SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Microsoft O365 Integration Guide

SecurAccess Integration Guide

Version 1.0 – 08/18

O365 (via ADFS) Integration Guide

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Microsoft Office 365 via ADFS (Active Directory Federation Service) for authorisation and access control.

The software used for the integration process is listed below:

ADFS 4.0 (Active Directory Federation Service - Windows 2016)
WAP (Web Application Proxy – Windows 2016)
SecurEnvoy SecurAccess Release v9.3.501

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2012 or higher.
  - An LDAP or Lightweight Directory Service database of users

  Note: Please see SecurEnvoy's SecurAccess version 9.3 deployment guide on how to setup MFA server solution (On the www,securenvoy.com website)

- An ADFS Server running version 3.0 and above, (previous versions of ADFS may work but have not been tested with full functionality)

- A Web Application Proxy (WAP) located in a DMZ and secured by a firewall

- This guide assumes that ADFS has been installed and previously configured to authenticate O365 users with a domain username and password already.

- Familiarity with the following technologies:
  - RADIUS configuration
  - Active Directory Federation Services Interface

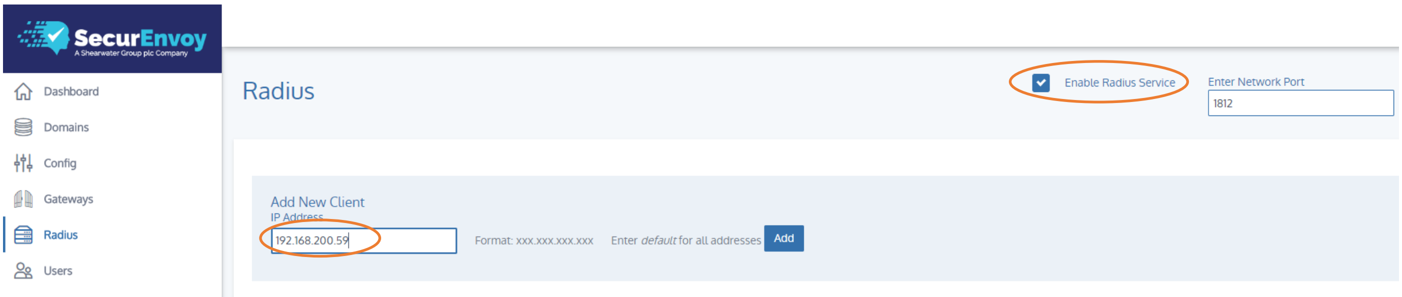
1.4 Authentication

The following section describes the steps required to configure ADFS to authenticate users via RADIUS through the SecurEnvoy SecurAccess Solution.

1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the ADFS server to communicate and authenticate as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the IP address of the ADFS server and click "Add"



Radius

☑ Enable Radius Service

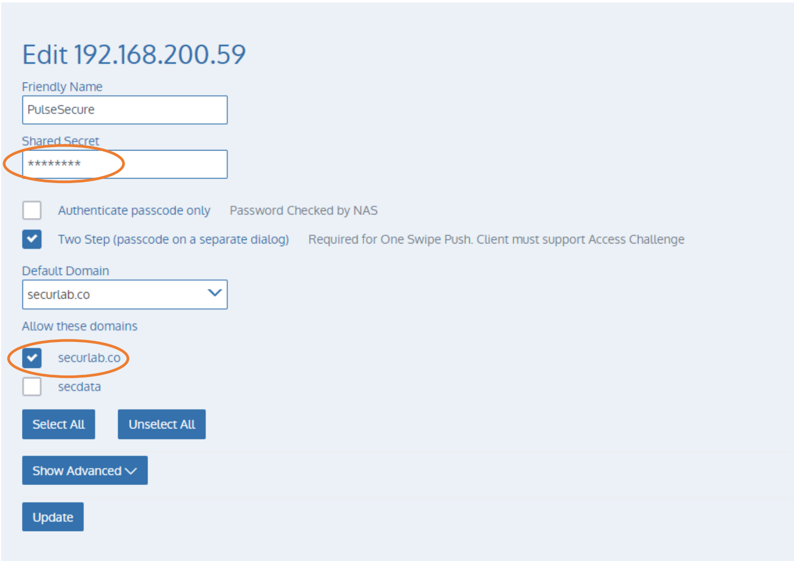
Enter Network Port: 1812

Add New Client

IP Address: 192.168.200.59

Format: xxx.xxx.xxx.xxx Enter *default* for all addresses

- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update



Edit 192.168.200.59

Friendly Name: PulseSecure

Shared Secret: ********

□ Authenticate passcode only Password Checked by NAS

☑ Two Step (passcode on a separate dialog) Required for One Swipe Push. Client must support Access Challenge

Default Domain: securlab.co

Allow these domains

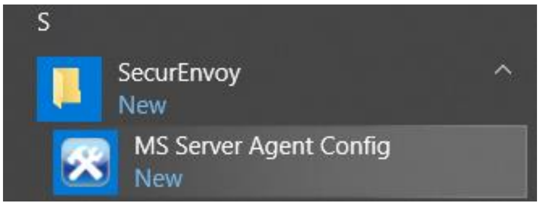
☑ securlab.co

□ secdata

From the ADFS console, locate and run the SecurEnvoy Server Agent installer which can be found in the latest downloaded SecurEnvoy software folder or ZIP file.

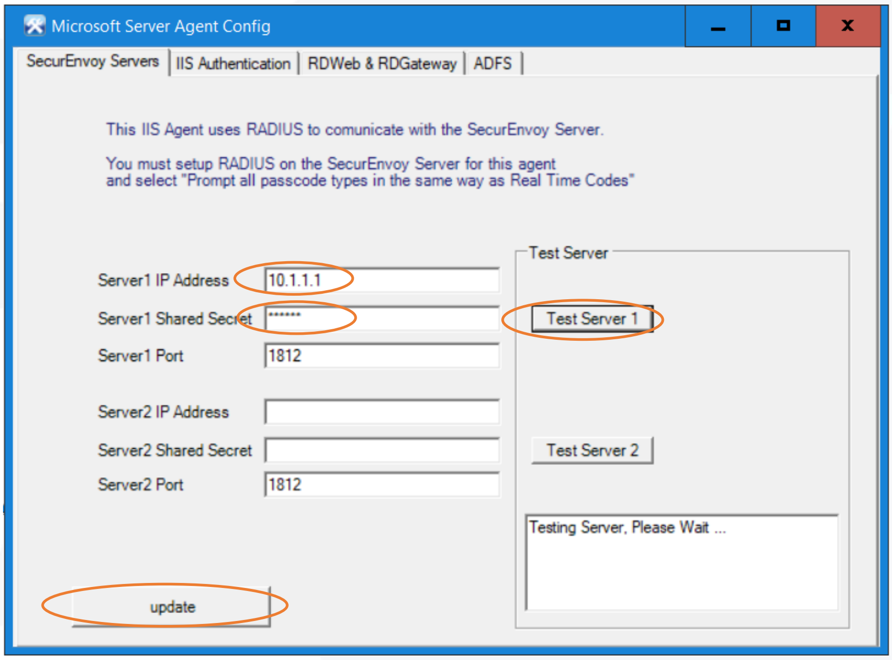
securenvoy.zip\Releasex.x.xxx\Agents\Microsoft Server Agent\setup.exe

On successful installation of the agent, locate and run the server agent



From the configuration console, we will configure the details of the SecurEnvoy Server that will authenticate O365 domains users.

