Authentication for Microsoft Entra hybrid identity solutions - Microsoft Entra ID

By omondiatieno

Archived: 2026-04-05 13:01:10 UTC

Choose the right authentication method for your Microsoft Entra hybrid identity solution

Note

Scope of this article: This article describes authentication methods for Microsoft Entra hybrid identity solutions. These authentication methods apply independently of the synchronization technology used (Microsoft Entra Connect Sync or Cloud Sync). The choice of synchronization technology does not determine or change the authentication behavior for user sign-ins.

Choosing the correct authentication method is the first concern for organizations wanting to move their apps to the cloud. Don't take this decision lightly, for the following reasons:

1. It's the first decision for an organization that wants to move to the cloud.
2. The authentication method is a critical component of an organization's presence in the cloud. It controls access to all cloud data and resources.
3. It's the foundation of all the other advanced security and user experience features in Microsoft Entra ID.

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

Note

Changing your authentication method requires planning, testing, and potentially downtime. Staged rollout is a great way to test users' migration from federation to cloud authentication.

Out of scope

Organizations that don't have an existing on-premises directory footprint aren't the focus of this article. Typically, those businesses create identities only in the cloud, which doesn't require a hybrid identity solution. Cloud-only identities exist solely in the cloud and aren't associated with corresponding on-premises identities.

Authentication methods

When the Microsoft Entra hybrid identity solution is your new control plane, authentication is the foundation of cloud access. Choosing the correct authentication method is a crucial first decision in setting up a Microsoft Entra hybrid identity solution. The authentication method you choose, is configured by using Microsoft Entra Connect, which also provisions users in the cloud.

To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

Microsoft Entra ID supports the following authentication methods for hybrid identity solutions.

Cloud authentication

When you choose this authentication method, Microsoft Entra ID handles users' sign-in process. Coupled with 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:

Microsoft Entra password hash synchronization. The simplest way to enable authentication for on-premises directory objects in Microsoft Entra ID. Users can use the same username and password that they use on-premises without having to deploy any other infrastructure. Some premium features of Microsoft Entra ID, like Microsoft Entra ID Protection and Microsoft Entra Domain Services, require password hash synchronization, no matter which authentication method you choose.

Microsoft Entra pass-through authentication. Provides a simple password validation for Microsoft Entra authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method. For more information on the actual pass-through authentication process, see User sign-in with Microsoft Entra pass-through authentication.

