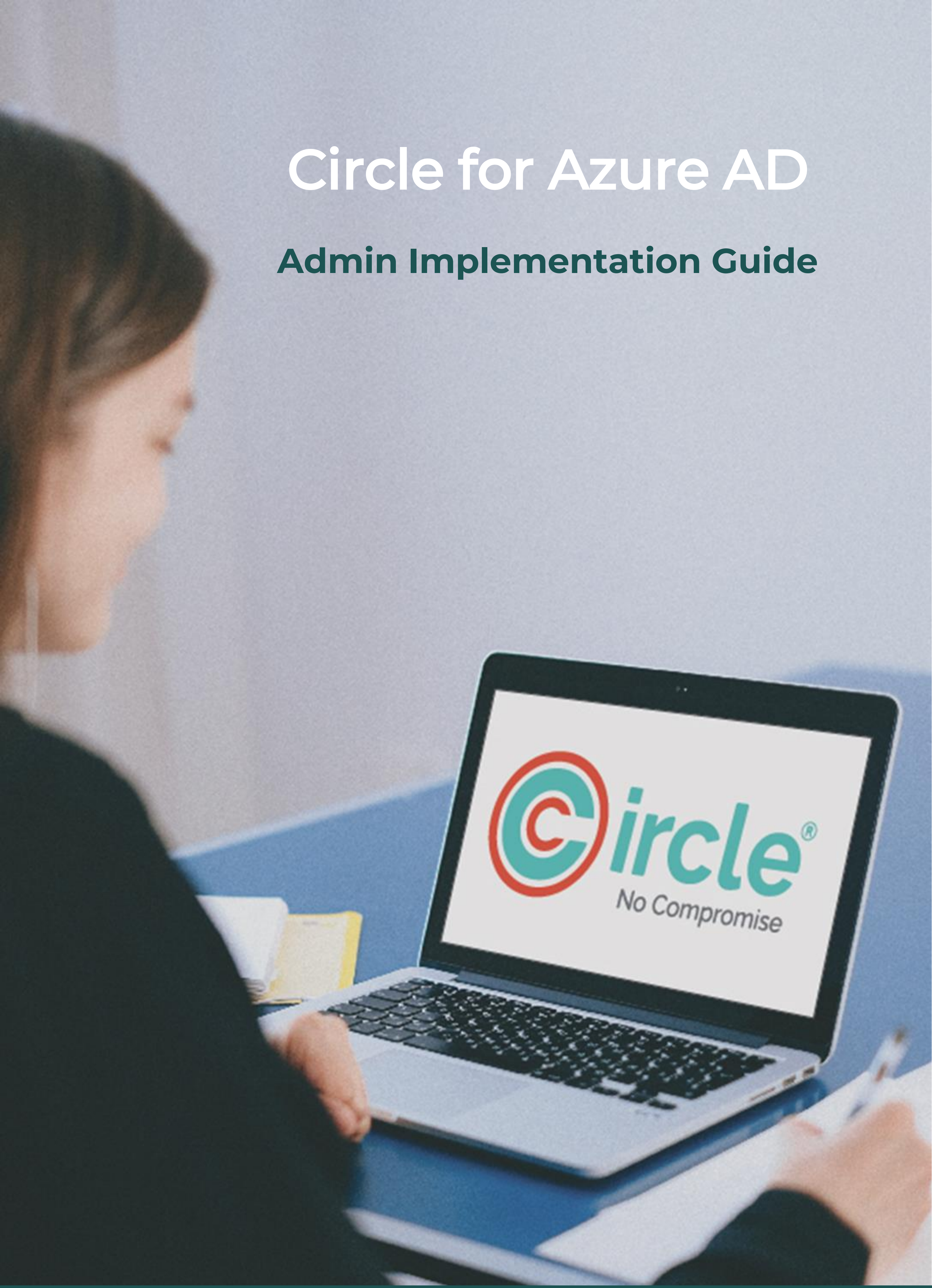
Circle for Azure AD

Admin Implementation Guide



Context

This guide helps you in the implementation of Circle Access for Azure AD with Single Sign-On feature. It is written for Azure AD administrators who **build, deploy, and maintain** the Circle Access service and features for their organizations.

About Circle Access

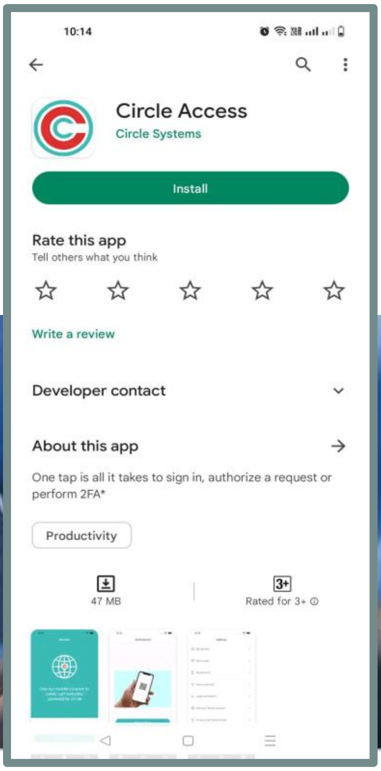
Circle Access provides uncompromising login to your Windows machines and authentication to your Office 365 and other SaaS applications tied to your Windows AD environment with a credential-free experience for your users. It provides cryptographic authentication that eliminates credential phishing and other credential-driven vulnerabilities while delivering a frictionless User Experience.

For more information about Circle Access, see ***https://www.circlesecurity.ai***

Circle Access for Azure Active Directory

Please find below the prerequisites for the setup and implementation of Circle Access for Azure AD:

1. Your computer should already be on Azure AD – If it’s not, then refer to this video to join Azure AD.
2. Use the same computer for the entire process – Preferably Windows so that you can set up and test Single Sign On.
3. Download and install Circle Service from this link on your computer.
4. Install Circle Access App on your mobile phone.



