



Moving into Azure

Find out in these articles from Redmond why Microsoft faces challenges bringing active directory users to Azure AD. Also, find out how to connect Active Directory and Azure AD.

- > Identity Clash *Page 1*
- > Connect Active Directory and Azure AD *Page 11*
- > Ad Retooled for the Changing Workplace *Page 20*

IDENTITYCLASH

Microsoft wants to bring Active Directory users to Azure AD, but rivals vie to manage enterprise user authentication in the cloud age with alternative offerings. BY JEFFREY SCHWARTZ

Well more than 90 percent of organizations use Microsoft Active Directory as their main store for employee authentication, identity management and to maintain access control policies. But as the growth of cloud-based Software-as-a-Service (SaaS) applications enterprises try to manage continues to grow, IT planners and architects must evaluate how they'll manage user identities. Early adopters are already

A number of factors are driving the shift in how organizations must be thinking about how they manage user authentication and identity management.

doing so. With a number of players—some established and others lesser known—vying to become your cloud identity management as a services provider, it invariably raises questions over the future role of Active Directory.

Most experts don't believe Active Directory is an endangered species anytime soon and that it'll have an important role even among those who turn to other identity management platforms. But at least some organizations could greatly de-emphasize or even curtail its use in the years ahead. Meanwhile, Microsoft is aggressively promoting and updating Azure Active Directory (Azure AD), which aims to seamlessly bring Active Directory to hybrid and public cloud environments.

A number of factors are driving the shift in how organizations must be thinking about how they manage user authentication and identity management. In addition to the number of externally hosted applications that organizations now need to manage access to, the universe of identities is also growing exponentially. Not only must IT manage employee credentials, but the identities of customers and partners, who naturally have different privileges. This shifting dynamic and the number of high-profile security breaches that have occurred in recent years have created this land grab by Microsoft and a number of established and lesser-known players to provide what many call Identity Management-as-a-Service (IMaaS).

Career-Defining Decisions

As many enterprise IT decision makers conduct these architectural assessments, these could be career-defining decisions for some. Very few say organizations will rip out Active Directory and replace it with something else to manage day-to-day authentication and policies—certainly it would make no sense to do so for existing systems. But by a number of estimates there are some—about 10 percent of organizations—that are looking to either eliminate or vastly reduce the role Active Directory plays for identity management and single sign-on for these vast array of SaaS applications and other resources.

One example of a large enterprise looking to sideline Active Directory is the Planned Parenthood Foundation of America. Overseeing this plan is Franklin Rosado, Planned Parenthood's director of enterprise



“We’re looking to deprecate Active Directory because we’re moving extremely heavily into the cloud.”

*Franklin Rosado,
Director of Enterprise
Architecture, Planned
Parenthood Foundation
of America*

strategy and system architecture. Rosado is a longtime “Softie,” as he calls himself—an MCSE since the 1990s. It’s no small effort as Planned Parenthood shifts user identities from Active Directory running on Windows Server machines by its 60 affiliates nationwide to the Okta Identity Platform, which provides single sign-on connectivity to numerous third-party SaaS services, Active Directory, Azure AD and Office 365, as well as other legacy directories. At a recent visit to Planned Parenthood’s New York headquarters, Rosado described its current architecture and reasoning for making the move. In addition to the 60 affiliates, Planned Parenthood’s IT organization supports some 600 clinics with file, print and key SQL Server-based data running on a traditional Windows Server-based network.

Cloud-First, Mobile-First

Planned Parenthood is very much on board with Microsoft CEO Satya Nadella’s notion that computing is shifting to a “cloud-first, mobile-first” model. But while Microsoft has described identity as one of the keys to the future of security and managing users in the “cloud-first, mobile-first” world, the huge non-profit organization is among the 10 percent who aren’t buying into Active Directory and it’s cloud-based iteration, Azure AD, to manage employee identities. Over the summer, Planned Parenthood kicked off the first stage of moving away from Active Directory to Okta. Rosado said his team has brought up several affiliate connectors on the system. It’s taken longer than he had anticipated, having targeted to have 50 percent connected by now. But Planned Parenthood was in the trenches last month working to bring online four major app connectors.

“We’re looking to deprecate Active Directory because we’re moving extremely heavily into the cloud,” Rosado said. “And we really see a lot of trends in the consumerization of IT and the depreciation of Active Directory sort of fits in the trends in the way we’re going in moving to the cloud and moving to mobile-first.”

Despite the deprecation of Active Directory, Planned Parenthood is relying on it to establish user identities at all of its major affiliate offices, and then map to the Okta Universal Directory. “It’s key for us to have Active Directory connected to Okta so we can then have that master stored at our main Okta domain,” he said. “We are extending the capability of Active Directory across the entire federation. We’re



“Basically, their service was a lot more cumbersome to get it to work with Active Directory.”

*Christopher Southerland,
Director of Information
Technology, Nova
Medical Centers*

actually using extension attributes, and defining the use of extension attributes such as job title, affiliate ID and facility IT in Active Directory for all of our affiliates and we’re extending the capability so that we can have that infrastructure down the road to really allow for automated provisioning and deprovisioning across the entire federation, and for a richer directory across the entire federation.”

The move is an eyebrow-raising rebuke of Microsoft’s effort to encourage organizations with ambitious cloud migration efforts such as this to transition enterprises from Active Directory servers—said to be used by well more than 90 percent of organizations to manage user identities and authentication—to its new cloud-based alternative, Azure AD Premium. But Planned Parenthood isn’t the only organization looking to “deprecate” Active Directory.

Nova Medical Centers, a Houston-based regional conglomerate of orthopedic clinics, is also moving off Active Directory. Each computer has unique identifiers in order to maintain HIPAA compliance, but because they’re connected via VPNs, there were numerous points of failure in its architecture, explains Christopher Southerland, Nova’s director of information technology. Asked why he didn’t consider Microsoft’s new Azure AD Premium, Southerland explains he tried it but was left unimpressed with the support, which he describes as “non-existent,” as well as with the offering itself and pricing.

