



Modernize your user authentication with Azure Active Directory



As **businesses** adapt to the pace of digital transformation, applications, and the access management layer behind them tend to be some of the first targets for modernization as they are fundamental to enabling increased user productivity.

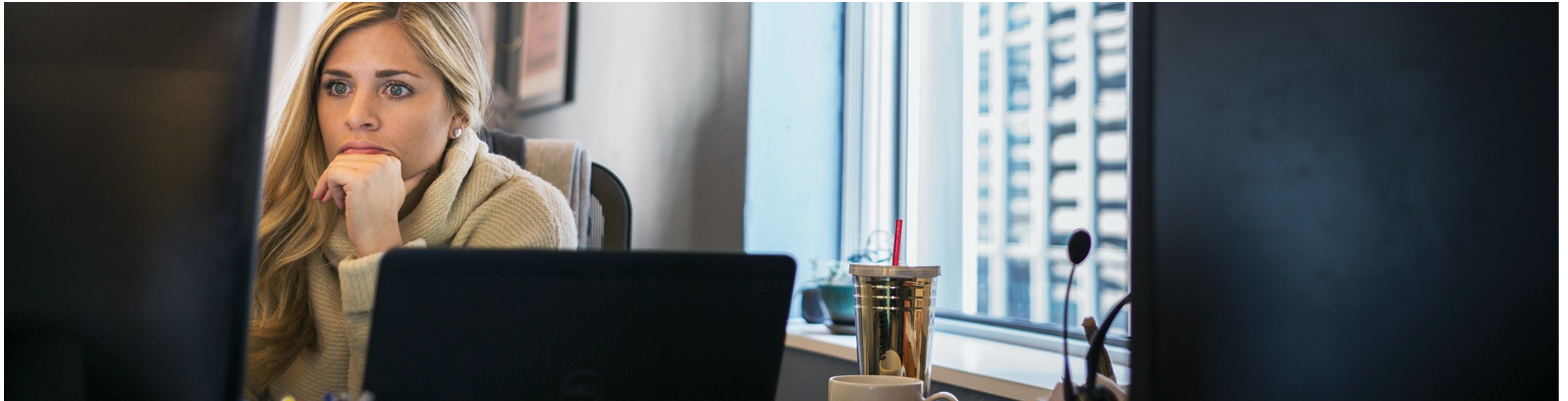
Organizations must now enable access to over 180 unique apps on average thanks to cloud hosting and the explosion of availability of popular software-as-a-service (SaaS) apps. Identity and access management (IAM) can be modernized via a hybrid identity approach, where on-premises user identities are synched with cloud directories to enable a common user identity for access to resources from anywhere. Still, a truly modernized IAM infrastructure should also consider the user authentication flow.



Federated Identity management

A popular option for user authentication has been federated identity management or federation. In federation, a user's host identity provider is trusted for the identity verification and authentication to external resources. Single sign-on is a part of this, in which a user's authentication token can be used across these external resources to gain access without entering new credential information.

Historically, Microsoft's Active Directory Federation Service (ADFS), a software component of on-premises Active Directory (AD), was the most used federation tool to authenticate to external resources. By driving authentication via ADFS, organizations were able to achieve SSO across various apps for their employees and partners and provide a streamlined user experience.



Expand your authentication beyond ADFS

If you are using ADFS today, you may be pleased with it. ADFS solves problems for users who need to access AD-integrated applications while working remotely, offering a flexible solution whereby they can authenticate using their standard organizational AD credentials via a web interface. It allows users from one organization to access another organization's applications beyond the realm of their AD domain.

You may wonder: if ADFS is working and has enabled SSO to cloud resources, is it not part of a transformed IAM solution? The answer is that there are newer tools available that can provide greater security and IT scalability through a more modern approach – this is cloud authentication.



Why should you adopt cloud authentication?

Has any of the following happened to you?

