

# Office365 Integration with SAASPASS

Single Sign-On, User Provisioning

[support@saaspass.com](mailto:support@saaspass.com)

## Contents

Before You Start Integration .....	3
Make Users Ready on SAASPASS .....	3
Single Sign-On Integration with SAASPASS .....	5
Verify Your Office365 Domain on SAASPASS .....	5
Create Office365 Application on SAASPASS.....	5
Federate Office365 Domain with SAASPASS .....	5
Federating Domain with SAASPASS Automatically .....	6
Federating Domain with SAASPASS Manually .....	6
Handling New Users.....	11
SAASPASS User Provisioning .....	11
Appendix A: Required Installations for Federation.....	14
Appendix B: Granting SAASPASS to Access Your Office365 Tenant .....	17
Appendix C: Ports Used by SAASPASS Products .....	21

In this document, you will find details about integrating your Office365 with SAASPASS. Once you completed integration, SAASPASS can handle Single Sign-On functionality for users and now can also manage user provisioning for you.

If you have any question about instructions here or anything else about Office365 integration, you can contact SAASPASS: [support@saaspass.com](mailto:support@saaspass.com)

## Before You Start Integration

You are about integrating your Office365 with SAASPASS mostly for Single Sign-On functionality. This means you will 'federate' your domain (e.g. yourdomain.com) with SAASPASS. By doing federation, you are delegating user authentication to SAASPASS and all domain users will be authenticated by SAASPASS. (Note that after federation, your domain is called 'Federated'. Otherwise it is 'Managed')

For any possible further needs, we strongly recommend you to keep a global administrator account on your Office365 tenant that is not belong to the domain you will federated. Generally, this would be account that belong to your default tenant domain which is like contoso.onmicrosoft.com.

Before doing federation, we recommend you to make your user accounts ready on SAASPASS and inform your users about SAASPASS usage.

## Make Users Ready on SAASPASS

On next step, you will federate your domain with SAASPASS and after you are done, all users that belong to the federated domain will be redirected to SAASPASS for authentication of Office365. Such users will be called as 'federated users'. Federated users should exist both on your Office365 tenant and SAASPASS admin portal for successful authentication.

So before that, you should make your existing users ready on SAASPASS.

There are various ways that you can create user accounts on SAASPASS for already existing Office365 users.

### **If your users are on-premises Active Directory and synced with Office 365 via DirSync (or AAD Connect):**

You should integrate your Active Directory with SAASPASS as well. To integrate your Active Directory, go to Groups & Users, click [+ ADD] and start integrating Active Directory. It is important that this AD configuration to have UPN Suffix defined and its value to be your federated domain name. For example, UPN Suffix configuration of AD should have 'yourdomain.com' which is the domain that you will federate.

The agent you will install on AD will take care of syncing accounts (that under the Organizational Units that you will select) with SAASPASS. So even if you add a new user to your AD, it will be synced to your Office365 with DirSync that you already have and will be synced to SAASPASS via SAASPASS AD Agent.

If you don't want to integrate AD with SAASPASS, there is Import Users option which is explained for In Cloud users below. Importing users can be used for Active Directory users as well.

*Hint:* If you enable SAASPASS to do user provisioning to Office365 (you will see details later in this document), you don't need to use DirSync to provision your users from AD to Office365. New user that you created on AD takes long time to be provisioned via DirSync. We recommend you to use SAASPASS User Provisioning unless you don't need different user account attributes to be provisioned to Office365 (SAASPASS will provision account name, email, first name and last name of user accounts only).

***If your users are on Cloud only:*** You should use SAASPASS Importing Users option. It is important to import users from Office365 to SAASPASS (not create them manually) because Office365 requires an attribute called Immutable ID to exist on accounts and match between Office365 and SSO provider (SAASPASS). By default, In-cloud users don't have Immutable ID. So importing users via SAASPASS will result in this attribute to be set both on SAASPASS and Office365 properly for each account.

To do this:

Navigate to management section of your Office365 application and open USER PROVISIONING.

Enable User Provisioning and follow instructions that provided here: [Appendix B: Granting SAASPASS to Access Your Office365 Tenant](#)

You will see 'IMPORT USERS FROM TENANT' section. START IMPORT and import will proceed. You will see new user accounts created and assigned to your application (via Application Smart Group) automatically. When import operation finished, you will see a summary report on the import section. If there are accounts that were failed to import, you can view report for each accounts to see the reason.

There are some rules of importing:

- SAASPASS will import a user account only if domain of the account is same as federated domain of Office365 application in SAASPASS. Otherwise, it will not be imported.
- SAASPASS will import user account if it doesn't match with any account in SAASPASS. For example, if there is existing email account with same account name or there is existing AD account with same UserPrincipalName, new account will not be created (but matched one will be assigned to the application anyway)
- You are able to perform 1 provisioning process in your company at a time. If there is already running import or export operation, you should wait for it to finish before attempting new one.

When you sync users from your AD or import users from Office365 tenant, SAASPASS will send verification link to email addresses that are represented by account names. This will let users to verify their accounts in SAASPASS (Only verified accounts can be authenticated for Office365). If you don't want verification links to be sent in this step, there are settings on each action to disable sending verification emails.

You can verify accounts manually if you know your user's SAASPASS IDs but it is easier if users verify themselves. If they didn't receive verification emails, inform them to add their email address (that are represented with their Office365 account name) to their SAASPASS account (on SAASPASS mobile application or SAASPASS web portal) and verify the verification email with SAASPASS app.

Now you have your users active/verified on SAASPASS. You should decide which users will access to your Office365 application on SAASPASS. Navigate to User Accounts section. If all user accounts that belong to your federated domain will have access to your application (which is generally valid for Office365 case), just choose the group of domain and assign to the application. If there are specific groups that you want to assign, choose them and assign to the app.

## User Accounts

OVERVIEW

USER ACCOUNTS

USER PROVISIONING

ASSIGNED GROUPS

Assign and unassign groups of users to be authenticated for this application.

ASSIGNED GROUPS	ACTIONS
Office365 1 (0)	
<div>ASSIGN</div>	<div>GROUPS &amp; USERS</div>

### Single Sign-On Integration with SAASPASS

This section gives you instruction about Single Sign-On integration with SAASPASS. You will simply create an Office365 application on SAASPASS and federate your domain with SAASPASS. Once you completed, users of your domain will be redirected SAASPASS for login and they will have Single Sign-On capability.

### Verify Your Office365 Domain on SAASPASS

First of all, Office365 application is about your domain that you will federate. So this domain should be verified for you on SAASPASS.

