Unified hybrid Active Directory

Five challenges you can overcome today

by One Identity

ONE IDENTITY by Quest

Table of Contents

ONE IDENTITY by Quest

Active Directory

is everywhere and Azure Active Directory (Azure AD), its cloud-based cousin, is growing rapidly. Currently, more than 95 percent of organizations worldwide use Active Directory (AD) and/or Azure AD.

AD is unavoidable and necessary for on-prem user authentication and authorization. You must go through AD. It's just how it's done. Now, mix in the cloud – and Azure AD– and your management complexity increases significantly. You could be in for a world of pain, if your on-prem or cloud identity environments are not managed, secured and synched properly.

95%

of organizations worldwide use Active Directory (AD) and/or Azure AD.

Today, there are north of 345 million Azure AD monthly active users and more than 30 billion Azure AD authentication requests a day. The majority of these transactions are to access the extremely popular productivity applications available via Microsoft 365, such as Teams, Exchange, SharePoint, OneDrive, etc., as well as other SaaS applications. However, reliance on the Azure platform continues to grow for traditional identity activities, such as multifactor authentication (MFA), federation, and self-service password reset management. It's important to note that most of these expanded capabilities are only available via Azure Active Directory Premium version, which is significantly more expensive than the Azure AD functionality necessary to use Office 365.

In all but the rarest of cases, organizations that adopt cloud-focused Azure AD do so while still firmly rooted in the on-prem AD world. This poses a huge and unexpected issue - Azure AD is not simply a cloud-based copy of an on-prem AD instance. It is a wholly separate environment. In other words, in organizations where on-prem AD and Azure AD coexist and are equally critical to success, the organization – and the IT team – must manage a two-part, hybrid AD environment.

The sprint to the cloud is fraught with complexity, risk and inefficiencies. If implemented and managed improperly, it can cause headaches or worse for your AD administrators and users. This ebook addresses five challenges that most organizations must overcome as they attempt to navigate the transition to a hybrid AD implementation.

Azure AD is not simply a cloud-based copy of an **on-prem AD instance**.