“Basically their service was a lot more cumbersome to get it to work with Active Directory, which is really odd,” Southerland explains. “You had to buy different modules, so if you had a server you had to buy storage space, if you had a network—a specific network—you had to buy network space. So the cost, when I actually talked to them initially, was \$200 a month for 50 locations. That was a lie. First of all they weren’t considering how much data we were pushing through, they just kind of made up a number. I actually got one location connected, we were doing some testing and it slowed down the computer considerably. The speed of the computer to actually log in was probably about 2 minutes. At the time I was testing it, you could only have 10 locations on the same network, and then you had to buy more, and then you had to subnet it out.”

Southerland had drawn up a plan to put in several new Active Directory servers at various locations, which included the hiring of

Active Directory administrators. Though he got approval to do it from the Nova board, Southerland did a last-minute Google search and stumbled upon a little-known company known as JumpCloud, which operates its own suite of Directory-as-a-Service SaaS-based offering. JumpCloud has its own directory and offers support for Active Directory as a service. Southerland says he can continue using Active Directory but doesn't have to.

Another benefit of JumpCloud versus Southerland's earlier plan to deploy new servers is the new service doesn't require VPN connectivity. "They have a management console that you log in to and all you do is create a user account just like you would in Active Directory, and you link the computers to that user or group [and] you can create groups, as well. You can do it all managed to the cloud. What I like about that is I have a technician in Georgia and I have a tech in San Antonio and two in Houston and we can all manage it remotely."

Microsoft Extends into Privileged Identity Management

Microsoft has added a few more tools to its Azure Active Directory (Azure AD) Privileged Identity Management preview.

The Privileged Identity Management preview, updated in August, is an emerging Microsoft service that lets organizations control IT personnel administrative access to Azure AD-managed resources. The preview has been updated with a few new features. For instance, it now has a security wizard that offers recommendations based on an "organization's specific security configuration," according to Microsoft.

Another addition to the preview is an updated security dashboard, plus security alerts regarding privilege changes. There's a "fix button" to roll back any unwanted privilege changes.

Microsoft added a new "workload-specific admin roles" specification that provides greater control over access privileges. Microsoft's example of this capability was granting SharePoint Online administrative access, but not administrative access to other Office 365 workloads.

A multifactor authentication option has been added to the preview. Multifactor authentication is a secondary identity verification process on top of passwords. Organizations can now require multifactor authentication when setting up privileged roles.

Last, Microsoft added a "security review" capability to the preview. It's a process by which IT pros are periodically asked to recertify their access privileges.

Microsoft first unveiled this Privileged Identity Management preview back in May, explaining that it adds control over Azure AD administrator roles for services such as Microsoft Intune, Office 365

Will Active Directory Migration Become a Trend?

Given how entrenched Active Directory has become over more than a decade, this has to be somewhat concerning to Microsoft, even if Planned Parenthood and Nova Medical account for a minority of enterprises that ultimately go as far as to deprecate it. “We see 10 [percent] to 15 percent of companies moving away from on-premises AD as their primary user store and moving it to the cloud (Okta, Centrify, OneLogin, Ping and so on),” says Forrester Research analyst Andras Cser. “Microsoft is very concerned about this.”

If that’s the case, company officials aren’t saying so. Alex Simmons, Microsoft’s senior director for Active Directory, says he’s well aware of the competition, but says the company is aggressively adding new features to Azure AD—on the order of several a week these days and 74 updates over the past year. Azure AD is a core component of the Microsoft Enterprise Mobility Suite (EMS), which also includes the Intune device configuration and management service and Azure Rights Management. Microsoft COO Kevin Turner recently identified

services and Azure SaaS apps. It’s a feature addition to Azure AD Premium subscriptions, which cost \$6 per user per month.

The Privileged Identity Management preview service currently works with the Azure preview portal, which provides a dashboard view. It uses color-coded rankings of security risks, based on things like the number of access privileges assigned (too many is considered to be a bad security practice). Global administrators can set up temporary or “just-in-time” access privileges, if wanted. IT pros, for their part, can request access to resources for approval under the system, but global administrators have control over the access.

Microsoft also has a different service that’s free called Azure Role-Based Access Control. The Azure Role-Based Access Control service also works with the Azure preview portal to control user access, but it appears to be a more general tool, whereas the Privileged Identity Management preview is specifically designed to be set up by a global administrator in an IT organization to control administrative access privileges by IT personnel over time.

The idea behind the Privileged Identity Management tool is that IT pros “have become a high-value target for attackers,” Microsoft explained back in its May announcement. Microsoft’s tool is designed to set up alerts should anything unexpected change regarding access privileges.

The Privileged Identity Management service might be used by larger organizations, perhaps, but the idea that IT pros are targeted isn’t paranoia. Even the U.S. National Security Agency is said to target system administrators, according to NSA documents leaked by Edward Snowden. —Kurt Mackie

EMS as a \$1 billion market opportunity and company officials have consistently talked up winning in identity management as a critical goal.

Microsoft recently revealed 14,000 mostly midsize and large enterprise customers are using EMS, where Azure AD has a “rich coupling” to Intune. Simmons says most of those are very large enterprises. Because Azure AD also is the directory for Office 365, Simmons says 6.5 million organizations totaling 50 million people log in to Azure AD every day. Simmons also points to customer-requested additions to Azure AD such as support for multifactor authentication, the ability to turn off SMS in favor of Auth-Code and one that has significant potential—support for the ability to join Azure AD by logging into Windows 10.

Microsoft Identity Manager 2016 Replaces FIM

Microsoft Identity Manager 2016 (MIM), the successor product to Forefront Identity Manager 2010 R2, is now available. The new release, which supports identity and access management for premises-based computing environments, is notable for Windows 10 client support. It also supports Windows 8.1 clients, Windows Server 2012 R2 and the latest System Center Service Manager.

Microsoft is touting MIM 2016 as a “modernized” product. It now has support for using REST-based APIs for certificate management in multiforest environments, for instance.

The company also points to its “hybrid identity management” support (for cloud and premises-based environments) with Azure Active Directory (Azure AD). MIM 2016 can be used to establish end-user single sign-on access privileges to cloud-based apps that are supported by Azure Active Directory. MIM 2016 also works with the Azure Management Portal to generate hybrid reports, but that capability possibly may require having an Azure Active Directory Premium subscription.