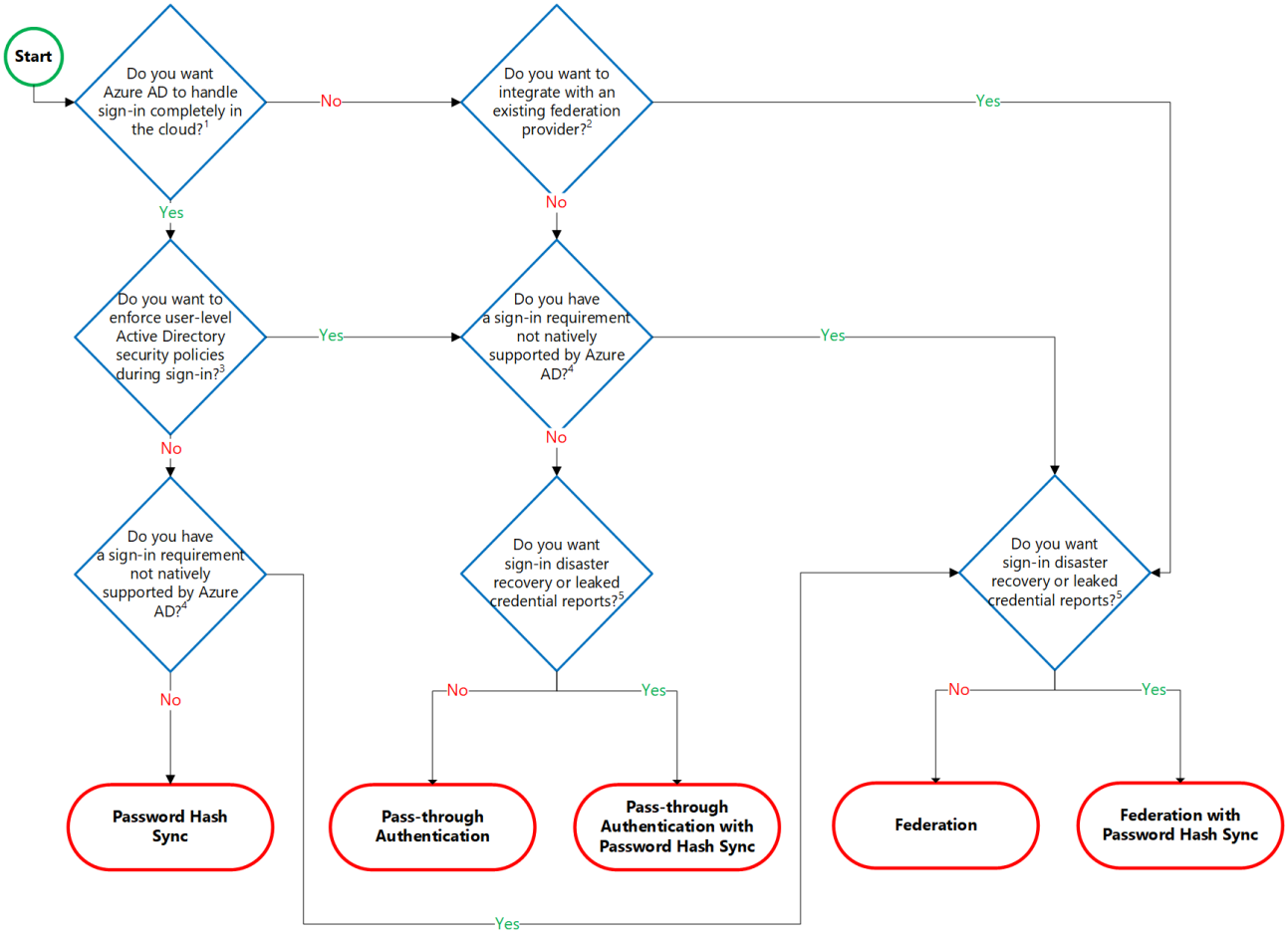
Federated authentication

When you choose this authentication method, Microsoft Entra ID hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

The authentication system can provide other advanced authentication requirements, for example, third-party multifactor authentication.

The following section helps you decide which authentication method is right for you by using a decision tree. It helps you determine whether to deploy cloud or federated authentication for your Microsoft Entra hybrid identity solution.

Decision tree



Details on decision questions:

1. Microsoft Entra ID can handle sign-in for users without relying on on-premises components to verify passwords.
2. Microsoft Entra ID can hand off user sign-in to a trusted authentication provider such as Microsoft's AD FS.
3. If you need to apply, user-level Active Directory security policies such as account expired, disabled account, password expired, account locked out, and sign-in hours on each user sign-in, Microsoft Entra ID requires some on-premises components.
4. Sign-in features not natively supported by Microsoft Entra ID:
    - Sign-in using third-party authentication solution.
    - Multi-site on-premises authentication solution.

5. Microsoft Entra ID Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the *Users with leaked credentials* report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.

Detailed considerations

Cloud authentication: Password hash synchronization

- **Effort**. Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Microsoft 365, SaaS apps, and other Microsoft Entra ID-based resources. When turned on, password hash synchronization is part of the Microsoft Entra Connect Sync process and runs every two minutes.

- **User experience**. To improve users' sign-in experience, use Microsoft Entra joined devices or Microsoft Entra hybrid joined devices. If you can't join your Windows devices to Microsoft Entra ID, we recommend deploying seamless SSO with password hash synchronization. Seamless SSO eliminates unnecessary prompts when users are signed in.