Challenge 1

Two tools too many

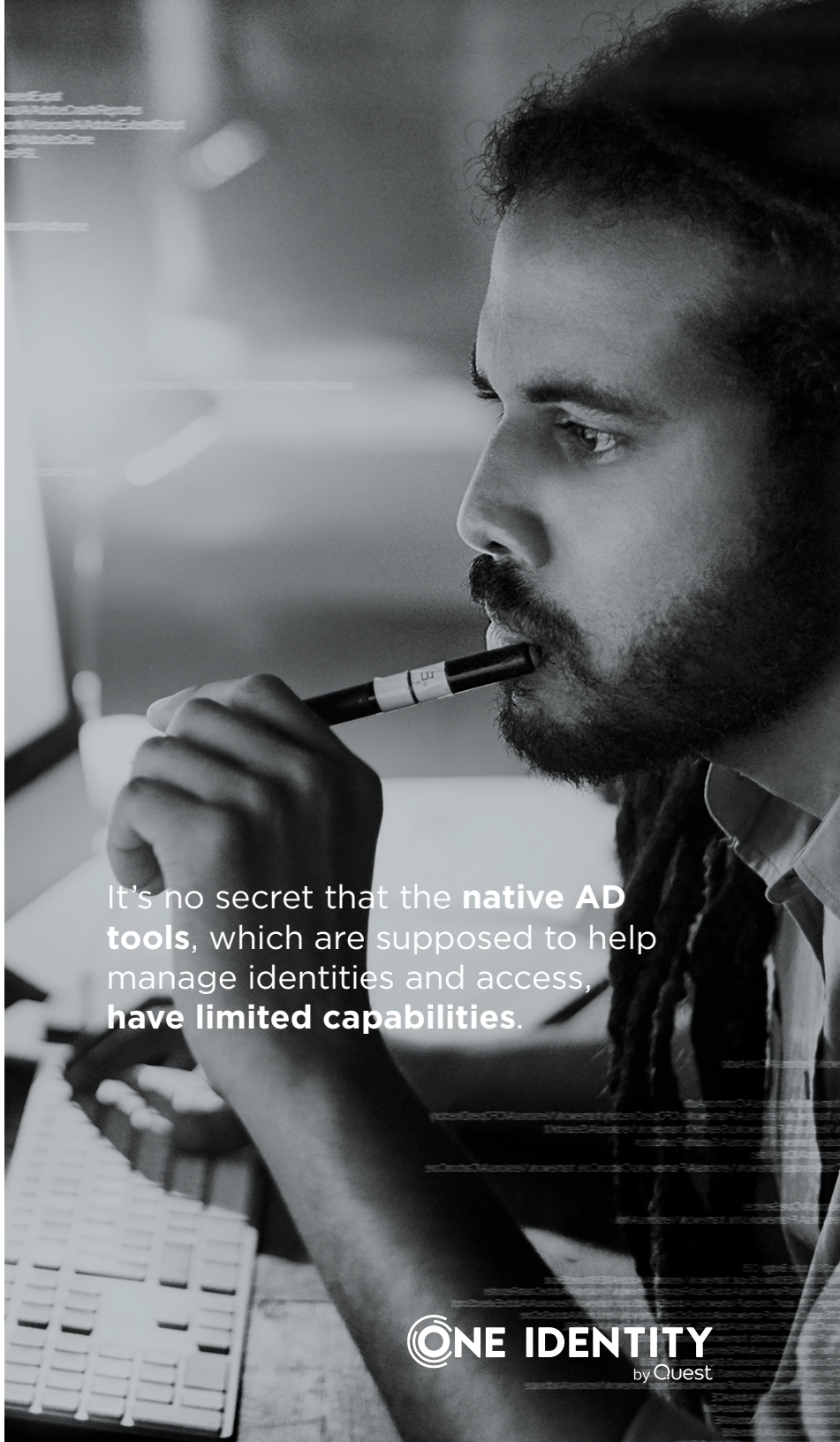
It's no secret that the native AD tools, which are supposed to help manage identities and access, have limited capabilities. Even with earnest efforts to improve native Active Directory Users and Computers (ADUC) tool, most organizations choose to adopt a third-party tool to streamline, automate and bring consistency to AD management tasks.

The situation is only exacerbated as organizations adopt Azure Active Directory (Azure AD). Azure AD does not use ADUC and requires its own management tool for basic administrative tasks.

To execute the same action, such as provisioning a user, in AD and Azure AD requires the use of separate tools with entirely unrelated interfaces, disparate functionality and divergent training methodologies. Therefore, an already cumbersome task for on-prem AD becomes doubly so when it must be duplicated for Azure AD. Again, Azure AD is not simply a cloud-version of AD. As a result, home-grown scripts, PowerShell automation and manual processes cannot be easily applied to Azure AD.

Pain Remedy 1: One tool to rule them all

The ideal solution to the two-tool challenge would be a single tool that overcomes the native limitations of ADUC and Azure AD's administrative interface. That tool exists in One Identity Active Roles. Active Roles provides a layer of automation, consistency, and ease-of-use that makes every administrative task for AD and Azure AD quick, easy, and accurate. Thousands of organizations rely on Active Roles every day to ensure the efficiency and security the administration of their on-prem AD demands. Today, those organizations can apply that same rigor and efficiency to Azure AD.



Active Roles' intuitive interface optimizes day-to-day administration and help-desk operations for hybrid AD environments via an MMC snap-in and a web interface. With support for multi-tenant, Active Roles provides single-action task execution for hybrid AD environments. Admin-users report significant time savings (often more than 80 percent) using Active Roles. They also report a dramatic increase in security (i.e., less opportunity for user error).

In fact, Active Roles provides administrative and workflow templates that ensure administrative tasks in the hybrid AD environment are executed correctly.

Inconsistent processes — typically called **workflows** — are often the culprit behind **synchronization** and **provisioning errors**.