Microsoft built “privileged access management” controls into MIM 2016 as a way to fine tune network access privileges by IT personnel. MIM 2016 uses Just Enough Administration, a Microsoft PowerShell scheme, to control administrative rights, for instance. It’s also possible to set time limits on IT personnel access privileges.

MIM 2016 also enables self-service capabilities for requesting access privileges, based on “group, profile, certificate and role management” categories. Self-service requests can be verified by multifactor authentication, which typically entails sending a text message or an automated phone call to a device to secondarily verify the user’s identity.

Although the product is commercially released, a deployment pack for MIM 2016 will be arriving later this year Microsoft’s announcement indicated. This deployment pack seems rather crucial. It will help automate “the preparation of the privileged identity management environment” and it will help harden that environment by “setting up the privileged AD forest security principals,” among other such details. —K.M.



“When you log into a Windows 10 device you can have it automatically enrolled in the Azure Active Directory domain of your company and have the mobile device management enrolled.”

*Alex Simmons,
Senior Director,
Active Directory,
Microsoft*

“When you log into a Windows 10 device you can have it automatically enrolled in the Azure Active Directory domain of your company and have the mobile device management enrolled. And then you get nice single sign-on between the device and all of your cloud applications,” Simmons says. “And then you’ll see it gain more and more capability as we go forward.”

Among other features added to Azure AD is support for administrative units, “so you can divide up your company into different regions that may be owned by different IT shops,” and a Web proxy that lets Azure AD connect into on-premises applications, Simmons says.

In a move to further expand Azure AD, Microsoft last month released a Public Preview of a business-to-consumer and business-to-business extension to Azure AD for those who want to create trust-based relationships. This will let organizations give access to supply chain partners, Simmons explains. “It’s the equivalent of setting up a trust between two tenants in Azure Active Directory, the difference being that it’s done at an individual group or user level between the tenants. So you wouldn’t just have Microsoft say, ‘I trust Intel,’ it would be Microsoft saying, ‘Oh, I want these five people or these three groups that Intel has specified to be able to use my applications.’”

Simmons also points to the new Passport feature in Windows 10 that lets users authenticate to systems using biometrics, such as facial recognition with systems that have new sensors or fingerprint scanners, “it works with both Azure AD and with Active Directory on-premises, or if you have a hybrid set up between the two.”

In addition to the various IDaaS providers vying to be your identity services provider, Simmons knows new entrants will continue to offer identity and mobility management including one of the latest entrants, VMware Inc. The virtualization giant, which last year acquired enterprise mobility management vendor AirWatch, recently launched VMware Identity Manager. Describing the launch of VMware Identity Manager “as the sincerest form of flattery,” Simmons says: “There are certainly other competitors in the marketplace who we spend more time worrying about and thinking about because they have more innovative solutions.”



“If you look at Microsoft’s architecture for Azure AD and what they deliver, there’s a lot of software required.”

*Todd McKinnon,
CEO, Okta Inc.*

Gartner Inc. analyst Mark Diodati predicts while Azure AD will be a widely deployed IDaaS offering, VMware could, over time, emerge as a formidable competitor. “VMware differentiates with its virtualization and mobile device management from its AirWatch acquisition, Diodati says. “Those are strong capabilities, plus VMware has a large customer base to sell to.”

But all of these IDaaS providers have to ask themselves how they will compete with Azure AD, Diodati says. Azure AD has strong pull-through from Windows 10 and Office 365 and the existing installed base of Active Directory. Still, many third parties offer value-add with more simplified implementation and richer connectivity tools.

On the single sign-on side of things, Diodati says there are a number of considerations customers must weigh such as whether to use a solution that offers standard SAML 2.0 federation technology (which Azure AD supports) or one that favors a password-vaulting approach. Another issue is not all software and SaaS services providers have APIs for user management. “It’s a maturity thing that’s evolving,” he says.

So why would an organization move to a third-party IDaaS from VMware, Okta Inc., Ping Identity Corp., OneLogin Inc. or Centrify Corp., among others, or a password-vaulting platform from the likes of BeyondTrust Inc. or CyberArk Software Ltd.?

“Right now you have to be about being neutral and connecting to thousands of applications, not just Exchange, and not just file and print and not just the Windows client,” says Okta CEO Todd McKinnon. “The heterogeneity is much different this time, our mindset is all about it, we’re not the Azure Active Directory team that is so tightly coupled with Office 365 that they don’t do a good job on other things.”

McKinnon argues Azure AD for hybrid implementations still requires connectivity tools that are much more complex. “If you look at Microsoft’s architecture for Azure AD and what they deliver, there’s a lot of software required,” he says. “You have to have DirSync, it’s now called AD Connect, but it’s DirSync, which is an on-premises script. The logic is on-premises, the failover is all on-premises. You have to have parts of Federated Identity Manager [now Microsoft

One company that offers a number of Active Directory management tools isn't betting against Microsoft or Azure AD: Dell.

Identity Manager (see “Microsoft Identity Manager Replaces FIM”)]. There's a technology legacy. It's clear they haven't started with a clean sheet of paper and said, ‘This thing should run in the cloud it shouldn't connect, of course, to on-premises.’ But all the management, all the failover, all the robustness should be in the cloud, not require a customer to put up a bunch of load balancers and a bunch of server farms, so I think there's just a technology legacy that is apparent in the solution they are delivering today.”

Microsoft's Simmons disagrees with that assessment. “We are the only company making advances on-premises and in the cloud to move your whole hybrid strategy ahead,” he says, arguing Microsoft is more invested in the security of those systems and in building out security capabilities than anybody else. “Some of that is because we have this advantage because we have signals from Office 365, and we have signals coming in from Microsoft account system and we just have this very large aperture of watching what's going on in the hacker world, and we can use all of that data to protect people's accounts.”

Bill Mann, senior VP of products at Centrify, believes there's another variable: “I think Azure Active Directory will be one of the players providing a directory service in the cloud, but I also think other vendors like Google and Amazon will be providing those directory stores,” Mann says.

One company that offers a number of Active Directory management tools isn't betting against Microsoft or Azure AD: Dell. Jackson Shaw, a senior product manager for Dell Software, was at Microsoft in 1999 on the Active Directory launch team, when it was first released in Windows 2000 Server and saw it go from an installed base of 0 to 85 percent when he left Microsoft in 2005.

