

# Discovering Azure AD Premium.

---

In this section we will start using AD Premium features, and see how it add value to our Company.

## **Some Useful info for this article and related components.**

Lab Company Name: MAqov.org

Global Admin: [admin@maqov.onmicrosoft.com](mailto:admin@maqov.onmicrosoft.com)

Links we will use:

Office 365 admin page: <https://Portal.office.com/>

Azure Service Management: <https://manage.windowsazure.com/>

SaaS Access Panel: <https://myapps.microsoft.com/>

we will need test users, test pc or VM with operating system windows 10.

## **Objective**

Learn how to use azure ad premium features like:

- Company Branding.
- Configure DNS for Office 365.
- Multifactor Authentication.
- Self –Service Features.
- Join windows 10 to Azure AD.

## **Prerequisites**

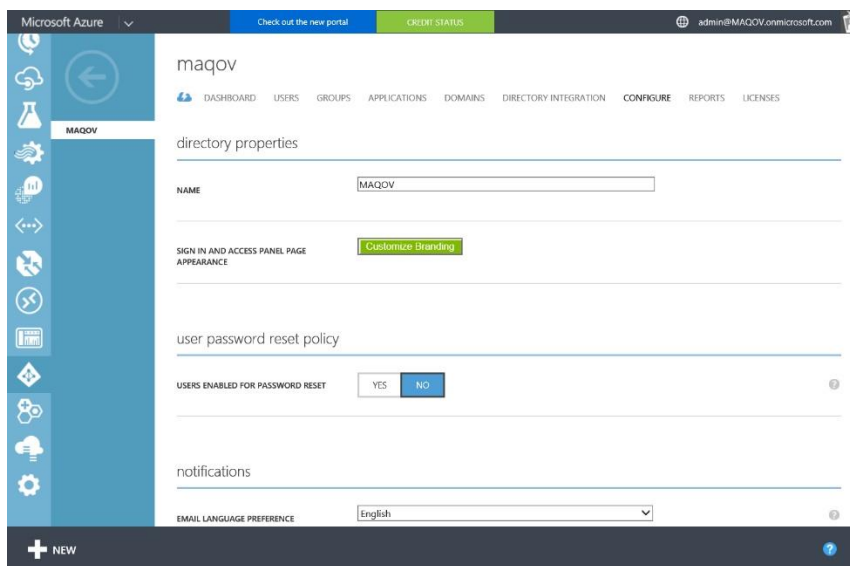
- Azure Subscription related to the Company domain, in our case "maqov.org"
- Office 365 Subscription related to the Company domain, in our case "MAQOV.org"
- EMS License.
- Test users with EMS License, and office 365 license.

# Company Branding

1. Navigate to the "**CONFIGURE**" tab of your directory.
2. under the "**directory properties**" section for the **Customize Branding** button.
3. Click the "**Customize Branding**" button.

This will bring up a dialog which asks you to provide the default customized branding info for your organization.

This default branding will be shown to every user in your organization.



4. Upload the **Banner logo** and **Sign in page** illustration images by browsing to the files locally,
5. Update the **Sign in page text** and **User ID Placeholder**.
6. Once you are finished setting these properties, click the check mark in the lower right to save your default branding settings.


## CUSTOMIZE DEFAULT BRANDING

Manage how company logos, text, and colors should appear on your organization's Sign In and Access Panel pages. You can also apply unique branding settings for different languages. [Learn more](#)


### BANNER LOGO ?

 calgary\_stampede-2560x1440.jpg

### SQUARE LOGO ?

 p1.jpg

### SQUARE LOGO, DARK THEME ?

 BROWSE FOR FILE...

### USER ID PLACEHOLDER ?

userID@maqov.org

### SIGN-IN PAGE TEXT HEADING ?

|

### SIGN-IN PAGE TEXT ?

Welcome to MAQOV Corp




MAQOOV.org

CUSTOMIZE DEFAULT BRANDING

Manage how company logos, text, and colors should appear on your organization's Sign In and Access Panel pages. You can also apply unique branding settings for different languages.  
[Learn more](#)

SIGN-IN PAGE ILLUSTRATION ?

 firewatch-2560x1440.jpg

SIGN-IN PAGE BACKGROUND COLOR ?

HIDE KMSI ?