- **Advanced scenarios**. If organizations choose to, it's possible to use insights from identities with Microsoft Entra ID Protection reports with Microsoft Entra ID P2. An example is the leaked credentials report. Windows Hello for Business has specific requirements when you use password hash synchronization. Microsoft Entra Domain Services requires password hash synchronization to provision users with their corporate credentials in the managed domain.

  Organizations that require multifactor authentication with password hash synchronization must use Microsoft Entra multifactor authentication or Conditional Access custom controls. Those organizations can't use third-party or on-premises multifactor authentication methods that rely on federation.

- **Business continuity**. Using password hash synchronization with cloud authentication is highly available as a cloud service that scales to all Microsoft datacenters. To make sure password hash synchronization doesn't go down for extended periods, deploy a second Microsoft Entra Connect server in staging mode in a standby configuration.

- **Considerations**. Currently, password hash synchronization doesn't immediately enforce changes in on-premises account states. In this situation, a user has access to cloud apps until the user account state is synchronized to Microsoft Entra ID. Organizations might want to overcome this limitation by running a new synchronization cycle after administrators do bulk updates to on-premises user account states. An example is disabling accounts.

  Understanding authentication timing: While "authentication occurs in the cloud" refers to where Microsoft Entra ID validates credentials (comparing the provided password hash against the stored hash), the availability of password changes for sign-in depends on the synchronization timing. When a user changes their password on-premises, the new password hash must be synchronized to Microsoft Entra ID before the user can sign in with it. This synchronization process typically runs every two minutes but may vary based on configuration.

Note

The password expired and account locked-out states aren't currently synced to Microsoft Entra ID with Microsoft Entra Connect. When you change a user's password and set the *user must change password at next logon* flag, the password hash will not be synced to Microsoft Entra ID with Microsoft Entra Connect until the user changes their password.

Refer to implementing password hash synchronization for deployment steps.

Cloud authentication: Pass-through Authentication

- **Effort**. For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

  Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests. For more information on this process, see the security deep dive on pass-through authentication.

- **User experience**. To improve users' sign-in experience, use Microsoft Entra joined devices or Microsoft Entra hybrid joined devices. If you can't join your Windows devices to Microsoft Entra ID, we recommend deploying seamless SSO with password hash synchronization. Seamless SSO eliminates unnecessary prompts when users are signed in.

- **Advanced scenarios**. Pass-through Authentication enforces the on-premises account policy at the time of sign-in. For example, access is denied when an on-premises user's account state is disabled, locked out, or their password expires or the logon attempt falls outside the hours when the user is allowed to sign in.

  Organizations that require multifactor authentication with pass-through authentication must use Microsoft Entra multifactor authentication or Conditional Access custom controls. Those organizations can't use a third-party or on-premises multifactor authentication method that relies on federation. Advanced features require that password hash synchronization is deployed whether or not you choose pass-through authentication. An example is the leaked credentials detection of Microsoft Entra ID Protection.

- **Business continuity**. We recommend that you deploy two extra pass-through authentication agents. These extras are in addition to the first agent on the Microsoft Entra Connect server. This other deployment ensures high availability of authentication requests. When you have three agents deployed, one agent can still fail when another agent is down for maintenance.

  There's another benefit to deploying password hash synchronization in addition to pass-through authentication. It acts as a backup authentication method when the primary authentication method is no longer available.

- **Considerations**. You can use password hash synchronization as a backup authentication method for pass-through authentication, when the agents can't validate a user's credentials due to a significant on-premises failure. Fail over to password hash synchronization doesn't happen automatically and you must use Microsoft Entra Connect to switch the sign-on method manually.

  For other considerations on Pass-through Authentication, including Alternate ID support, see frequently asked questions.

Refer to implementing pass-through authentication for deployment steps.

