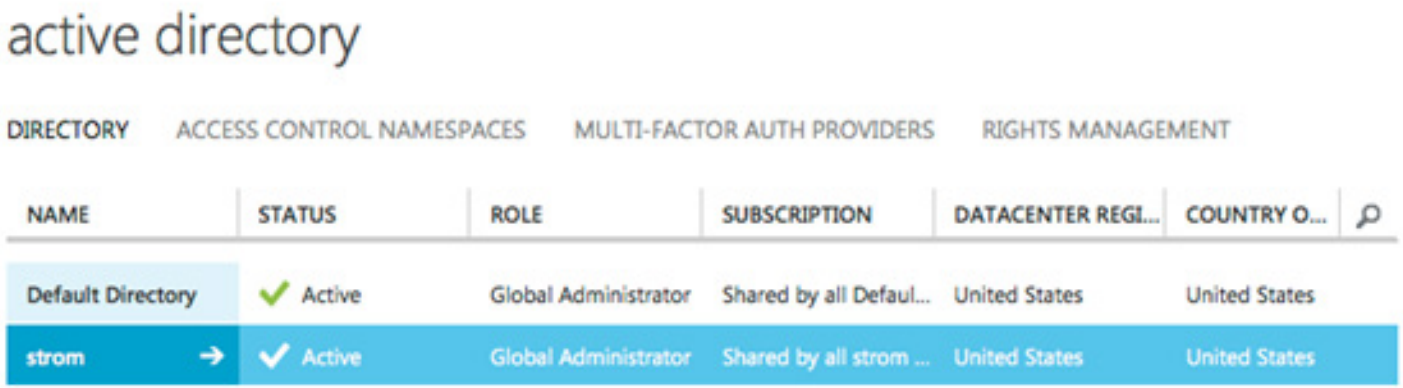


FIG. 1. MICROSOFT AZURE ACTIVE DIRECTORY SINGLE SIGN-ON ACCESS CONTROL IS 'BARE BONES' COMPARED TO OTHER SSO TOOLS.

For hybrid management, you should start by downloading the Azure AD Connector to integrate your on premises directories with Azure AD. The AD Connector installs various pieces of software on your Windows Server AD Forest. Azure AD supports several identity providers, including Windows

Live ID, Facebook, Google, Yahoo, JSON Web Tokens, OpenID, SAML and WS-Federation.

It also has an SaaS app catalog that you can browse to add SSO logins. You then add each app to your portal page with a simple three-step process to permit the sign-on relationship, enable automatic provisioning and assign particular users to that app.

Administrators have three choices on how the sign-on happens: either by establishing a federation between Azure and the app service provider (this is probably the preferred method), having Azure store the user's account credentials, or using some other existing SSO relationship. Azure AD Reporting offers more than a dozen reports, including account provisioning activity, irregular sign-ons, and sign-ons from multiple locations.

If you are looking to add multifactor authentication (more than user name and password) to on premises applications and cloud services, you'll need an Azure AD Premium account and the Enterprise Mobility Suite. Azure Multifactor Authentication is a service (formerly PhoneFactor) that adds a second layer of security via a text message, phone call, mobile app notification or verification code and third party Open Authentication tokens, according to Microsoft. Once a separate Windows application, it's now integrated with the

overall Azure service. Azure Multifactor Authentication is far more limited than other vendors' MFA tools, however, as shown in Fig. 2. Although, it does offer a one-time bypass feature if a user is locked out of their account. This means employees can reset their AD passwords from within their own portal pages. (That's one less IT support call when they forget their password).

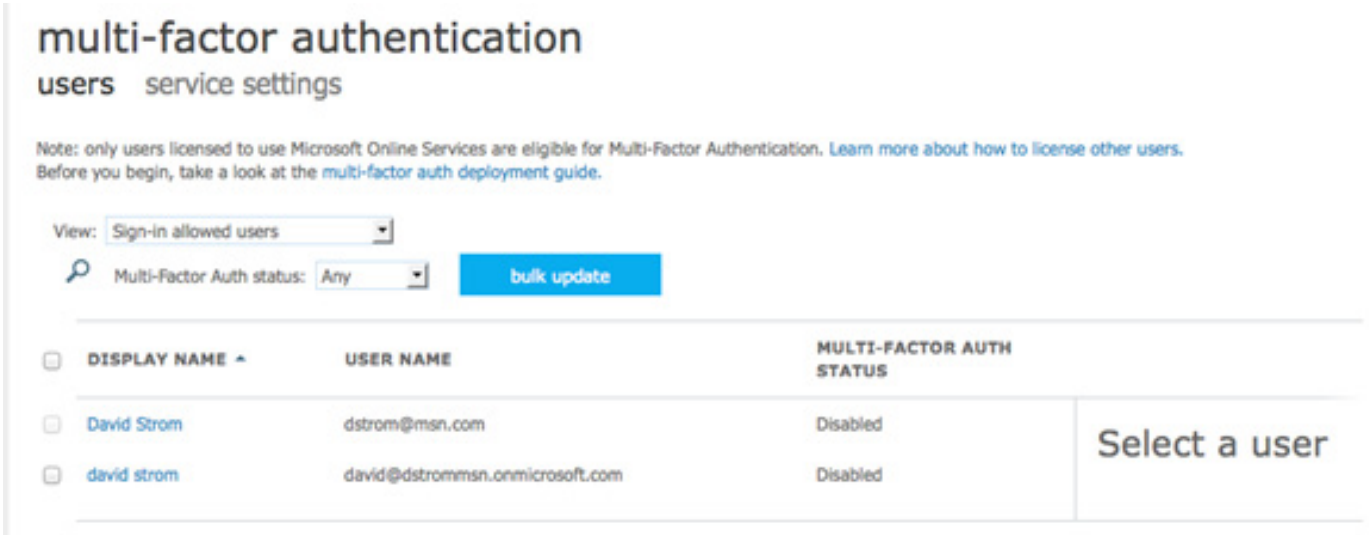


FIG. 2. AZURE MULTIFACTOR AUTHENTICATION FOR ON PREMISES APPLICATIONS AND CLOUD SERVICES REQUIRES AN AZURE PREMIUM ACCOUNT AND THE ENTERPRISE MOBILITY SUITE.

If you already are using the Azure cloud, then it makes sense to take a closer look at what Azure AD will buy you and whether your developers can incorporate its SSO tools into your home-grown apps.

Azure AD has three different pricing options. The free version is included with an Azure or Office 365 subscription and can provide SSO for up to 10 apps per user. There are also basic and premium subscription levels (the latter for unlimited apps that also includes the SSO for no extra charge, which is probably the preference for most enterprises) that are covered by various Microsoft corporate purchase agreements or online for $6 per user per month.

DAVID STROM is a freelance writer and professional speaker based in St. Louis. He is former editor in chief of TomsHardware.com, Network Computing magazine and DigitalLanding.com. Read more from Strom at Strominator.com.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.