10:14

Circle Access

Circle Systems

Install

Rate this app

Tell others what you think

☆ ☆ ☆ ☆ ☆

Write a review

Developer contact

About this app

One tap is all it takes to sign in, authorize a request or perform 2FA*

Productivity

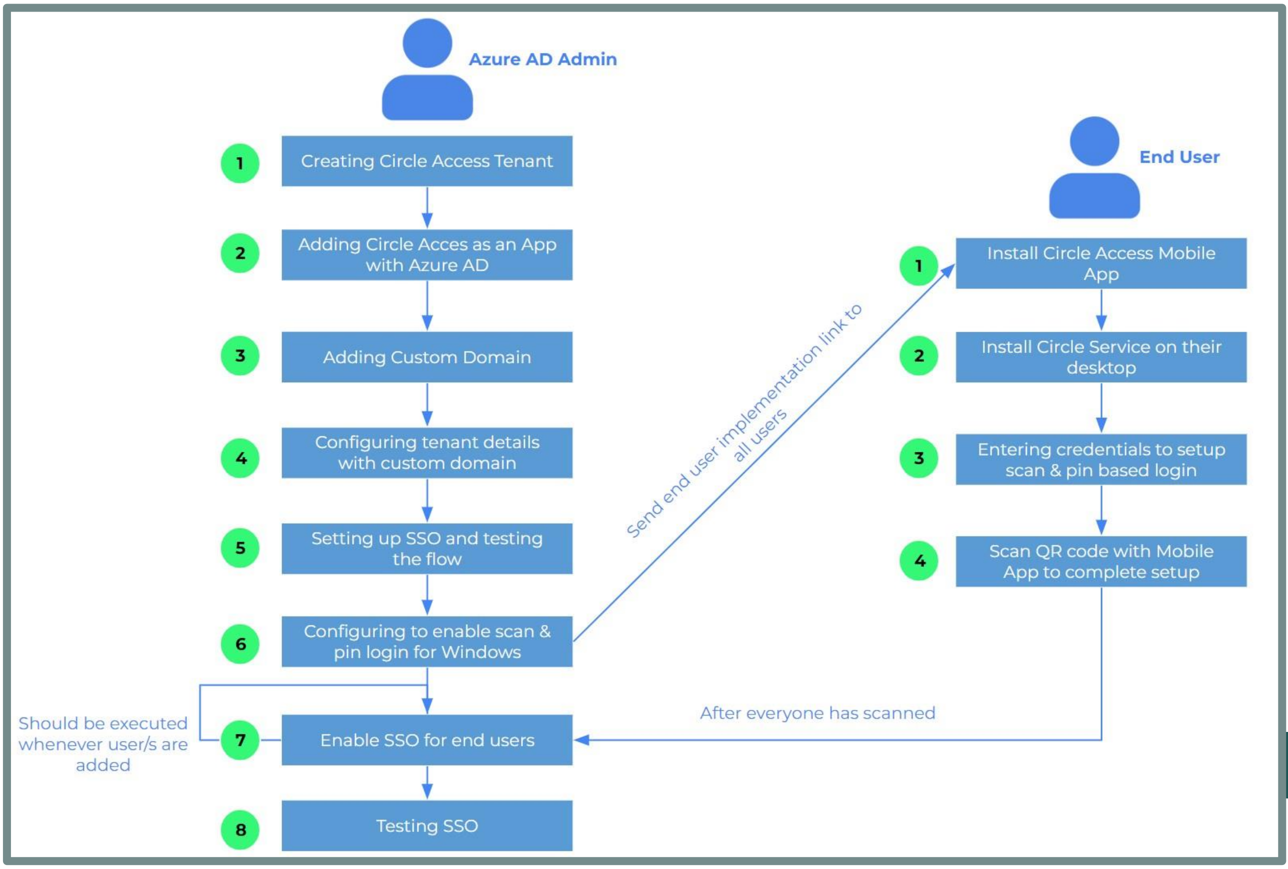
47 MB

Rated for 3+

Overall Summary

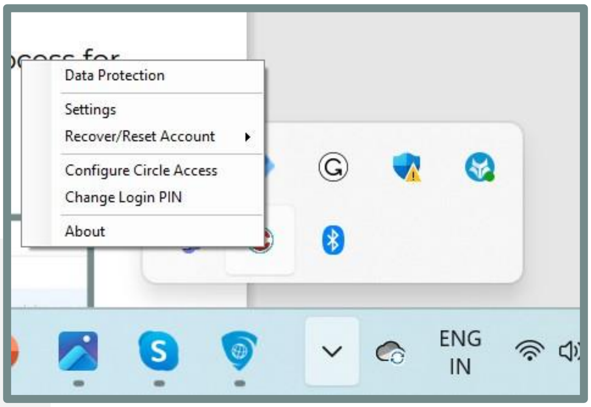
Implementation of Circle Access for Azure Active Directory is a multi-step implementation, and for Admins, it starts from

- Creating a tenant with Circle Access and adding Circle Access as an application with Azure.
- Enable the SSO and test the SSO implementation for Azure Active Directory.
- Then, share the registration URL and end-user implementation guide with the end users.
- The SSO script should be executed every time to enable Circle Access SSO for newly added user/users who complete Circle Access setup.

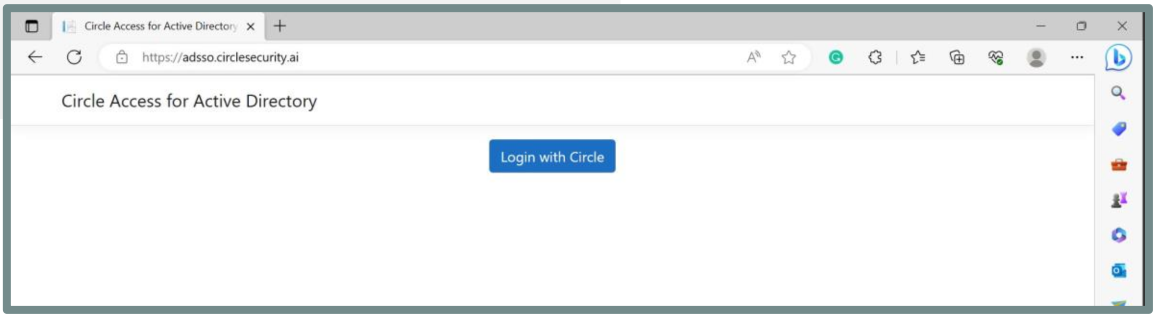

Azure AD Admin
1 Creating Circle Access Tenant
2 Adding Circle Acces as an App with Azure AD
3 Adding Custom Domain
4 Configuring tenant details with custom domain
5 Setting up SSO and testing the flow
6 Configuring to enable scan & pin login for Windows
7 Enable SSO for end users
8 Testing SSO
Should be executed whenever user/s are added
Send end user implementation link to all users
End User
1 Install Circle Access Mobile App
2 Install Circle Service on their desktop
3 Entering credentials to setup scan & pin based login
4 Scan QR code with Mobile App to complete setup
After everyone has scanned

1 Creating Circle Access Tenant

Right-click on the Circle tray icon and select ‘Configure Circle Access’.

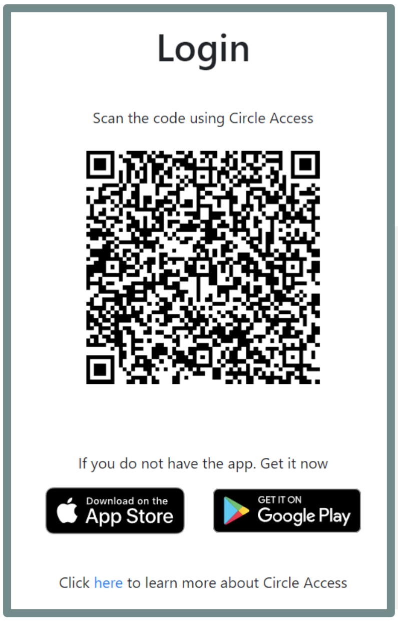


This will open a web browser, with **https://adsso.circlesecurity.ai**, and click the ‘Login with Circle’ button.


Circle Access for Active Directory
https://adsso.circlesecurity.ai

Circle Access for Active Directory

Open Circle Access on your mobile phone and scan the QR code.



Login

Scan the code using Circle Access

If you do not have the app. Get it now

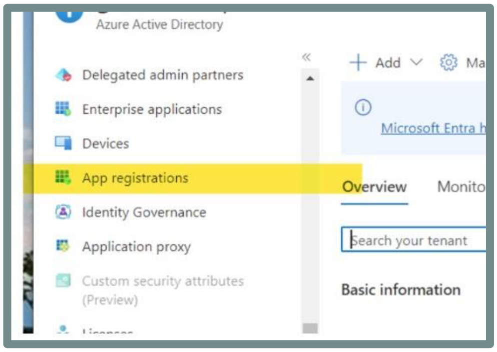
Click here to learn more about Circle Access

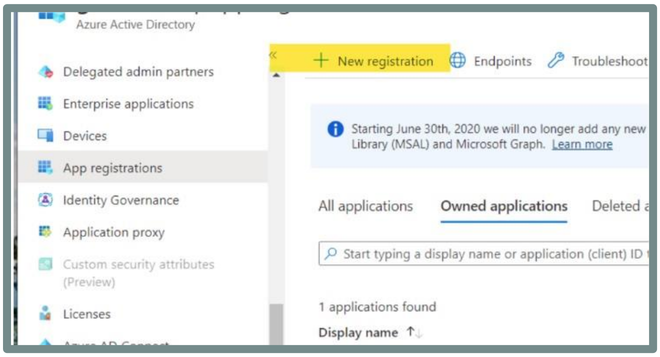
The website will then prompt you to scan one more QR code. Scan the code, and it will automatically create a tenant with the required license and encryption keys that are stored in a Secure Capsule on your computer.

2 Adding an App in ‘App Registrations’ and establishing trust with Azure AD

On the Azure Active Directory portal page, go to “App Registrations”:

Select 'App registration'→ ‘New Registration’



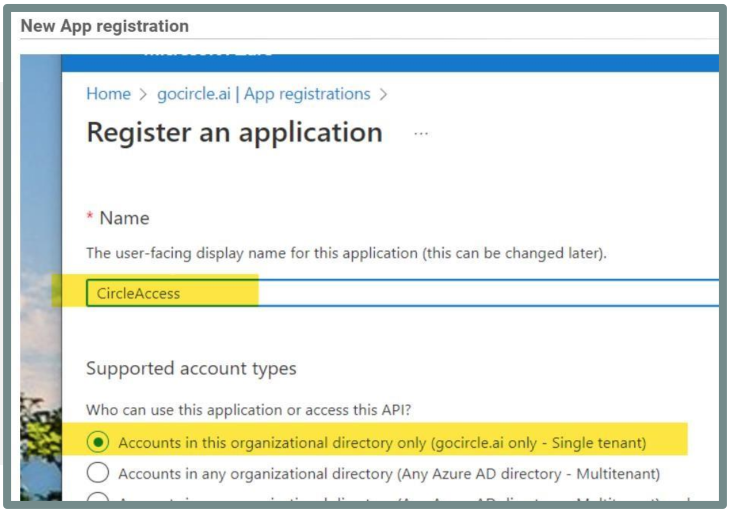


Starting June 30th, 2020 we will no longer add any new Library (MSAL) and Microsoft Graph. Learn more

Start typing a display name or application (client) ID

1 applications found

The below page will be displayed. Register the application **‘Circle Access’**



New App registration

Home > gocircle.ai | App registrations >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

CircleAccess

Supported account types

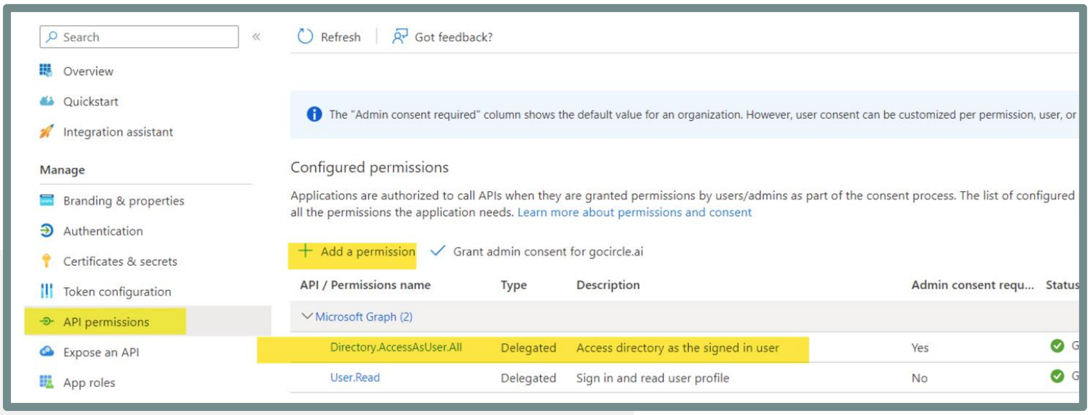
Who can use this application or access this API?