Federated authentication

- **Effort**. A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Microsoft Entra hybrid identity solution. The maintenance and management of the federated system falls outside the control of Microsoft Entra ID. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

- **User experience**. The user experience of federated authentication depends on the implementation of the features, topology, and configuration of the federation farm. Some organizations need this flexibility to adapt and configure the access to the federation farm to suit their security requirements. For example, it's possible to configure internally connected users and devices to sign in users automatically, without prompting them for credentials. This configuration works because they already signed in to their devices. If necessary, some advanced security features make users' sign-in process more difficult.

- **Advanced scenarios**. A federated authentication solution is required when customers have an authentication requirement that Microsoft Entra ID doesn't support natively. See detailed information to help you choose the right sign-in option. Consider the following common requirements:

  - Third-party multifactor providers requiring a federated identity provider.
  - Authentication by using third-party authentication solutions. See the Microsoft Entra federation compatibility list.
  - Sign in that requires a sAMAccountName, for example DOMAIN\username, instead of a User Principal Name (UPN), for example, user@domain.com.

- **Business continuity**. Federated systems typically require a load-balanced array of servers, known as a farm. This farm is configured in an internal network and perimeter network topology to ensure high availability for authentication requests.

  Deploy password hash synchronization along with federated authentication as a backup authentication method when the primary authentication method is no longer available. An example is when the on-premises servers aren't available. Some large enterprise organizations require a federation solution to support multiple Internet ingress points configured with geo-DNS for low-latency authentication requests.

- **Considerations**. Federated systems typically require a more significant investment in on-premises infrastructure. Most organizations choose this option if they already have an on-premises federation

investment. And if it's a strong business requirement to use a single-identity provider. Federation is more complex to operate and troubleshoot compared to cloud authentication solutions.

For a nonroutable domain that can't be verified in Microsoft Entra ID, you need extra configuration to implement user ID sign in. This requirement is known as Alternate login ID support. See Configuring Alternate Login ID for limitations and requirements. If you choose to use a third-party multifactor authentication provider with federation, ensure the provider supports WS-Trust to allow devices to join Microsoft Entra ID.

Refer to Deploying Federation Servers for deployment steps.

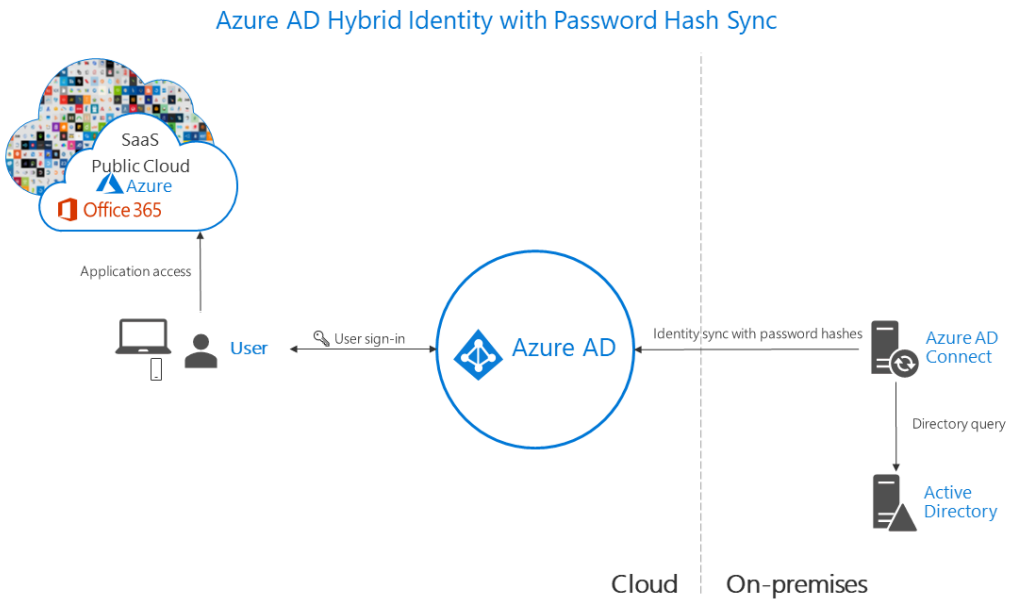
Note

When you deploy your Microsoft Entra hybrid identity solution, you must implement one of the supported topologies of Microsoft Entra Connect. Learn more about supported and unsupported configurations at Topologies for Microsoft Entra Connect.