Enter in the IP address of the SecurEnvoy Server and the Shared Secret, configured in section 1.41 of this document.
Once details have been entered click on Test Server 1 to confirm that the SecurAccess server is IP reachable and is accepting authentication challenges with the correct shared key.



This IIS Agent uses RADIUS to comunicate with the SecurEnvoy Server.

You must setup RADIUS on the SecurEnvoy Server for this agent
and select "Prompt all passcode types in the same way as Real Time Codes"

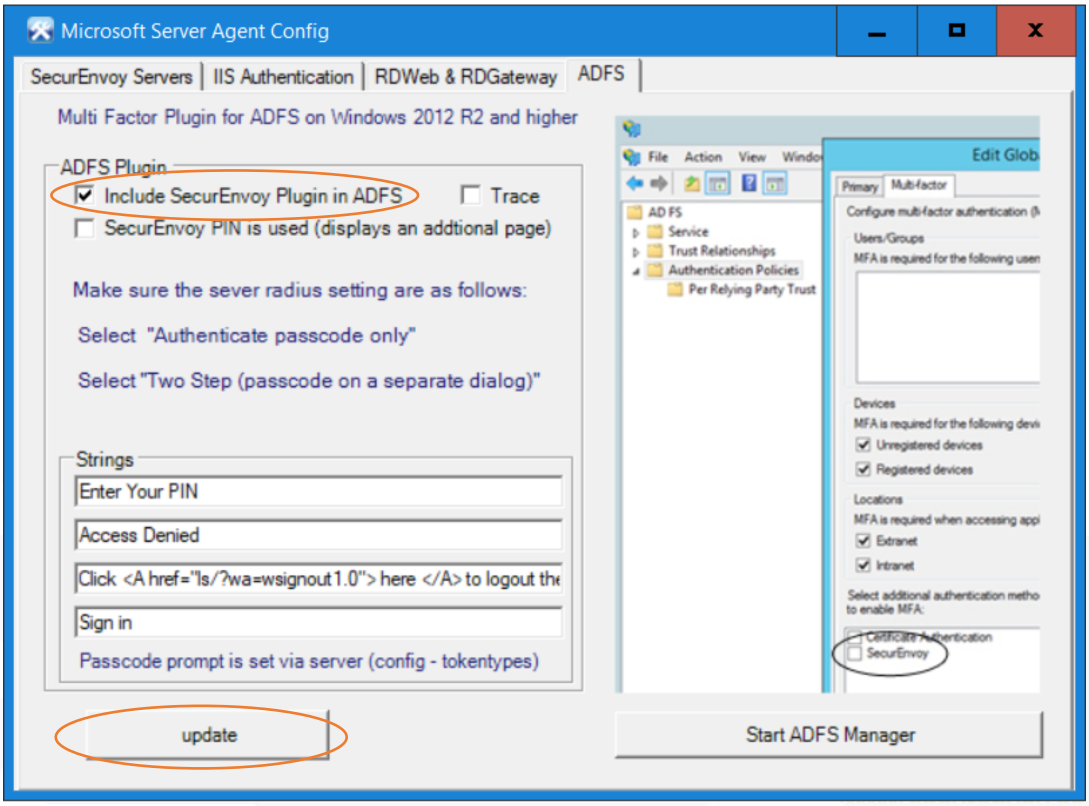
Server1 IP Address: 10.1.1.1
Server1 Shared Secret: ******
Server1 Port: 1812

Server2 IP Address:
Server2 Shared Secret:
Server2 Port: 1812

Testing Server, Please Wait ...

1.41 Setup RADIUS – ADFS

By selecting the ADFS tab at the top of the Microsoft Server Agent Config, this will allow us to configure ADFS to support the redirection of user authentication to SecurEnvoy MFA.
Tick "Include SecurEnvoy Plugin in ADFS" and click Update at the bottom of the page.



Microsoft Server Agent Config

SecurEnvoy Servers | IIS Authentication | RDWeb & RDGateway | ADFS

Multi Factor Plugin for ADFS on Windows 2012 R2 and higher

ADFS Plugin

☑ Include SecurEnvoy Plugin in ADFS ☐ Trace

☐ SecurEnvoy PIN is used (displays an addtional page)

Make sure the sever radius setting are as follows:

Select "Authenticate passcode only"

Select "Two Step (passcode on a separate dialog)"

Strings

Enter Your PIN

Access Denied

Click <A href="ls/?wa=wsignout1.0"> here </A> to logout the

Sign in

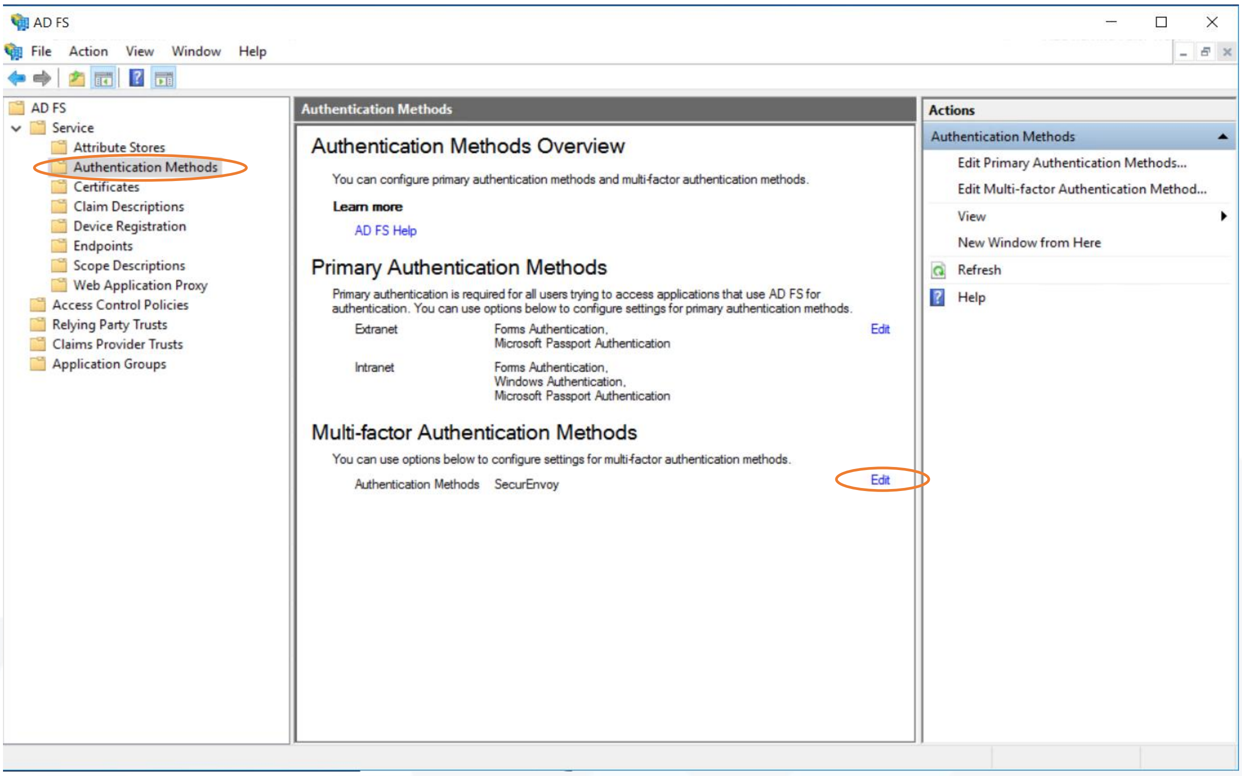
Passcode prompt is set via server (config - tokentypes)

Click on "Start ADFS Manager" to load the ADFS configuration.

