Office 365 Kim

https://comm.support.ca.com/kb/how-to-configure-o365-integration-in-pam/kb000072500Top of Form

**Environment:**

Any version of PAM supporting O365 integration.

**Instructions:**

**Before proceeding, you must ensure that your ADFS(STS) and your O365 is integrated successfully and your enterprise users are able to login via browser.**
Then you can configure the following in the PAM GUI.

**Security Token Service (STS) Endpoint URL**
This is your ADFS server in your enterprise.
STS is a component in ADFS that you would have configured.
The **https://<FQHN>/adfs/services/trust/2005/usernamemixed** is one of the applications already deployed on ADFS (without involving PAM) and this is where the O365 exchange some information with STS.

If your STS is hosted on https://dummy.com then you should enter https://dummy.com/adfs/services/trust/2005/usernamemixed as the "Security Token Service (STS) Endpoint URL.
It is hardcoded and you just need to replace the <FQHN> with whatever hostname you are using for the STS.

**Security Token Service (STS) Endpoint Reference URI**
This would have been more clearer if it just said, "Enter O365 EntityID"
This is Microsoft decided EntityID value to be used for O365 so you just need to enter "**urn:federation:MicrosoftOnline**"

**Microsoft Online Portal URL**
This is the login page and also where MicrosoftOnline accepts SAML token. This is also decided by Microsoft so just enter "**https://login.microsoftonline.com/login.srf**".

**Microsoft Online Portal Context Data**
If you have a fiddler(from telerik) or any HTTP header tracing tools you would be able to get the request going to "**https://login.microsoftonline.com/login.srf**" URL.
The value of "**wctx**" parameter **VALUE** would be what you need to copy and paste in to this field.

**Additional Information:**

<https://communities.ca.com/people/SungHoon_Kim/blog/2018/03/01/pam-and-o365-integration>

[Microsoft Office 365 Configuration - CA Privileged Access Manager - 3.1.1 - CA Technologies Documentation](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fdocops.ca.com%2Fca-privileged-access-manager%2F3-1-1%2FEN%2Fimplementing%2Fconfigure-your-server%2Fmicrosoft-office-365-configuration)

And before we go further into the details, I will need to provide some overview of the prerequisites and some of the things that are good to know.

When you want to start setting up O365, the common use case is that you already have an Active Directory Domain and AD users.

You want AD users to access O365 with the AD Domain Credentials.

And there can be several options to login the user.

Federation(using SAML Token) is one of the options.

==============================================

To setup O365, you will need to have a Web Service called Security Token Service(aka STS) hosted locally within your enterprise.

Active Directory Federation Service(aka ADFS) can provide this service.

There can be other 3rd party Federation Capable Web Access Management softwares(like CA Single Sign-On) that provides the STS too.

==============================================

You will need to setup ADFS and host STS service which **requires to be accessible from internet**.

And this STS service must be hosted over **HTTPS**.

And the Server Certificate for HTTPS must be **issued by a Publicly Trusted Certificate Authority**(such as the Verisign or Comodo and etc).

And this STS service need to have registered internet domain and resolvable from **public DNS**.

Let's say you have registered internet domain "dummy.com" and at the registrar website you have configured the DNS to be forwarded to your enterprise DNS server to ensure your web services and their FullyQualifiedHostNames(aka FQHN) are resolvable from public DNS.

In this sample, [https://dummy.com](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fdummy.com) is the server that is hosting STS.

Yours might be [https://adfs123.test.lab](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fadfs123.test.lab) or [https://sts.xyz.lab](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fsts.xyz.lab) and so on.

So, you already have ADFS deployed with STS service and it is accessible from internet at [https://dummy.com](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fdummy.com)

================================================

To configure the O365, you will have to have O365 licenses for the users.

If you have MSDN, you will need to have premium one or above to get 1 user license and you can configure O365.

How the O365 is configured, I won't cover here as Microsoft Document should have sufficient information.

For those who are guessing how it is managed, you actually install some software(powershell for Azure) on the machine running AD and you use powershell commandline to logon to O365 and administer from command line.

That is where you can import certificates, switch the login mechanism to Federation and so on.

=================================================

So you are able to access [https://portal.microsoftonline.com](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fportal.microsoftonline.com) and when you enter your email address you get redirected to your company login page.

Once you submit the correct credentials you get redirected to [https://login.microsoftonline.com/login.srf](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsoftonline.com%2Flogin.srf) and get access to the Office Applications.

**Customer must be at this stage already before they can talk about PAM integration!!!**

===================================================

Now you can refer to the PAM documentation.

| **Documentation** |
| --- |
| 1. Go to **Configuration**, **3rd Party**, **Microsoft Office 365**.
2. Enter your Office 365 configuration information:
	1. Enter the **Security Token Service (STS) Endpoint URL**. In general, specify the appropriate URL that is exposed by your organization Active Directory Federation Service (ADFS). The endpoint must support the WS-Trust 2005 (username mixed mode) protocol.For example: [https://](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2F)<ADFS Server FQDN>/adfs/services/trust/2005/usernamemixedThis value is user-supplied and might change.
	2. Enter the **Security Token Service (STS) Endpoint Reference URI**. When ADFS is federated with Microsoft Online (MSOL), this value is typically:urn:federation:MicrosoftOnline
	3. Enter the **Microsoft Online Portal URL**. The URL of the MSOL portal. For example: [https://login.microsoftonline.com/login.srf](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsoftonline.com%2Flogin.srf)
	4. Enter the **Microsoft Online Portal Context Data**. This parameter contains context information that is relevant to MSOL. Its value is derived by following the procedure for "creating a smart link" as described in Microsoft documentation.