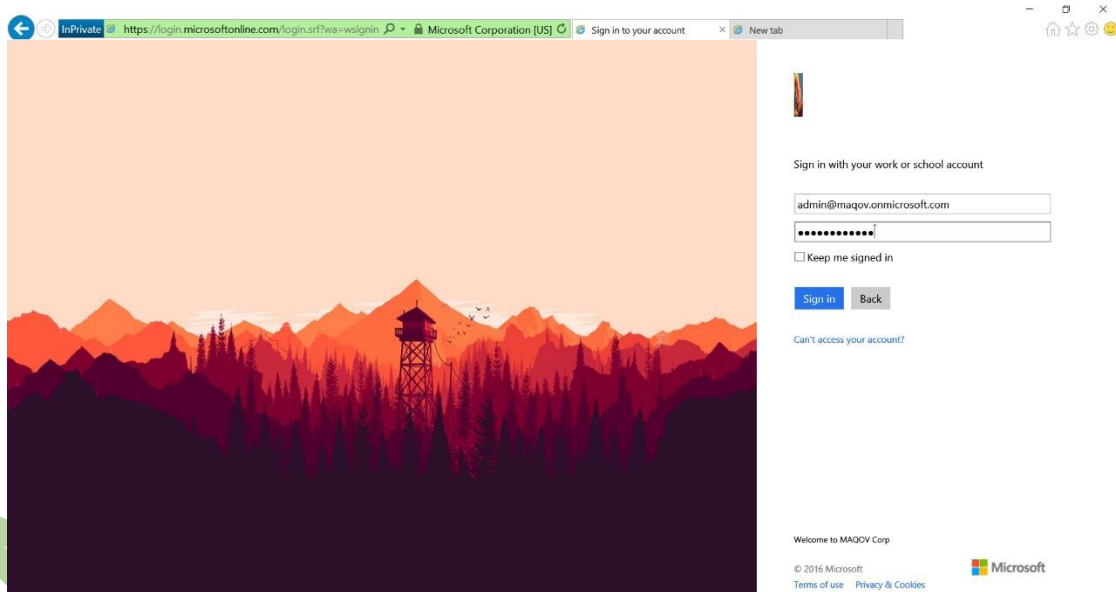
SHOWN

HIDDEN

POST LOGOUT LINK LABEL ?

POST LOGOUT LINK URL ?

7. Let us test by opening the following link <https://myapps.microsoft.com>, and then login.

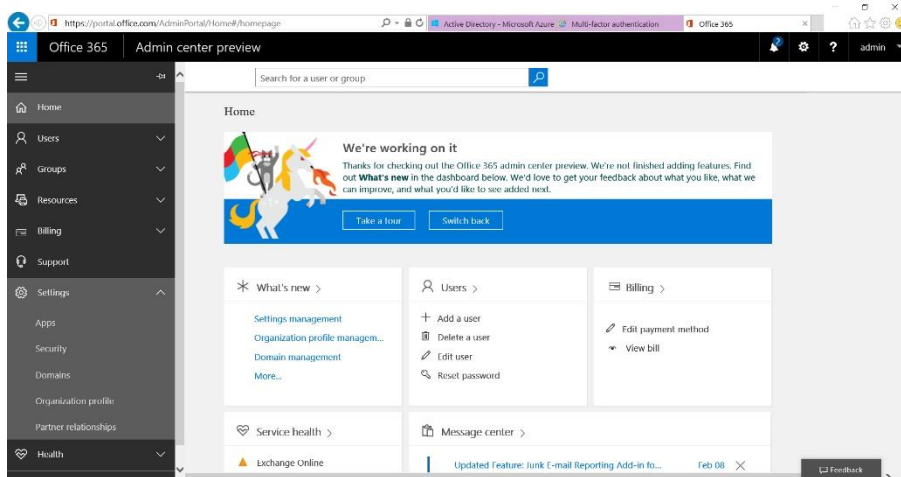


It's fine you can add the look and feel related to your corporate and make the end user expose to the same brand for the cloud services.

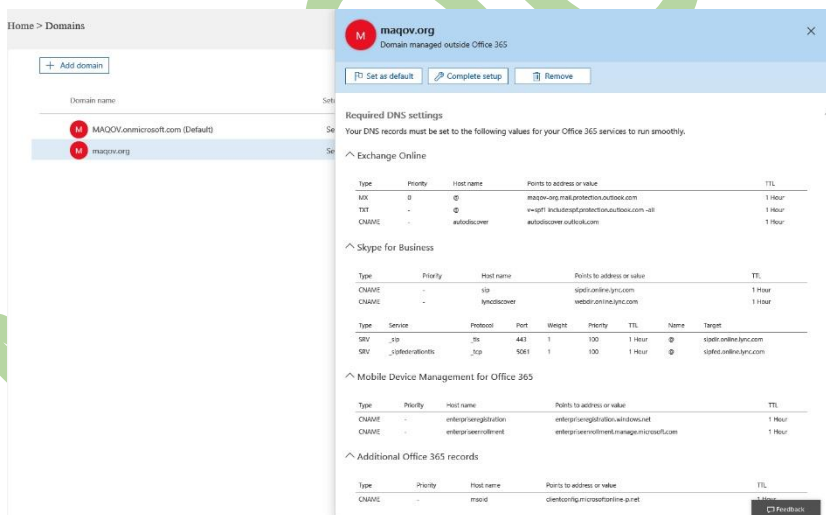
# Configure DNS for Office 365

In this section we will be introduced to how to update your external DNS to enable our Office 365 email.

