Swivel Secure, ADFS and Office 365

Authentication for Office 365

Abstract

This whitepaper 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.

9th September 2011

Chris Russell

SWIVEL
the power of knowing

Contents

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 whitepaper 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.

Office 365 and ADFS

An enterprise can configure Office 365 to use ADFS. For details refer to the Microsoft website, http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652539.aspx

If an Enterprise does this when a member of that Enterprise attempts to access Office 365, Office 365 uses ADFS to check with the Enterprise's ADFS servers to check if the user should be granted access.

The technology behind this is that Office 365 redirects the user to the Enterprises ADFS servers and within this redirect there is 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 redirect the user back to Office 365 with a SAML assertion which will then allow Office 365 to grant the user access
- OR
- If the user has already authenticated to the domain, immediately respond with the SAML assertion and not require the user 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 an user's AD account is disabled then 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 credential 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 does not address is the potential requirement for stronger authentication, especially if the user is accessing Office 365 from a remote location.

ADFS and Strong Authentication

In order to add strong authentication to Office 365 you can deploy a filter to the ADSF server. This filter ensures that the user must complete a Swivel-based authentication before they are issued with their ADFS Token.

To do this the following steps are required.

- Set the ADFS Server to use Forms Based Authentication.
- Install the provided login page (this can be customised to your requirements).
- Deploy and configure the filter to use you Swivel Authentication Server.

Now, when the user is redirected to the ADFS server they are presented with the Swivel Login page that will prompt them for their

1. Username
2. Active Directory Password
3. Swivel one-time code

The filter will check the Swivel credential with the Authentication Server and if it is correct will submit the username and AD credential. If the AD credential is correct then the user will be issued with the ADFS token as before.

The filter can be deployed against any ADFS server but id this is done the user will need to authenticate to Office 365 even if they have already authenticated to their domain.

Risk Based Authentication

Risk based authentication means requiring different levels of authentication depending on a number of risk factors. Perhaps the clearest example of this is to require additional levels of authentication if the user is accessing data from a location other than their office.

Using Swivel and Office 365 you can achieve this by deploying the Swivel 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 credentials. Only both credentials have been successfully submitted is the secure token issued to the user.

Other Cloud Services

ADFS is actually based on the SAML standards which means the above model is not reserved just for Office 365.