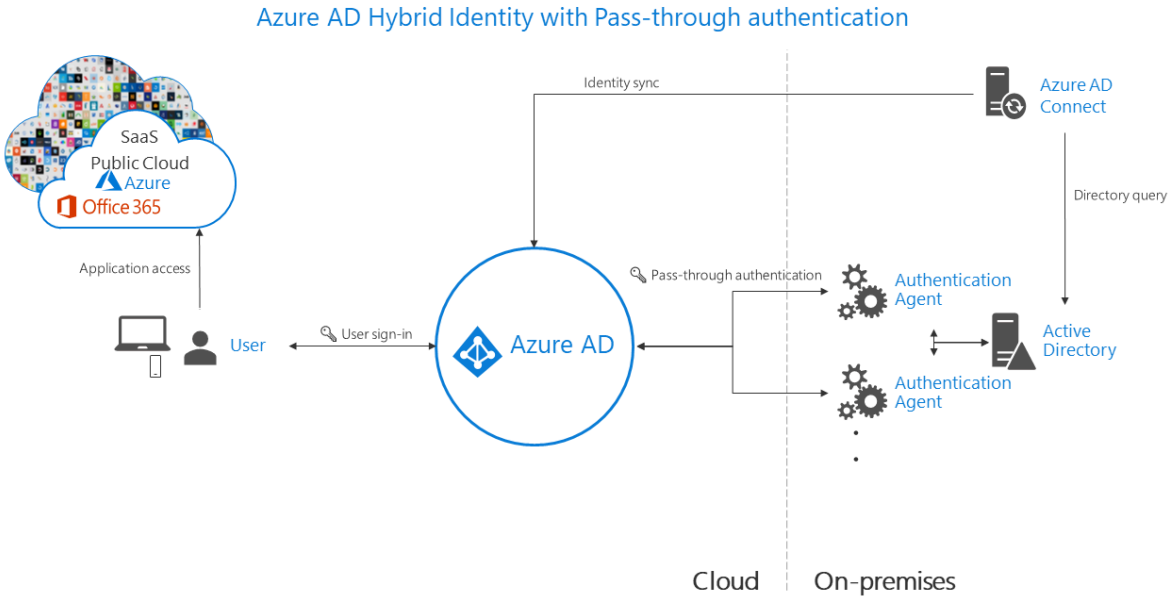
Architecture diagrams

The following diagrams outline the high-level architecture components required for each authentication method you can use with your Microsoft Entra hybrid identity solution. They provide an overview to help you compare the differences between the solutions.