● Accounts in this organizational directory only (gocircle.ai only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Once you’ve registered ‘Circle Access’ as an application, the next step is to establish trust with the Azure AD.

Go to API permissions and add the Microsoft Graph **Directory.AccessAsUser.All** permission:



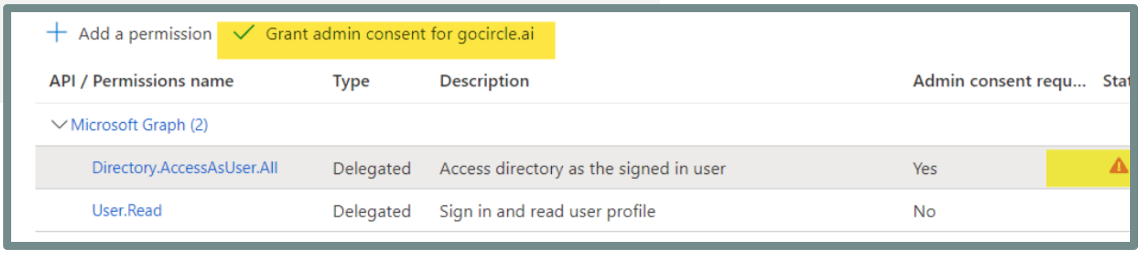
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured all the permissions the application needs. Learn more about permissions and consent

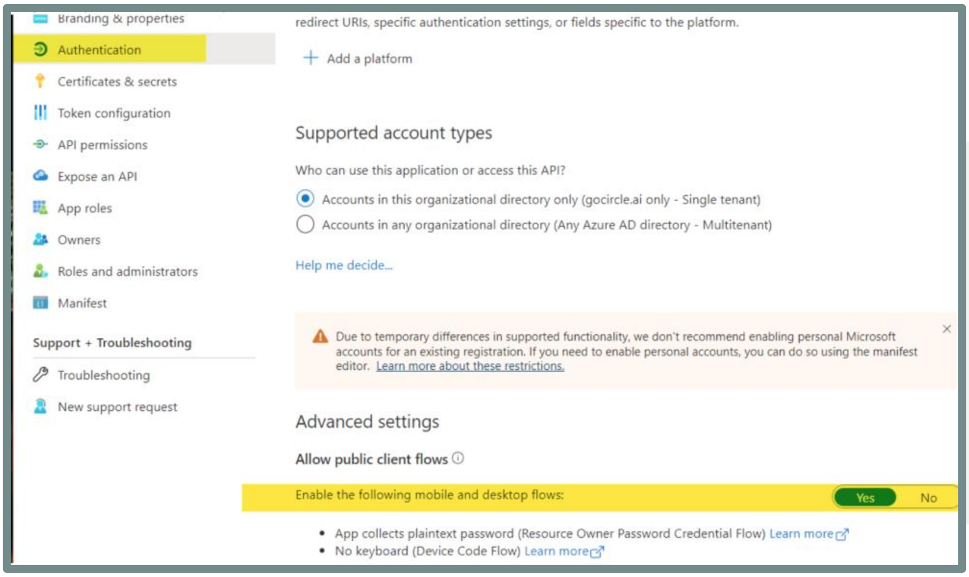
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	✓ G
User.Read	Delegated	Sign in and read user profile	No	✓ G

Provide access with Admin consent.



API / Permissions name	Type	Description	Admin consent requ...	Stat
Microsoft Graph (2)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	⚠
User.Read	Delegated	Sign in and read user profile	No	

Next, change the permission for ‘**Allow public client flows**’ to ‘**Yes**’



redirect URIs, specific authentication settings, or fields specific to the platform.

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (gocircle.ai only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

⚠ Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

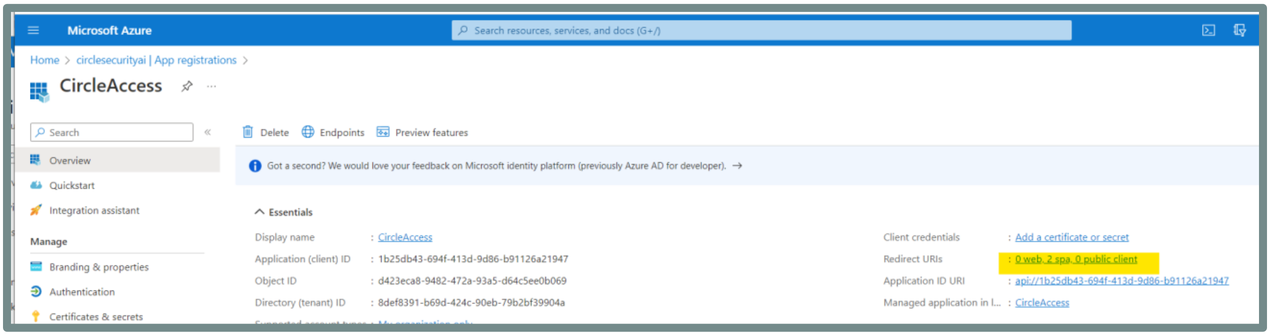
Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more

Next, go back to the **‘Overview’** and click on the ‘**Redirect URIs**’



Microsoft Azure

Search resources, services, and docs (G+/)

Home > circlesecurityai | App registrations >

CircleAccess

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

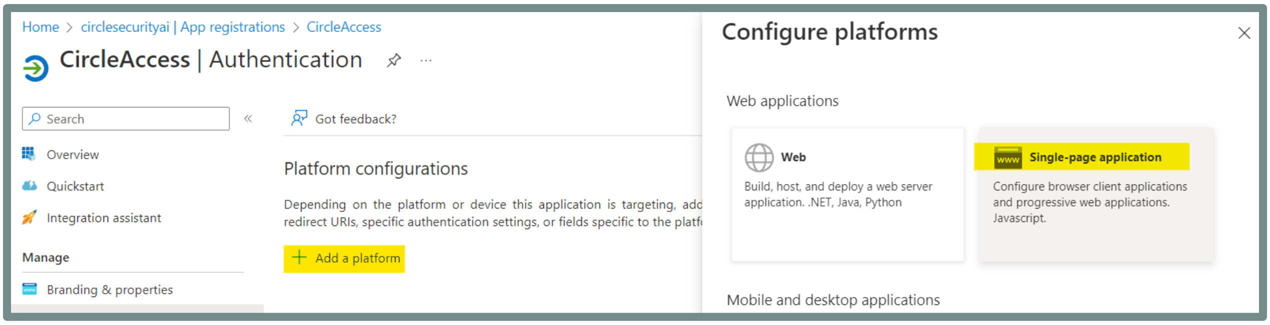
Delete · Endpoints · Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: CircleAccess	Client credentials	: Add a certificate or secret
Application (client) ID	: 1b25db43-694f-413d-9d86-b91126a21947	Redirect URIs	: 0 web, 2 spa, 0 public client
Object ID	: d423eca8-9482-472a-93a5-d64c5ee0b069	Application ID URI	: api://1b25db43-694f-413d-9d86-b91126a21947
Directory (tenant) ID	: 8def8391-b69d-424c-90eb-79b2bf39904a	Managed application in l...	: CircleAccess

Click the **‘Add a platform’** button then select the ‘**Single-page application**’



Home > circlesecurityai | App registrations > CircleAccess

CircleAccess | Authentication

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Got feedback?