1.42 Configure ADFS – MFA Authentication

On loading of the ADFS configuration manager, we will look to configure ADFS to utilise SecurEnvoy as the Multi-Factor Authentication method.

Select Authentication Methods from the left-hand navigation window and then click on Edit



Authentication Methods Overview

You can configure primary authentication methods and multi-factor authentication methods.

Learn more

AD FS Help

Primary Authentication Methods

Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.

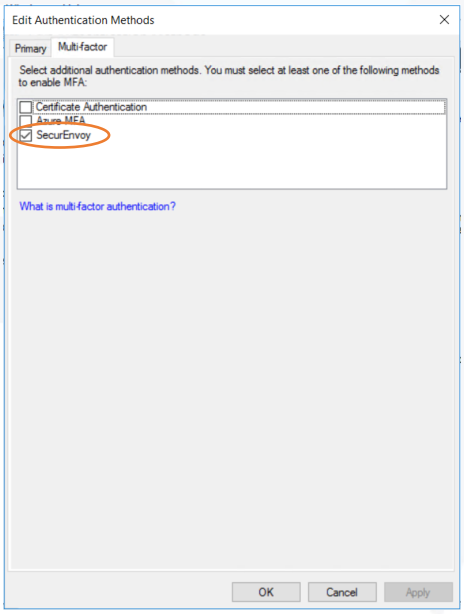
Extranet	Forms Authentication, Microsoft Passport Authentication	Edit
Intranet	Forms Authentication, Windows Authentication, Microsoft Passport Authentication	

Multi-factor Authentication Methods

You can use options below to configure settings for multi-factor authentication methods.

Authentication Methods SecurEnvoy Edit

Make sure SecurEnvoy is ticked in the authentication methods and click OK to confirm the changes.



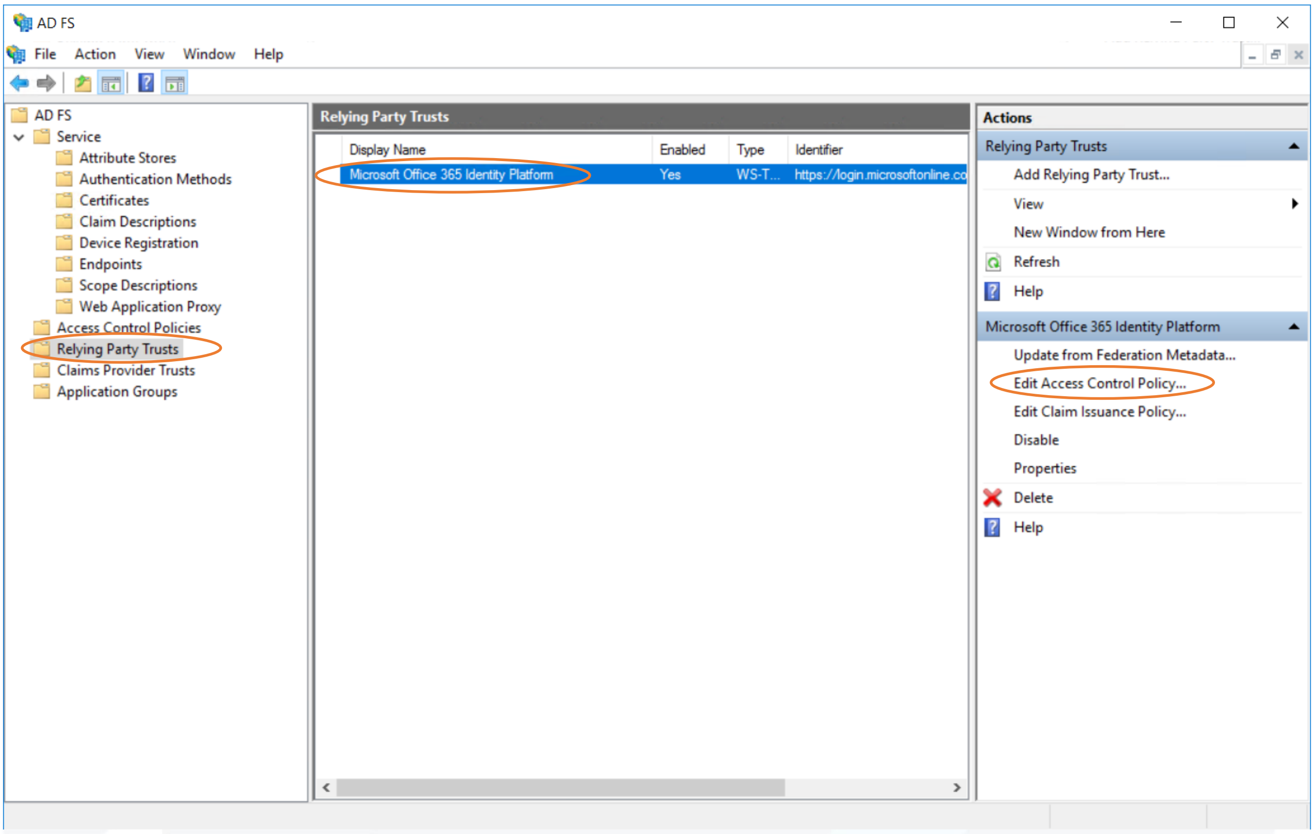
Select additional authentication methods. You must select at least one of the following methods to enable MFA:

□ Certificate Authentication
□ Azure MFA
☑ SecurEnvoy

What is multi-factor authentication?

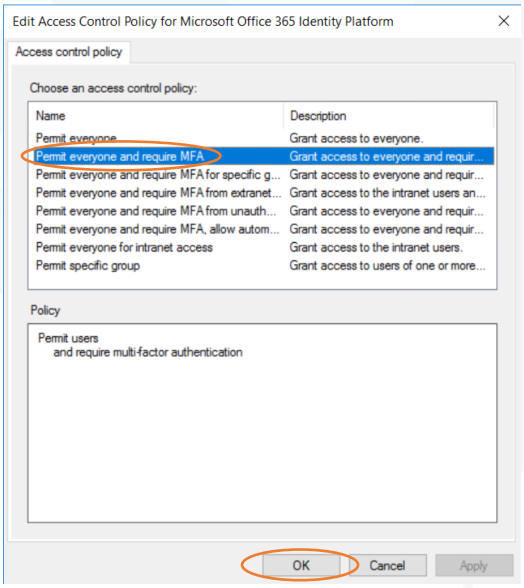
We will then need to update the access control Policy for the Relying Party. In this case its Microsoft Office 365 Identity Platform.

Select Relying Party Trusts from the left-hand Navigation Window and highlight “Microsoft Office 365 Identity Platform”
On highlighting the Party Trust, select Edit Access Control Policy from the Actions menu.