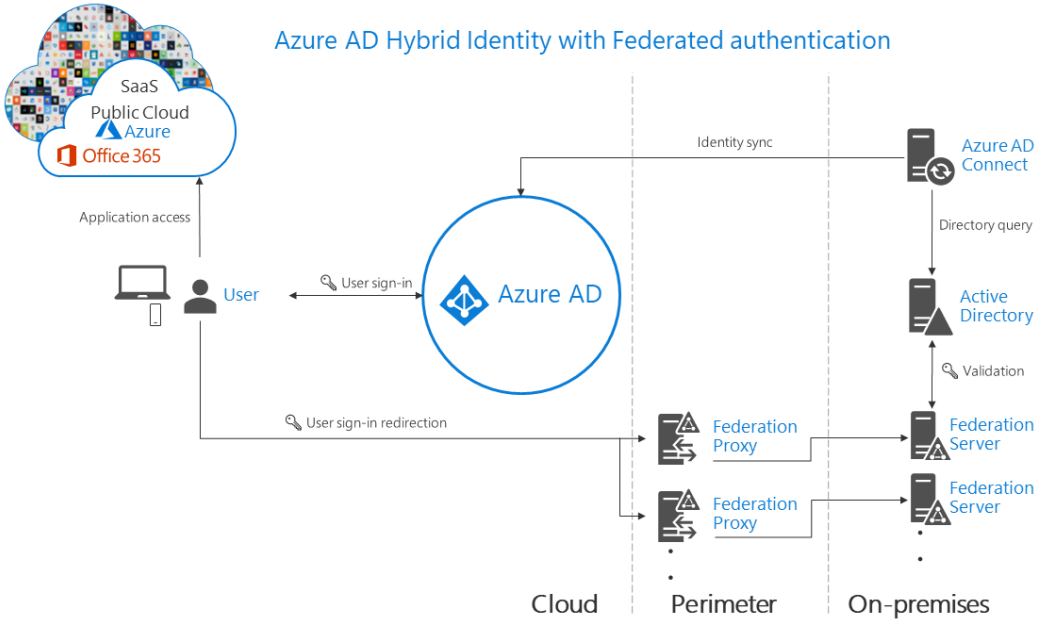
- Simplicity of a password hash synchronization solution:



- Agent requirements of pass-through authentication, using two agents for redundancy:



- Components required for federation in your perimeter and internal network of your organization:



Comparing methods

Consideration	Password hash synchronization	Pass-through Authentication	Federation with AD FS
Where does authentication happen?	In the cloud - password hash is synchronized and	In the cloud, after a secure password verification exchange with the on-	On-premises

Consideration	Password hash synchronization	Pass-through Authentication	Federation with AD FS
	Microsoft Entra ID validates credentials	premises authentication agent	
What are the on-premises server requirements beyond the provisioning system: Microsoft Entra 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 a TLS/SSL certificate requirement?	No	No	Yes
Is there a health monitoring solution?	Not required	Agent status provided by the Microsoft Entra admin center	Microsoft Entra Connect Health
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with Microsoft Entra joined devices, Microsoft Entra hybrid joined devices, the Microsoft Enterprise SSO plug-in for Apple devices, or Seamless SSO	Yes with Microsoft Entra joined devices, Microsoft Entra hybrid joined devices, the Microsoft Enterprise SSO plug-in for Apple devices, or Seamless SSO	Yes
What sign-in types are supported?	UserPrincipalName + password	UserPrincipalName + password	UserPrincipalName + password

Consideration	Password hash synchronization	Pass-through Authentication	Federation with AD FS
	Windows-Integrated Authentication by using Seamless SSO Alternate login ID Microsoft Entra joined Devices Microsoft Entra hybrid joined devices Certificate and smart card authentication	Windows-Integrated Authentication by using Seamless SSO Alternate login ID Microsoft Entra joined Devices Microsoft Entra hybrid joined devices Certificate and smart card authentication	sAMAccountName + password Windows-Integrated Authentication Certificate and smart card authentication Alternate login ID
Is Windows Hello for Business supported?	Key trust model Hybrid Cloud Trust	Key trust model Hybrid Cloud Trust *Both require Windows Server 2016 Domain functional level*	Key trust model Hybrid Cloud Trust Certificate trust model
What are the multifactor authentication options?	Microsoft Entra multifactor authentication Custom Controls with Conditional Access*	Microsoft Entra multifactor authentication Custom Controls with Conditional Access*	Microsoft Entra multifactor authentication Third-party MFA 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