Only confirmation needed is you to have a verified email that belongs to that domain in SAASPASS. If you don't have such email yet, you can create it on your SAASPASS mobile application and verify the verification email that is sent to that email.

Once you have the email verified, access your company's account on SAASPASS as admin, navigate to Domains section on SAASPASS admin portal and ADD NEW Domain. Type your email address that you verified and domain will be verified for your company.

### Create Office365 Application on SAASPASS

You should create Office365 application on SAASPASS using your company admin account. Navigate to Applications section, find Office365 application and ADD it. On the form, you will be asked for choosing the federated domain. You should choose the domain that you want to federate with SAASPASS (and you just verified on previous step) and complete creating application. On the Overview of application, you will find APP KEY & PASSWORD. Navigate there and find your APP KEY. You should note it for domain federation.

### Federate Office365 Domain with SAASPASS

*Note: Before federating your domain, you should be sure that your domain is not set to Default domain on your tenant since Default domains cannot be federated (When you add a new domain to your tenant, it might be set to Default automatically).*

*If is default, follow this instruction to set your primary domain (e.g. contoso.onmicrosoft.com) to*

*Default:*

<https://support.microsoft.com/en-us/help/2787250/-you-cannot-delete-the-default-domain-error-when-you-try-to-remove-a-domain-from-office-365>

*There are two ways that you can federate your Office365 domain with SAASPASS. You can let SAASPASS to do it for you automatically in a single click or you can also do it manually.*

### Federating Domain with SAASPASS Automatically

Federating a domain with an identity provider is not trivial when you want to do it by yourself as you will see on the manual way. But SAASPASS makes it so easy that you can federate your domain without requiring an environment, any installation or script execution.

Go to your Office365 application management page and navigate to Configure SSO tab. You will see CONFIGURE SSO button that will let you automatically federate your domain with SAASPASS.

SAASPASS requires you to provide administrator username and password for your Office365 tenant. Once you provide your credentials and confirm your request, SAASPASS will federate your domain and your SSO configuration will be done. Authentication of Office365 users will be federated to SAASPASS from now on. Try with one of user accounts that belong to the domain to confirm if authentication is redirected to SAASPASS.

You completed federation successfully. Now login attempts to Office365 with federated accounts will be redirected to SAASPASS for Single Sign-On.

For SAASPASS to be able handle, you will need to create these user accounts on SAASPASS.

*Note: Administrator credentials that you provide will NOT be stored anywhere on SAASPASS. SAASPASS using it to connect to your tenant to complete domain federation and it is not used anymore.*

### Federating Domain with SAASPASS Manually

Before federation, you will need to install some tools on a machine that you can use to access to Office365 tenant for federation. You can see instructions for installations here: [Appendix A: Required Installations for Federation](#)

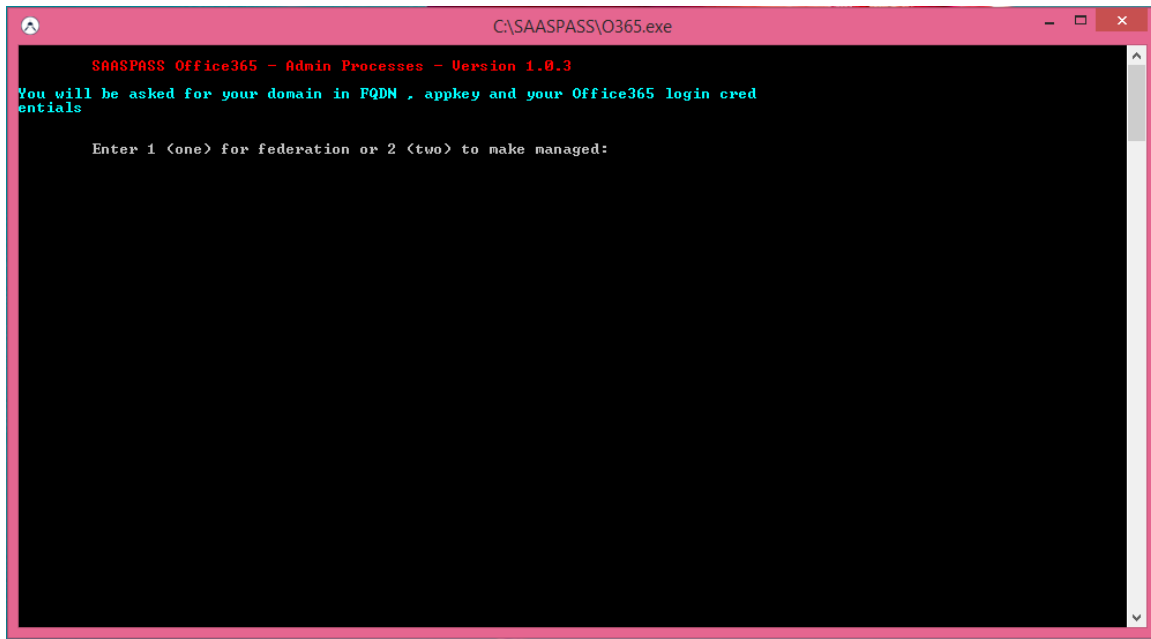
If you already have them, just continue steps below.

After installations:

#### STEP 1

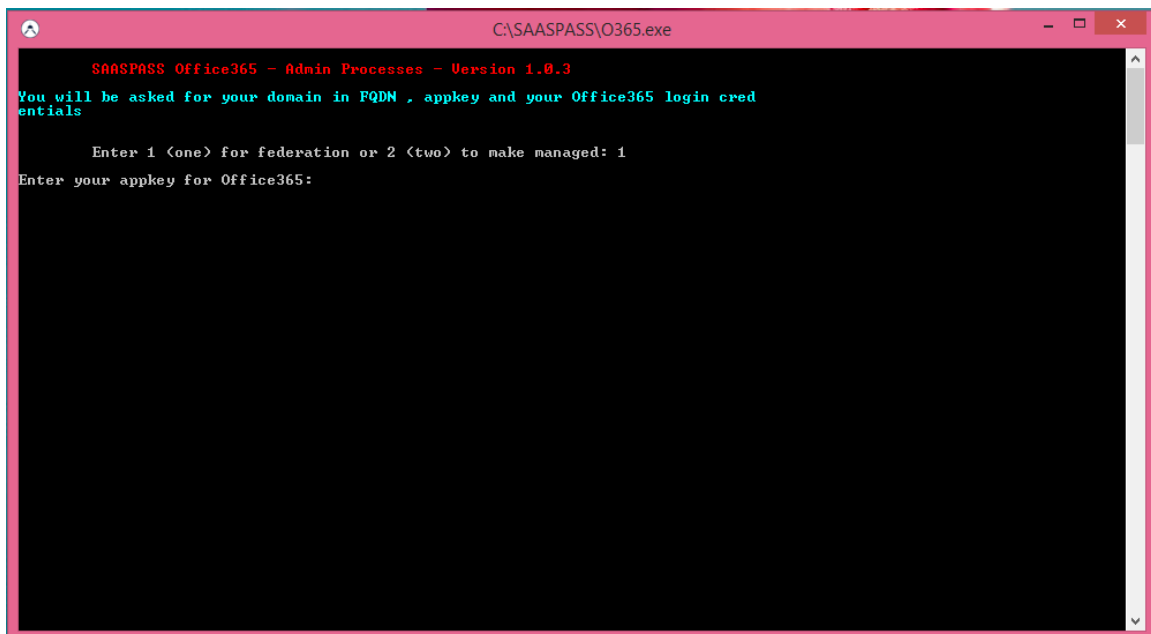
Download this SAASPASS installation [executable](#).