ONE IDENTITY by Quest

Challenge 2

Inconsistency

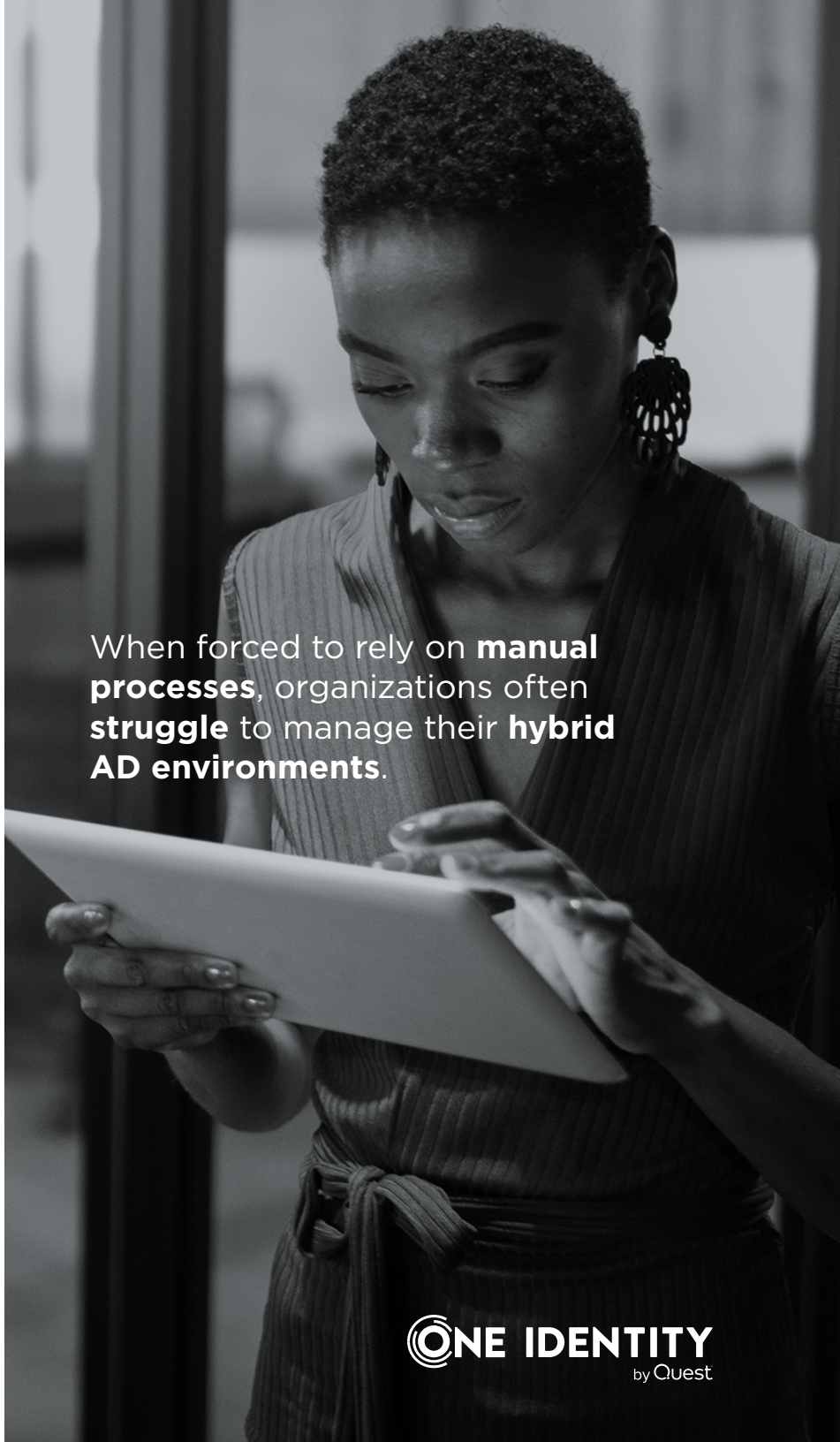
When forced to rely on manual processes, organizations often struggle to manage their hybrid AD environments. Typically, they do the best they can but fall into bad habits of 'just get it done' with little thought on how it should be done.

