A BIO-key® Solution.

White Paper

The Hidden Costs of AD FS

Table of Contents

What is AD FS?

Active Directory Federation Services (or AD FS as it is commonly known) is an access control service provided by Microsoft. This service enables federation to a wide variety of applications – primarily those hosted or provided by Microsoft. Additionally, AD FS takes advantage of many existing Microsoft systems by integrating with them at a foundational level.

As a Single Sign-On (SSO) solution, AD FS is installed on the Windows Server Operation System and requires Internet Information Services (IIS) – a service that only runs on Windows Servers. Furthermore, AD FS utilizes the WS Federation, OAuth, OpenID Connect and SAML standards to provide token-based SSO to additional systems in order to reduce login prompts and streamline usability for a wide range of end-users.

All in all, this particular solution sounds like a dream come true to most organizations: AD FS relies on Active Directory, which is the primary User Repository for many, and it also happens to be free.

However, the free option doesn't always make for the best choice.

Why Would I Want *Identity Federation*?

Before going into the nitty gritty details, it is important to understand why Federation or any given SSO solution is something that should even be considered for your environment. With the rapid increase of adoption rates for web-based and cloud-hosted applications, this is an important question to ask, and one that will be asked of any administrator before long.

Many organizations and end-users understand the term 'Federation' in the same way that most people understand the Theory of Relativity. The core concept is widely available, but digging too deep can leave you muddy and confused about why you jumped in to the deep end in the first place. It is great to have a high-level understanding of the concepts, but that does not cover the minutiae involved in appreciating and taking advantage of the system as a whole.

As a form of True Single Sign-On, federation requires a more fine-tuned understanding before you can truly take advantage of its many benefits.

Identity Provider (IdP) to verify the identity of a user before providing SSO to their entire suite of web-applications.

What is SSO?

For a more general understanding of Federation, a more popularized term would be Single Sign-On (SSO). Federation is a method by which organizations can provide SSO to various applications – thus improving the end-user experience and introducing a large host of benefits into their environments. In this scenario, a service acts as an Identity Provider (IdP) to verify the identity of a user before providing SSO to their entire suite of web-applications.

Make no mistake, federation allows for a series of benefits when implemented correctly and with specific user scenarios in mind. Some of the more useful benefits are:

- Streamlined User Experience
- Utilize a Single Login Attempt for Multiple Applications
- Simplified Account Management
- Ability to Integrate with Additional Services
    - Self-Service Password Reset
    - Multi-Factor Authentication

In a very real way, federation is the industry's approach to improving usability without sacrificing security. This approach appeals to both end-users and administrators alike, and provides a lasting solution that is able to evolve alongside the growing and ever-changing industry trends.

How Does It Work?

Identity Federation is a method of linking multiple digital identities to a single user. This means consolidating various attributes located in a central repository and being able to associate that with multiple services that may or may not be able to connect to the central repository directly. In cases where this connection is NOT possible, Federation enables users to maintain a single identity without being required to prove themselves with each consecutive login.

In many cases, Federation is the first step to a successful SSO implementation. In the case of AD FS, Federation ties in directly to the Active Directory repository and utilizes a trust-relationship with a wide variety of services to provide a limited implementation of SSO.

What are the Limitations of AD FS?

As is the case with all services, it is important to understand the full scope of what is meant to play such a large role in future infrastructure and end-user experience. Microsoft's solutions are no different. Implementing services such as Office 365 or SharePoint are not without their limitations or drawbacks, and Microsoft's Federated Services solution is no exception to the rule.

Staying informed - from the first stage of researching a new solution, until well beyond the point of purchase - is a necessary means of ensuring that any new solution will provide what is needed for a given environment without any surprises along the way.

While AD FS is a strong solution in its own right, there are some limitations that are not always apparent at first glance:

LDAP Repositories Only

As implied by the name, AD FS has a standard requirement to be joined to an AD FS domain controller. Essentially, AD FS needs to be joined to an Active Directory domain to be utilized in any real fashion.

Of course, that integration is often par for the course. Active Directory is one of the most popular User Repositories in use, and integrates quite easily with many additional services. For the purposes of AD FS, Active Directory becomes the primary identity holder in a Federation environment.

A benefit to AD FS is that it has the capability to integrate with any LDAP v3 compliant repository. With that integration in mind, any non-Active Directory repository must be connected to your AD FS farm by creating a local claims provider trust. This requires a bit more work, but it is definitively possible.