Open the downloaded .exe file and give the file one minute to populate. It will request that you type and submit the number "1".



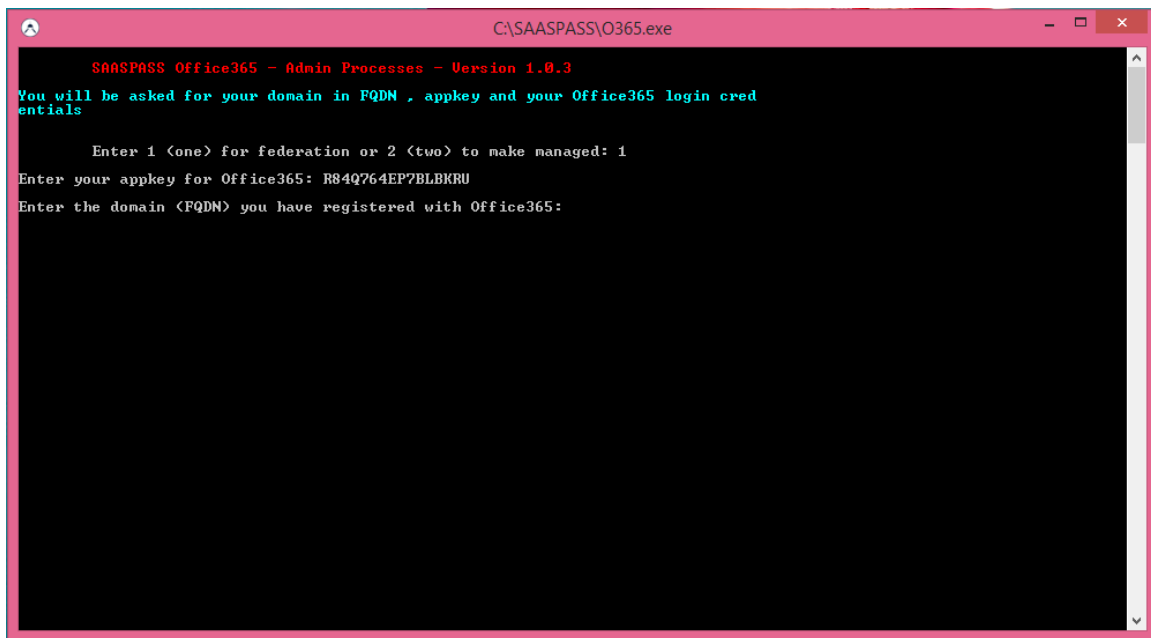
## STEP 2

Enter your Office 365 Application Key. Your application key is the one provided to you on SAASPASS admin portal, for your Office365 Application. Go to your application management, see APPKEY & PASSWORD section. Scan barcode or enter SAASPASS OTP to identify yourself again. Do not share these credentials for your application's security.



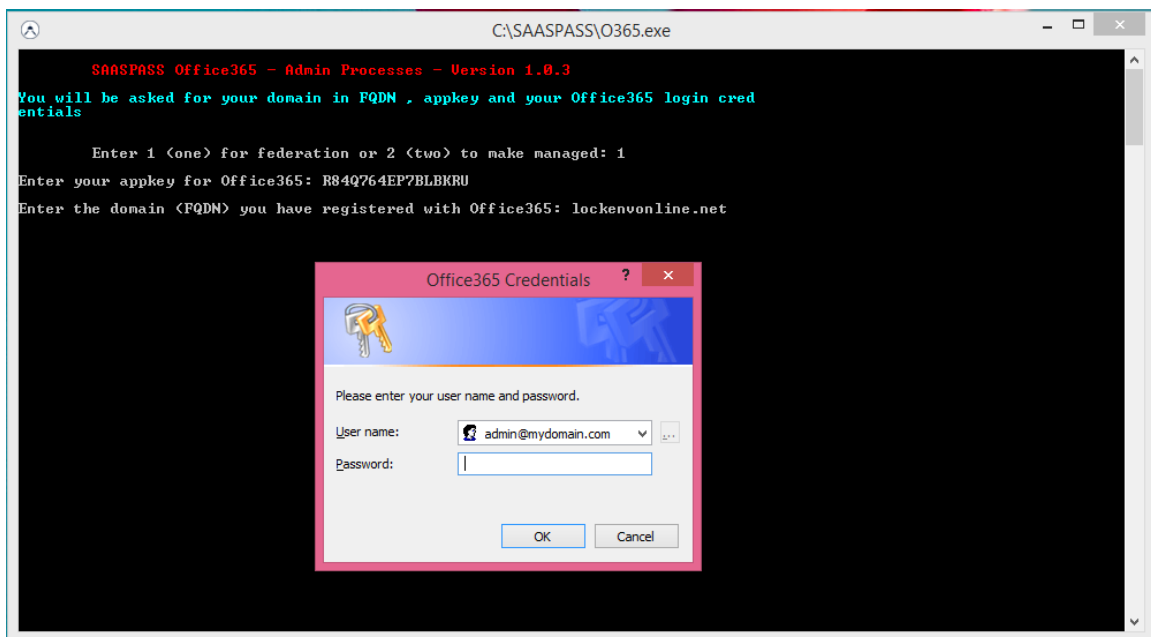
## STEP 3

Submit the domain you have registered (for federation) with Office 365.



