How PingFederate and ADFS Tackle Office 365 Federation
Office 365 is the biggest and fastest growing productivity suite in the market, and for good reason. It seamlessly integrates with existing infrastructure and provides expansive tools for your users to do their jobs. Getting users secure, convenient access to these tools is paramount for an efficiently run enterprise, and a comprehensive federation server helps you meet those needs.

The federation server authenticates users to Office 365 by taking the on-premises authentication, translating it to a standard token and presenting that to Azure Active Directory, which controls access to Office 365. Traditionally, Microsoft has recommended ADFS as the federation server of choice for single sign-on (SSO) to Office 365 with Azure Active Directory. Now, however, with Microsoft's partnership with Ping Identity, PingFederate is officially supported as a federation server for Azure AD for secure, one-click access to applications such as Office 365 and Intune.

It is important to understand the feature-by-feature comparison between Active Directory Federation Services (ADFS) and PingFederate as you decide which fits better into your infrastructure and overall federation needs. With the inclusion of PingFederate as a configuration option through Azure AD Connect, it will be even easier to pick the correct federation solution for your organization. The comparison in this solution brief is intended to describe only the federation server needs for Office 365 and Azure Active Directory.

**PROTOCOLS**

Azure Active Directory accepts WS-Fed, WS-Trust U/P and WS-Trust Kerberos tokens. The federation server will need to be able to support these protocols to ensure secure authentication with Azure Active Directory.

- WS-Fed is used for passive authentication, which includes modern authentication AAD applications that convert to passive flows.
- WS-Trust is used for EAS, login to AAD Join, PRT acquisition for AAD with DJ++ device, or Domain Join Office seamless SSO.

*All of these protocols are supported out of the box with both ADFS and PingFederate.*

**AUTHENTICATION TYPES**

In today's mobile workforce, users authenticate from many different directions. Some authenticate from their mobile devices, some from on network and some directly into the federation server. It is essential that your federation server be flexible and able to give access to users with minimal friction.

- Desktop SSO & Windows Integrated Authentication
- Certificate Authority: The federation server sends issuer and serial # as claims, and Azure AD validates against certificate authority registered.
- Multifactor authentication (MFA) with AAD Conditional Access
- Username / Password

*All of these authentication types are supported out of the box with both ADFS and PingFederate.*
DEVICE REGISTRATION
Mobile workforces need to be able to authenticate from multiple devices seamlessly. To balance this need for convenience with an enterprise's need for security, your federation server must be able to support device registration, giving users a one-time process to prove it is their device and can be trusted.

- Support Windows 10 DJ++ registration over WS-Trust Kerberos
- Support Windows Integrated Authentication or Multi-Authentication URI for Windows 7 / 8.1 registration
- Send Windows Integrated Authentication URI as AuthContext Ref claim for Windows 7 / 8.1

All of these device registration methods are supported out of the box with both ADFS and PingFederate.

SIGN-ON EXPERIENCES
Consistency in sign-on experience ensures a frictionless digital experience for the user; they should recognize the screen every time they sign in, no matter the device or their location. The federation server should support:

- Sign-on pages similar to Azure AD layout
- Customized sign-on experiences for the enterprise
- Login prompt on WS-Fed for Office multi-account scenarios

All of these sign-on experiences are supported out of the box with both ADFS and PingFederate.

OTHER CLAIMS
Each enterprise has slightly different requirements for their users’ digital experiences. The federation server needs to be flexible and offer a variety of options for the enterprise to ensure security and convenience.

- Inside vs. outside the corporate network. The authentication flow should manage certificates, MFA and SSO for longer-lived sessions based on the user’s IP address.
- Keep me signed-in and PSSO claim for longer-lived sessions.
- Password Expiry Notification. The federation server needs to send password expiry information to Azure AD for notification to user.
- Primary Authentication Method
- AuthnContextRef to send additional claims to convey MFS or WIA or MultiAuthentication.

All of these claims, with one exception, are supported out of the box with both ADFS and PingFederate.

PingFederate collects the password expiry information but does not currently send it in the token to Azure AD, so PingFederate will need to use other means to notify the user of an expiring password rather than a dialogue box in Office 365.
WHICH FEDERATION SERVER SHOULD YOU CHOOSE?

Since ADFS and PingFederate are both supported and available as a configuration option in Azure AD Connect, it all depends on the needs of your overall organization. If you have installed and configured ADFS, you know what it has to offer. If you currently use PingFederate, it is now a Microsoft-supported option for federation.

For more information on what else PingFederate can do for your organization, please see https://www.pingidentity.com/en/platform/single-sign-on/software-sso.html.