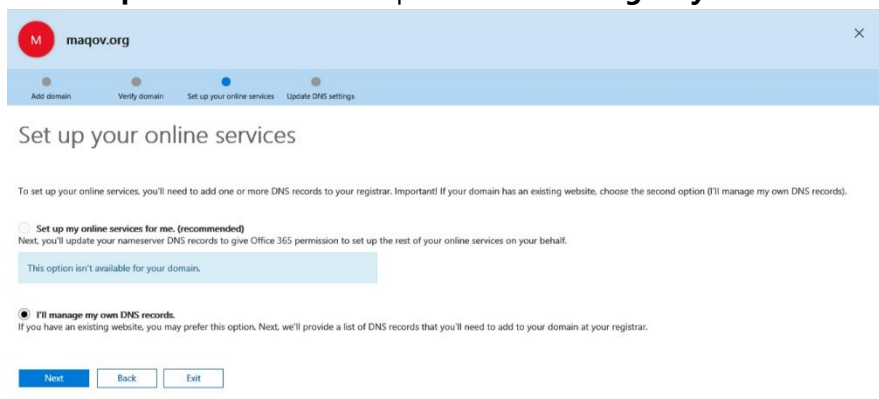
1. Open IE in an InPrivate session, browse <https://portal.office365.com>
2. Login with a **global admin** on your tenant.
3. On the **left panel**, expand **settings, domain**.



4. Select your **domain**, in our case "**maqov.org**", to **complete setup**.
5. On the **middle panel**, click **Complete setup** button.

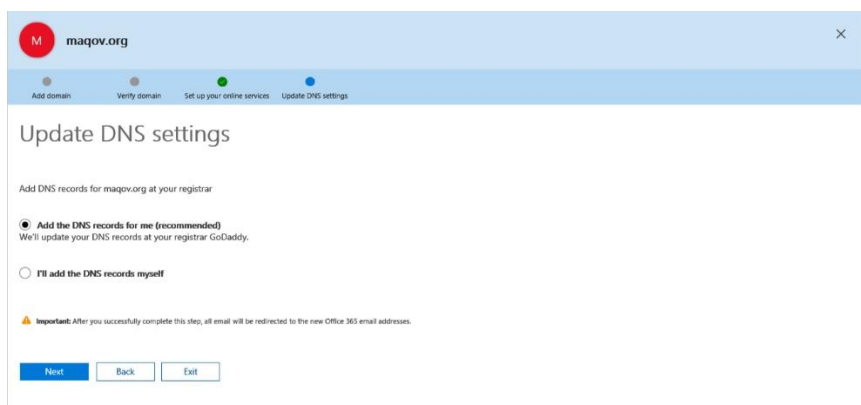


6. On “**Setup online services**” Step Select “**I’ll manage my own DNS records**”.



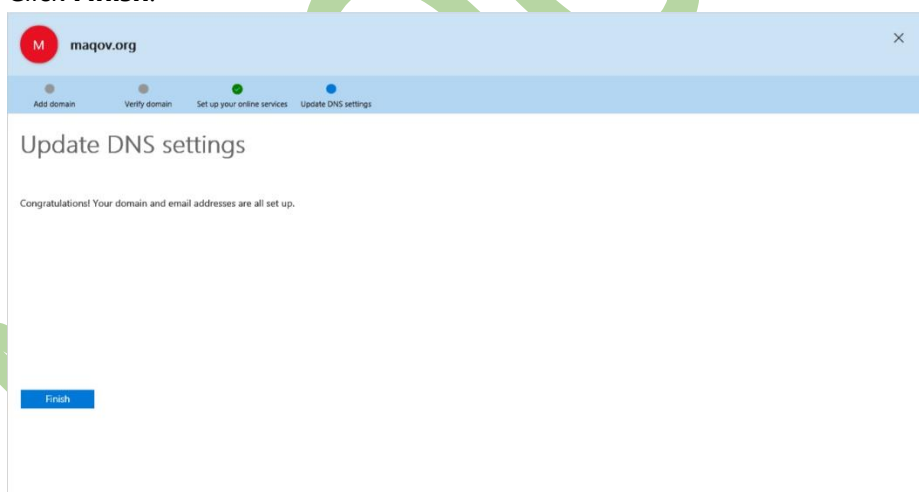
The screenshot shows the 'Set up your online services' step in the maqov.org setup wizard. The progress bar at the top indicates that 'Set up your online services' is the current step, with 'Add domain' and 'Verify domain' completed and 'Update DNS settings' pending. The main heading is 'Set up your online services'. Below it, a message states: 'To set up your online services, you'll need to add one or more DNS records to your registrar. Important! If your domain has an existing website, choose the second option (I'll manage my own DNS records)'. There are two radio button options: 'Set up my online services for me, (recommended)' and 'I'll manage my own DNS records'. The first option is currently selected, but a light blue message box below it says 'This option isn't available for your domain.' The second option, 'I'll manage my own DNS records', is selected. Below this, a message says: 'If you have an existing website, you may prefer this option. Next, we'll provide a list of DNS records that you'll need to add to your domain at your registrar.' At the bottom, there are three buttons: 'Next' (highlighted in blue), 'Back', and 'Exit'.