#### STEP 4

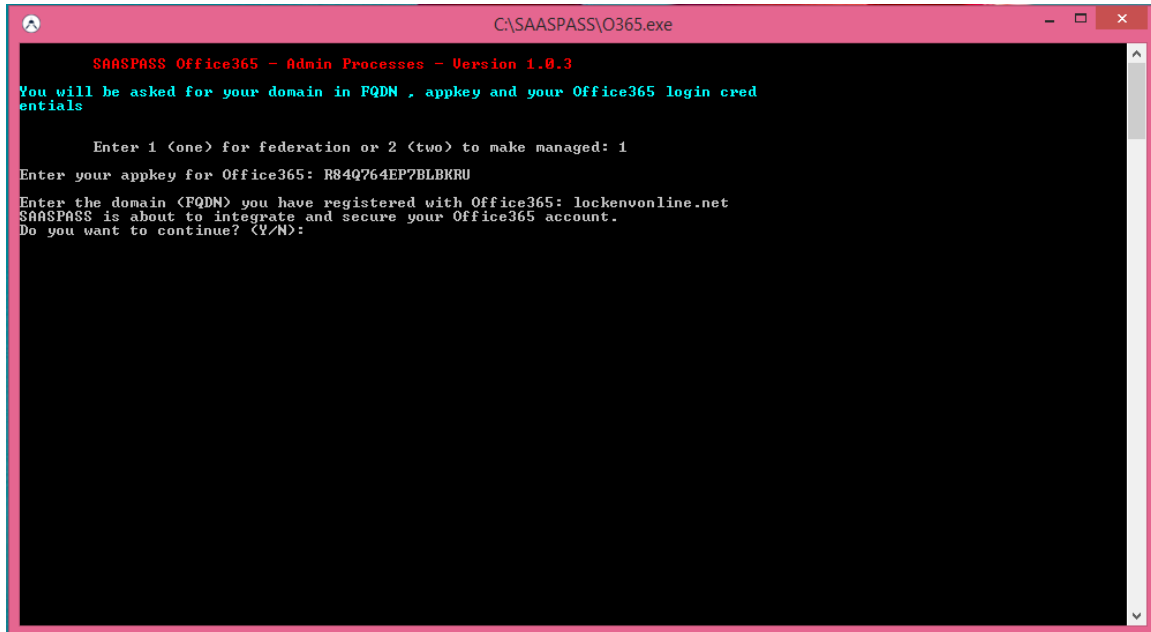
Enter your Office 365 login credentials.





## STEP 5

Type and submit "Y".



```
C:\SAASPASS\O365.exe

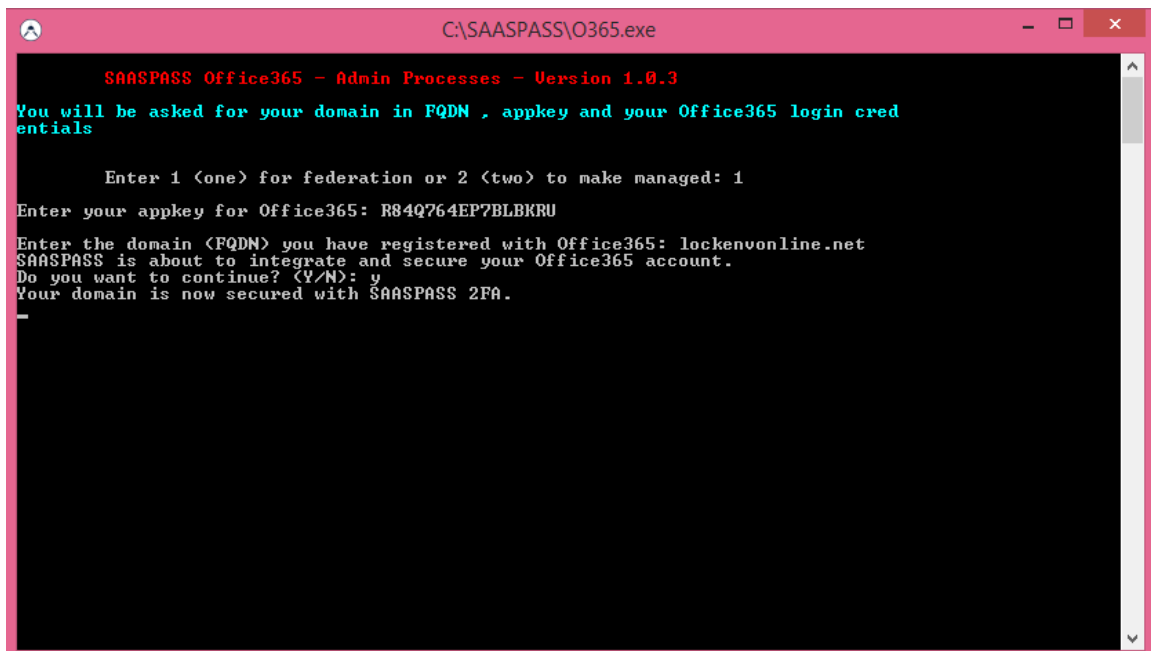
SAASPASS Office365 - Admin Processes - Version 1.0.3

You will be asked for your domain in FQDN , appkey and your Office365 login credentials

Enter 1 <one> for federation or 2 <two> to make managed: 1
Enter your appkey for Office365: R84Q764EP7BLBKRU
Enter the domain <FQDN> you have registered with Office365: lockenvonline.net
SAASPASS is about to integrate and secure your Office365 account.
Do you want to continue? <Y/N>:
```

## STEP 6

All set! You're secured with SAASPASS 2FA.



```
C:\SAASPASS\O365.exe

SAASPASS Office365 - Admin Processes - Version 1.0.3

You will be asked for your domain in FQDN , appkey and your Office365 login credentials

Enter 1 <one> for federation or 2 <two> to make managed: 1
Enter your appkey for Office365: R84Q764EP7BLBKRU
Enter the domain <FQDN> you have registered with Office365: lockenvonline.net
SAASPASS is about to integrate and secure your Office365 account.
Do you want to continue? <Y/N>: y
Your domain is now secured with SAASPASS 2FA.
```