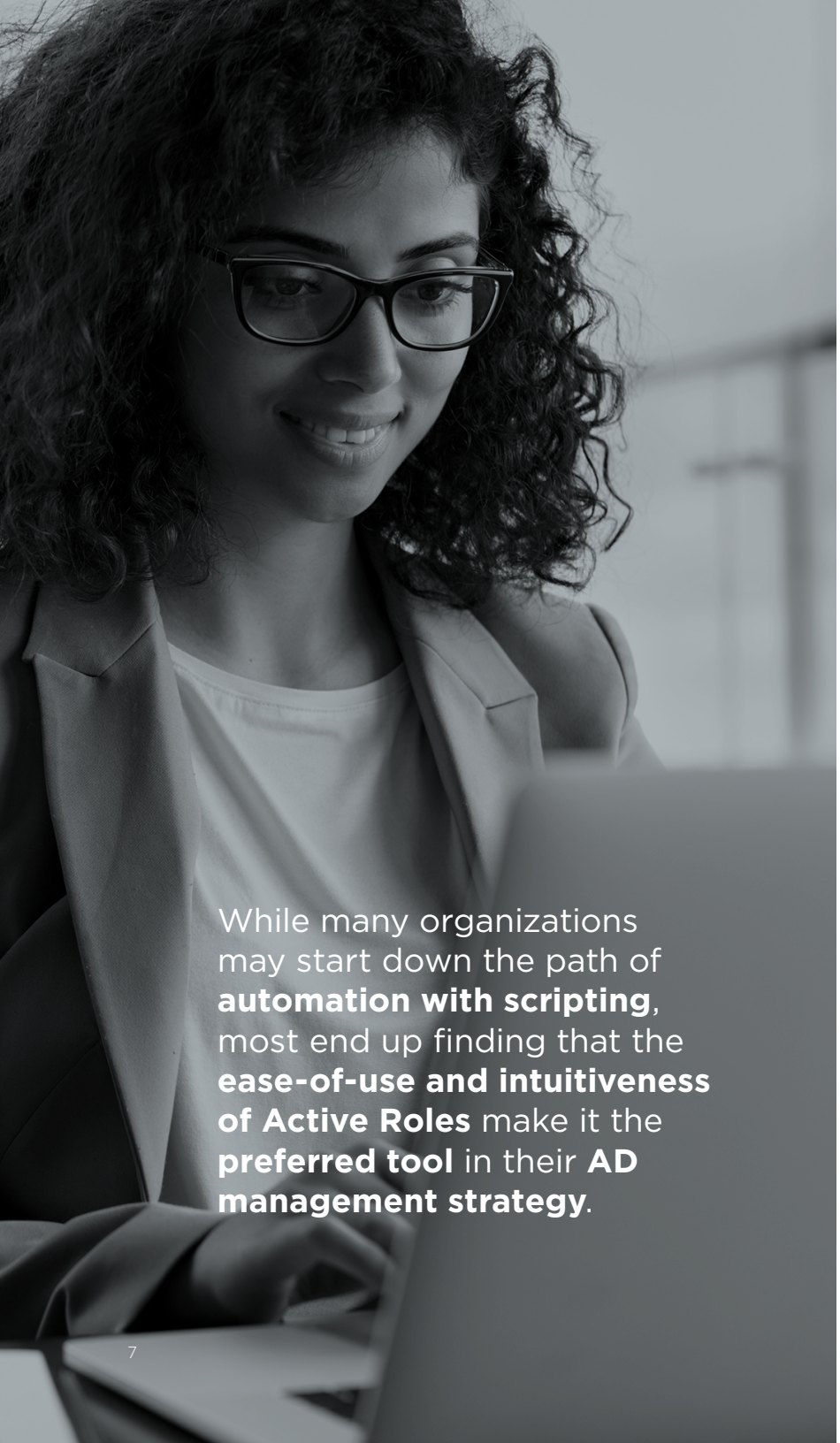
It's understandable: We have impatient users demanding immediate results; native management tools with limited capabilities that make it difficult to do things consistently in one environment, much less two. Finally, this leads to overreliance on tribal knowledge and 'that's how it's always been done.'