7. On “**update DNS Settings**” Step, select “**Add DNS Records for me**”.



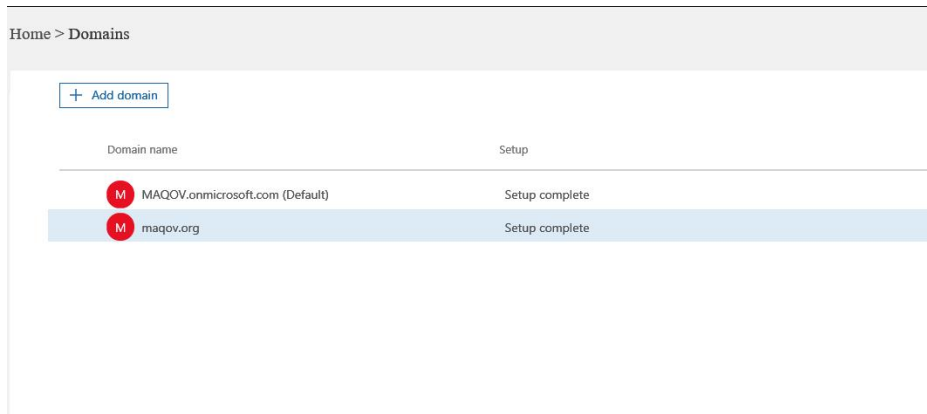
The screenshot shows the 'Update DNS settings' step in the maqov.org setup wizard. The progress bar at the top indicates that 'Update DNS settings' is the current step, with 'Add domain', 'Verify domain', and 'Set up your online services' completed. The main heading is 'Update DNS settings'. Below it, a message states: 'Add DNS records for maqov.org at your registrar'. There are two radio button options: 'Add the DNS records for me (recommended)' and 'I'll add the DNS records myself'. The first option is selected. Below this, a message says: 'We'll update your DNS records at your registrar GoDaddy.' An important note with a warning icon states: 'Important! After you successfully complete this step, all email will be redirected to the new Office 365 email addresses.' At the bottom, there are three buttons: 'Next' (highlighted in blue), 'Back', and 'Exit'.

8. On the prompt pop up message, login by **Go Daddy** credentials, and then click **Ok**.
9. Click **Finish**.

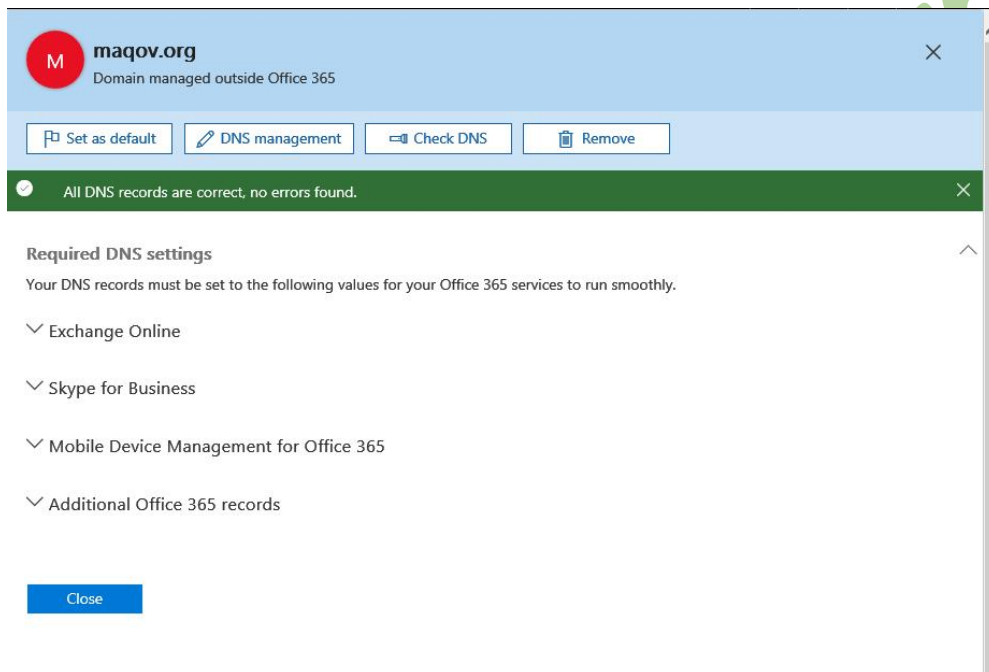


The screenshot shows the 'Update DNS settings' step in the maqov.org setup wizard. The progress bar at the top indicates that 'Update DNS settings' is the current step, with 'Add domain', 'Verify domain', and 'Set up your online services' completed. The main heading is 'Update DNS settings'. Below it, a message states: 'Congratulations! Your domain and email addresses are all set up.' At the bottom, there is a single button: 'Finish' (highlighted in blue).