## STEP 7

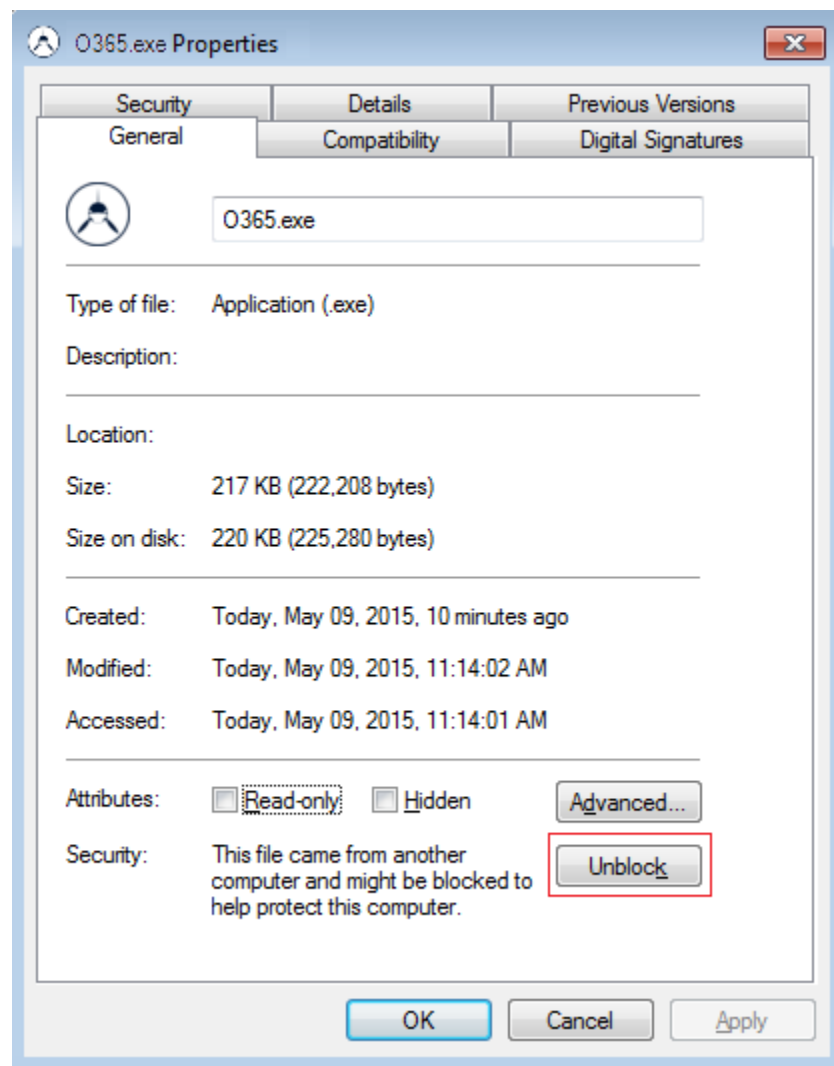
To allow you to direct your custom sub-domain to your newly secured O365 account you will need to set up a URI redirect in your DNS service. For your *sub-domain mail.mydomain.com* should now point to the following:

<https://login.microsoftonline.com/PostToIDP.srf?msg=AuthnReq&realm=mydomain.com&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline>

*Note: The URI redirect is different from a CNAME record, it is alternatively called “Web Forward record” by some DNS providers.*

*If your script is not starting after you execute please do following:*

- Right click on the “O365.exe”
- Choose “Properties”
- Under “General” tab click on “Unblock” button
- Start again “O365.exe”



You completed federation successfully. Now login attempts to Office365 with federated accounts will be redirected to SAASPASS for Single Sign-On.

For SAASPASS to be able handle, you will need to create these user accounts on SAASPASS.

**Converting domain back to Managed:** If for any reason, you want to convert your domain back to Managed (un-federation), you can use same .exe file that mentioned for manual federation. It provides choice to convert your domain to Managed (press '2' when it is prompted to federate/managed). Please also inform us if you had difficulties with Office365 integration. [support@saaspass.com](mailto:support@saaspass.com)

## Handling New Users

Remember any Office365 account that belongs to federated domain should exist both on Office365 tenant and SAASPASS. But after federating your domain with SAASPASS, you are not be able to create new users for that domain on Office365 Admin Center manually due to Office365 restrictions.

There are various ways you can follow to create new user accounts on Office365.

Powershell commands: You can use Powershell commands (scripts) to create new user accounts. But this requires experience about PowerShell.

DirSync: DirSync (or AAD Connect) is Microsoft tool that enables you sync your on-premises Active Directory with Office365 tenant. It is powerful tool for syncing Active Directory users since it lets a user account to be created on Office365 automatically after you created the account on your local AD. It also has migration options for existing user account passwords. With this way, users can continue using their existing passwords to login Office365. DirSync has option to provision user accounts with many account attributes that exist on Active Directory. But DirSync has significant disadvantages. You need to know how to configure properly and this might not be easy. DirSync is not fast to provision new account to Office365. After user accounts are provisioned, you will need to assign license to accounts so that they can access Office365 apps. DirSync is not handling user licenses.

Before provisioning your users, you should add Office365 domain as UPN suffix for your AD and also to update all users accounts to use this UPN suffix so that they will be ready for migrating to Office365.

Or you can use SAASPASS for user provisioning.

## SAASPASS User Provisioning

SAASPASS is now more efficient product for your Office365 SSO Integration, having Provisioning option. You can let SAASPASS to handle user provisioning for you.

With SAASPASS User Provisioning, you can configure your Office365 application to handle user provisioning functionality. After configuration, any user account that is assigned to the application will automatically be created on your Office365 tenant!

To enable SAASPASS handling user provisioning:

Navigate to management section of your Office365 application and open USER PROVISIONING.

Enable User Provisioning and follow instructions that provided here: [Appendix B: Granting SAASPASS to Access Your Office365 Tenant](#)

Now SAASPASS is ready for user provisioning. There are 2 ways that provisioning action will be taken.

### Manual Provisioning / Export

Under EXPORT USERS TO TENANT, clicking START EXPORT will start provisioning process. For accounts that are assigned to your Office365 application will be created on your tenant if not exist already.

### Auto Provisioning / Export

Also there is auto-provisioning option. If you enable Auto Provisioning / Export, SAASPASS will automatically provision user account on tenant, when a new account is available (assigned and verified) for your Office365 application in SAASPASS. With this way, you don't need to manually export each time that you assigned account to the application. But keep in mind that auto-provisioning will effective after you enabled it. If there were already some accounts assigned to the application but you didn't provision (export) them before, you need to export them manually for once.

### About User Licenses

When new user account is created on Office365 Tenant, it might need some default license(s) to be assigned so that user can access Office365 applications. You can tell SAASPASS to assign these licenses to new user accounts if you don't want to do this on Office365 Admin Portal.

Under DEFAULT LICENSE LIST, you can see available licenses for your tenant. If it is not there yet, click REFRESH LICENSES.