Platform configurations

Depending on the platform or device this application is targeting, add redirect URIs, specific authentication settings, or fields specific to the platf

+ Add a platform

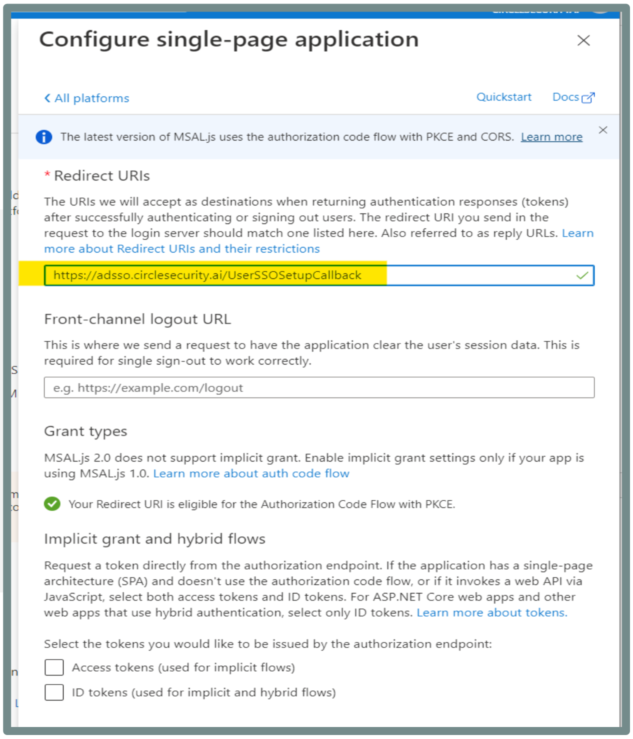
Configure platforms

Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python

Single-page application
Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications



Configure single-page application

< All platforms · Quickstart · Docs

The latest version of MSAL.js uses the authorization code flow with PKCE and CORS. Learn more

* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://adsso.circlesecurity.ai/UserSSOSetupCallback ✓

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout

Grant types

MSAL.js 2.0 does not support implicit grant. Enable implicit grant settings only if your app is using MSAL.js 1.0. Learn more about auth code flow

✓ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

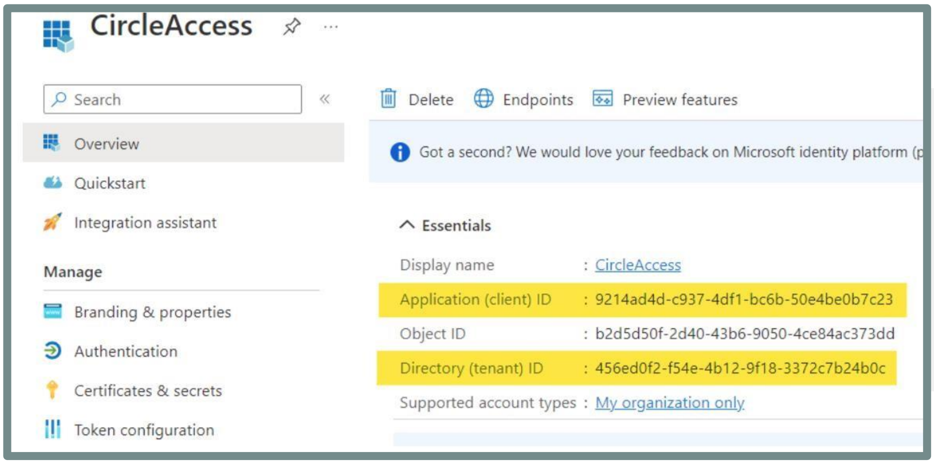
□ Access tokens (used for implicit flows)

□ ID tokens (used for implicit and hybrid flows)

On the ‘Configure single-page application’, enter **‘https://adsso.circlesecurity.ai/UserSSOSetupCallback**’ for the ‘Redirect URIs’ and click ‘Configure’ at the bottom of the page to save it.

Circle Access will need the following two ids in the later steps, so copy and paste them somewhere

- The Directory (tenant) ID
- The Application (client) ID



Got a second? We would love your feedback on Microsoft identity platform (p

Display name : CircleAccess

Application (client) ID : 9214ad4d-c937-4df1-bc6b-50e4be0b7c23

Object ID : b2d5d50f-2d40-43b6-9050-4ce84ac373dd

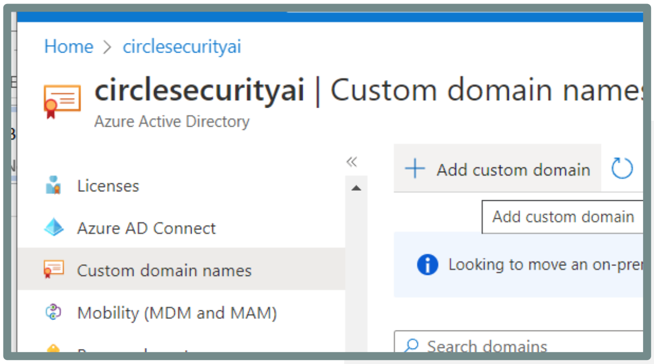
Directory (tenant) ID : 456ed0f2-f54e-4b12-9f18-3372c7b24b0c

Supported account types : My organization only

3 Adding a custom domain

After completing the application registration and enabling trust, we need to add a federated domain for Azure AD Single Sign On

In the Azure Portal, on the Azure Active Directory screen, add a custom domain:



Home > circlesecurityai

circlesecurityai | Custom domain name

Azure Active Directory

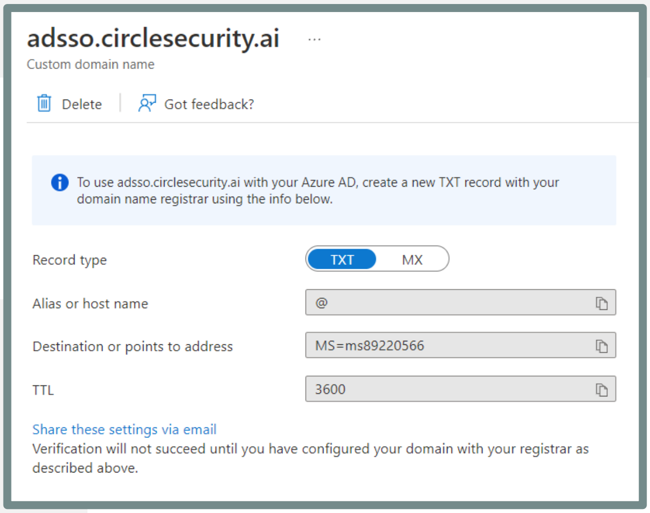
Looking to move an on-pre

Circle Security will provide a subdomain for you; we'll work with you to find the one that works for you.

Something like acme.mylogin.ai

The domain can be named at your convenience, but you will have to remember it as it will be needed in the later steps.

Azure requires proof that you own the domain, so you'll need to create a TXT or MX record.



adsso.circlesecurity.ai ...

Custom domain name

To use adsso.circlesecurity.ai with your Azure AD, create a new TXT record with your domain name registrar using the info below.

Record type: TXT MX

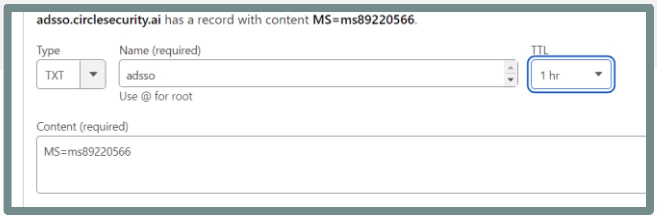
Alias or host name: @

Destination or points to address: MS=ms89220566

TTL: 3600

Share these settings via email

Verification will not succeed until you have configured your domain with your registrar as described above.



adsso.circlesecurity.ai has a record with content **MS=ms89220566**.

Type: TXT

Name (required): adsso

Use @ for root

TTL: 1 hr

Content (required): MS=ms89220566

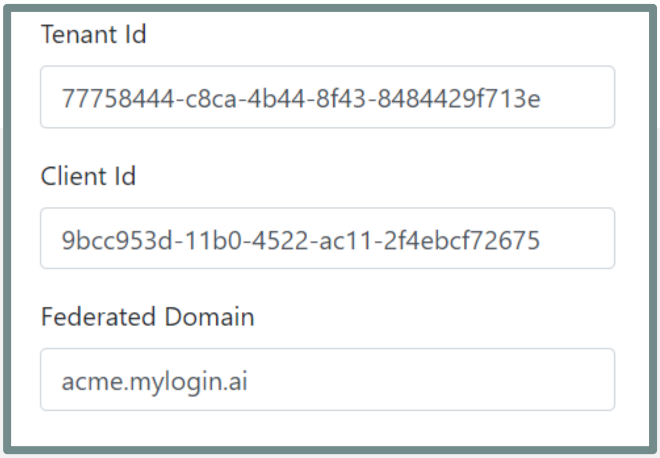
The Circle Sales Engineer will add the required TXT record

4 Setting up a Circle Access for AD SSO tenant

Head over to **https://adsso.circlesecurity.ai,** click on Login with Circle and scan login

Here you will see the tenant that was automatically created in Step 1.

Click ‘Edit’ and enter the Tenant id and the Client id from the App Registration in Step 2 and Custom Domain from Step 3; here’s an example.