GetMore Online

See what recommendations Gartner Inc. analyst Mark Diodati gave at the recent Catalyst conference in San Diego at Redmondmag.com/Mackie082115.

“There's probably not a week that goes by where Microsoft isn't adding something new to Azure Active Directory or Azure Active Directory Premium, and they are going to be releasing a lot more capability around threat management,” Shaw says. “I think what you'll see is that gravitational field increases and increases. If I thought there was a real market for an alternative, it's something I'd be pushing Dell to get into.” **R**

Jeffrey Schwartz is editor in chief of Redmond.

CONNECT

Active Directory and Azure AD

How to link Active Directory on-premises with Microsoft Azure AD using Redmond's new connector. BY JOHN O'NEILL SR.

As the number of Microsoft Azure services and users expand, the need for a foundational, shared identity platform is clear. Microsoft is putting significant emphasis on Azure Active Directory (Azure AD) as that shared identity platform.

The challenge for countless IT pros implementing Azure is rooted in the fact migration isn't an instantaneous event.

The challenge for countless IT pros implementing Azure is rooted in the fact migration isn't an instantaneous event. Most organizations won't move 100 percent to the cloud anytime soon. Transitions of this scope occur over many months and often years. In many organizations, computing architectures will always consist of a combination of on-premises and cloud compute and storage resources. The challenge that has emerged is integrating the local, on-premises Active Directory with Azure AD running in the cloud.

Microsoft has supported federation between local Active Directory and Azure AD since the release of the cloud-based version more than two years ago. Unfortunately, Azure AD is complex to implement, fraught with problems and limited in functionality. With the recent release of Azure AD Connect, linking the two is now easier. For most implementations, connecting on-premises Active Directory with Azure AD is now a simple, wizard-based process. With just a handful of clicks, local Active Directory accounts and passwords are

Express Wizard automatically configures password synchronization from the local Active Directory server to Azure AD.

synchronized into Azure AD for use by all Azure services. These accounts can then be used for signing into Office 365, Azure Site Recovery and even Azure RemoteApp.

Don't let the Azure AD Connect Express Wizard fool you. The tool is still performing many product installations and configuration tasks. Products installed by Azure AD Connect include:

- Azure AD Connector
- SQL Server 2012 CLI Utilities
- SQL Server 2012 Native Client
- SQL Server 2012 Express LocalDB
- Azure AD Module for Windows PowerShell
- Online Services Sign-in Assistant for IT Pros
- Visual C++ 2013 Redistribution Package

In addition to installing these products, the Express Wizard automatically configures password synchronization from the local Active Directory server to Azure AD, defines synchronizing all local AD object attributes and kicks off an initial synchronization (see **Figure 1**). The Express Wizard can only be used to synchronize a single local AD Forest with Azure AD.

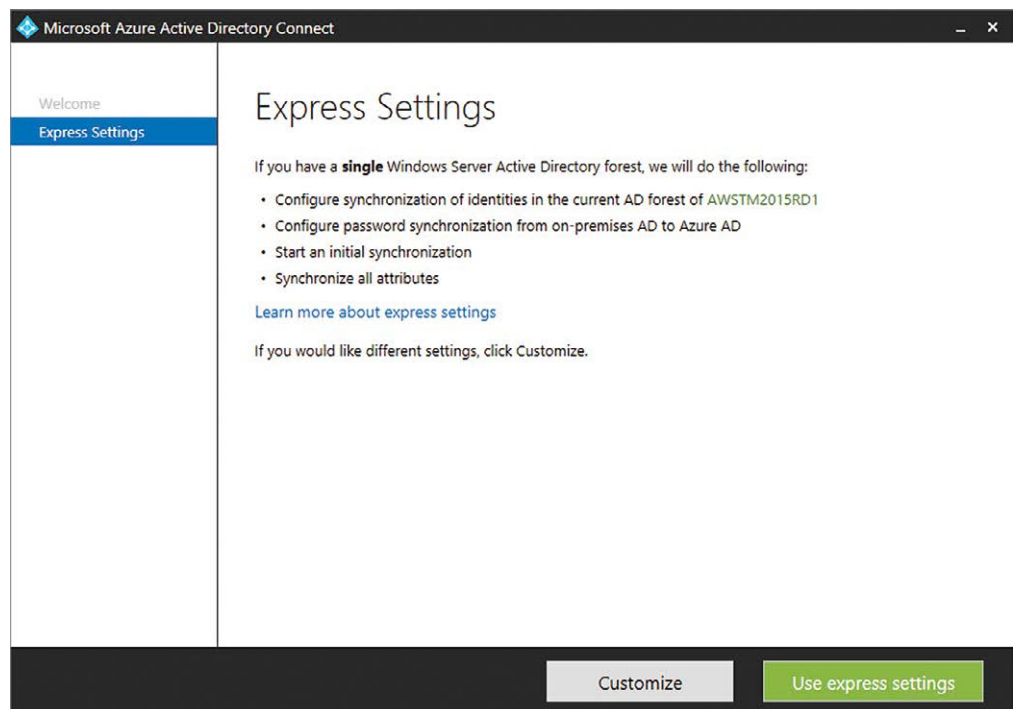


Figure 1. The Azure AD Connect Express Wizard is ready to run.

The Azure AD Connect Express Wizard supports 100,000 local AD objects using SQL Express.

