Office 365 swivelsecure

Swivel Secure, ADFS and Office 365

Authentication for Office 365

Abstract

This datasheet describes how, by exploiting the capabilities of Active Directory Federation Services (ADFS), you can deliver both secure and efficient authentication to Office 365 and other cloud services utilising AuthControl Sentry®.

Introduction:

Office 365 is Microsoft's cloud-based office automation suite. Being a cloud-based service there are additional authentication considerations to be made. This datasheet describes how, by exploiting the capabilities of Active Directory Federation Services (ADFS) you can deliver secure authentication with AuthControl Sentry®, a multi-factor authentication solution from Swivel Secure.

Office 365 and ADFS

An enterprise can configure Office 365 to use ADFS. For details refer to the Microsoft **website.**

If an Enterprise implements single sign-on (SSO) and the users attempt to access Office 365, the application utilises the ADFS servers to check if the users should be granted access or not.

The technology behind Office 365 redirects the user to the Enterprise' ADFS servers containing a redirect with a SAML authentication request.

The ADFS server interprets this request and can either:

- Prompt the user to supply their username and password and if these credentials are correct, it redirects the user back to Office 365 with a SAML assertion allowing Office 365 to grant the user access.
- OR If the user has already authenticated to the domain, immediately respond with the SAML assertion, ensuring the user is not requested to authenticate again.

There are a number of benefits to this approach, but the important ones for this article are:

- Local Active Directory remains the reference for user accounts. If a user's AD account is disabled, the user will no longer be able to access Office 365.
- There is no need for an additional username and password for Office 365 authentication, the existing AD credentials will be used for LAN and Office 365 Authentication.
- If a user has already authenticated to their domain they do not need to re-authenticate to Office 365.

However the one element that this dœs not address is the potential requirement for stronger authentication, especially if the user is accessing Office 365 from a remote location.

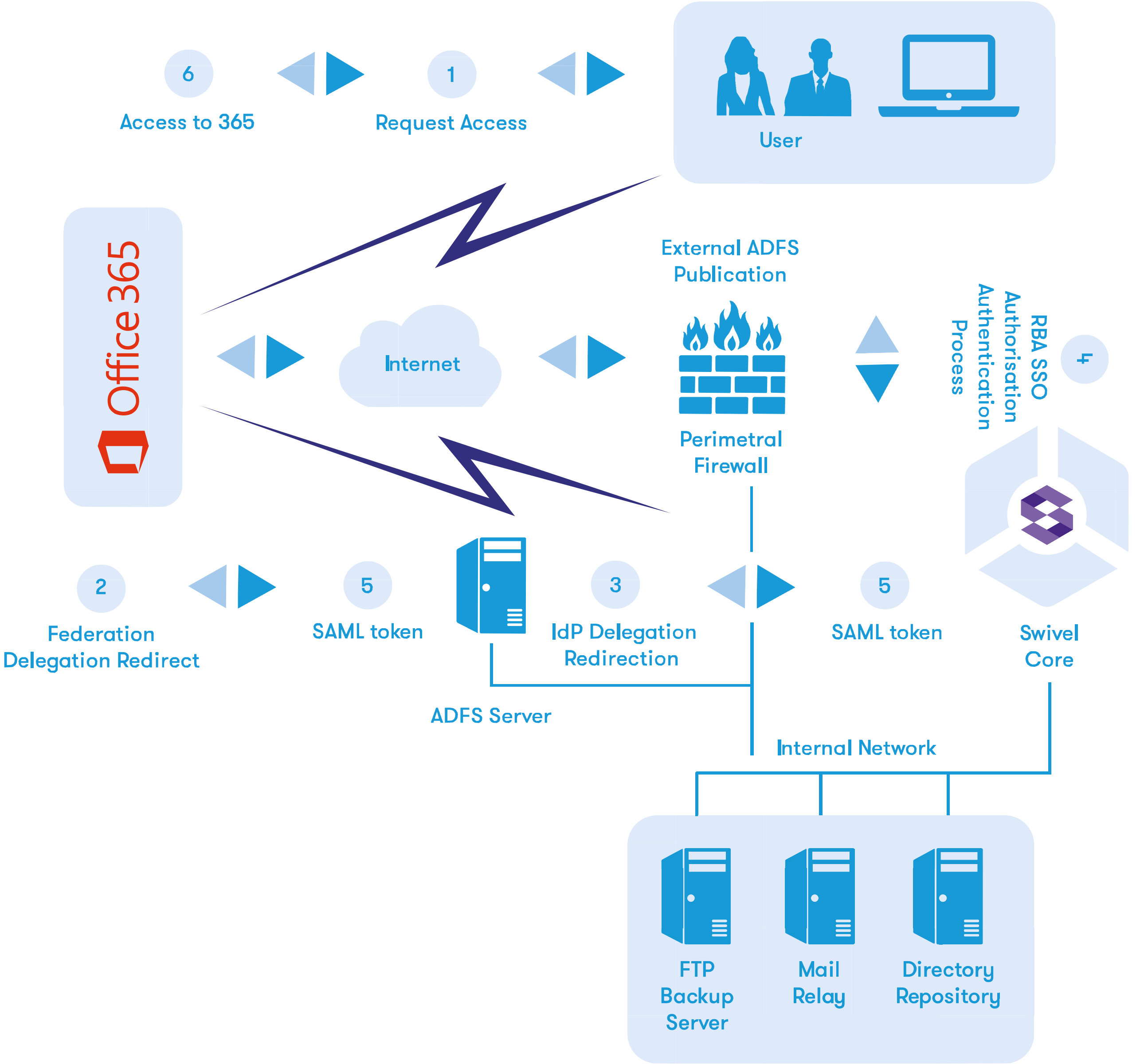
Risk-Based Authentication with ADFS:

Risk-based authentication (RBA) means requiring different levels of authentication depending on a number of risk factors. The clearest example is where additional levels of authentication would be requested if the user is accessing data from a location other than their office.

Using Swivel Secure's AuthControl Sentry® and Office 365, you can implement (RBA) by deploying AuthControl Sentry® as a filter against the ADFS Proxy only and not the internal ADFS servers.

In this scenario when the user is on the LAN and authenticated to the domain, when the user attempts to access Office 365 they are redirected to an ADFS server and this server confirms that the user has authenticated and automatically issues the secure token.

When the user is not authenticated to the domain, the user is redirected to the ADFS Proxy. The ADFS Proxy prompts the user for their username, password and Swivel Secure credentials i.e. the one time-code (OTC). Only when both credentials have been successfully submitted is the secure token issued to the user.



Office 365 with ADFS diagram process step-by-step

1. The user requests access to Office 365
2. Office 365 uses the Federation Delegation Redirect to the ADFS server
3. ADFS then delegates the request to AuthControl Sentry as a Trusted Claims Provider
4. AuthControl Sentry checks the user's credentials including Active Directory password and establishes if stronger authentication is required based on parameters such as their Geo-location, group membership, IP range etc
5. AuthControl Sentry issues a SAML token (cookie) to the user upon successful authentication
6. User is redirected back to Office 365 with the SAML token (cookie) which signs them in automatically

Other Cloud Services:

ADFS is based on SAML standards so the example provided above is not exclusive to Office 365, other integrations can benefit from the same configuration.

AuthControl Sentry® **multi-factor authentication.**

Swivel Secure is an industry leader in authentication solutions. Founded in 2001, Swivel Secure protects thousands of organizations in over 52 countries.

The award winning AuthControl Sentry® delivers multi-factor authentication, combined with risk-based authentication and single sign-on for securely authenticating all applications, both cloud and on-premise.