Display Name	Enabled	Type	Identifier
Microsoft Office 365 Identity Platform	Yes	WS-T...	https://login.microsoftonline.co

On editing the Access Control Policy, the following dialogue will be presented.
Select Permit Everyone and require MFA from the list and click OK


Edit Access Control Policy for Microsoft Office 365 Identity Platform
Access control policy
OK
Cancel
Apply

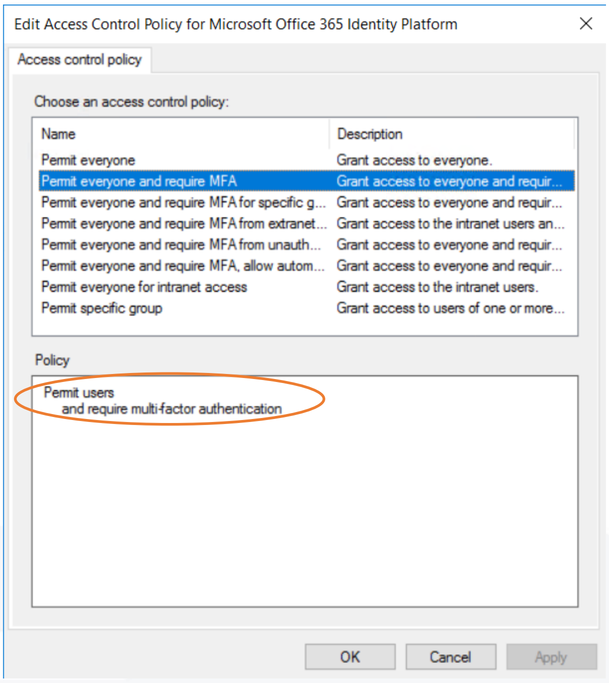
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir...
Permit everyone and require MFA for specific g...	Grant access to everyone and requir...
Permit everyone and require MFA from extranet...	Grant access to the intranet users an...
Permit everyone and require MFA from unauth...	Grant access to everyone and requir...
Permit everyone and require MFA, allow autom...	Grant access to everyone and requir...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

Policy

Permit users
and require multi-factor authentication

It has been identified that in some circumstances it is not possible to update an O365 Relying party to request an MFA authentication from the GUI configuration in ADFS.
If this is the case, it is possible to enable this using windows PowerShell.


Edit Access Control Policy for Microsoft Office 365 Identity Platform
Access control policy

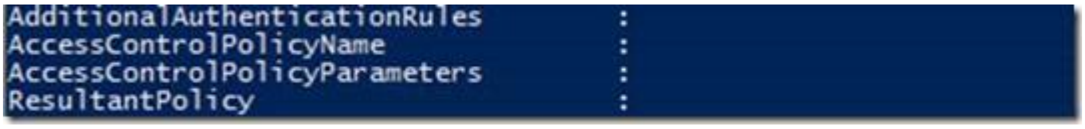
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir...
Permit everyone and require MFA for specific g...	Grant access to everyone and requir...
Permit everyone and require MFA from extranet...	Grant access to the intranet users an...
Permit everyone and require MFA from unauth...	Grant access to everyone and requir...
Permit everyone and require MFA, allow autom...	Grant access to everyone and requir...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

Policy

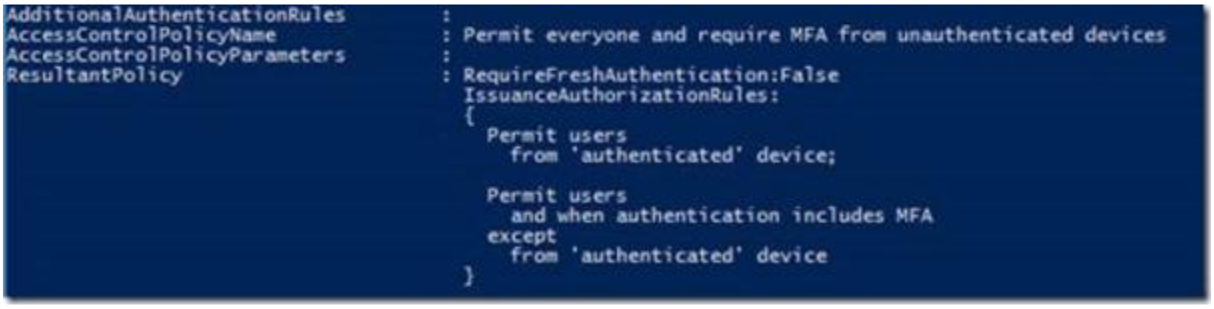
```
Permit users
  and require multi-factor authentication
```

Looking at our O365 RP in PowerShell (`Get-ADFSRelyingPartyTrust`), we see no access policies configured. Under the O365 Relying Party it's blank.



```
AdditionalAuthenticationRules          :
AccessControlPolicyName                :
AccessControlPolicyParameters          :
ResultantPolicy                        :
```

Compare this to an RP that does have an access control policy configured:

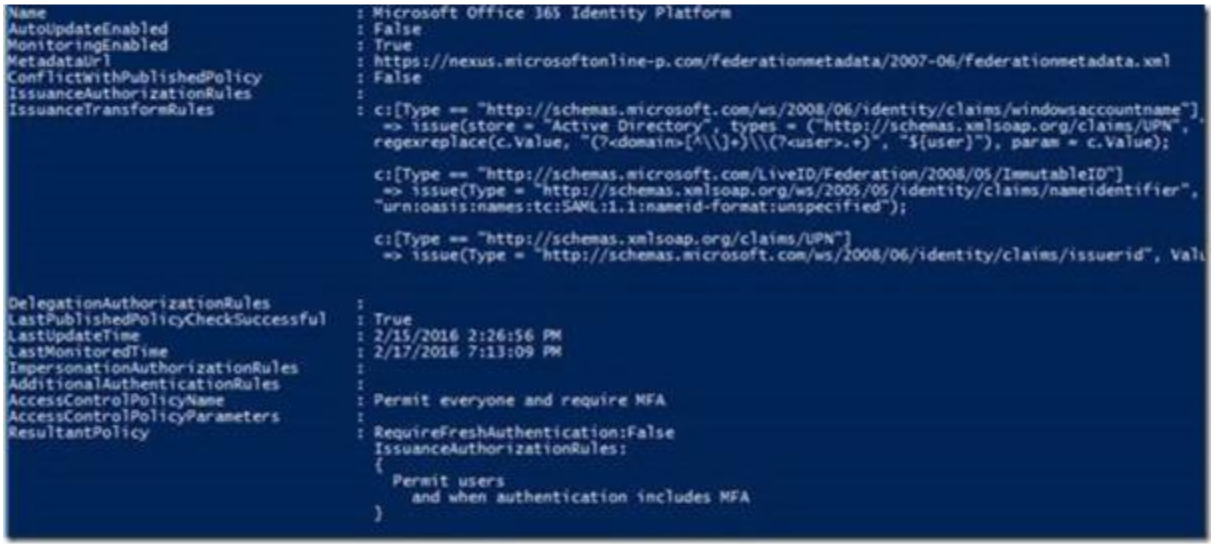


```
AdditionalAuthenticationRules          :
AccessControlPolicyName                : Permit everyone and require MFA from unauthenticated devices
AccessControlPolicyParameters          :
ResultantPolicy                        : RequireFreshAuthentication:False
                                         IssuanceAuthorizationRules:
                                         {
                                           Permit users
                                             from 'authenticated' device;

                                           Permit users
                                             and when authentication includes MFA
                                           except
                                             from 'authenticated' device
                                         }
```

Since the UI doesn't allow enabling MFA in an access policy for our O365 RP, playing around with PowerShell reveals that it is possible using the `Set-ADFSRelyingPartyTrust` cmdlet.

```
Set-AdfsRelyingPartyTrust -AccessControlPolicyName 'Permit everyone and require MFA' -
targetidentifier https://login.microsoftonline.com/extSTS.srf
```

Check the O365 relying party (`Get-ADFSRelyingPartyTrust`) that an Access Control Policy has been added.



```
Name                                : Microsoft Office 365 Identity Platform
AutoUpdateEnabled                   : False
MonitoringEnabled                   : True
MetadataUrl                         : https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml
ConflictWithPublishedPolicy         : False
IssuanceAuthorizationRules          :
IssuanceTransformRules              : c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
                                       => issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/UPN",
                                      regexreplace(c.Value, "(?<domain>[^\\]+)\\(?<user>.+)", "${user}"), param = c.Value);

                                      c:[Type == "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"]
                                       => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
                                      "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");

                                      c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]
                                       => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid", Valu


DelegationAuthorizationRules        :
LastPublishedPolicyCheckSuccessful  : True
LastUpdateTime                      : 2/15/2016 2:26:56 PM
LastMonitoredTime                   : 2/17/2016 7:13:09 PM
ImpersonationAuthorizationRules     :
AdditionalAuthenticationRules       :
AccessControlPolicyName             : Permit everyone and require MFA
AccessControlPolicyParameters       :
ResultantPolicy                     : RequireFreshAuthentication:False
                                      IssuanceAuthorizationRules:
                                      {
                                        Permit users
                                          and when authentication includes MFA
                                      }
```

In the GUI, we then see the applied policy (`Permit Everyone and require MFA`) appearing.