You can choose one or more licenses and save. Now for any new user account that SAASPASS will create on tenant, these licenses will be assigned to it by default.

### User Provisioning Rules

There are some rules you should consider for user provisioning:

- SAASPASS will export a user account to Office365 if it is assigned to your Office365 application and verified. Pending (not verified) accounts will not be exported even if they are assigned to the application.
- SAASPASS will export a user account that is in email format if domain of email is same with federated domain of Office365 application. Otherwise, account will not be exported.
- SAASPASS will export an Active Directory account if federated domain of Office365 application is defined as UPN Suffix for the Active Directory. (So if you have AD integrated and AD users need to be exported to Office365 Tenant, navigate to AD management page and enter federated domain in UPN Suffix area.)
- When SAASPASS creates new user account on Office365 Tenant, it is generating a strong password and setting for new account. This is required by Office365. You can reset this password later if you need (Note: SAASPASS is NOT storing this password anywhere in SAASPASS servers. It is just for first time password generation on account creation process).
- You are able to perform 1 provisioning process in your company at a time. If there is already running import or export operation, you should wait for it to finish before attempting new one.

When export operation finished, you will see a summary report on the export section. Report will tell you if export was successful and if it was, there will be number of successful, failed or matched accounts displayed. If export wasn't successful, you will see possible reason explanation.



### Tip

You might be thinking which way (Traditional ways or SAASPASS way) will be suitable for you regarding user provisioning for Office365. You should think your needs and decide which way to follow. But here are some ideas from SAASPASS that can help you about decision:

- If your users (existing or new once) are not on Active Directory and you need to create them on Office365 cloud only, (see difference in first section of document if you need), then you don't use DirSync of course. Now to create users on Office365 tenant for federated domain, you have option to use Powershell scripts or SAASPASS. There is no doubt that SAASPASS is more easy and efficient for this case. Because you just need to assign the user account to Office365 and SAASPASS will create user on Office365 tenant for you.
- If your users are on Active Directory, you can use any of the ways that explained above (traditional ways or SAASPASS way). Know that you can use DirSync and SAASPASS (also Powershell if needed) in the same time for user provisioning. But to avoid possible conflicts or extra works, you should think smart. Here are some tips:
  - SAASPASS is about Single Sign-On and its goal is eliminating passwords. If you want to migrate user's existing passwords to Office365 to be used for some purposes (obviously this reason wouldn't be for SAASPASS SSO integration), then you can continue using DirSync for user provisioning. You will need to decide your migration policy for user account passwords and DirSync will do this job. (Note: As explained above on Export section, SAASPASS is generating new strong password for the account that will be created on Office365 tenant).
  - SAASPASS is bringing secure Single Sign-On functionality to your Office365 application. So when SAASPASS creates new account on Office365, it creates account with data that it needs for SSO. These data are account name, immutable id, display name and some other attributes. But if for some reason, you need to migrate your Active Directory users with their full profile information (like job, department, city etc.), then you can continue using DirSync for user provisioning.

Except above reasons, if you don't have specific need, SAASPASS will be enough and very efficient for user provisioning comparing to DirSync. So you can integrate your Active Directory with SAASPASS using SAASPASS AD Agent and you can enable user provisioning on your Office365 application management.

## Appendix A: Required Installations for Federation

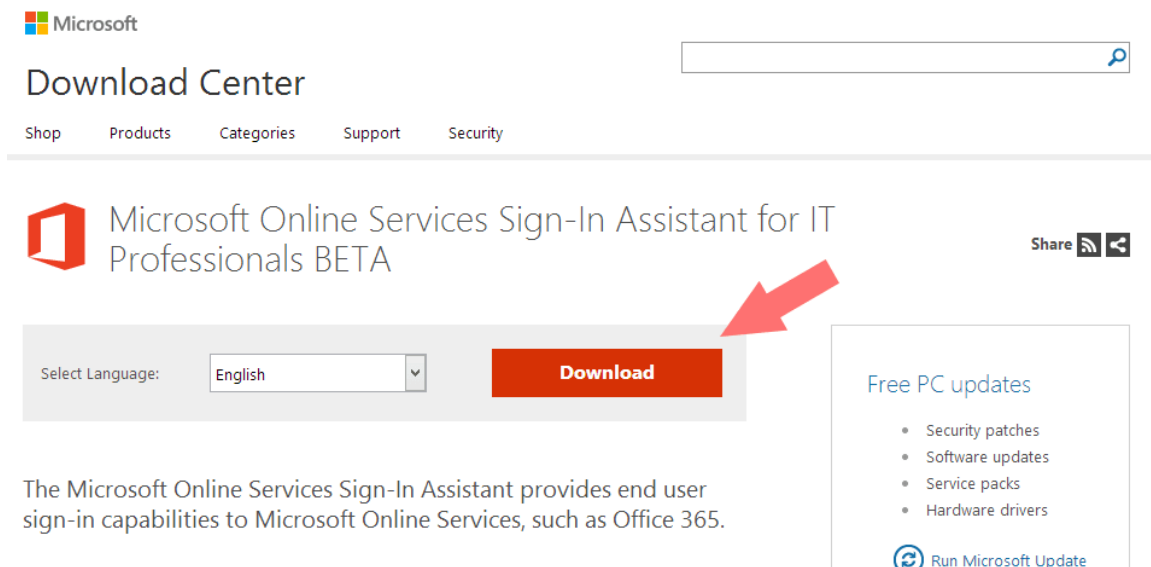
### Installation prerequisites:

- Operating System: Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012.
- Microsoft .NET 3.52 Framework
- Microsoft Online Services Sign-In Assistant for IT Professionals BETA
- Windows Azure AD Module

### STEP 1

Go to the Microsoft Download Center here:

<https://www.microsoft.com/en-us/download/details.aspx?id=39267>. Choose Microsoft Online Services Sign-In Assistant for IT Professional BETA. Choose your language and choose “Download”.



### STEP 2

When you click download, choose your system setup and click “Next”.

Choose the download that you want

<input type="checkbox"/> File Name	Size
<input type="checkbox"/> msoidcli_32.msi	3.9 MB
<input checked="" type="checkbox"/> msoidcli_64.msi	5.6 MB

Download Summary:

1. msoidcli\_64.msi

Total Size: 5.6 MB

Next

### STEP 3

Accept the terms and choose “Install”.

Microsoft Online Services Sign-in Assistant Setup

Please read the Microsoft Online Services Sign-in Assistant License Agreement

**MICROSOFT SOFTWARE LICENSE TERMS**

**MICROSOFT ONLINE SERVICES SIGN-IN ASSISTANT**

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any.