These processes — typically called workflows — are often the culprit behind synchronization and provisioning errors. Typical areas of inconsistency for the hybrid AD environment include:

- Aligning group membership with job role in both AD and Azure AD
- Gaining appropriate line-of-business approvals for provisioning actions
- Assigning correct permissions to individual admins (least-privilege model)
- Designing easily repeatable processes for particular tasks

As Azure AD is not simply a cloud copy of AD, consistency does not mean you cut and paste an on-prem AD workflow into the cloud, such as PowerShell-scripted workflow. However, it does mean ensuring that your workflows address the unique needs of both AD and Azure AD.





Pain Remedy 2: Templates are cool

Active Roles includes pre-defined workflow templates for AD and Azure AD (individually and for hybrid environments) that are based on the experience and innovation of thousands of organizations that use Active Roles to automate, streamline and secure the administration of their hybrid AD environments.

These **templates** include everything from **provisioning actions** in the directories, **seeking approval** from the appropriate line-of-business (LOB) managers, **making additions to groups**, DL membership assignment in Exchange/Exchange Online and virtually every imaginable scenario.

In fact, Active Roles includes out-of-the-box access templates for Microsoft 365 and Exchange.

Moreover, Active Roles includes customizable templates and workflows to address the unique needs of any organization. While many organizations may start down the path of automation with scripting, most end up finding that the ease-of-use and intuitiveness of Active Roles make it the preferred tool in their AD management strategy. Its depth of coverage – including the hybrid AD environment – and legacy of helping organizations overcome the toughest AD/Azure AD challenges, make Active Roles the industry-leading Active Directory management and security solution.

ONE IDENTITY by Quest

Challenge 3

It all starts with provisioning

Much of the AD/Azure AD-management burden is from user provisioning. This involves setting up accounts in the directory, placing people in the correct groups, and making sure they have access to the proper accounts and access to all the necessary applications such as Exchange, SharePoint, Microsoft 365 – and myriad other cloud-based applications that are available via Azure AD. But setting up the accounts is one thing, turning them off (or de-provisioning) is another and, perhaps, the more important. After all, the risk associated with a terminated employee retaining access to valuable intellectual property is extremely high – but easily avoidable with the right tools.

As discussed earlier, native tools simply do not cut it when it comes to provisioning. Setting up on-prem access requires use of ADUC for AD, a different interface and process for Exchange, and the list goes on-and-on. That does not even bring into account the additional tools required to set up the same individual in Azure AD and all its associated cloud services.

There are a number of challenges with provisioning/re-provisioning/de-provisioning in the hybrid AD environment, namely:

- The use of multiple native tools introduces significant room for human error and inconsistencies. Access is determined by the way you configure user accounts. If this is done incorrectly, then the access provided is wrong.

Native tools do not cut it when it comes to **provisioning**.

- The amount of time it takes to "fully" provision a user in the hybrid environment means that users may experience long periods of inactivity and lack of productivity waiting for access to be granted.
- Delays in de-provisioning (or re-provisioning) introduce risk as inappropriate access may be retained long after it should have been terminated.
- The authoritative data source (typically, an HR system) is difficult to enable for AD, not to mention Azure AD, resulting in large amounts of human intervention required to do the most basic provisioning/re-provisioning/de-provisioning action.
- Synchronization between AD and Azure AD cannot be relied on if the original AD data is flawed – a direct result of provisioning errors.

The bottom line is: If you cannot get provisioning right, you cannot proceed with confidence in the security or efficacy of your hybrid AD environment.

Pain Remedy 3: Provisioning done right … and done once

So how do you get provisioning right? To start, eliminate the potential for human error. This is done through a single tool that provides thorough provisioning (and de-provisioning) coverage for both AD and Azure AD. Active Roles is one such tool. Using template workflows and automation, Active Roles streamlines the hybrid AD provisioning process to a single action – including AD, Azure AD, Exchange, SharePoint, Microsoft 365 and many other SaaS applications.