1.5 Modern Authentication

1.51 Outlook Online, Client Authentication

Modern authentication in Office 365 enables authentication features like multi-factor authentication (MFA) and is based on the Active Directory Authentication Library (ADAL) and OAuth 2.0.

When you enable modern authentication in Exchange Online, it is possible to login to Office 365 mailboxes with Outlook 2016 and Outlook 2013 (version 15.0.4753 or later, with a required registry setting) clients. Other Outlook clients that are available in Office 365 (for example, Outlook Mobile and Outlook for Mac 2016) always use modern authentication as default to log in to Office 365 mailboxes.

You should synchronize the state of modern authentication in Exchange Online with Skype for Business Online to prevent multiple log in prompts in Skype for Business clients.

Connect to Exchange Online PowerShell as shown below
Windows PowerShell needs to be configured to run scripts, and by default, it isn't. Run the following command in an elevated Windows PowerShell window (a Windows PowerShell window you open by selecting Run as administrator):

```
Set-ExecutionPolicy RemoteSigned
```

Once the above has been enabled, it is then possible to connect to Exchange Online by typing the following within an elevated privileged PowerShell window.

```
$UserCredential = Get-Credential
```

Enable modern authentication by typing

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
Finish https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential
-Authentication Basic -AllowRedirection

Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

Note:
For Office 365 Germany, use the ConnectionUri value: https://outlook.office.de/powershell-liveid/ as a replacement.

- Finish by typing the following commands into the PowerShell Window

```
Import-PSSession $Session -DisableNameChecking
Remove-PSSession $Session
```

1.52 Skype For Business Online, Client Authentication

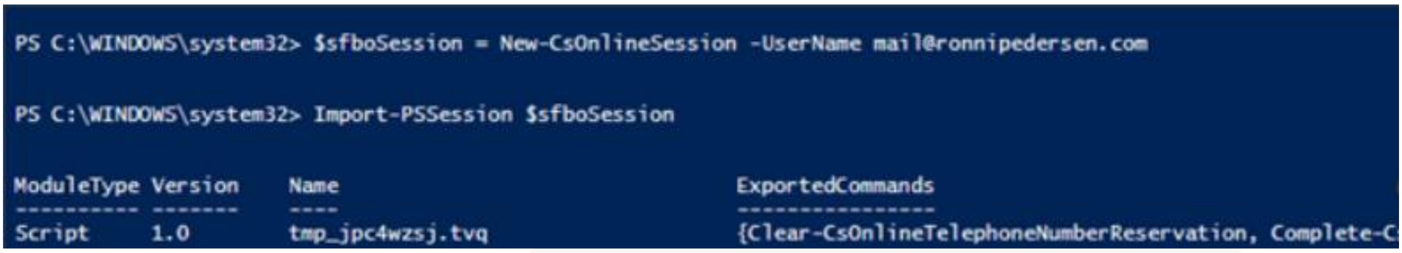
If using windows 2012 or earlier, it will be required to install Skype for Business Online, Windows PowerShell Module:

This is not required if connecting from a Windows 2016 server.

https://www.microsoft.com/en-us/download/details.aspx?id=39366

- Connect to Skype for Business using PowerShell replacing with your user/domain name,

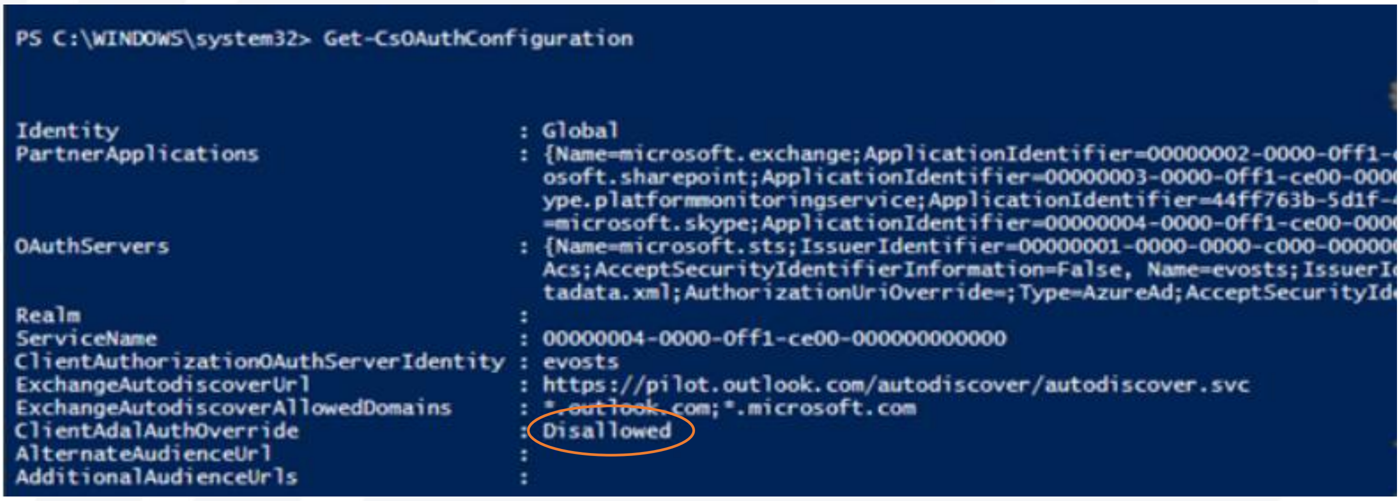
```
$sfboSession = New-CsOnlineSession -UserName user@domain.com
Import-PSSession $sfboSession
```



```
PS C:\WINDOWS\system32> $sfboSession = New-CsOnlineSession -UserName mail@ronnipedersen.com

PS C:\WINDOWS\system32> Import-PSSession $sfboSession

ModuleType Version    Name                           ExportedCommands
---------- -------    ----                           ----------------
Script     1.0        tmp_jpc4wzsj.tvq               {Clear-CsOnlineTelephoneNumberReservation, Complete-C
```