Your on-premises network goes down, and your users cannot access their resources


Your on-premises IAM footprint has become too extensive and costly

You've lost time to patch your on-premises federation server manually

Advanced threats have mandated adopting a higher level of digital security

If you can say “yes” to any of these scenarios, you require the flexibility and security that can only be achieved from the cloud. Microsoft's Azure Active Directory (Azure AD), a cloud IAM universal platform for managing and security identities and its cloud authentication capabilities, is your solution to transform beyond ADFS.





Azure AD – your secure authentication solution in the cloud

Azure AD enables you to grant your employees and partners SSO to all your apps. Whether you're using popular SaaS apps (like Office, ServiceNow, Concur), legacy on-premises apps, or custom apps, your employees and partners can securely log on to these apps with Azure AD through a common user identity bridged across your hybrid identity infrastructure. Azure AD allows users to get the same experience, whether they are accessing apps from the office, at home, or abroad. Fine-grained access controls can secure access to these apps via Conditional Access policies and intelligent, risk-based Identity Protection so that you can set the right balance between user productivity and your organization's security.

Azure AD streamlines the user experience and reduces your complexity that comes with managing identity, security, and access to your company's critical data. What may be less clear to you is how to assess where you are on your authentication journey and how to take the next step to truly modernize your authentication.

Your cloud authentication options

Azure AD offers three core authentication options to allow you to modernize and still meet the needs of your overall digital transformation journey:



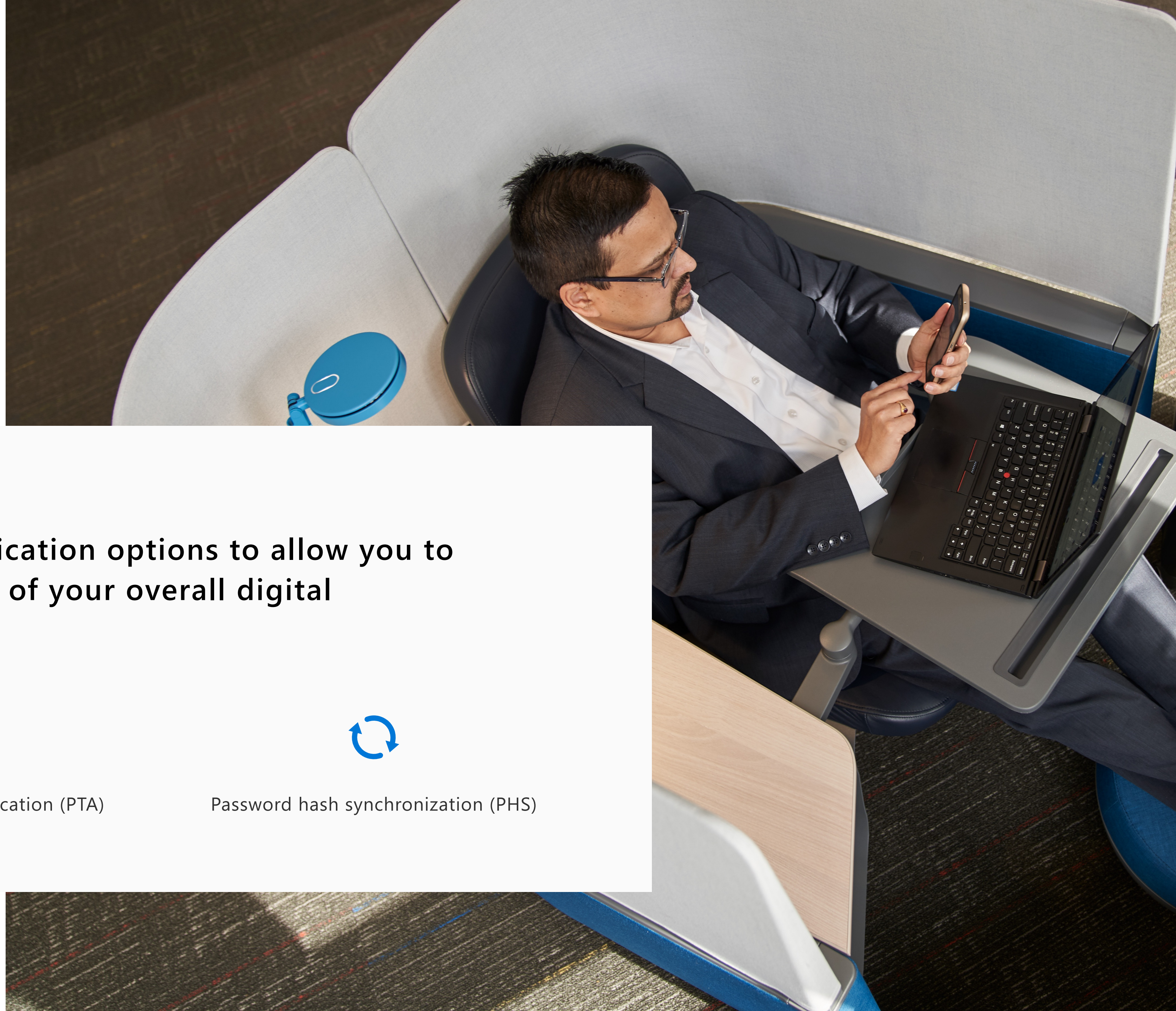
Cloud-only authentication



Pass-through authentication (PTA)



Password hash synchronization (PHS)





Cloud-only authentication

Cloud-only authentication is valid only for those businesses that have fully migrated their user identities to the cloud and do not have dependencies on synchronizing with any on-premises identity directories (which would be achieved with Azure AD Connect). If you can embrace cloud-only authentication, you have reached a fully modernized state. However, you likely still have some on-premises IAM infrastructure that you are not yet ready to decommission fully. In this scenario, you will focus on PTA or PHS that apply to hybrid identity scenarios.



Pass-through authentication

PTA is sometimes the first step businesses take in adopting cloud authentication before moving to a PHS model. In PTA, an authentication agent must be installed on-premises along with existing AD infrastructure. Password validation requests are sent to this agent and passed through to AD to verify credentials and enable user authentication in Azure AD.



Password hash synchronization

PHS is a highly modern authentication approach and requires no additional on-premises infrastructure outside of your existing AD stores and credentials. In PHS, an encrypted hash of a hash of your AD credentials is stored in Azure AD, not the clear text passwords themselves, and user authentication in the cloud is against this data, so no additional communication must happen between the cloud and on-premises during the authentication process.