But it doesn't stop there. When a user's access needs to be changed or removed, updates are made automatically across all relevant systems (such as the HR system) and applications in the hybrid AD environment, as well as any AD-joined systems, such as Unix, Linux and Mac OS. With Active Roles, incidents of human error, oversight or malice are virtually eliminated.

Challenge 4

A syncing ship

Azure AD includes a capability called Azure AD Connect, which synchronizes users, groups, attributes, and passwords from the on-prem AD to Azure AD. This single capability accelerated the adoption of Microsoft 365 – the smooth migration of legacy Office users to the cloud, often without user realization. It enables users to login once to access on-prem and cloud-based resources seamlessly and easily.

Of course, this smooth migration is much easier said than done.

Typically, **security** for the cloud-based access is based on **permissions and memberships established** in the on-prem AD world.

Any errors, risk factors or security gaps that exist in the on-prem AD – perhaps caused by limitations of the native tools – will replicate to the Azure AD environment.

For example: Let's say that you have a group in AD called Finance and employee A was added to the group as a necessity when employee B was on leave and needed coverage. However, when employee B came back from leave, employee A was never removed from the group. This could happen for a number of reasons, such as AD administrative staff was too busy – or forgot - to de-provision the access when it was no longer needed; possibly, the Finance manager didn't realize the risk of this over-provisioning action; or the native tools just made it too difficult or time-consuming to do. Whatever the reason, when AD is synched with Azure AD, the same inappropriate rights associated with this user are now also present in Azure AD. If there are Finance resources available on SharePoint, OneDrive or any of the hundreds of applications that could potentially be enabled via Azure AD, this user has permission (or at least rights) to access and manipulate this sensitive data.

Situations like this pose a significant risk for organizations. Consider the implications of inadvertent errors from your on-prem AD being replicated out to Azure AD and all the resources to which Azure AD connects your users.

Pain Remedy 4: Everything shipshape

The solution is simple – if there are no errors in AD, they cannot be replicated to Azure AD. So how do you ensure that your on-prem AD is shipshape? Since the source of most errors is the human factor, removing as much opportunity for error is key to a clean and safe AD – and thus, a clean and safe Azure AD.

Active Roles provides the automation and built-in workflows necessary to ensure that users are granted appropriate rights and placed in the correct groups, along with all the approvals, audit trails, and checks-and-balances required to reduce risk. If it is easy (or automatic) to grant people correct rights and consequently revoke rights, when necessary, it is easy to keep AD clean. Active Roles can even communicate with an authoritative data source (such as an HR system) to automatically initiate actions on AD and Azure AD accounts. In the case of our example, when employee B returned from leave, Active Roles would automatically reinstate those rights and revoke the rights of employee A.

With Active Roles central to your AD-management strategy, **the potential for errors** – and replicating them in Azure AD – **is significantly reduced**.

Challenge 5

Who gives you the right?

The glaring security gap in native AD/Azure AD management tools is the lack of privileged account management. With these tools, an administrator account is required to do any action – such as provisioning a user, placing people in groups, resetting a password, installing updates, backing up the directory, deploying a new domain controller or any other necessary admin actions. The problem is that this account is tied to the directory and not an individual. That means a number of people share the credential and that everyone uses the same administrator login info. Plus, this one login has access to everything. It does not matter if the action is to simply reset a user's password or to deploy a new domain controller – everyone with that login has the same rights.