- Verify the current settings (optional)

```
Get-CsOAuthConfiguration
```



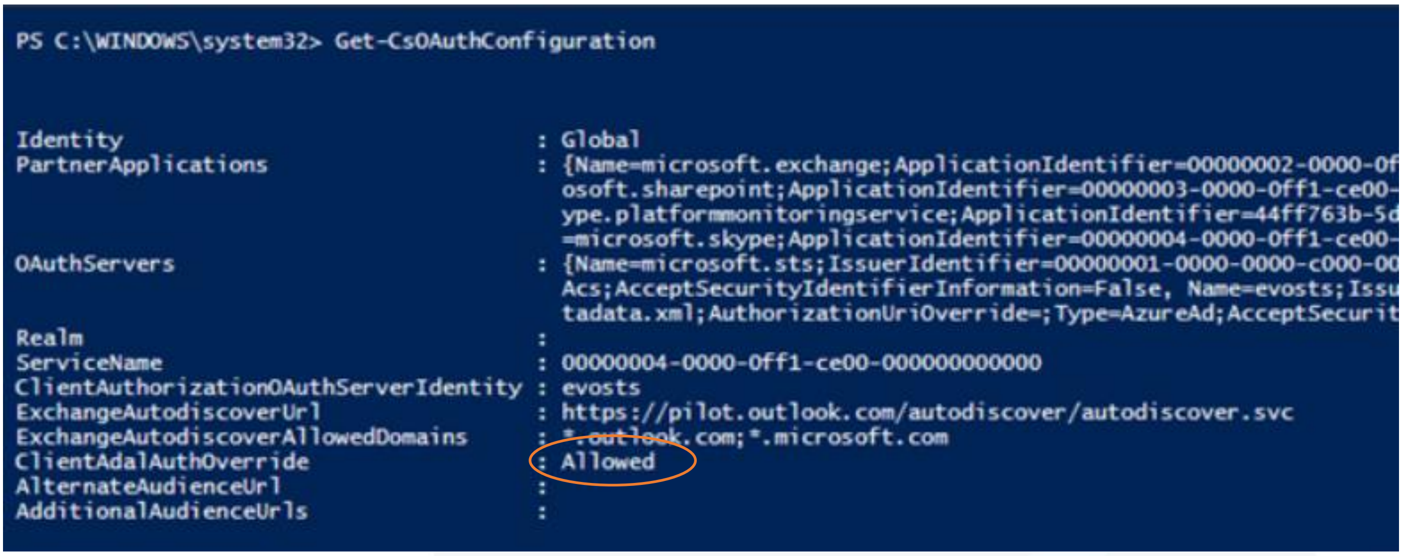
```
PS C:\WINDOWS\system32> Get-CsOAuthConfiguration


Identity                             : Global
PartnerApplications                  : {Name=microsoft.exchange;ApplicationIdentifier=00000002-0000-0ff1-
                                       osoft.sharepoint;ApplicationIdentifier=00000003-0000-0ff1-ce00-000
                                       ype.platformmonitoringservice;ApplicationIdentifier=44ff763b-5d1f-
                                       =microsoft.skype;ApplicationIdentifier=00000004-0000-0ff1-ce00-000
OAuthServers                         : {Name=microsoft.sts;IssuerIdentifier=00000001-0000-0000-c000-00000
                                       Acs;AcceptSecurityIdentifierInformation=False, Name=evosts;IssuerI
                                       tadata.xml;AuthorizationUriOverride=;Type=AzureAd;AcceptSecurityId
Realm                                :
ServiceName                          : 00000004-0000-0ff1-ce00-000000000000
ClientAuthorizationOAuthServerIdentity : evosts
ExchangeAutodiscoverUrl              : https://pilot.outlook.com/autodiscover/autodiscover.svc
ExchangeAutodiscoverAllowedDomains   : *.outlook.com;*.microsoft.com
ClientAdalAuthOverride               : Disallowed
AlternateAudienceUrl                 :
AdditionalAudienceUrls               :
```

- Enable modern authentication for Skype for Business Online

```
Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed
```

- Verify that the change was successful by running the following:

```
Get-CsOAuthConfiguration
```



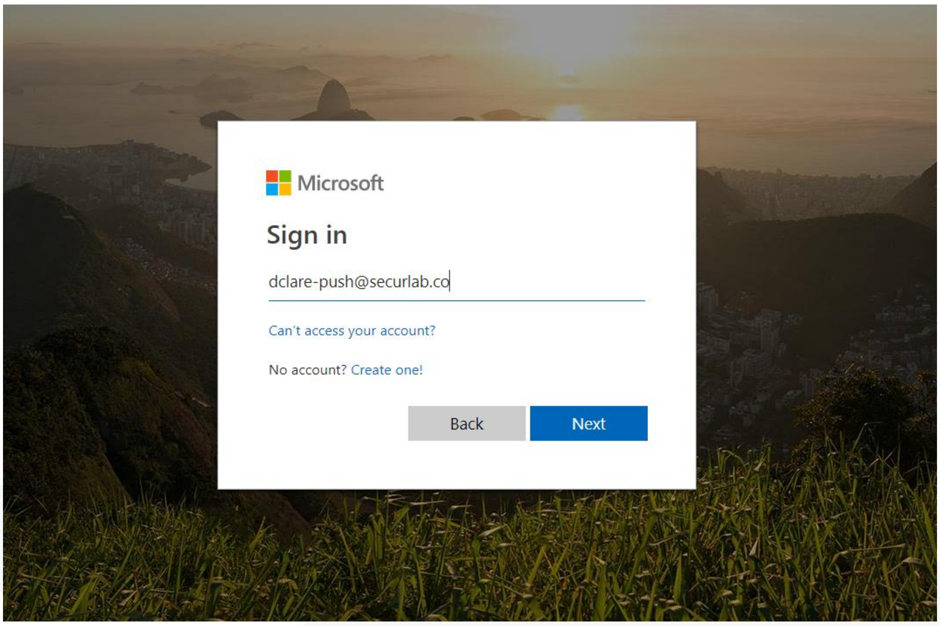
```
PS C:\WINDOWS\system32> Get-CsOAuthConfiguration


Identity                               : Global
PartnerApplications                    : {Name=microsoft.exchange;ApplicationIdentifier=00000002-0000-0f
                                         osoft.sharepoint;ApplicationIdentifier=00000003-0000-0ff1-ce00-
                                         ype.platformmonitoringservice;ApplicationIdentifier=44ff763b-5d
                                         =microsoft.skype;ApplicationIdentifier=00000004-0000-0ff1-ce00-
OAuthServers                           : {Name=microsoft.sts;IssuerIdentifier=00000001-0000-0000-c000-00
                                         Acs;AcceptSecurityIdentifierInformation=False, Name=evosts;Issu
                                         tadata.xml;AuthorizationUriOverride=;Type=AzureAd;AcceptSecurit
Realm                                  :
ServiceName                            : 00000004-0000-0ff1-ce00-000000000000
ClientAuthorizationOAuthServerIdentity : evosts
ExchangeAutodiscoverUrl                : https://pilot.outlook.com/autodiscover/autodiscover.svc
ExchangeAutodiscoverAllowedDomains     : *.outlook.com;*.microsoft.com
ClientAdalAuthOverride                 : Allowed
AlternateAudienceUrl                   :
AdditionalAudienceUrls                 :
```

Important: Please note, that it might take up to 24 hours before modern authentication starts to work.

1.6 Client Logon – O365 Web

The following section describes the login process and demonstrates what will be presented back to the user.