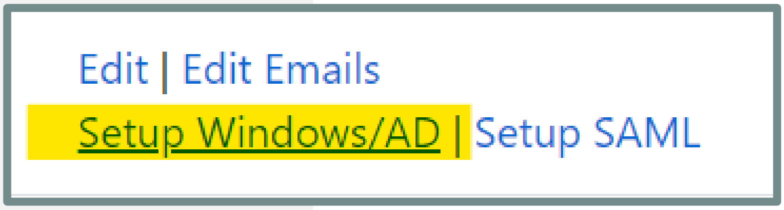


Tenant Id
77758444-c8ca-4b44-8f43-8484429f713e

Client Id
9bcc953d-11b0-4522-ac11-2f4ebcf72675

Federated Domain
acme.mylogin.ai

And click Save. This will take you back to the Tenant List screen. Find your newly created tenant entry and click the ‘Setup Windows/AD’ link.



Edit | Edit Emails
Setup Windows/AD | Setup SAML

5 Setting up Single Sign On and testing the flow

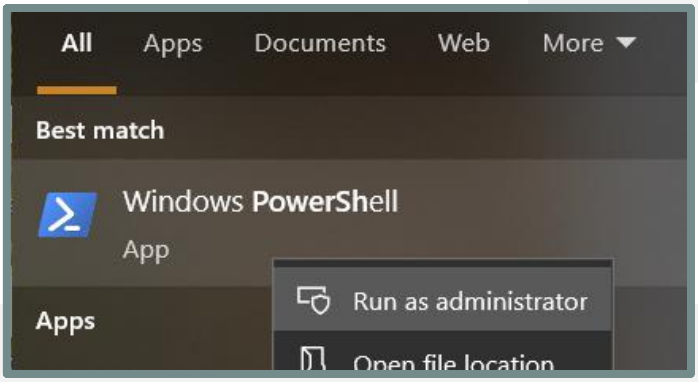
Note: For this step, you'll need Azure Administrator credentials and running on a computer with PowerShell.

At the end of the previous step, we were looking at the details of our newly created tenant.

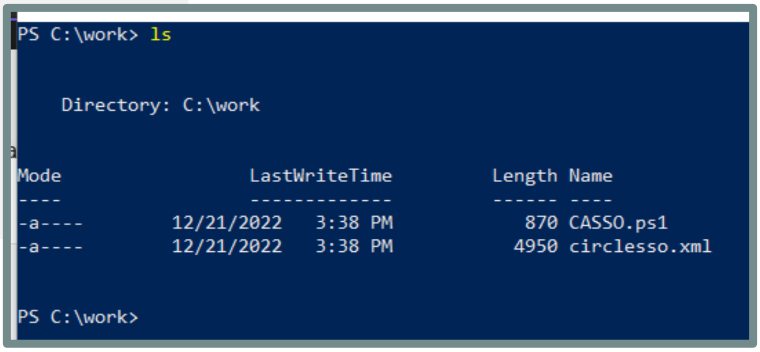
On the lower part of that screen, in the 'Implementation Helpers' section, you'll see three buttons.

Click on '**Download SSO Metadata file**' and on **'Download SSO PowerShell file'** to get the SSO setup files.

Open a Windows PowerShell as an Administrator



Create a folder called c:\work (or anything) and copy the two downloaded files into it.



```
PS C:\work> ls


    Directory: C:\work


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/21/2022   3:38 PM            870 CASSO.ps1
-a----        12/21/2022   3:38 PM           4950 circlesso.xml


PS C:\work>
```

Run the .\CASSO.ps1 script.

(**Note:** If you get a warning about scripts not being allowed, run this PowerShell command to enable them: Set-Execution Policy Unrestricted)

Agree to all the warnings/permissions ***(r/y/a)***

Then you'll be asked the log in to Azure, enter the admin credentials, and the script should finish.

Let's test the SSO flow now.

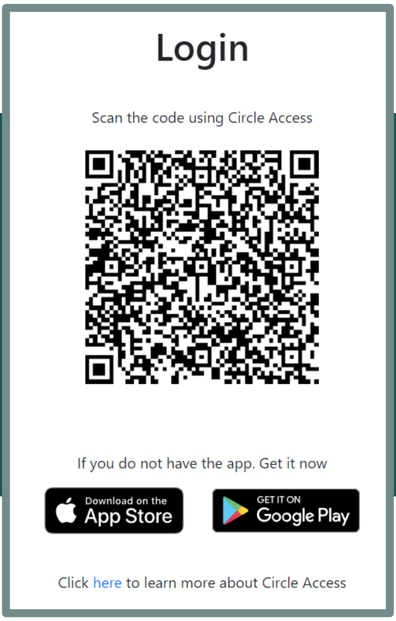
Open an Incognito window and navigate to **https://myapps.microsoft.com**. You will be prompted to enter an email address enter **BubbaJones@<YOURFEDERATEDDOMAIN>.** (e.g**.,** ***bubbaJones@acme.mylogin.ai***).

(**Note:** It doesn't need to be an actual email address, Microsoft is trying to figure out the federated domain name to route the login request to Circle Security servers)

When you hit enter and if you see a QR code, if we set the SSO correctly

(**Note 1**: if you don't get the QR code, sometimes it takes a while for Microsoft to set up the actual federation)

(**Note 2**: If you scan this QR code, you'll get an error since Azure AD doesn't know to recognize your phone yet)



Login

Scan the code using Circle Access

If you do not have the app. Get it now

Click here to learn more about Circle Access

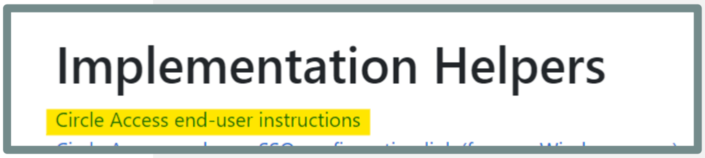
6

Circle Access end user Configuration

At the end of Step 4, you were looking at the details of your tenant.

Click on the ‘Circle Access end-user instructions’ right under ‘Implementation Helpers’. The highlighted text below is an example.

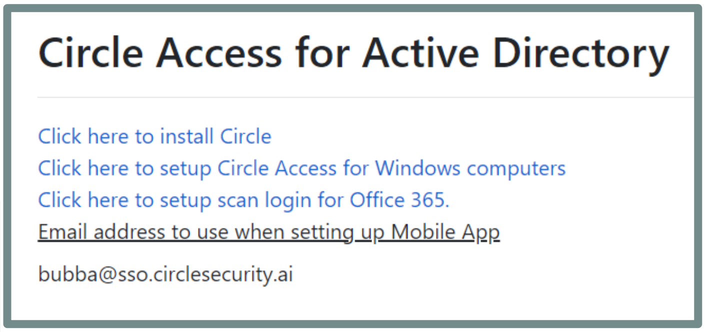
Note: Share the URL of ‘Circle Access end-user instructions’ and the End user implementation guide with the end users to onboard them on Circle Access for Azure AD. Our Customer Success team will help you in compiling the content and also support you during the onboarding process.



Implementation Helpers

Circle Access end-user instructions

You will be directed to the page that your end-users will be using for their implementation.

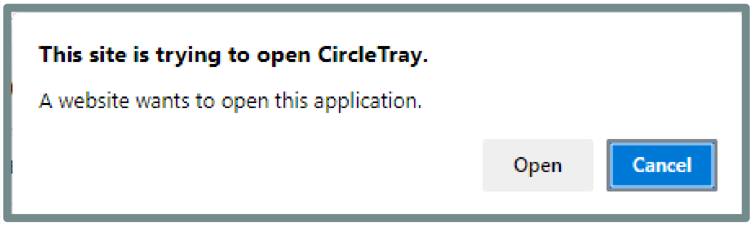


Circle Access for Active Directory

Click here to install Circle
Click here to setup Circle Access for Windows computers
Click here to setup scan login for Office 365.
Email address to use when setting up Mobile App

bubba@sso.circlesecurity.ai

Click the second link and you see a message like this:



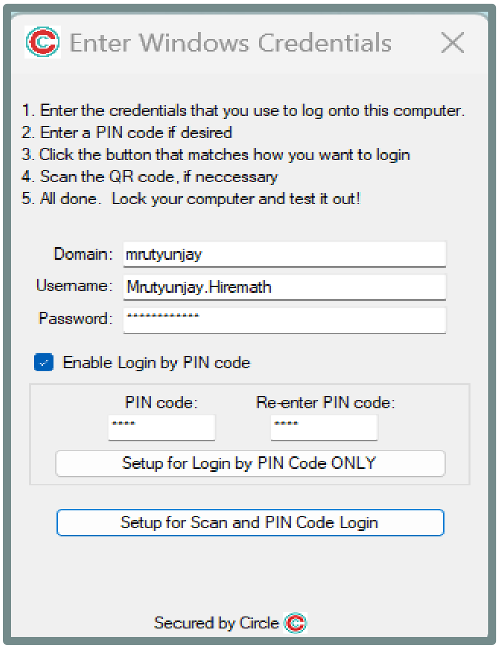
This site is trying to open CircleTray.

A website wants to open this application.

Click ‘**Open**’, and you’ll get a dialog asking for your credentials.

Enter your username and your password.

Click ‘Setup for Scan and PIN Code login’ and if your credentials are valid, a QR code will pop up.