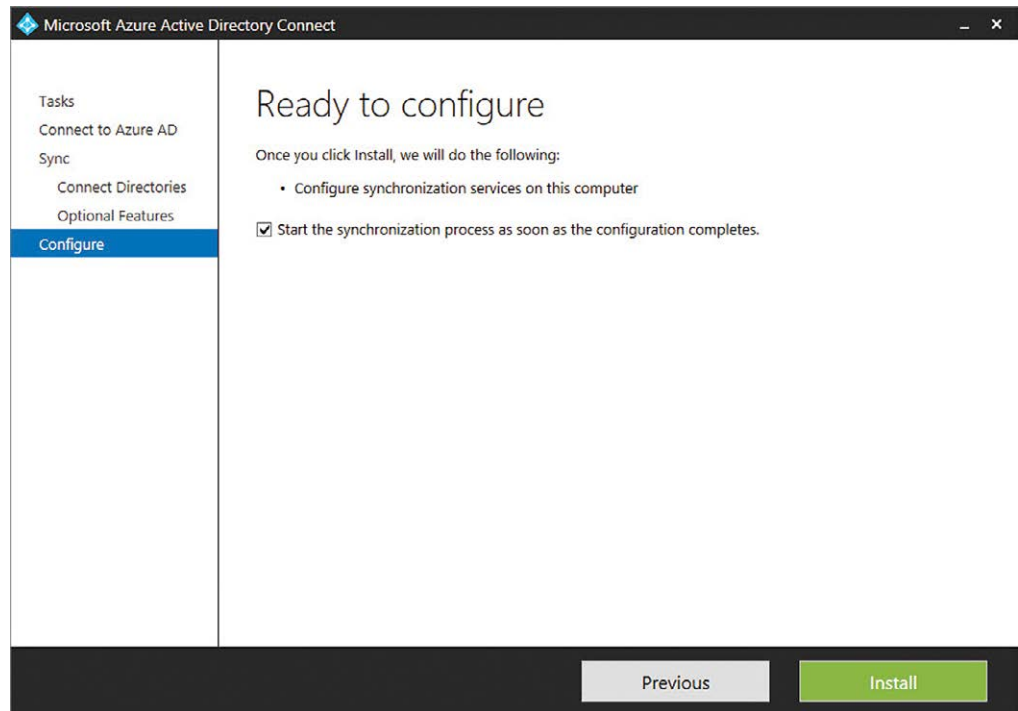


Figure 2. *Manual synchronization in Azure AD Connect.*

Azure AD Connect, like any software, does have a few prerequisites. First, Azure AD Connect must be installed on Windows Server 2008 or later. Unlike previous versions of the DirSync tool, Azure AD Connect is supported when installed on a domain controller. Still, I recommend running the tool on a member server and leaving the DC to focus on being a DC.

Additionally, the Azure AD Connect Express Wizard supports 100,000 local AD objects using SQL Express. More than 100,000 objects requires using a full version of SQL Server. Finally, the local AD domain and forest functional levels must be Windows Server 2003 or later.

After the Azure AD Connect Express Wizard completes an initial synchronization, a scheduled task is created to synchronize the directories every three hours. Running an on-demand synchronization isn't a problem, though. The scheduled task can be kicked off manually. Another option is to run the Azure AD Connect tool again, select the Customize synchronization options task when prompted, Click Next, enter the Azure AD admin credentials, click Next, enter the local AD enterprise admin credentials, click Next, leave the default Optional Features checked, click Next, ensure the box for

An Azure account is an obvious prerequisite for setting up directory synchronization.

Start the synchronization process as soon as the initial configuration completes is checked, and click Install (see **Figure 2**). The tool will quickly prompt that configuration to complete so the synchronization process will be initiated.

An Azure account is an obvious prerequisite for setting up directory synchronization. If needed, sign up for a 30-day trial using a valid Microsoft Account at bit.ly/1VyZIMd. Use any valid Microsoft Account including an Office365 account. The process for signing up for an Azure account is simple:

1. Click Try It Now
2. Sign in using the Microsoft Account
3. Enter name, e-mail, phone and company name
4. Select Region
5. Verify the account by text or phone call
6. Verify by credit card (annoying, I know)
7. Agree to licensing terms
8. Watch paint dry or water boil for 5 minutes or so
9. Click Start Managing My Service
10. Sign in using the Microsoft Account again, if prompted

Complete the next steps using the Azure Management Portal (bit.ly/1Ochv7J):

1. Click Active Directory from the list on the left
2. Click New
3. Click Directory
4. Click Custom Create
5. Enter a friendly display name for the directory
6. Enter the domain name that will preface
.onmicrosoft.com; for instance, AWSTM2015RD1 becomes
AWSTM2015RD1.onmicrosoft.com
7. Select the appropriate Country or Region
8. Click the checkmark to create the directory in Azure

Azure accounts use a default domain name of onmicrosoft.com. This domain is appended to the user-specified domain resulting in something like TM2015RD1.onmicrosoft.com. Usernames are then of the sort JONeillSr@TM2015RD1.onmicrosoft.com. Add a custom domain, for example AWSTM2015RD1.com, so that users can sign in with familiar user names such as JONeillSr@AWSTM2015RD1.com.

The process isn't difficult, but there are some hoops to jump through to verify proper domain ownership. This prevents cyber squatters and the like from hijacking someone else's domain in Azure. As usual, begin by signing into the Azure Management Portal:

There are some hoops to jump through to verify proper domain ownership.

1. In the left-side column, scroll down to Active Directory
2. Click the name of the directory created earlier
3. Click Domains
4. Click Add a Domain
5. Specify the already registered Internet domain name (see **Figure 3**); AWSTM2501RD1.com in this instance
6. Clear the checkbox for I plan to configure this domain for single sign-on with my local Active Directory; this option requires deploying full AD FS servers on-premises
7. Click Add
8. Click Next
9. Record the DNS information necessary to verify domain ownership
10. On the external Internet-accessible DNS server open DNS Manager
11. Expand the forward lookup zone for the domain
12. The next steps vary, depending on the Windows Server version in use on the DNS server

Figure 3. Adding a Domain.

In cases where multiple DNS servers exist, ensure replication occurs before moving forward.

If using Windows Server 2003 on the DNS server:

1. Right-click the domain folder to which you want to add the SPF record
2. Click Other New Records
3. In the Select a resource record type list, click Text (TXT), and then click Create Record
4. A parent domain record is being added so leave the Record name box blank (do not use @)
5. In the Text box, type MS={TXT record details recorded from Azure Management Portal}. For instance, type MS=ms71067285
6. Click OK
7. Click Done

If using Windows Server 2008/2012 on the DNS server:

1. On the DNS Manager page for the domain, go to Action, then Text (TXT)
2. In the New Resource Record dialog box, make sure that the fields are set to precisely the values displayed in the Azure Management Portal wizard
3. Choose OK

In cases where multiple DNS servers exist, ensure replication occurs before moving forward.

If hosted DNS is used, Microsoft offers a resource on how to manage those records at various providers (see bit.ly/1N0gUpJ).

Once the DNS changes have been made and replicated to all DNS servers, return to the Azure Management Portal and Click Verify. If all is well, "Successfully verified the domain" will display and then click the checkmark to continue.