Privacy Statement

☒ I accept the terms in the License Agreement and Privacy Statement

Print

Back

Install

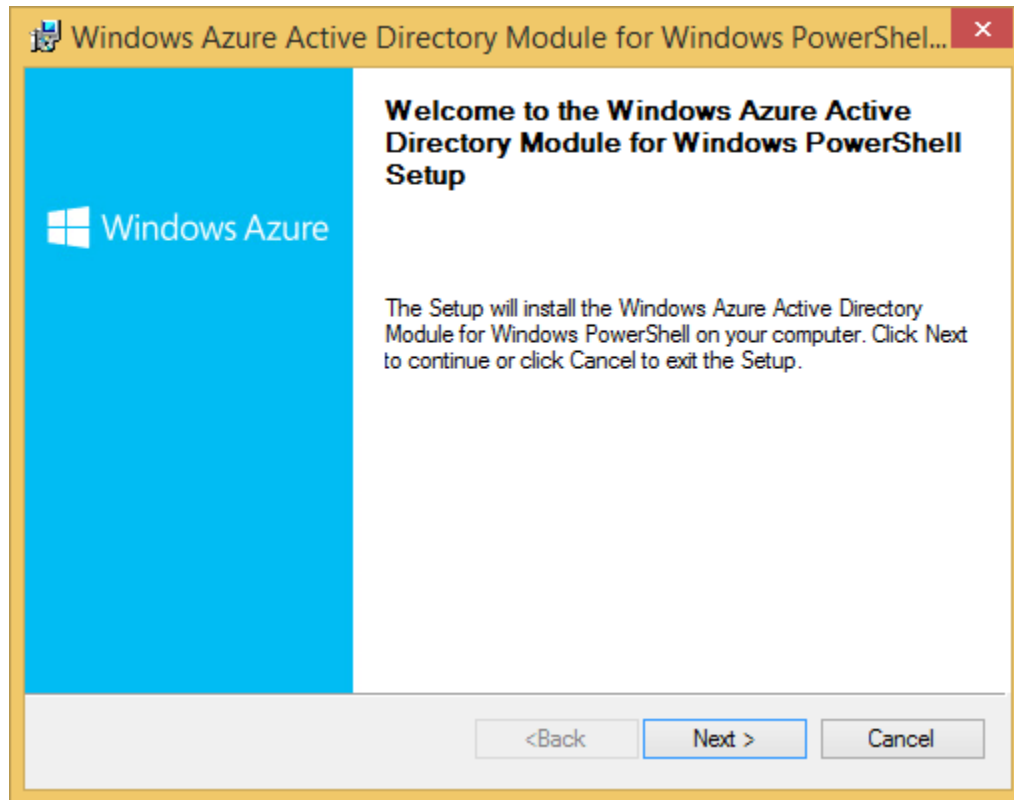
Cancel

#### STEP 4

Navigate to this link: <https://docs.microsoft.com/en-us/powershell/msonline/>  
Follow instructions there and download the module appropriate for your system.

#### STEP 5

After downloading, install the module.



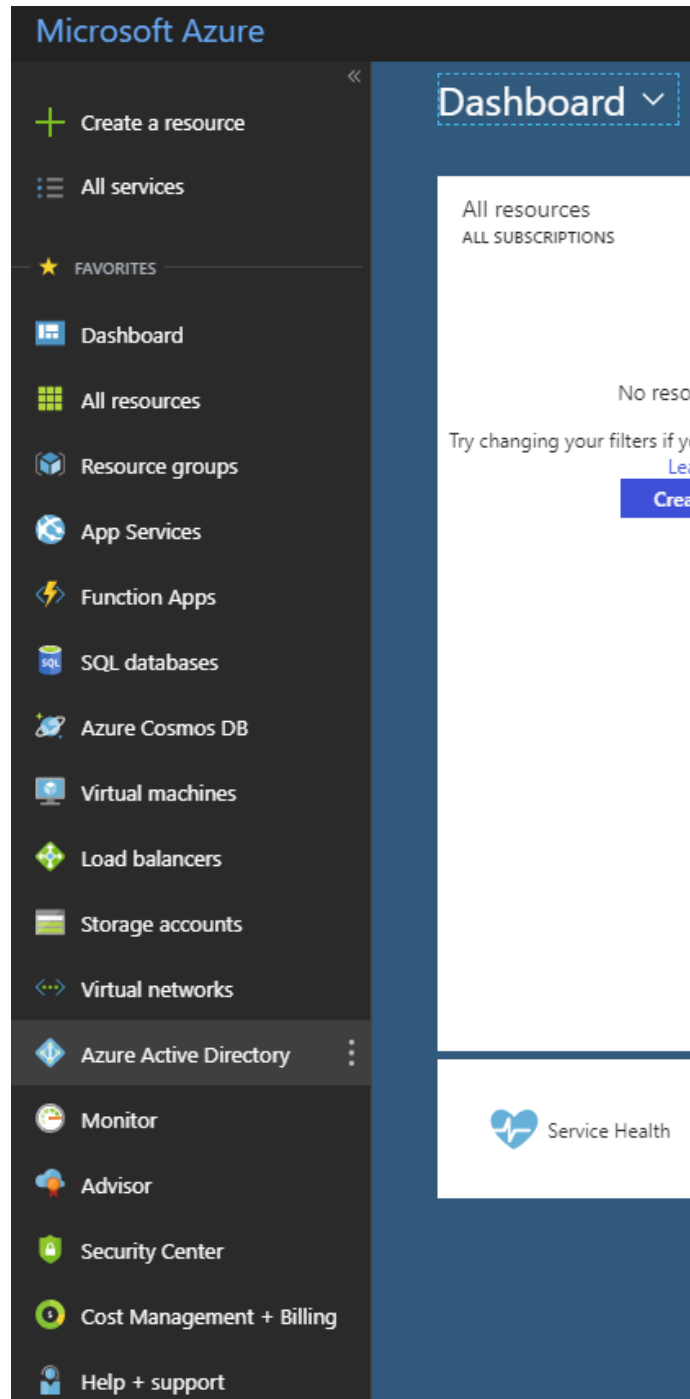


## Appendix B: Granting SAASPASS to Access Your Office365 Tenant

To enable SAASPASS to handle user provisioning (export / import) for Office365, it needs to be granted for accessing your Office365 Tenant. Follow these steps to enable.