Consideration	Password hash synchronization	Pass-through Authentication	Federation with AD FS
What are the Conditional Access options?	Microsoft Entra Conditional Access, with Microsoft Entra ID P1 or P2	Microsoft Entra Conditional Access, with Microsoft Entra ID P1 or P2	Microsoft Entra Conditional Access, with Microsoft Entra ID P1 or P2 AD FS Access Control Policies
Is blocking legacy protocols supported?	Yes	Yes	Yes
Can you customize the logo, image, and description on the sign-in pages?	Yes, with Microsoft Entra ID P1 or P2	Yes, with Microsoft Entra ID P1 or P2	Yes
What advanced scenarios are supported?	Smart password lockout Leaked credentials reports, with Microsoft Entra ID P2	Smart password lockout	Multisite low-latency authentication system AD FS extranet lockout Integration with third-party identity systems

Note

Custom controls in Microsoft Entra Conditional Access do not currently support device registration.

Recommendations

Your identity system ensures your users' access to apps that you migrate and make available in the cloud. Use or enable password hash synchronization with whichever authentication method you choose, for the following reasons:

1. **High availability and disaster recovery**. Pass-through Authentication and federation rely on on-premises infrastructure. For pass-through authentication, the on-premises footprint includes the server hardware and networking the Pass-through Authentication agents require. For federation, the on-premises footprint is even larger. It requires servers in your perimeter network to proxy authentication requests and the internal federation servers.

To avoid single points of failure, deploy redundant servers. Then authentication requests will always be serviced if any component fails. Both pass-through authentication and federation also rely on domain controllers to respond to authentication requests, which can also fail. Many of these components need maintenance to stay healthy. Outages are more likely when maintenance isn't planned and implemented correctly.

2. **On-premises outage survival**. The consequences of an on-premises outage due to a cyber-attack or disaster can be substantial, ranging from reputational brand damage to a paralyzed organization unable to deal with the attack. Recently, many organizations were victims of malware attacks, including targeted ransomware, which caused their on-premises servers to go down. When Microsoft helps customers deal with these kinds of attacks, it sees two categories of organizations:

    - Organizations that previously also turned on password hash synchronization on top of federated or pass-through authentication changed their primary authentication method to then use password hash synchronization. They were back online in a matter of hours. By using access to email via Microsoft 365, they worked to resolve issues and access other cloud-based workloads.

    - Organizations that didn't previously enable password hash synchronization had to resort to untrusted external consumer email systems for communications to resolve issues. In those cases, it took them weeks to restore their on-premises identity infrastructure, before users were able to sign in to cloud-based apps again.

3. **ID protection**. One of the best ways to protect users in the cloud is Microsoft Entra ID Protection with Microsoft Entra ID P2. Microsoft continually scans the Internet for user and password lists that bad actors sell and make available on the dark web. Microsoft Entra ID can use this information to verify if any of the usernames and passwords in your organization are compromised. Therefore, it's critical to enable password hash synchronization no matter which authentication method you use, whether it's federated or pass-through authentication. Leaked credentials are presented as a report. Use this information to block or force users to change their passwords when they try to sign in with leaked passwords.

Conclusion

This article outlines various authentication options that organizations can configure and deploy to support access to cloud apps. To meet various business, security, and technical requirements, organizations can choose between password hash synchronization, Pass-through Authentication, and federation.

Consider each authentication method. Does the effort to deploy the solution, and the user's experience of the sign-in process address your business requirements? Evaluate whether your organization needs the advanced scenarios and business continuity features of each authentication method. Finally, evaluate the considerations of each authentication method. Do any of them prevent you from implementing your choice?

Next steps

In today's world, threats are present 24 hours a day and come from everywhere. Implement the correct authentication method, and it will mitigate your security risks and protect your identities.

Get started with Microsoft Entra ID and deploy the right authentication solution for your organization.

If you're thinking about migrating from federated to cloud authentication, learn more about changing the sign-in method. To help you plan and implement the migration, use these project deployment plans, or consider using the new Staged Rollout feature to migrate federated users to using cloud authentication in a staged approach.