From the local server where Azure AD Connect will be installed, sign in to the Azure Management Portal:

1. Click Active Directory from the list on the left
2. From the displayed list click the Azure AD Directory name created earlier
3. Step two of the Quick Start wizard is "Integrate with your local directory," under this click Download Azure AD Connect

4. A new tab opens, which is the download link for Azure AD Connect
5. Click the Download button
6. Click the arrow next to save, then click Save and Run
7. Azure AD Connect will download and automatically run setup

Quick tip: When using Internet Explorer in Windows Server 2012 R2, the message, "Your current security settings do not allow this file to be downloaded," may appear when trying to download a file such as the Azure AD Connect Installer. Here's how to enable downloading in Internet Explorer:

1. Click the gear icon
2. Click Internet Options
3. Click the Security tab, then click Custom Level
4. Scroll down to Downloads, File Download, and click the Enable radio button, as shown in **Figure 4**
5. Click OK
6. Click Yes to confirm
7. Click OK
8. Retry the download; it should work fine

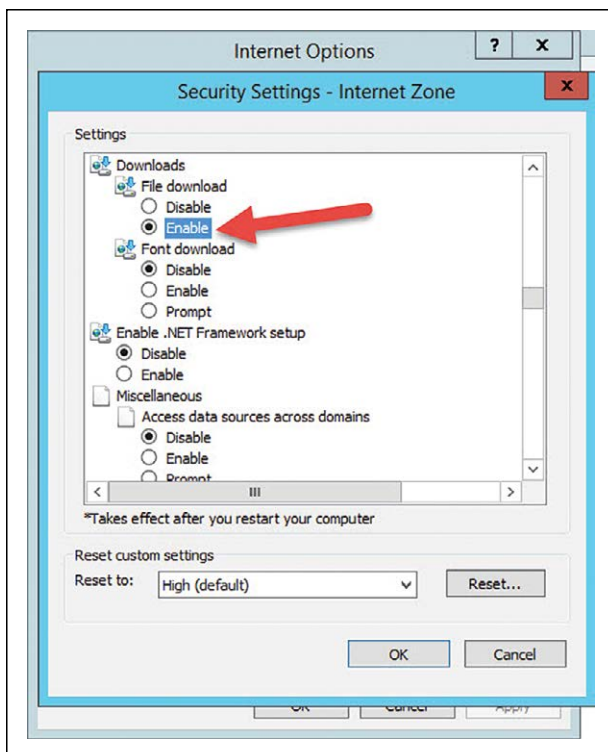


Figure 4. Enabling downloads in Internet Explorer.

Once the Azure AD Connect setup starts, it's only a few clicks to have it running!

1. Click the checkbox to agree to the license terms, then click Continue
2. Click Use Express Settings
3. Wait briefly while necessary components are installed
4. Enter the Azure AD Global Administrator credentials, then click Next. The Azure AD Global Administrator is the Microsoft Account used when creating the Azure account
5. Wait while a connection to Azure is made and the credentials verified
6. Enter the local Active Directory Enterprise Administrator credentials, then click Next
7. Wait briefly while the local AD account is verified

8. Ensure the checkbox is selected to “start the synchronization process as soon as the configuration is complete,” then click Install; this doesn’t take long, but now is a great time to grab a fresh energy drink from the fridge
9. Once configuration is complete, click Exit

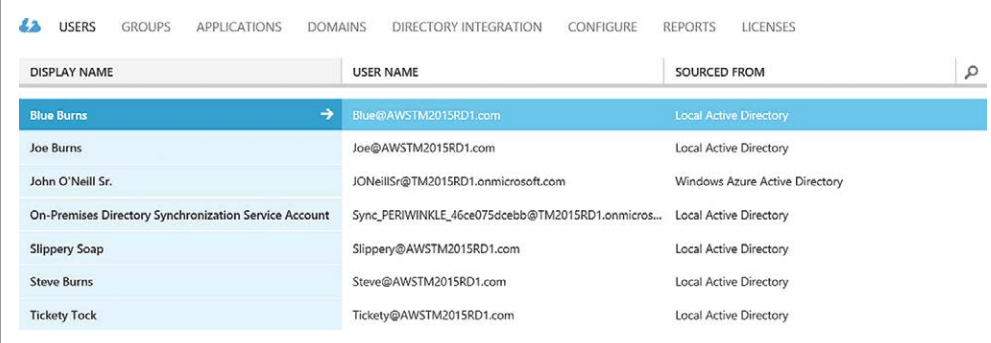
Bingo! Local AD and Azure AD are now synchronizing accounts. Verify local accounts are present in Azure AD by signing in to the Azure Management Portal:

1. Click Active Directory from the list on the left
2. Click the Azure AD Directory name in the displayed list
3. Click Users
4. Verify the on-premises AD user accounts are listed (see **Figure 5**)

Some features, such as specific reports and the AD Connect Health tool, require an Azure AD Premium license.

Some features, such as specific reports and the AD Connect Health tool, require an Azure AD Premium license. Sign up for an Azure AD Premium trial through the Azure Management Portal:

1. Click Active Directory from the list on the left
2. Click the Azure AD Directory name in the displayed list
3. Step three of the Quick Start wizard is “Get Azure AD Premium,” under this click Try it now
4. Click the Try Azure Active Directory Premium now link
5. Click the Checkmark
6. The Web page will display “Activating your Azure Active Directory Premium trial;” wait a couple moments, then click the link to refresh
7. The Azure AD Premium licenses are displayed with 100 Active and none assigned



DISPLAY NAME	USER NAME	SOURCED FROM
Blue Burns	Blue@AWSTM2015RD1.com	Local Active Directory
Joe Burns	Joe@AWSTM2015RD1.com	Local Active Directory
John O'Neill Sr.	JONellSr@TM2015RD1.onmicrosoft.com	Windows Azure Active Directory
On-Premises Directory Synchronization Service Account	Sync_PERIWINKLE_46ce075dcebb@TM2015RD1.onmicros...	Local Active Directory
Slippery Soap	Slippery@AWSTM2015RD1.com	Local Active Directory
Steve Burns	Steve@AWSTM2015RD1.com	Local Active Directory
Tickety Tock	Tickety@AWSTM2015RD1.com	Local Active Directory

Figure 5. Local AD users in Azure AD.