Enter Windows Credentials

1. Enter the credentials that you use to log onto this computer.
2. Enter a PIN code if desired
3. Click the button that matches how you want to login
4. Scan the QR code, if neccessary
5. All done. Lock your computer and test it out!

Domain: mrutyunjay

Username: Mrutyunjay.Hiremath

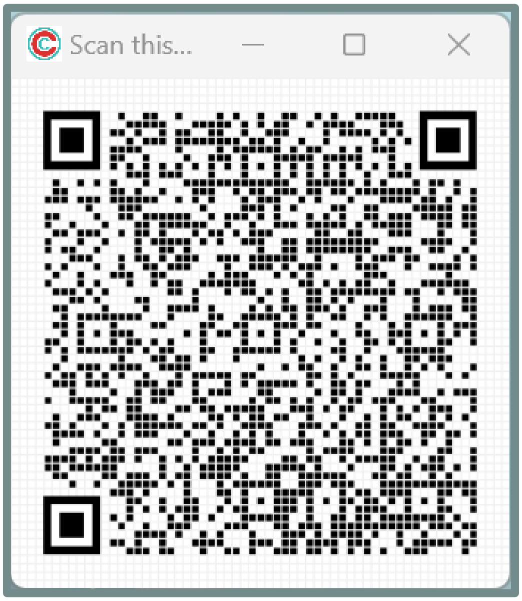
Password: ************

☑ Enable Login by PIN code

PIN code: ****

Re-enter PIN code: ****

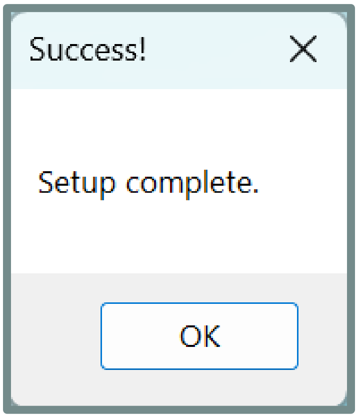
Setup for Login by PIN Code ONLY
Setup for Scan and PIN Code Login
Secured by Circle



Scan the QR code using the Circle Access App on your mobile phone.

If the scan is successful, you’ll see a ‘Setup Complete’ message.

Click OK to close this. At this point, you can restart your Windows computer and log in by scanning the QR code or with the pin.



Setup complete.

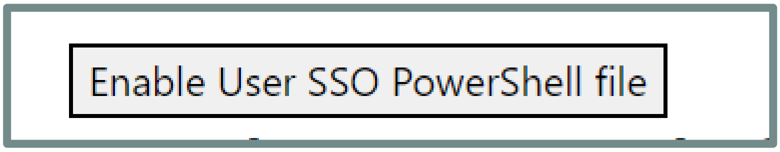
7 Enabling Single Sign On for end users

Your domain has already been configured to support Single Sign On. Now we just need to associate your end user's device with their Azure AD account.

At the end of the previous step, the user registers their credentials and scans a QR code. When this happens, their device ID and username is associated in your Circle Access tenant.

We need to now configure Azure AD for the user to have the correct device id.

When you log into your tenant at ***https://adsso.circlesecurity.ai,*** there is a button like this one.



Click to download the PowerShell script that will associate the the Azure AD user to device their devices.

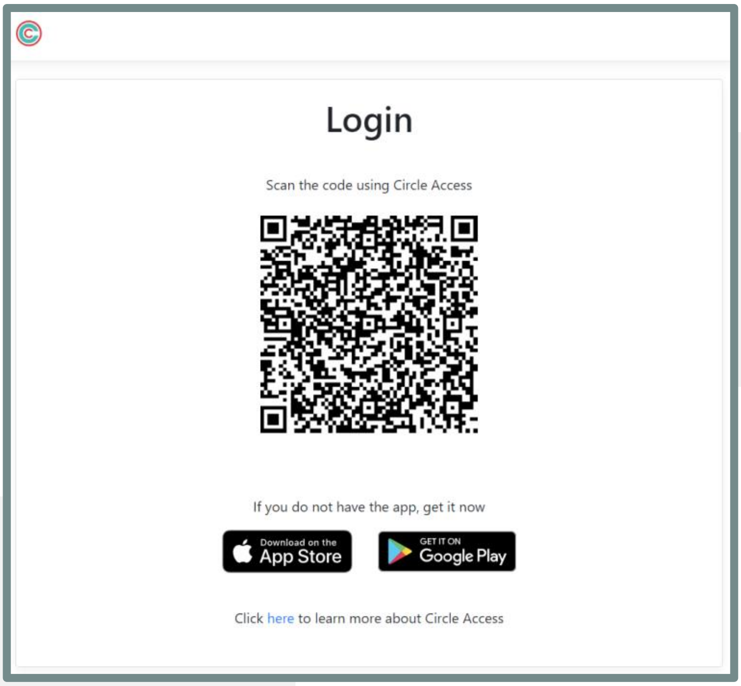
Run the script from an administrator PowerShell.

(**Note:** The script will only enable SSO for users who have registered their credentials with Circle Access i.e., to all the users who have completed Circle Access for Azure AD setup from their end. So it needs to be executed every time when new user/users are onboarded to Circle Access to enable SSO.)

Testing Single Sign On

Test the SSO by entering the URL in your browser window
https://myapps.microsoft.com/<FEDERATEDDOMAIN>
(e.g., **https://myapps.microsoft.com/acme.mylogin.ai**)

This will take you Circle Access QR Code page to scan and login to your Microsoft Office apps and when you scan the QR Code, you should see something like this, which means Microsoft says you're logged in!



Login

Scan the code using Circle Access

If you do not have the app, get it now

Click here to learn more about Circle Access

Appendix

Adding another SSO administrator.

When your Circle Access tenant was created on the website, it was tied to the mobile device used to log in. If you want to add another user or device to this tenant, you can use the **'Add New Administrator'** button on the main tenant list page.

Here are the steps:

1. Click the 'Add New Administrator' button
2. Read the short description and instructions and click the 'Add New Administrator' button
3. Scan the QR Code with the NEW device
4. All done.
5. You can now log into Circle Access Tenant

(**https://adsso.circlesecurity.ai**) with the new device.

Setting up Circle Access Mobile MFA

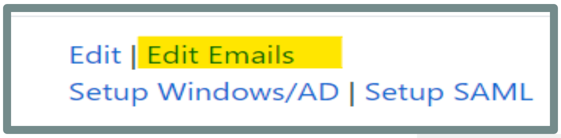
Circle Access Mobile MFA works with Circle Browser, an internet browser that's integrated in Circle Access.

Circle Browser will 'lock' and require a Circle Access mobile scan to unlock if:

- The tablet was locked
- The browser loses focus for a certain amount of time

Here are the steps to configure Mobile MFA for your users:

1. Log into your Circle Access Tenant and click the 'Edit Emails' link



Edit | Edit Emails
Setup Windows/AD | Setup SAML

2. On the next screen, in the box, enter the email address of the users who will be allowed to scan unlock Circle Browser. No need to worry about duplicates or non-email fields. Anything that doesn't look like an email, will be ignored.

3. Your users will need to set up Circle Access on their mobile device with an email that's also in this list.

Setting up Mobile Application to work without a password

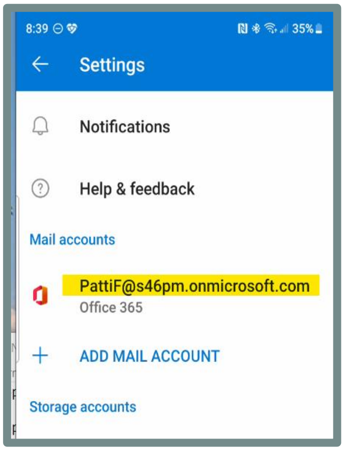
One of the many attractive features of Circle Access is the ability to prevent phishing attacks; it does this by changing the password and never revealing it to the user. This poses a problem in situations where a password is required, most notable is a native mobile application (e.g. Microsoft Outlook).

While the mobile user could use Circle Access Single Sign-On with a web client to access their email, many users like to use a native application like Outlook on their mobile device. Here are the steps to configure an application to work with Circle Access without knowing the password. I'm going to be setting up Microsoft Outlook for Android.

1. Ensure Circle Access SSO is configured and the user is enabled to use it.
2. On the mobile device, open Outlook and remove your company email (in my example, I'm removing ***Pattf@s46pm.onmicrosoft.com).***

   a. Click the icon in the upper left hand corner, then click the gear

   b. Select the account remove



8:39 35%

Settings

Notifications

Help & feedback

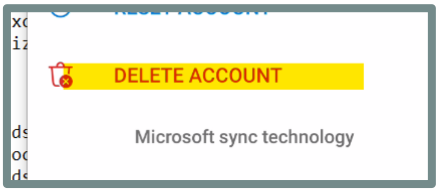
Mail accounts

PattiF@s46pm.onmicrosoft.com
Office 365

ADD MAIL ACCOUNT

Storage accounts

   c. Scroll to the bottom and click 'Delete account

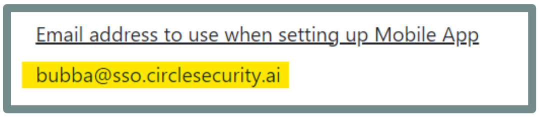


DELETE ACCOUNT

Microsoft sync technology

d. Click **'Add Account'** and ignore any of the **'Accounts found'** and click 'Skip these accounts' link at the bottom.