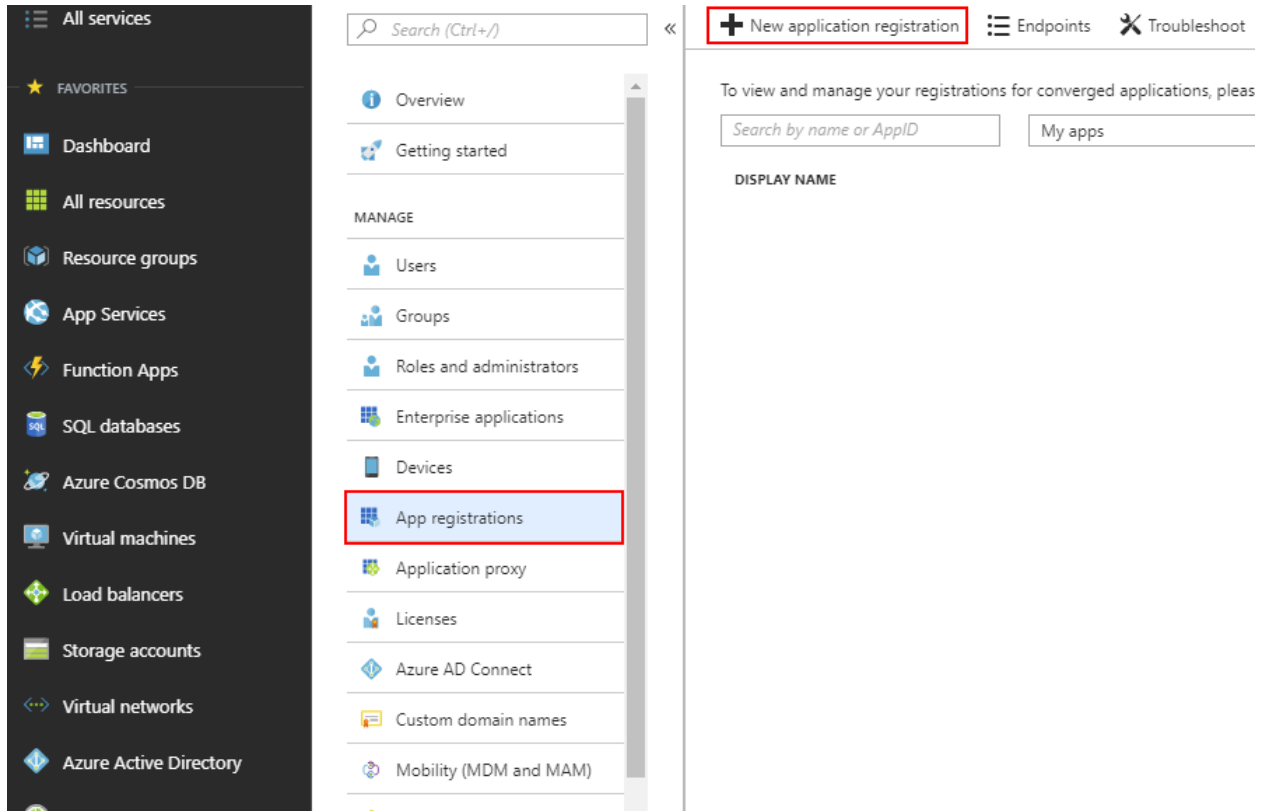
### STEP 1

Login to the Microsoft Azure Portal and navigate to Azure Active Directory.



## STEP 2

Once you are there, click on your **Azure Active Directory** and then on the left side of the menu click on **App registrations**. Once you are in that view, at the top click on the **New application registration** to add a new application.



## STEP 3

When you click on the **New application registration** button just follow the below images to create your **Application**.

\* Name ⓘ  
SAASPASS - Office 365 ✓




Application type ⓘ  
Web app / API ✓

\* Sign-on URL ⓘ  
http://mydomain ✓

Select **Web Application And/OR Web API**. Once on the third step enter your domain information.

#### STEP 4

When you finish creating your **Web Application** click on it and navigate to **Settings** tab from the top menu bar.

 Settings  Manifest  Delete




---

Display name SAASPASS - Office 365	Application ID ebfc3830-38ef-49d0-a00d-df917bdd8959
Application type Web app / API	Object ID adcad697-0db6-46ed-99dd-c3078c2c5132
Home page <a href="https://mydomain">https://mydomain</a>	Managed application in local directory <a href="#">SAASPASS - Office 365</a>

⤴

#### STEP 5

In the **Settings** tab, you will need to copy your **Client ID** and generate a new **Client Secret**.

 Settings  Manifest  Delete

---

Display name SAASPASS - Office 365	Application ID <b>ebfc3830-38ef-49d0-a00d-df917bdd8959</b>
Application type Web app / API	Object ID adcad697-0db6-46ed-99dd-c3078c2c5132
Home page <a href="https://mydomain">https://mydomain</a>	Managed application in local directory <a href="#">SAASPASS - Office 365</a>

⤴

Properties >

Reply URLs >

Owners >

API ACCESS

Required permissions >

**Keys >**

TROUBLESHOOTING + SUPPORT

Troubleshoot >

New support request >

DESCRIPTIONEXPIRESVALUE

1 ✓ In 2 years ✓ Value will be displayed on save ...

Key description Duration ✓ Value will be displayed on save ...

Public Keys

THUMBPRINTSTART DATEEXPIRES

No results.

Additionally we need to add permissions for the application to have access to the Azure Active Directory so please make sure you select **Read and write directory data** as well **Read and write domains** on both **Application Permissions** and **Delegated Permissions**, then click on the **Save** button.

Filter settings

GENERAL

Properties >

Reply URLs >

Owners >

API ACCESS

Required permissions >

Keys >

+ Add

Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	2	1

APPLICATION PERMISSIONS

REQUIRES ADMIN

Read directory data	Yes
<input checked="" type="checkbox"/> Read and write domains	Yes
<input checked="" type="checkbox"/> Read and write directory data	Yes
Read and write devices	Yes

## STEP 6

Navigate to SAASPASS Admin Portal and under **User Provisioning** of your Office 365 Application, enter the **Client ID** and **Client Secret**.

## Appendix C: Ports Used by SAASSPASS Products

The following outlines the TCP and UDP ports used by SAASSPASS products.

Your network administrator may need this information to make sure your computer or device can connect to services, such as automatic software updates, or the Online portal.

Network administrators may also wish to use port-watching software in addition to the information below when making decisions on how to set up firewalls or similar access control schemes.

- 443 TCP Secure Sockets Layer (SSL, or "HTTPS") TLS Online Portal, Barcode Instant Login , Proximity
- 5222 TCP XMPP client connections Mobile App , Computer Connector