It's taken Microsoft a few iterations, but connecting local AD and Azure AD is now a simple point-and-click affair.



John O'Neill Sr. will demonstrate how to link Active Directory and Azure AD with Azure AD Connector at TechMentor/Live! 360 next month in Orlando, Fla.

REPORT	DESCRIPTION
ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
Users with leaked credentials	Users with leaked credentials
ACTIVITY LOGS	
Audit report	Audited events in your directory
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
Self service groups activity	Provides an activity log to all group self service activity in your directory
INTEGRATED APPLICATIONS	
Application usage	Provides a usage summary for all SaaS applications integrated with your directory.
Account provisioning activity	Provides a history of attempts to provision accounts to external applications.
Password rollover status	Provides a detailed overview of automatic password rollover status of SaaS applications.

Figure 6. The Premium Reports available in Azure AD Premium.

8. Click Azure Active Directory Premium
9. Click Assign users
10. In the Show dropdown list select All Users, then click the checkmark
11. Select the users to assign premium licenses; multiple users can be selected using Ctrl+Click
12. Click the Assign button
13. When completed, click the previous arrow to go back to the domain management page
14. Click reports and notice that all premium reports are now available (see **Figure 6**)

It's taken Microsoft a few iterations, but connecting local AD and Azure AD is now a simple point-and-click affair. As Azure services are in the plans for more and more organizations, connecting these directories early on makes perfect sense. If you're using Office 365, Azure Site Recovery or any other Azure service, give Azure AD Connect a go. Odds are, you won't regret it. **R**

John O'Neill senior is a Microsoft MVP and has 20 years of experience as an IT pro working in various roles as a consultant, architect, executive, speaker and author. Follow him on Twitter @JohnONeillSr.



for the Changing Workplace

Windows Server 2016 Technical Preview 3 introduces major changes to Active Directory including LDAP v3 authentication via AD FS and sign-on support using biometrics, OpenIDConnect and OAuth. BY JOHN O'NEILL SR.

Windows Server 2016 will likely end up introducing the most significant updates to date in the evolution of Active Directory.

Windows Server Active Directory first appeared 15 years ago with the launch of Windows 2000 Server. It had the ambitious aspiration at the time taking on Novell Directory Services, what was then the incumbent default enterprise network directory. While Active Directory didn't become pervasive overnight, Microsoft ultimately achieved critical mass by enhancing it in various ways over the years. It did so by always adhering to the same basic structure as when it first debuted so long ago.

Windows Server 2016 will likely end up introducing the most significant updates to date in the evolution of Active Directory. While it's true Active Directory is still backward-compatible with the directory services model enterprises use today, Microsoft is introducing a number of new or improved features and capabilities into Active Directory.

Windows Server 2016 Active Directory can still do the same things it always does with domain controllers today, but it also introduces a variety of new or enhanced capabilities.

In order to understand the nature of these changes, it's important to realize things were much different when Microsoft introduced Active Directory. When Microsoft released Windows 2000 Server, the idea of operating in the cloud was unheard of. In fact, basic Internet connectivity was just first starting to take off. Consequently, Active Directory was designed to be an enterprise-level authentication and policy control mechanism, and that's really about it.

Today things aren't so simple. Organizations typically have resources in the local datacenter, in remote datacenters, in Software-as-a-Service (SaaS) clouds, and in Infrastructure-as-a-Service (IaaS) clouds. Active Directory was never designed to function in IT environments where resources are so widely decentralized.

This is where Windows Server 2016 Active Directory comes into play. Windows Server 2016 Active Directory can still do the same things it always does with domain controllers today, but it also introduces a variety of new or enhanced capabilities to help organizations cope with the decentralized nature of today's IT resources.

Active Directory Federation Services

One of the Active Directory components that has received a lot of attention over the last few years is Active Directory Federation Services (AD FS). AD FS is a Windows Server component that provides users with single sign-on access to IT resources that are located outside of traditional organizational boundaries. Today the most common use for AD FS is probably allowing Active Directory users to seamlessly access Microsoft Office 365.

As well as AD FS works, however, its primary limitation to date is that it's designed to work with Active Directory. Although most organizations have Active Directory in place, larger organizations may also have any number of non-Microsoft directories from the likes of IBM Corp., Oracle Corp. or even legacy Novell, among numerous others. In the past, there hasn't been a way to seamlessly connect users of these directories to Office 365 or other line-of-business (LOB) apps.

In Windows Server 2016, Microsoft is adding support for any LDAP v3 directory. This means users with accounts in non-Microsoft

Any LDAP directory will be able to authenticate user accounts and will communicate with the AD FS server in order to establish claims-based authentication.

directories will be able to authenticate through AD FS and access Office 365 or other LOB apps, so long as the directory is LDAP v3 compliant.

To understand how this LDAP support works, it's important to understand how AD FS normally handles Office 365 connectivity. Users, when they log in, are authenticated by a DC. When the login is complete, the DC issues a Ticket Getting Ticket, which is stored in a cache on the user's desktop.

For example, if the user decides to access Microsoft Office 365, the login page redirects the browser to the Microsoft Federation Gateway. At this point, the user can enter his regular domain credentials. Upon doing so, the Microsoft Federation Gateway contacts the organization's AD FS server. The AD FS server acquires the user's Ticket Getting Ticket and presents it to the DC, which responds by issuing a service ticket. This service ticket is sent to the AD FS server and establishes the user's identity. With this service ticket in hand, the AD FS server can contact Active Directory and request a series of attributes for the user. One of the attributes returned in this exchange is the user principal name (UPN). AD FS then uses this information to create a token, which is passed through the user's Web browser, back to the Microsoft Federation Gateway. The gateway verifies the authenticity of the token and then creates its own token, which contains the user's UPN. This token is sent back to the user's Web browser and is then used to log the user into Office 365.

This process is sometimes referred to as claims-based authentication. A claim is really nothing more than the assertion of a piece of information such as a name or a UPN. A claim is issued by a claims provider and then encapsulated into a security token.