10. Now we can see that the domain setup is completed.



11. Let us check the DNS records, select the domain, on the middle panel click “**check DNS**”.



## Integrate SaaS Applications

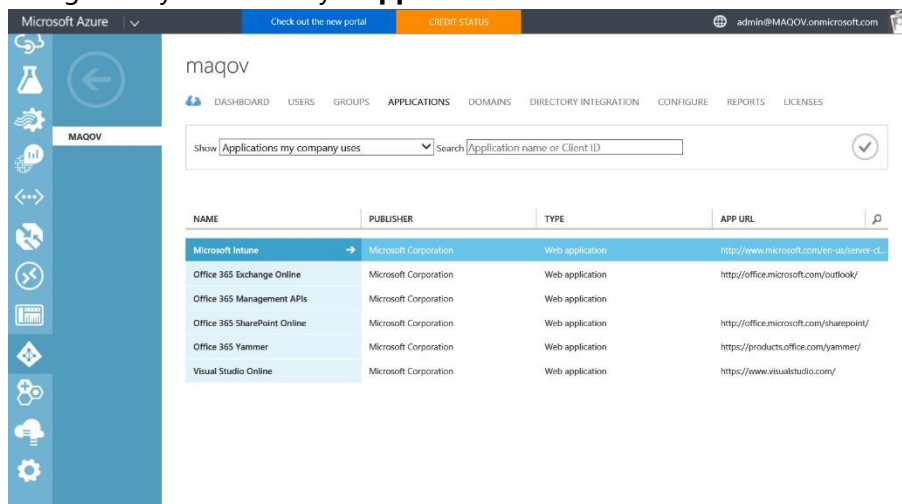
After branding our directory, let's integrate some applications!

In this section, you'll learn how to add a simple password single sign on application, assign some user it, and verify it's working by accessing the access panel to see the application.

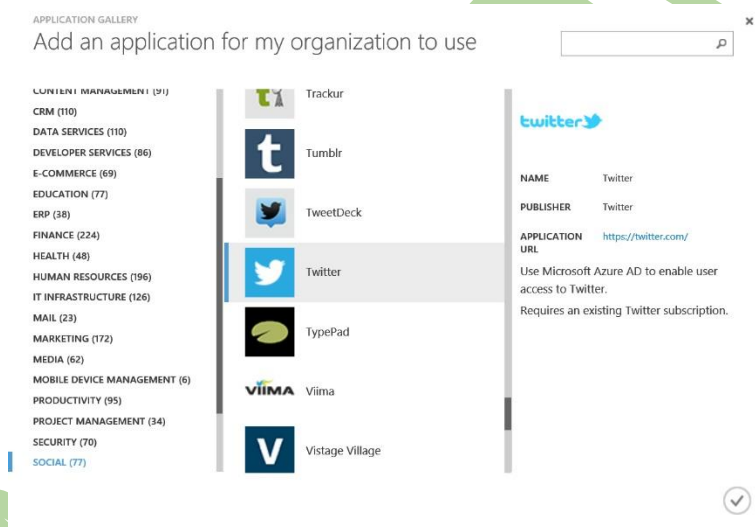
For example, your company's twitter account used by marketing team.

1. In Internet Explorer open a session for <https://manage.windowsazure.com>
2. In the left hand pane scroll to scroll and select **ACTIVE DIRECTORY**
3. Select the tenant you created.

4. Navigate to your directory's **Applications** tab.

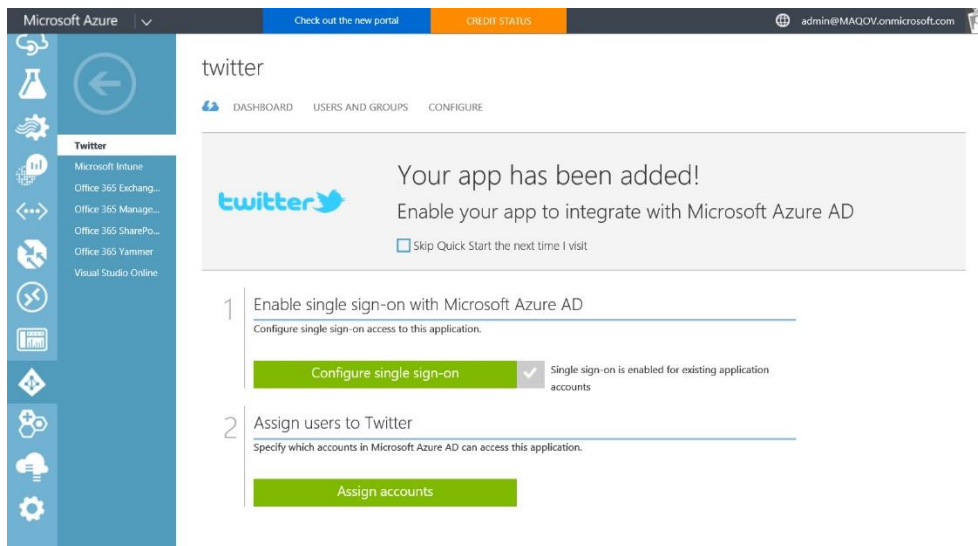


5. Once there, click on the **ADD** button at the bottom of the page.
6. Click on the **Add an application from the gallery** option to open the **Azure AD App Gallery**.
7. Once there, search for **Twitter**.



8. Note: you can use any app you like, it need not be twitter, just make sure you have an account already set up in that application you can use to test sign in.
9. If you want to sign up for twitter for this demo, you can do so here: <https://twitter.com/>.
10. Once you find twitter, click the check box to add it to your Azure AD Directory.
11. That's it! Now twitter has been integrated into your directory.