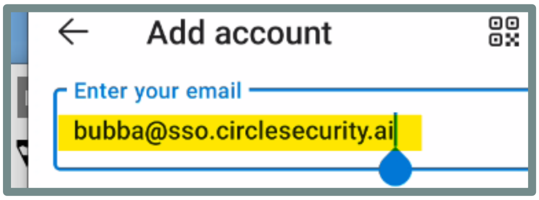
e. Here you'll enter the email address that will tell Microsoft that this is a federated account. You can find it on your Circle Access Tenant page ***(https://adsso.circlesecurity.ai)***. In my example, it's **bubba@sso.circlesecurity.ai**. [Note: only the domain part of the email address needs to be valid, it could be **professorsnape@sso.circlesecurity.ai** and work just as well



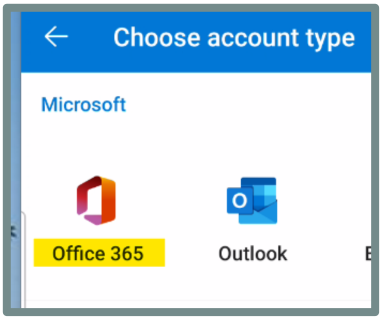
Email address to use when setting up Mobile App

bubba@sso.circlesecurity.ai

Enter this email address to the ‘Enter your email’ field in Outlook and click ‘Continue’. and click ‘Continue’



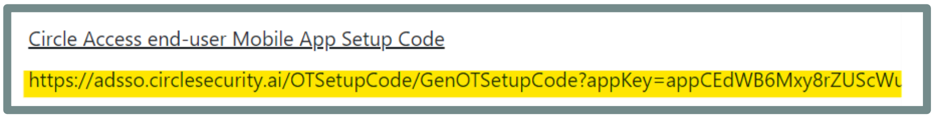
Enter your email
bubba@sso.circlesecurity.ai



f. On the next screen, pick ‘Office 365’ for the ‘account type’

g. This will redirect you to a screen where you enter a ‘mobile set up code’.

   i. Users can use the URL on the Circle Access Tenant to get a setup code or

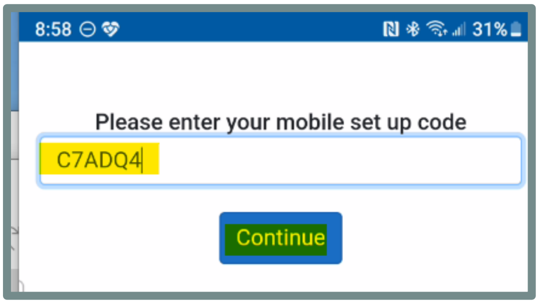


Circle Access end-user Mobile App Setup Code

https://adsso.circlesecurity.ai/OTSetupCode/GenOTSetupCode?appKey=appCEdWB6Mxy8rZUScWu

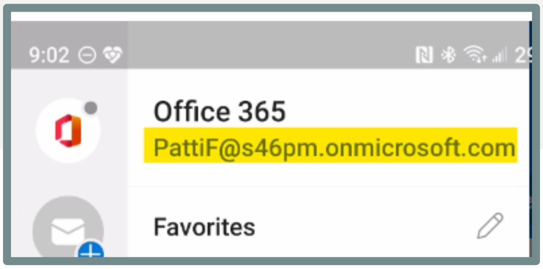
   ii. They can click the ‘Get Setup Code’ button in the mobile app and follow the instructions.

h. Enter the one-time code and press Continue



Please enter your mobile set up code
C7ADQ4

i. Outlook will think about it a minute and then the account will be added.



PattiF@s46pm.onmicrosoft.com

[Note: The Outlook app will ask you to re-enter your credentials every time the password is changed; which means this process will need to be repeated. It is recommended that you configure Circle Access to change your password infrequently due to this.]

Setting up a scheduled task to automate SSO enrolment

Circle Access for Azure AD includes a Single Sign On feature to allow people to log into their accounts on public computers or anywhere where they can't leverage Windows Scan Login.

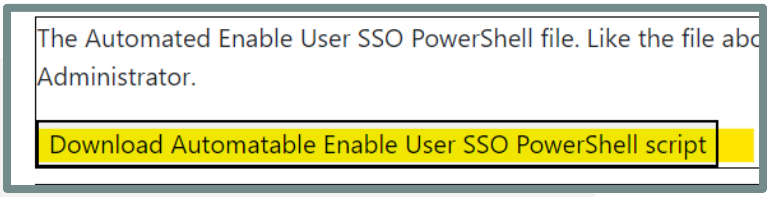
The way federation works with Azure requires a two-step process, one performed by the user and another one performed by the Azure Administrator. The following steps will document how to set up an automatic task to do the admin's part.

The end result will be that after a user does their part, they will automatically enabled to use SSO without the administrator having to get involved.

[Note: Since hacker like to use the task scheduler to re-infect cleaned computers, Microsoft requires credentials to create a scheduled task. If you are using Circle Access Password change feature, you will not be able to use your credentials. Most companies have a standard domain admin account, use that account to save the task]

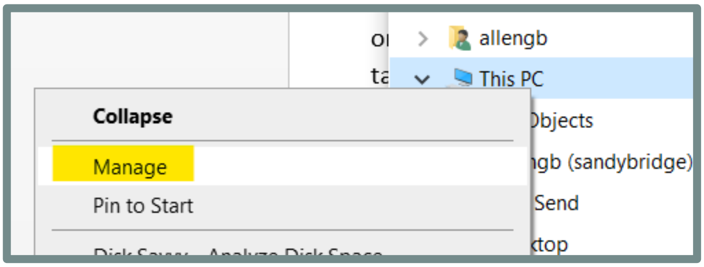
Step 1.

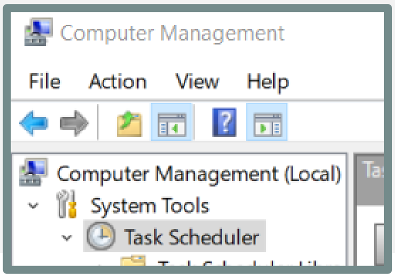
On your Circle Access SSO tenant page, use the 'Download Automatable Enable User SSO PowerShell script' and put it somewhere on your hard drive. For this test, I put it in C:\Circle


The Automated Enable User SSO PowerShell file. Like the file abc
Administrator.

Download Automatable Enable User SSO PowerShell script

Step 2. Open Windows Explorer and right click on 'This PC'





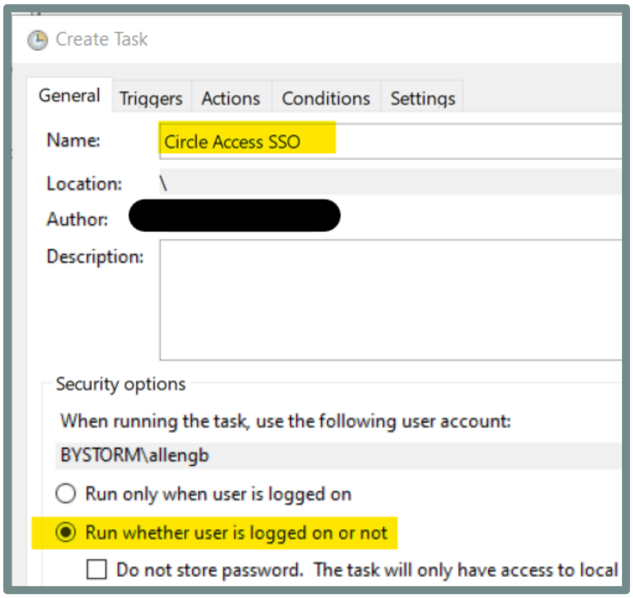
This will bring up the Computer Management application

Step 3: Right click on the 'Task Scheduler' and select 'Create Task'

Step 4: Set up a new task:

On the General Tab

For the Name field, enter 'Circle Access SSO' and select 'Run whether user is logged on or not'



Create Task

Name: Circle Access SSO

Location: \

Author: [redacted]

Description:

Security options

When running the task, use the following user account:

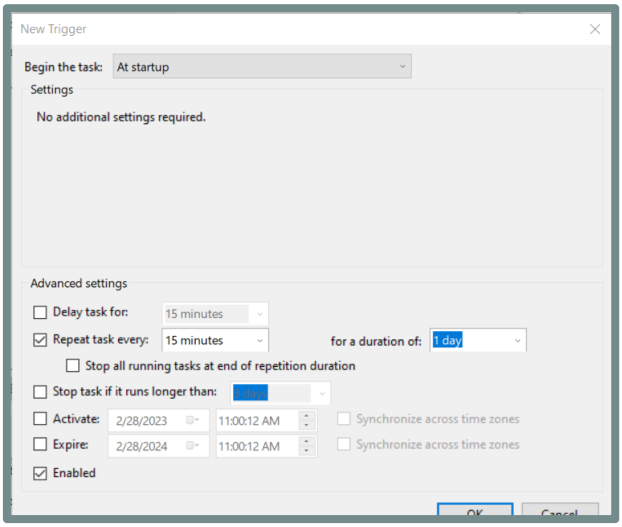
BYSTORM\allengb

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local

On the Triggers tab, for 'Begin the task'...pick 'At startup' and configure the task to repeat every '15 minutes'



New Trigger

Begin the task: At startup

Settings

No additional settings required.