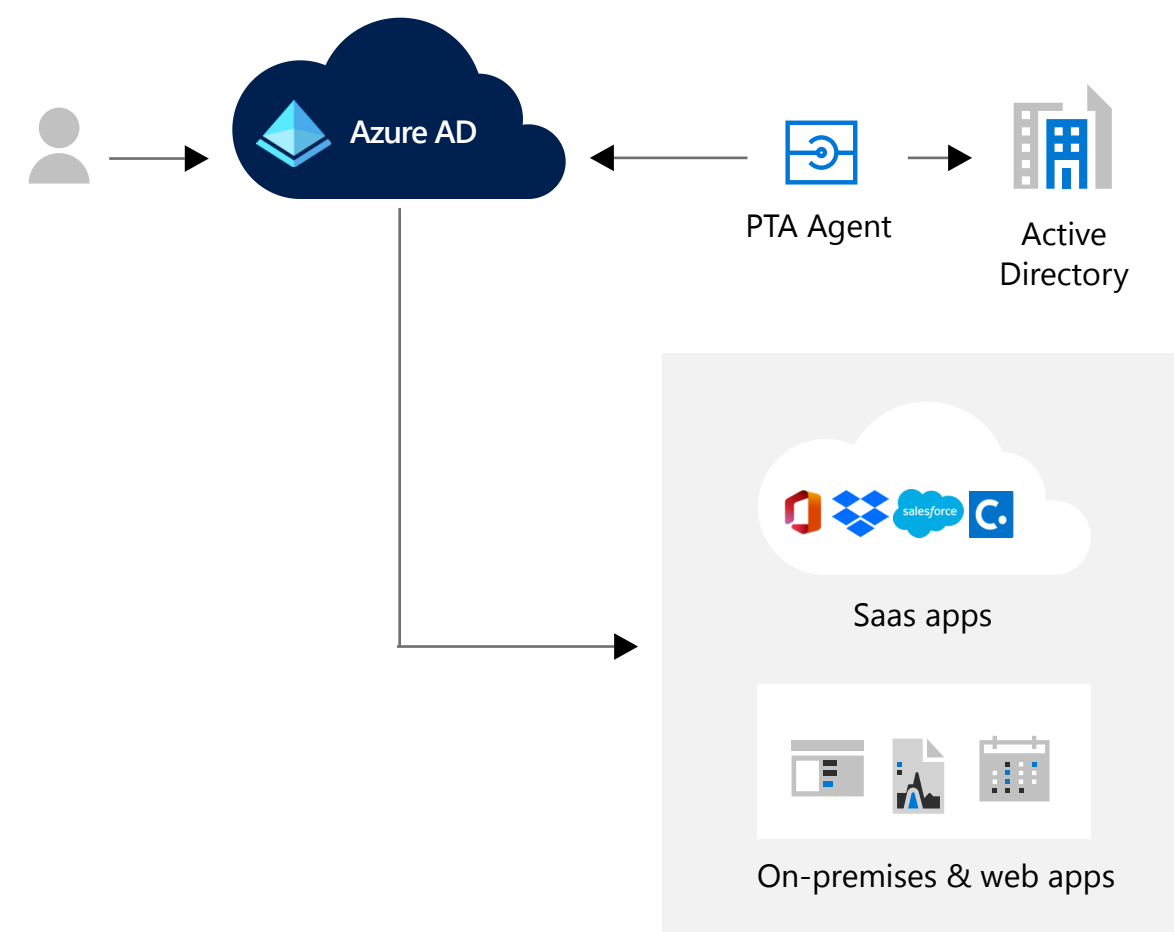


Your cloud authentication options

Let's look at [PTA](#) and [PHS](#) in more detail to help you decide which option is better for you.



Pass-through authentication



By adopting a PTA as a first step of cloud authentication, but still having some connectivity to your on-premises AD, you gain the following:

User experience

Users use the same passwords to sign in to both on-premises and cloud-based applications

Users spend less time talking to the IT helpdesk resolving password-related issues as they can complete self-service password management tasks in the cloud

Deployment and administration

There is no need for complex on-premises deployments or network configurations as PTA only requires a lightweight agent to be installed on-premises

There is no management overhead as the PTA agent automatically receives improvements and bug fixes

Security

On-premises passwords are never stored in the cloud in any form, even the encrypted hash of a hash used in the PHS model

Protects your user accounts by working seamlessly with Conditional Access policies, multi-factor authentication (MFA), and Identity Protection and by filtering out brute force password attacks