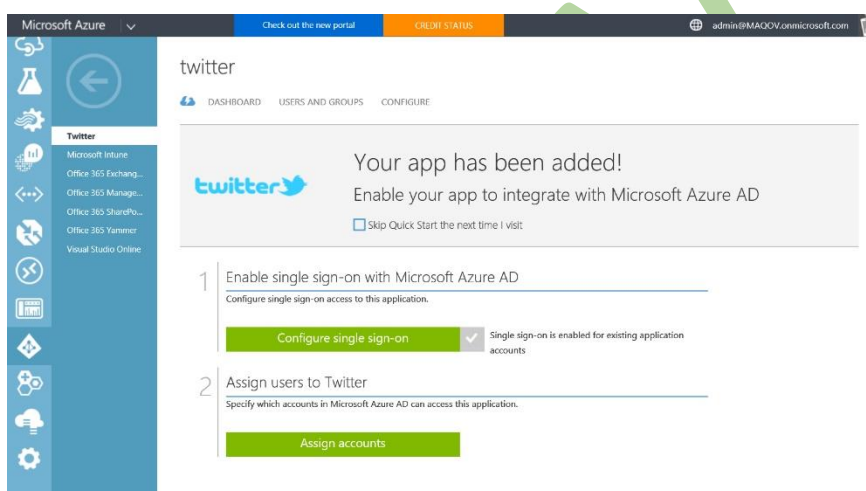




12. Notice that the application has already been integrated for Password Single-sign-On.

13. You will now need to assign some users or groups to this app before those users will be able to see twitter on their Access Panel.

14. Click on the **USERS AND GROUPS** tab to see which users and groups have been assigned to Twitter.



15. Select the group Users **Mobility User1** and then click the **ASSIGN** button at the bottom of the screen to grant access to **Twitter**.

16. On the next screen, click the **checkbox "I want to enter twitter credentials on behalf of the user"**, and then enter the credentials of the corporate twitter account.

17. Open IE then browse <https://myapps.onmicrosoft.com>

18. you will now be asked to install the **Access Panel browser extension**.

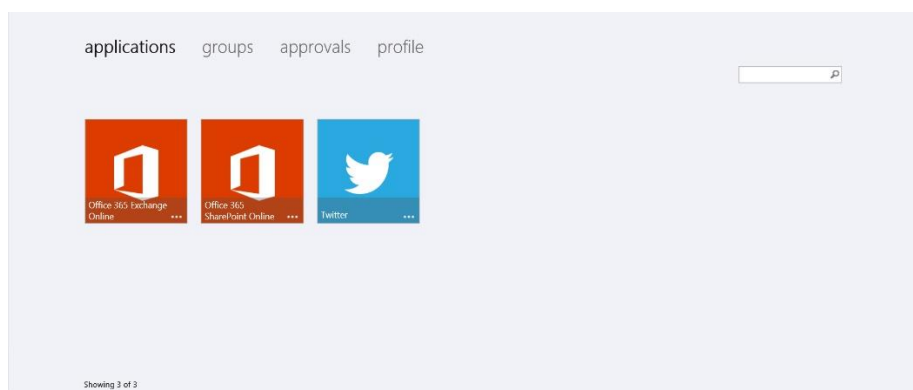
This extension allows you to securely store and retrieve passwords for your users in AAD, effectively enabling single sign in to cloud applications. Click on the green Install now button to begin the installation process. Note ***This plug-in does not work when using a private browser mode.***

19. In Internet Explorer, click the "run" button to run the installation wizard. In other browsers, follow the instructions provided to install the browser extension.

20. Click Next -> Install -> Finish on the extension setup wizard to install the extension (this will close any open Internet Explorer windows).

21. Follow the instructions on the screen to complete installation of the browser extension (will require you to re-start internet explorer once again).