- Browse to your Office 365 Login Page

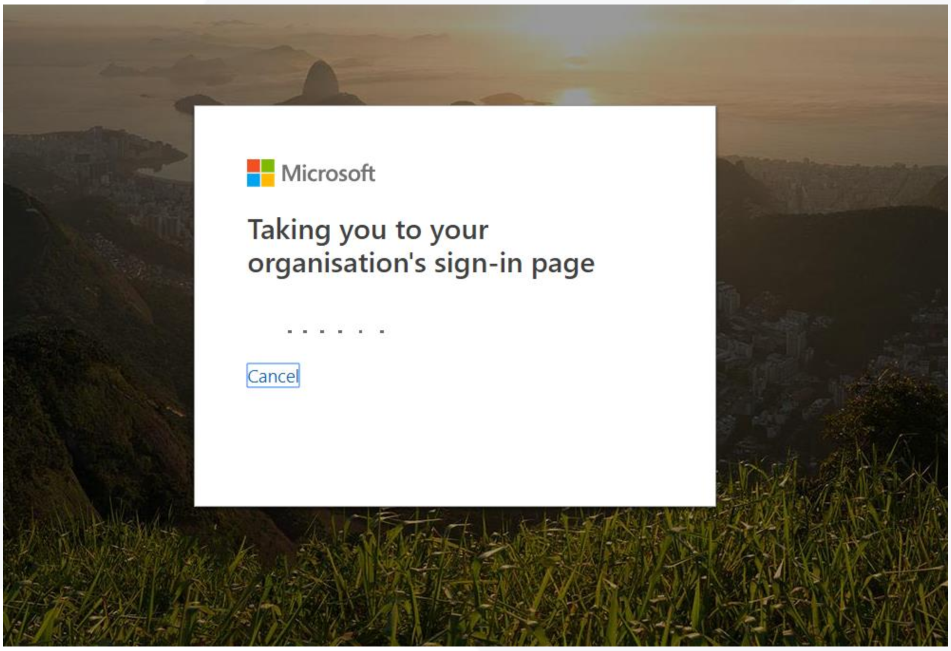


Microsoft

Sign in

dclare-push@securlab.co

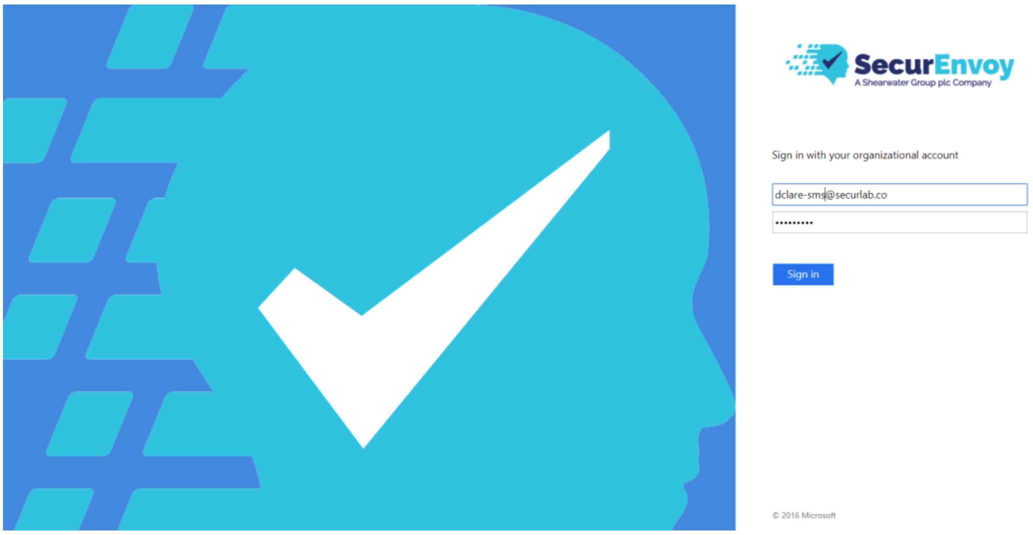
- Enter in your username from Active Directory or Local Directory Service account and the login will be redirected to your ADFS page via the Web Application Proxy



Microsoft

Taking you to your organisation's sign-in page

- On redirection to the ADFS web page, Enter domain username and password

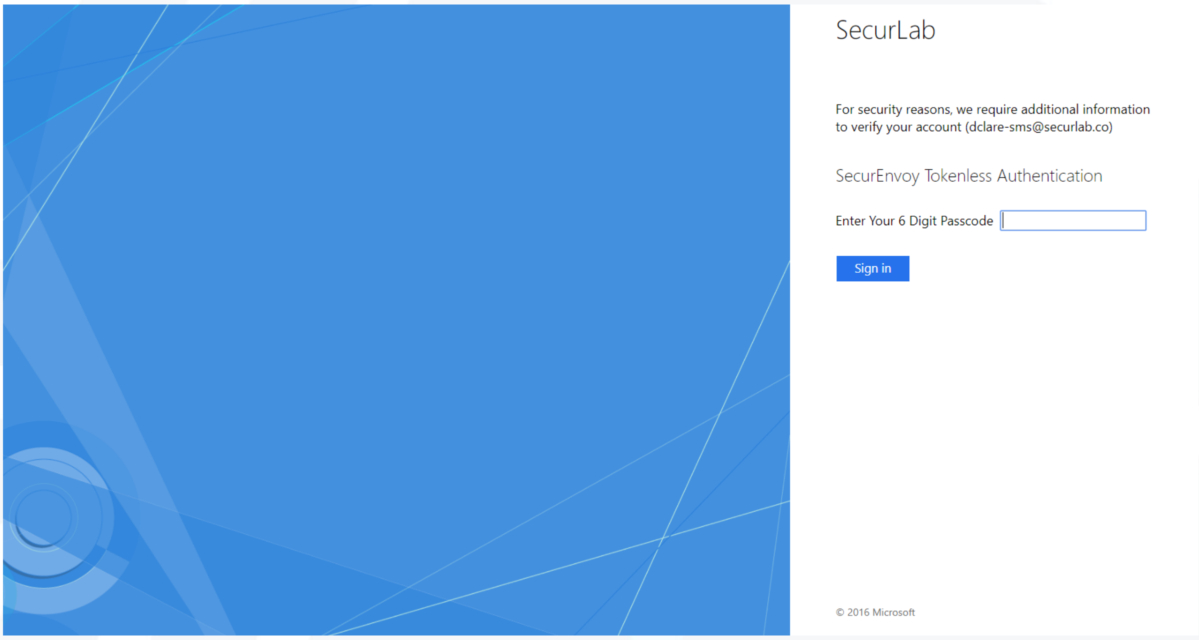


Sign in with your organizational account

dclare-sms@securlab.co

•••••••••

- At which point you will be asked to enter the 6-digit token received via SMS or soft token, or you will receive a Push notification to the phone if PUSH has been enabled.