However, the ability to integrate with LDAP repositories can also be viewed as a limitation, in that LDAP v3 is the extent of the integration possibilities for AD FS. Any organization or environment which utilizes a separate repository store will either have to convert to LDAP, or search elsewhere.

Limited Support For *Industry Standard Protocols*

We have previously discussed the AD FS support for the SAML, OAuth, OIDC and WS-Federation protocols for SSO. These are all industry standard protocols for SSO. Other industry standard protocols include:

- Shibboleth
- CAS
- Kerberos
- NTLM

While SAML and WS-Fed are major players in the industry for SSO, they are by no means the only protocols worth considering. Many commonly used applications – including Ellucian's Banner application and related products - do not support SAML, but instead require CAS or a Shibboleth-specific IdP in order to utilize SSO via federation.

In these scenarios, AD FS falls short with its lack of support for a more extensible array of industry standard protocols. Although AD FS provides a solid implementation, this limitation requires customers to setup additional services alongside AD FS to improve usability without reducing security. In many cases, this is an additional investment that only becomes apparent long after the initial commitment to AD FS.

Lacking *Standard Features*

As the name implies, AD FS is strictly a federation service. This is important because it speaks to the lack of additional standard features that customers have come to expect alongside the implementation of federation. Alongside true SSO capabilities, end-users and administrators alike expect to be able to reset a forgotten password or unlock accounts when passwords have been entered incorrectly too many times.

Features Expected in standard Federation Environments

- SSO
- Self-Service Password Reset
  - Forgotten Passwords
- Account Unlock
- Change Password
  - Update Known Passwords
- Multi-Factor Authentication Support

With AD FS, these features are not available without integrating the service alongside additional Microsoft applications. Specifically speaking, Self-Service Password Reset capabilities within AD FS environments require Azure MFA and Microsoft Identity Manager (MIM).

Big Name = Big Cost

It is a fine thing to work with a company as respected and prominent in the market as Microsoft, there is no doubt about that. However, with such a big name comes even bigger costs. The many promises of Microsoft require heavy upkeep and severe virtualization, which is paid for directly by those who utilize the service.

Microsoft's Free services are fantastic, but the old adage holds true: there is no such thing as a free lunch. Implementing AD FS will get your foot in the door with basic functionality, but a fully functional environment with no hassle?

That requires something else entirely.

In for a Penny, In for a Pound

Integration with Azure Active Directory and related services is the biggest hidden cost associated with AD FS implementations. This integration only becomes necessary down the line when environments begin to consider additional functionality within federated environments. At that point, it becomes a much bigger hassle to find a new solution, which allows Microsoft to capitalize on those users who are unwilling to start from scratch.

Once you see the prices for Azure, however, you may find it worthwhile to look elsewhere.

Azure AD Pricing Estimates:
https://azure.microsoft.com/en-us/pricing/details/active-directory/

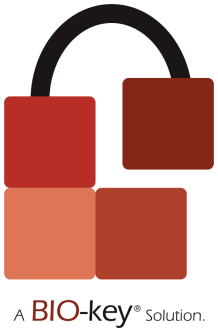
A Reasonable Alternative Without the Hidden Costs

When it comes to Single Sign-On, a true IdP provides the full gamut of standard features without any gimmicks or hidden charges. SSO is a large undertaking, with integration points in many systems throughout a given environment, and the simplest solution does not always have to leave you wanting.

With PortalGuard, true SSO is enabled alongside a fully featured authentication package that is capable of integrating with many service providers, utilizing a wide range of Industry Standard Protocols. For one low price, PortalGuard provides:

- True SSO to service providers using industry standard protocols
- Full Range of Password Management capabilities
  - Self-Service Password Reset
  - Password Recovery
  - Self-Service Account Unlock
  - Password Change
- The ability to secure authentication further using Multi-factor Authentication
  - Over 15 different OTP methods that include:
    - Hard Tokens
    - Mobile Devices
    - Enterprise-level Biometrics
- Fully Customizable Front End
  - Accessibility for any user on any device

Federation is a necessary feature in both individual and expanding environments, and PortalGuard provides a reasonable alternative to AD FS without the hidden costs. If you think that your environment could benefit from a complete SSO solution, contact us today.



About Us

BIO-key's PortalGuard offers both a cloud-based and on-premises turnkey user authentication solution-set for campuses with external-facing web applications for their students, staff, and faculty. This all-in-one integrated design includes Two-Factor methods, Single Sign-On, Centralized Self-Service Password reset/unlock, Password Synchronization, plus transparent barriers to confirm user identities by validating their context.