22. Reopen the IE and login to <https://myapps.onmicrosoft.com>

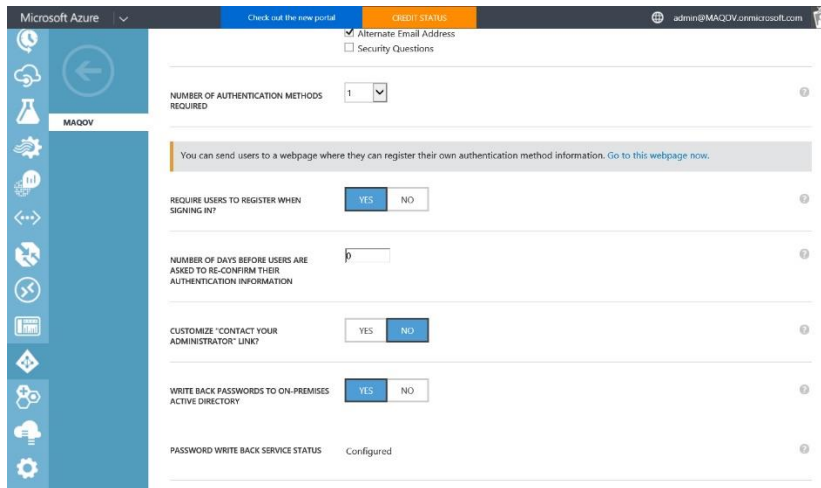


23. Click on twitter account. It will open the corporate twitter account to the assigned user.

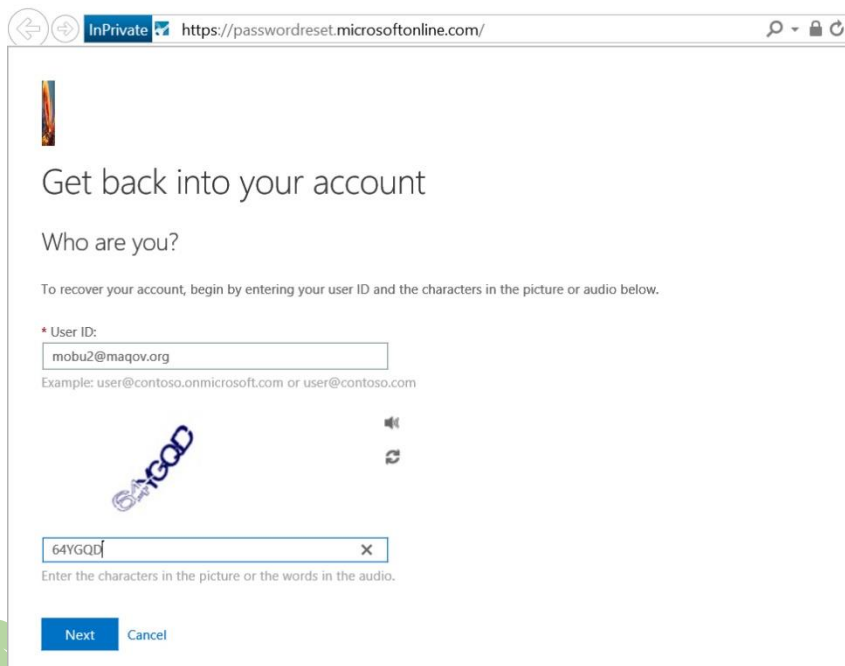
## Self-Service Password Reset

In this section we will focus on enable self-service password reset using additional security option as a second factor authentication, so that users in your organization can easily recover their passwords if they have forgotten them.

1. In Internet Explorer open a session for <https://manage.windowsazure.com>
2. In the left hand pane scroll to scroll and select **ACTIVE DIRECTORY**
3. Select your **Azure Active Directory**, Navigate to the **CONFIGURE** tab of your directory
4. at the **user password reset** policy section.
5. Set the **Users enabled for password reset** toggle to **YES** to reveal the rest of the password reset configuration.
6. Set the password reset policy **AUTHENTICATION METHODS AVAILABLE TO USERS** to allow: **Mobile Phone**, *note you can add more options.*
7. Keep **NUMBER OF AUTHENTICATION METHOD REQUIRED** to 1
8. Set **REQUIRE USERS TO REGISTER WHEN SIGNING IN TO ACCESS PANEL** to **NO**
9. Change the **NUMBER OF DAYS BEFORE USERS MUST CONFIRM THEIR CONTACT DATA** to never which is **0**.
10. Set the **CUSTOMIZE "CONTACT YOUR ADMINISTRATOR"** link to **NO**
11. Scroll down to the Notifications section.
12. Set the **NOTIFY USERS AND ADMINS WHEN THEIR OWN PASSWORD HAS BEEN RESET** to **NO**.
13. Verify your settings are correct and then click the **Save** button at the bottom of the screen to commit your changes.



14. Login to <https://passwordreset.microsoftonline.com>
15. Enter the credential of the local domain user or azure ad user, I will enter a local domain user to test the password **writeback** option.



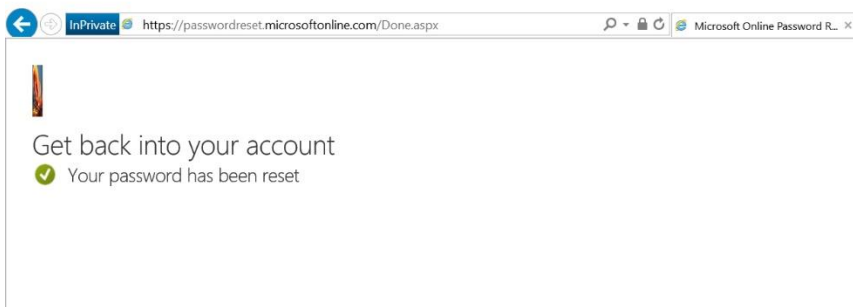
16. You will prompt to setup the authentication phone number, just select the country and then write your mobile phone, you will receive a phone call, just press the # key.
17. Once the request has been verified, the page will refresh, and you will be allowed to select a new password.
18. Enter a new password, confirm it, and click the **finish** button to save it to the directory.

**Note:**

*if you get an error telling you that "This password does not meet your corporate password policy" even though you entered a strong password, it is because the Minimum password age is set to 1 day in the Default Domain Policy for corp. in our case "maqov.org"*

*In other word, Azure AD enforces the password policy of the on-premises AD DS.*

19. Sign back in with the new password
20. If you see the access panel screen, congrats, you've just successfully reset a password with a few clicks.