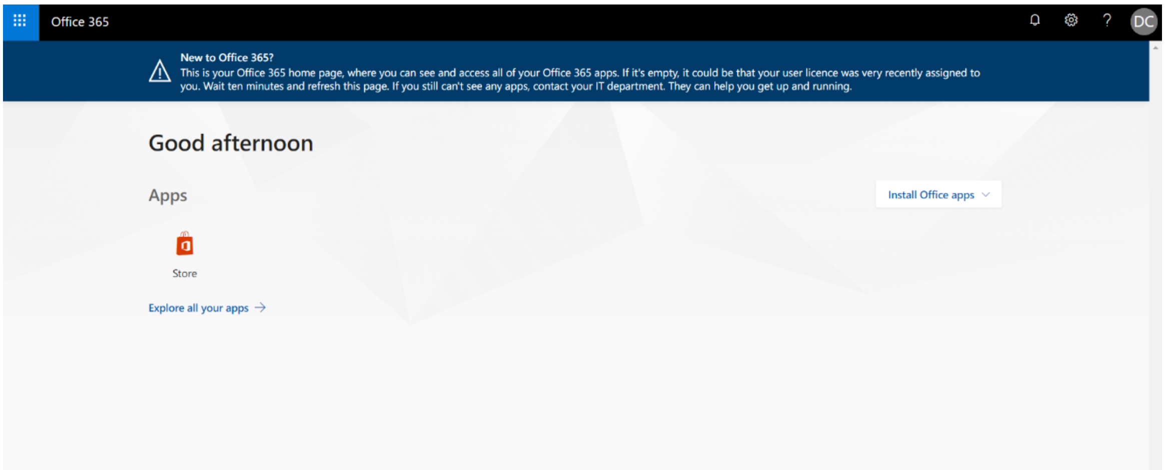
SecurLab

For security reasons, we require additional information to verify your account (dclare-sms@securlab.co)

SecurEnvoy Tokenless Authentication

Enter Your 6 Digit Passcode

- On successful login you will be presented with your O365 Applications



New to Office 365?
This is your Office 365 home page, where you can see and access all of your Office 365 apps. If it's empty, it could be that your user licence was very recently assigned to you. Wait ten minutes and refresh this page. If you still can't see any apps, contact your IT department. They can help you get up and running.

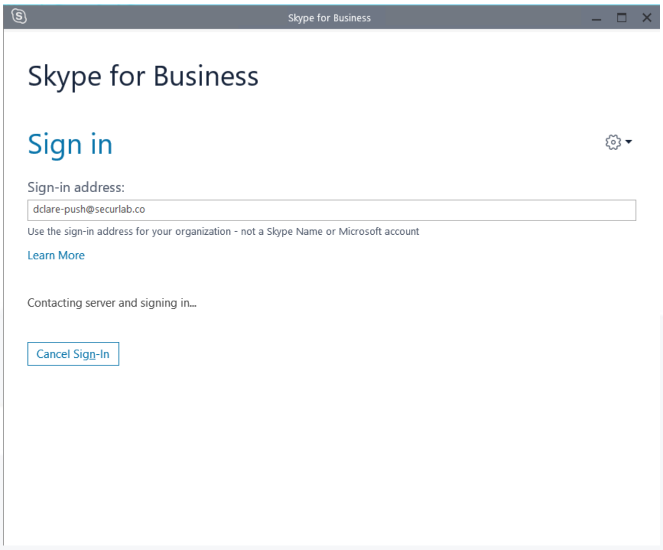
Good afternoon

Apps

1.7 Client Logon – O365 Modern Authentication

The following section describes the login process and demonstrates what will be presented back to the user when using the desktop app and authentication with Modern Authentication.

- Load Outlook, Skype for Business or OneDrive Client and at the prompt type in the users O365 sign-in address.



Skype for Business

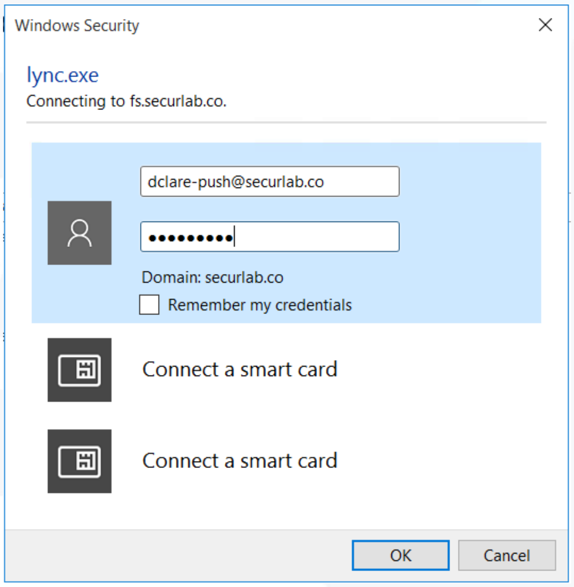
Sign in

Sign-in address:
dclare-push@securlab.co
Use the sign-in address for your organization - not a Skype Name or Microsoft account

Learn More

Contacting server and signing in...

On successful connection to O365 online, a redirect to the domain ADFS server will occur and presenting the user with the opportunity to enter the fully qualified domain username and domain password.

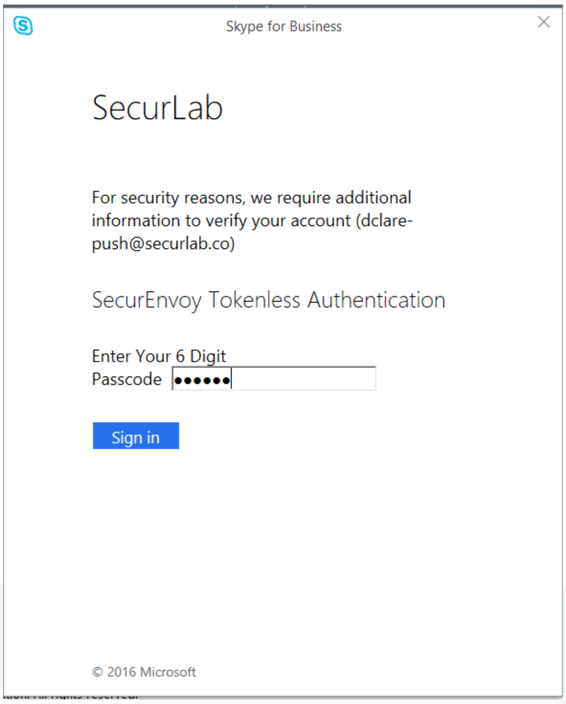


Windows Security

lync.exe
Connecting to fs.securlab.co.

dclare-push@securlab.co
••••••••••
Domain: securlab.co
□ Remember my credentials

Dependent on the token type used, the user will either receive a PUSH notification to the mobile app or will be presented with the opportunity to enter the 6-digit SMS or Mobile soft token.



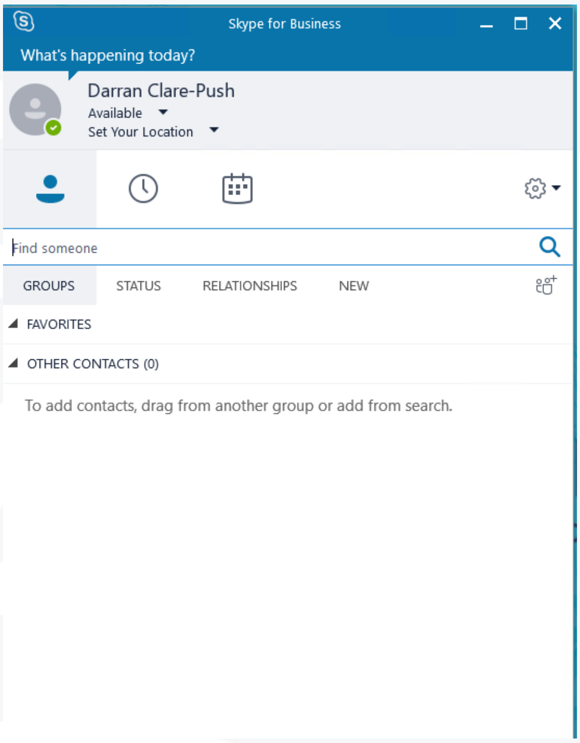
SecurLab

For security reasons, we require additional information to verify your account (dclare-push@securlab.co)

SecurEnvoy Tokenless Authentication

Enter Your 6 Digit Passcode ●●●●●●

© 2016 Microsoft



Darran Clare-Push
Available
Set Your Location

To add contacts, drag from another group or add from search.

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010
Company No. 04866711 VAT Number GB 862076128