Identity Baseline tools in Azure

02/11/2019 • 4 minutes to read • Contributors

In this article

Identity Baseline is one of the Five Disciplines of Cloud Governance. This discipline focuses on ways of establishing policies that ensure consistency and continuity of user identities regardless of the cloud provider that hosts the application or workload.

The following tools are included in the discovery guide on Hybrid Identity.

Active Directory (on-premises): Active Directory is the identity provider most frequently used in the enterprise to store and validate user credentials.

Azure Active Directory: A software as a service (SaaS) equivalent to Active Directory, capable of federating with an on-premises Active Directory.

Active Directory (IaaS): An instance of the Active Directory application running in a virtual machine in Azure.

Identity is the control plane for IT security. So authentication is an organization's access guard to the cloud. Organizations need an identity control plane that strengthens their security and keeps their cloud apps safe from intruders.

Cloud authentication

Choosing the correct authentication method is the first concern for organizations wanting to move their apps to the cloud.

When you choose this method, Azure AD handles users' sign-in process. Coupled with seamless single sign-on (SSO), users can sign in to cloud apps without having to reenter their credentials. With cloud authentication, you can choose from two options:

Azure AD password hash synchronization: The simplest way to enable authentication for on-premises directory objects in Azure AD. This method can also be used with any method as a back-up failover authentication method in case your on-premises server goes down.

Azure AD Pass-through Authentication: Provides a persistent password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.

> **Note**
>
> Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours should consider the pass-through Authentication method.

Federated authentication:

When you choose this method, Azure AD passes the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS) or a trusted third-party federation provider, to validate the user's password.

The article choosing the right authentication method for Azure Active Directory contains a decision tree to help you choose the best solution for your organization.

The following table lists the native tools that can help mature the policies and processes that support this governance discipline.

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO	Federation with AD FS
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent	On-premises
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent	Two or more AD FS servers Two or more WAP servers in the perimeter/DMZ network
What are the requirements for on-premises internet and networking beyond the provisioning system?	None	Outbound internet access from the servers running authentication agents	Inbound internet access to WAP servers in the perimeter Inbound network access to AD FS servers from WAP servers in the perimeter Network load balancing
Is there an SSL certificate requirement?	No	No	Yes
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center	Azure AD Connect Health
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO	Yes
What sign-in types are supported?	UserPrincipalName + password Windows Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password sAMAccountName + password Windows Integrated Authentication Certificate and smart card authentication Alternate login ID

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO	Federation with AD FS
Is Windows Hello for Business supported?	Key trust model Certificate trust model with Intune	Key trust model Certificate trust model with Intune	Key trust model Certificate trust model
What are the multi-factor authentication options?	Azure Multi-Factor Authentication Custom Controls with conditional access*	Azure Multi-Factor Authentication Custom Controls with conditional access*	Azure Multi-Factor Authentication Azure Multi-Factor Authentication server Third-party multi-factor authentication Custom Controls with conditional access*
What user account states are supported?	Disabled accounts (up to 30-minute delay)	Disabled accounts Account locked out Account expired Password expired Sign-in hours	Disabled accounts Account locked out Account expired Password expired Sign-in hours
What are the conditional access options?	Azure AD conditional access	Azure AD conditional access	Azure AD conditional access AD FS claim rules
Is blocking legacy protocols supported?	Yes	Yes	Yes
Can you customize the logo, image, and description on the sign-in pages?	Yes, with Azure AD Premium	Yes, with Azure AD Premium	Yes
What advanced scenarios are supported?	Smart password lockout Leaked credentials reports	Smart password lockout	Multisite low-latency authentication system AD FS extranet lockout Integration with third-party identity systems

> **Note**
>
> Custom controls in Azure AD conditional access does not currently support device registration.

Next steps

The Hybrid Identity Digital Transformation Framework whitepaper outlines combinations and solutions for choosing and integrating each of these components.

The Azure AD Connect tool helps you to integrate your on-premises directories with Azure AD.