The following sample shows how you might create your URL:wctx=wa=wsignin1.0&rpsnv=2&ct=1372192193&rver=6.1.6206.0&wp=MCMBI&wreply=https:%2F%2Fportal.microsoftonline.com%2Flanding.aspx%3Ftarget%3D%252fdefault.aspx&lc=1033&id=271346Take apart this URL by its parameters with line breaks that are added for clarity:wctx=wa=signin1.0&rpsnv=2&ct=1372192193&rver=6.1.6206.0&wp=MCMBI&wreply=https:%2F%2Fportal.microsoftonline.com%2Flanding.aspx%3Ftarget%3D%2Fdefault.aspx&lc=1033&id=271346Decoding the smart link is not a listed step in the Microsoft procedure, but we recommend decoding. A useful link for decoding is:[http://coderstoolbox.net/string/#!encoding=url&action=decode&charset=us\_ascii.](https://communities.ca.com/external-link.jspa?url=http%3A%2F%2Fcoderstoolbox.net%2Fstring%23%2521encoding%3Durl%26action%3Ddecode%26charset%3Dus_ascii)This value is user-supplied and might change. 1. Click **Save**.
2. Click **Ping** to test the information you entered.
 |

Ok, so here is my version.

You will need some level of understanding on what those are. Then things will be easier.

**Security Token Service (STS) Endpoint URL**

Federation is an agreement between 2 parties(aka Entities).

The 2 parties are

1) Identity Partner(aka IP)

2) Resource Partner(aka RP)

As the name suggests, IP is the party who has the usernames and passwords.

RP is where the services(like O365) are.

STS and PAM are at IP side.

And when you deploy ADFS and STS, that IIS Web Server is going to have Federation Applications Deployed.

The [https://](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2F)<FQHN>/adfs/services/trust/2005/usernamemixed is one of the applications already deployed on ADFS (without involving PAM) and this is where the O365 exchange some information with ADFS/STS.

If your STS is hosted on [https://dummy.com](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fdummy.com) then you should enter[https://dummy.com/adfs/services/trust/2005/usernamemixed](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Fdummy.com%2Fadfs%2Fservices%2Ftrust%2F2005%2Fusernamemixed) as the "Security Token Service (STS) Endpoint URL.

It is hardcoded and you just need to replace the <FQHN> with whatever hostname you are using for the STS.

**Security Token Service (STS) Endpoint Reference URI**

This would have been more clearer if it just said, "Enter O365 EntityID"

EntityID is a unique name for particular party(which can be either the IP or RP) and it is a name used to identify each other between the federation parties.

Microsoft said they named O365 as "urn:federation:MicrosoftOnline" so you just need to enter this value.

All customers federating to O365 (regardless of what product they use for federation) would need to enter this EntityID as the O365.

It is case sensitive so enter exactly as above.

**Microsoft Online Portal URL**

When you try to logon to O365, you would be redirected to login page so you can identify yourself(authenticate).

Microsoft has decided that they would use [https://login.microsoftonline.com/login.srf](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsoftonline.com%2Flogin.srf) as the login page.

This page also accepts SAML Token.

All customers federating to O365 (regardless of what product they use for federation) would need to enter this URL.

**Microsoft Online Portal Context Data**

This is the tricky part where people gets confused.

The documentation certainly did improve but you may need more information.

If you are familiar with capturing HTTP header trace, it would be an advantage.

If you know how to use Fiddler(from Telerik) then this would be easy. You can use any HTTP analyser kind of tools.

FYI: [How to install fiddler and capture https traffic](https://communities.ca.com/people/SungHoon_Kim/blog/2016/02/15/how-to-install-fiddler-and-capture-https-traffic)

You will first have to use the normal browser(PAM is not involved yet) and perform the normal login accessing the O365.

[Fiddler Sample#1 - GET request to [https://login.microsoftonline.com/login.srf?xxxxyyyyzzzz](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsoftonline.com%2Flogin.srf%3Fxxxxyyyyzzzz) ]



[Fiddler Sample#2 - POST request to [https://login.microsftonline.com/login.srf](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsftonline.com%2Flogin.srf) ]



When you submit your email at the O365 login page you will see the browser going to [https://login.microsoftonline.com/login.srf](https://communities.ca.com/external-link.jspa?url=https%3A%2F%2Flogin.microsoftonline.com%2Flogin.srf) regardless of whether it is GET or POST request.

In the Request, the Query Parameter has "**wctx**"

The value is what you want to enter as "Microsoft Online Portal Context Data".



Hopefully this information will make things easier.

Bottom of Form