A claims provider also acts as an authentication mechanism. As such, Active Directory is treated as a local claims provider. The way Microsoft is enabling LDAP v3 support for AD FS is each LDAP directory will be treated as a claims provider. In other words, any LDAP directory will be able to authenticate user accounts and will communicate with the AD FS server in order to establish claims-based authentication.

Added support for LDAP v3 means users with accounts in non-Microsoft directories will be able to authenticate through AD FS and access Office 365 or other line-of-business apps.

The nice thing about this approach is that in some cases it eliminates the need for forest-level trusts. LDAP directories and Active Directory can communicate with the AD FS server without the need for any sort of trust relationship between one another. This same basic principle can also apply to organizations that have multiple Active Directory forests. Such organizations will be able to connect each Active Directory forest to AD FS without the need for directory-level trust. This might be especially useful in the case of corporate mergers or acquisitions.

Although AD FS has been discussed primarily with regard to its support for LDAP v3, Microsoft has introduced a significant number of new AD FS-related features in the most recent Windows Server 2016 Technical Preview. Although space limitations prevent explaining all of the new features in detail, some of the AD FS-related changes are geared toward developers, such as enhancements for building modern applications with OpenIDConnect and OAuth. Other features, however, are designed to simplify deployment, such as enhanced support for geo deployments using SQL with merge replication and support for certificate-based authentication (smart card authentication) over Port 443.

Microsoft Passport

Microsoft is also introducing a number of security enhancements for Active Directory. One of the most useful new security features is Microsoft Passport, which isn't to be mistaken for the Microsoft Passport the company offered several years ago.

The new Microsoft Passport is an authentication mechanism designed to overcome some of the problems with password-based authentication. Passwords are not only easily forgettable, they're not a true proof of identity, because anyone who knows a user's credentials can log in as that user.

Windows 10 seeks to decrease reliance on passwords by introducing PIN and biometric authentication capabilities (see the June 2015 cover story, "Hello, Windows 10," at bit.ly/1hXuPD4). PIN-based authentication requires a user to enter a four-digit numerical code rather than entering a password. Microsoft claims PIN-based authentication is more secure than password-based authentication because the PIN is device-specific and cannot be used remotely. Biometric authentication in Windows 10 can be based on a user's

Azure AD Join is similar to the Workplace Join feature, but is designed to provide a better overall experience.

fingerprint, eyes, or face, but requires special hardware such as a fingerprint scanner or a facial recognition camera. The nice thing about biometrics (or PINs for that matter) is a password can't be stolen as it is typed in or transmitted across the network.

The problem with relying solely on biometric authentication is Active Directory was originally designed to support the use of passwords or smart cards—not biometrics or PINs. This is where Microsoft Passport comes into play.

Most modern hardware is equipped with a TPM chip that allows cryptographic keys to be stored at the hardware level. During the login process, the user uses a PIN or biometrics to gain access to the device. Upon doing so, the device OS sends the authentication information to an identity provider (in this case, Active Directory). The device then creates a public key, which it signs and sends to the identity provider for registration. The identity provider registers the key and then requests the device sign in using its private key. If the sign on is valid then the identity provider issues an access token that allows access to protected resources.

Azure AD Join

While enterprise client PCs are commonly joined to an Active Directory domain, mobile devices cannot usually be domain-joined. This means such devices cannot be secured by Group Policies, nor can the device identity be stored in Active Directory.

Microsoft attempted to address this problem in the previous version of Windows with its Workplace Join feature (see the February 2015 article, “Manager Mobile Devices and Policies in Active Directory,” at bit.ly/1NcPH65). This feature still exists in Windows 10, but has been renamed to Work Access. Workplace Join didn't allow mobile devices to be joined to Active Directory in the traditional sense, but authorized users could enroll their devices in an Active Directory-based workplace in order to gain access to protected resources.

With Workplace Join, it was difficult to set up and it could only be used to control access to specific types of resources. In Windows Server 2016, Microsoft is introducing Azure AD Join. Azure AD Join is similar to the Workplace Join feature, but is designed to provide a better overall experience.

In the case of a corporate device such as a Windows PC joined to Active Directory, users are able to log in using their regular Active Directory credentials.

The Workplace Join feature was designed to provide access to protected resources for users working from personal devices. Azure AD Join can still do that, but it's also designed to work with corporate-owned, Active Directory-joined devices, as well as corporate devices that aren't Active Directory-joined (such as tablets and phones).

In the case of a corporate device such as a Windows PC joined to Active Directory, users are able to log in using their regular Active Directory credentials. Upon doing so, they'll be able to access the Windows Store without the need for a personal Microsoft account. A user can add a personal Microsoft account to the machine but doing so only enables single sign-on for work/personal resources. It doesn't cause the user's settings to be roamed.

In the case of corporate-owned devices that aren't domain-joined, users are able to log in using Azure AD credentials. Upon authenticating into Azure AD, the user is able to perform a self-service device setup and the setup process automatically registers the device in Azure AD and enrolls the device for mobile device management (assuming Azure AD Premium is being used). As was

At a Glance

- Connectivity to any LDAP v3 directory, enabling accounts in non-Microsoft directories to authenticate through AD FS and access Office 365 or other line-of-business apps.
- OpenIDConnect and OAuth support for developers building modern applications
- Enhanced support for geo deployments using SQL with merge replication
- Enables certificate-based authentication (smart cards and so on) over Port 443
- Microsoft Passport to allow biometric and PIN (device-centric) authentication
- Azure AD Join to provide a better login experience than the prior Workplace Join feature

Personal Microsoft accounts are primarily used with personal devices.

the case for a domain-joined device, there's no requirement for the user to associate a personal Microsoft account with the device.

Personal Microsoft accounts are primarily used with personal devices. A user can log in to a personal device using a personal Microsoft account and use the device in the same way as before. Users who want to access corporate resources are able to add either an Active Directory or an Azure AD account to the device, which will provide the user with SSO access to protected resources. It's also possible to use conditional access control to limit access to corporate resources based on the device. For example, an administrator might create a policy that requires mobile devices to be secured with a PIN and to use device-level encryption. Conditional access control is an Azure AD Premium feature.

Looking at Windows Server 2016 TP3, the next release of the server OS promises some very welcome improvements to Active Directory, especially with regard to security. These enhancements will allow for use of non-Microsoft LDAP directories, biometric authentication and conditional access control for mobile devices. **R**

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.