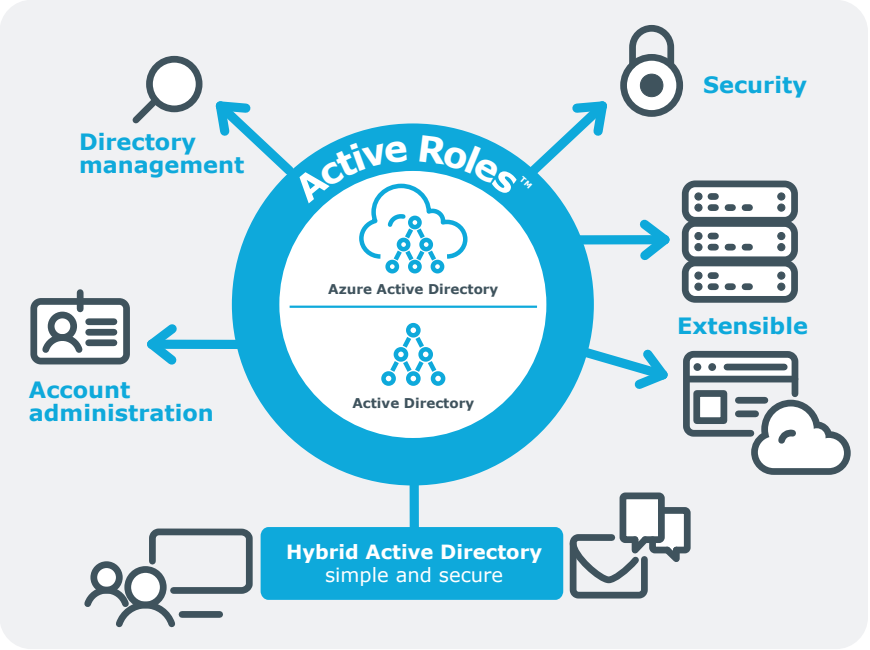
This situation is fraught with risk due to lack of individual accountability for the admin account. On top of that, the on-prem AD admin account does not apply to Azure AD (and vice versa), and the permissions are still all-or-nothing, which now opens up your cloud environment to risk.

Pain Remedy 5: The right rights

The correct way to issue admin rights in a hybrid AD environment is to grant privileged users only enough permission to do their job – nothing more, nothing less. This is a concept called least-privilege access. Active Roles provides a least-privilege layer of security for AD and Azure AD by which you can manage what individual admins are allowed to do and what they are not allowed to do. It removes the potential for individuals to take actions inadvertently or maliciously beyond their role and responsibility.

With Active Roles, you have a single tool that enables you to define administrative roles across AD, Azure AD, Microsoft 365, and other SaaS applications. Along with modern authentication using OAUTH, Active Roles has robust and personalized approval procedures that establish an IT process and oversight consistent with business requirements, with responsibility chains that complement the automated management of directory data.

The admin tasked with resetting passwords can only reset passwords (maybe you want them to handle both AD and Azure AD environments); the provisioning admin(s) cannot access or manipulate logs; and the software-install person is insulated from doing day-to-day user administration tasks. Active Roles acts as an additional layer of control and security around the hybrid AD environments.



ONE IDENTITY by Quest

But wait there's more...

Our hybrid capabilities don't stop with the cloud

In addition to solving the five challenges mentioned above, Active Roles also delivers:

- Auditing with change history and user activity reporting for both AD and Azure AD
- Application-license management to optimize SaaS expense control
- Integration with leading AD management tools for auditing, migration, Group Policy management and change auditing
- Extensive scripting and customization capabilities
- Modular architecture to meet today and tomorrow's business needs
- Integration with enterprise IAM functionality including:
  - Enterprise provisioning and AD governance
  - AD bridging
  - Password vaulting
  - User and LOB self-service
  - Multifactor authentication
  - Secure remote access
  - Risk-based adaptive security

Conclusion

With the rapid rise of Azure Active Directory, the majority of organizations will maintain on-prem AD while also growing their cloud deployment. This hybrid AD environment presents unique challenges that can be extremely painful to manage with native tools or manual processes. One Identity's Active Roles is the ideal solution to avoid or minimize the pain of the hybrid challenges described above, as well as close security gaps, reduce risk, and – above all – drive consistency and efficiencies in any hybrid AD environment.

ONE IDENTITY by Quest

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

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

One Identity LLC
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

eBook-2022-Top-5-ways-managing-hybrid-AD-enviroonments-US-PG-71382

ONE IDENTITY by Quest