Advanced settings

□ Delay task for: 15 minutes

☑ Repeat task every: 15 minutes for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Activate: 2/28/2023 11:00:12 AM □ Synchronize across time zones

□ Expire: 2/28/2024 11:00:12 AM □ Synchronize across time zones

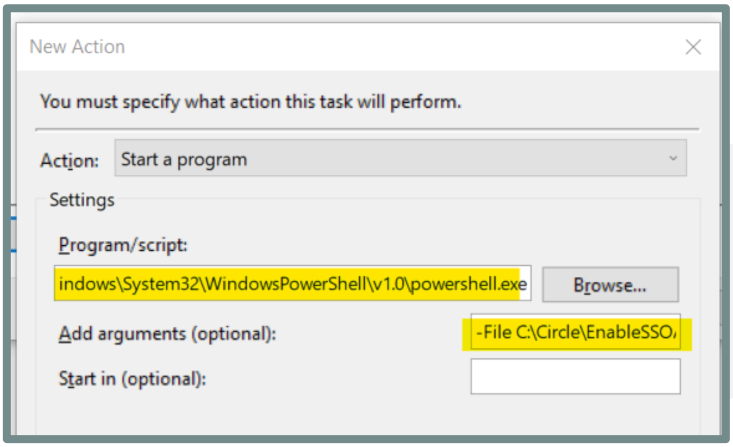
☑ Enabled

On the Actions tab, click 'New' and for Action pick 'Start a program'

In the Program/script field...enter:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

And in the arguments field, enter –file and the path to the script you downloaded earlier (C:\Circle\EnableSSOAuto.ps1 in my case)


New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: indows\System32\WindowsPowerShell\v1.0\powershell.exe

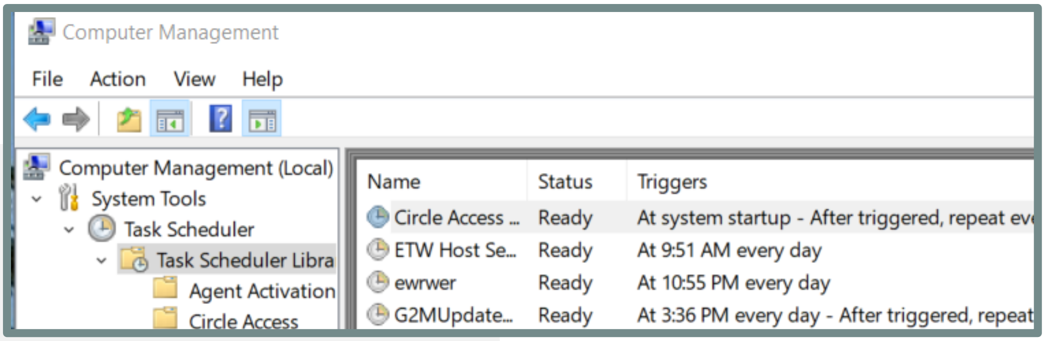
Add arguments (optional): -File C:\Circle\EnableSSO/

Start in (optional):

Click Ok to close the New Task dialog.

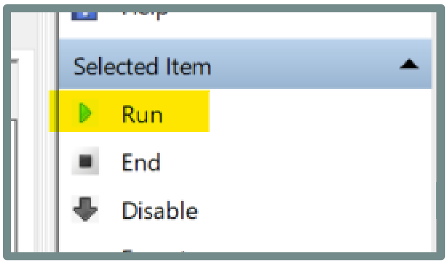
Step 5: Test the newly created task

Click on **'Task Scheduler Library'** and find the 'Circle Access' task

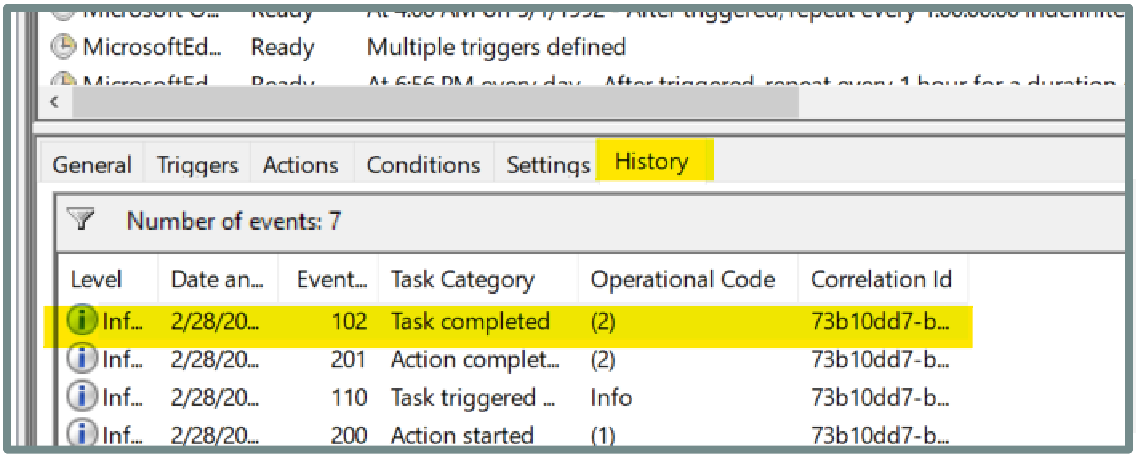

Computer Management

Name	Status	Triggers
Circle Access ...	Ready	At system startup - After triggered, repeat ev
ETW Host Se...	Ready	At 9:51 AM every day
ewrwer	Ready	At 10:55 PM every day
G2MUpdate...	Ready	At 3:36 PM every day - After triggered, repeat

Select it and on the right, click the 'Run' button to test it.



To see the results of the run, check the History tab and look for **'Task completed'**



MicrosoftEd... Ready Multiple triggers defined

Number of events: 7

Level	Date an...	Event...	Task Category	Operational Code	Correlation Id
Inf...	2/28/20...	102	Task completed	(2)	73b10dd7-b...
Inf...	2/28/20...	201	Action complet...	(2)	73b10dd7-b...
Inf...	2/28/20...	110	Task triggered ...	Info	73b10dd7-b...
Inf...	2/28/20...	200	Action started	(1)	73b10dd7-b...

Circle Access IdP/SSO for Hybrid deployments

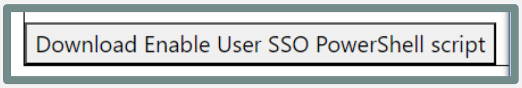
The Circle Access setup is a bit different for hybrid deployments, where the primary domain is on-premises and is synchronized with Azure AD.

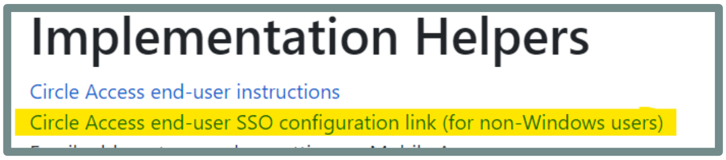
Since the user will be logging into the on-premises domain instead of Azure AD, Circle Access won't know which Azure account to associate with the mobile device.

To work around this, have your users use the non-Windows SSO configuration link. You'll find it on your Circle Access Tenant page.

After your users have associated their Microsoft credentials with their device, you will need download and run the 'Enable User SSO PowerShell' script.

The button is also on your tenant page





Implementation Helpers

Circle Access end-user instructions

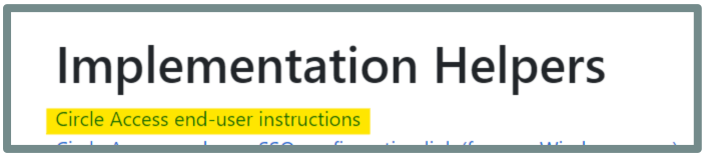
Circle Access end-user SSO configuration link (for non-Windows users)

This last bit isn't necessary if you've setup a scheduled task to run the **'Automatable'** script.

Implementation support for end users

Once the Admin setup is completed, you need to share the following steps and instructions with your end users to complete the onboarding process –

1. The highlighted URL (as mentioned in Step 6)



Implementation Helpers

Circle Access end-user instructions

2. Share the end user implementation guide for Circle Access for Azure AD, which mainly consists of step 6

3. Once the user is onboarded to Circle Access for Azure AD, trigger the PowerShell command to enable SSO.

4. Notify the end user to test the SSO as per the End user implementation guide

Thank You