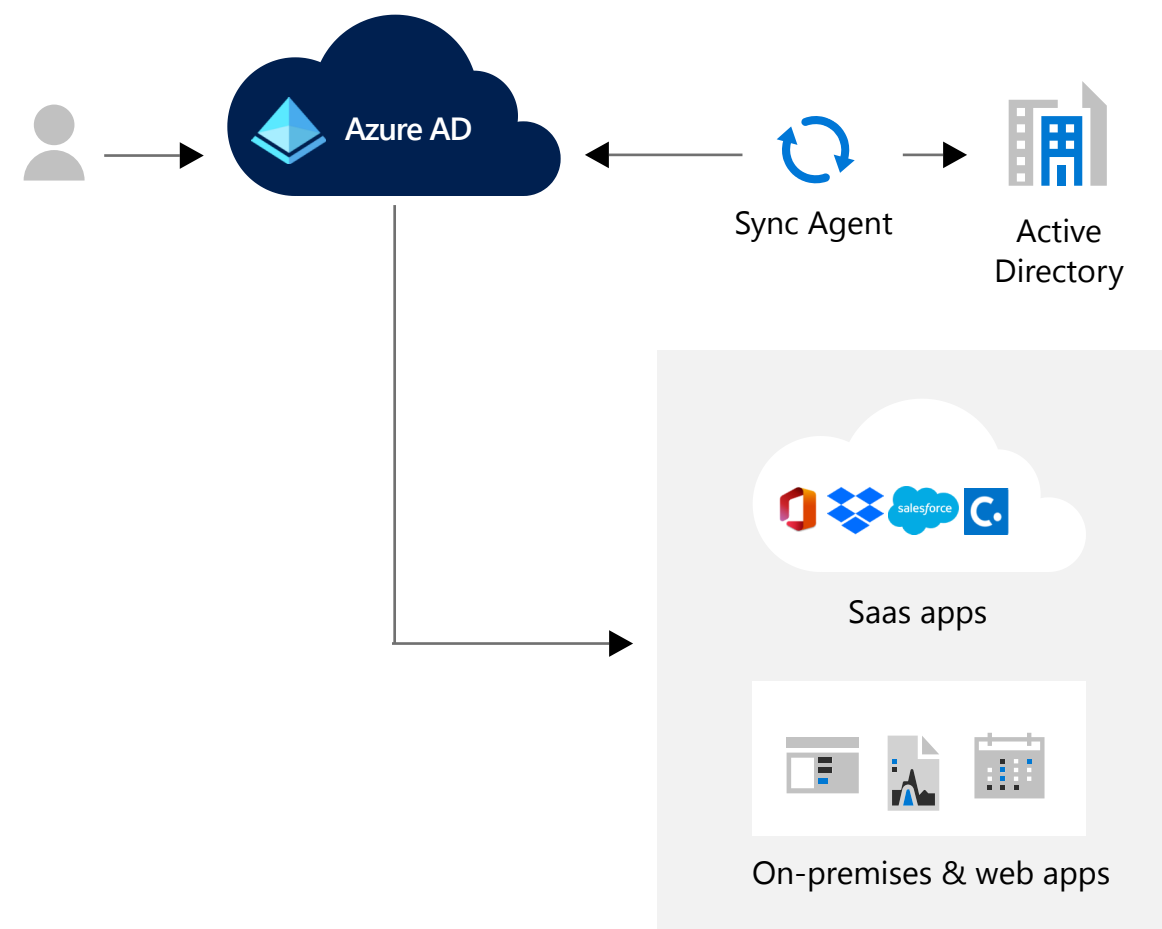
The PTA agent only makes outbound connections from within your network, so there is no requirement to install the agent in a perimeter network or DMZ

The communication between the PTA agent and Azure AD is secured using certificate-based authentication, and these certificates are automatically renewed every few months by Azure AD

Availability

Additional authentication agents can be installed on multiple on-premises servers to provide higher availability of sign-in requests

Password hash synchronization



By adopting PHS as the ideal cloud authentication solution for hybrid identity scenarios, you can gain many of the same benefits as PTA. PHS will provide the same great user SSO common identity benefits and self-service empowerment, as well as security gains via Conditional Access, MFA, and Identity Protection. PHS also unlocks the following benefits:

User experience

Synchronization has no impact on users who are already authenticated

Deployment and administration

There are no on-premises deployments required at all in PHS, not even an authentication agent

Passwords hashes are synchronized every two minutes to ensure consistency between your on-premises and cloud identity environments

Security

PHS enables leaked credential reporting so you can protect yourself from your most significant identity compromise

Availability

If you're on-premises infrastructure has an outage, PHS allows your users to still authenticate to their resources via the cloud



Next Steps



No matter which Azure AD cloud authentication model suits your particular needs, you will gain a more seamless user experience ensuring high productivity and greater security controls to protect your organization from threats, all while providing a highly available, modern authentication infrastructure. Once you have embraced hybrid identity and modernized your authentication, you can connect all your apps to Azure AD to achieve your management and security gains.

To learn more about Azure AD and get started with deploying cloud authentication, visit azure.com/azuread