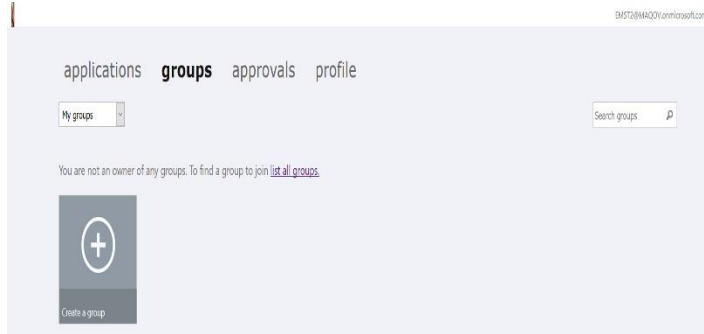


## Self-Service Group Management

1. in the Azure Management Portal, navigate to the **CONFIGURE** tab of your directory
2. Scroll down until you see the **group management** section.
3. Set **DELEGATED GROUP MANAGEMENT ENABLED** to **YES**
4. Set **USERS CAN CREATE SECURITY GROUPS** to **YES**
5. Set **USERS WHO CAN USE SELF-SERVICE FOR SECURITY GROUPS** to **ALL**
6. Set **USERS CAN CREATE O365 GROUPS** to **YES**
7. Set **USERS WHO CAN USE SELF-SERVICE FOR O365 GROUPS** to **ALL**.
8. Set **ENABLE DEDICATED GROUPS** to **YES**. Dedicated groups are groups whose membership is automatically calculated. The only one available for now is "**All Users**".
9. Set **ENABLE "ALL USERS" GROUP** to **YES**
10. Leave **DISPLAY NAME FOR "ALL USERS" GROUP** the same.
11. Click the **save** button at the bottom of the screen.

12. Now your users can request to join groups that others create, as well as create their own groups, by using the Access Panel.
13. Test User Group Management feature, and we can see also how the workflow works.
14. Login to <https://myapps.onmicrosoft.com>

15. Using Test Account, [EMST2@maqov.onmicrosoft.com](mailto:EMST2@maqov.onmicrosoft.com)



16. Select **groups**, and then create group.

17. On the display name: "**sales**".

18. On the group policy, Select the Option "this group requires Owner Approval".

In our case [emst2@maqov.onmicrosoft.com](mailto:emst2@maqov.onmicrosoft.com) is the group **owner**, and user [MobU1@maqov.com](mailto:MobU1@maqov.com) is the **requester**.

19. Click "**Create**".

Create Group

Display name  
Sales

Description (optional)

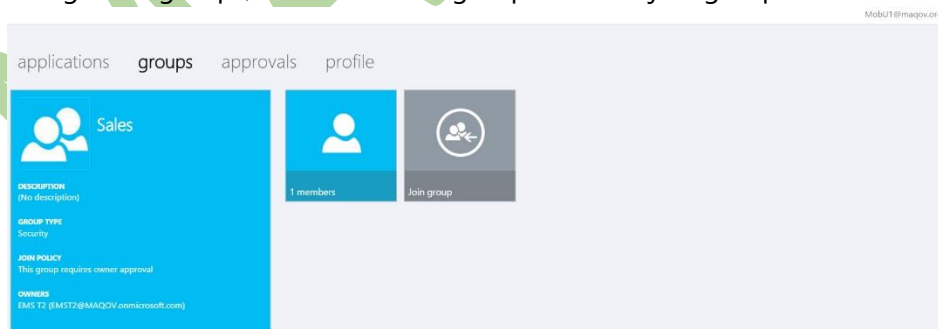
Group policy  
This group requires owner approval

Group type  
Security

Create

20. From the computer related to user [MOBU1@maqov.org](mailto:MOBU1@maqov.org) browse <https://myapps.microsoft.com>.

21. Navigate to groups, select the sales group and click join group.



22. On the OWNER Computer he will receive an email to approve or reject on the requester request.

MS msonlineserviceteam@microsoftonline.com  
To: EMS T2;

Reply all | v  
Wed 2/10/2016 1:32 PM

From: msonlineserviceteam@microsoftonline.com  
Sent: Wed 2/10/2016 1:32 PM  
To: EMS T2;

### Someone wants to join your group

Security group name: **Sales**  
Requestor: **MobU1@maqov.org**

Business justification: **kindly add me to the group.**  
[Act on this Request](#)

[Manage Groups](#) | [Privacy](#) | [Legal](#)

23. Click "Act on this is request", you will be redirected to the Approval tab.

EMST2@MAQOV.onmicrosoft.com

applications groups **approvals** profile

My Approvals v

RESOURCE	NAME	REQUESTER	REQUEST	BUSINESS JUSTIFICATION
<input checked="" type="checkbox"/> GROUP	Sales	MobU1@maqov.org	MobU1@maqov.org requested to join "Sales"	kindly add me to the group.

24. Click **approve**, click **Yes**.

## Approve selected requests

Do you want to approve selected requests?

Yes

No

25. On the requester email, he will get stating that your request is approved.

MS msonlineserviceteam@microsoftonline.com  
To: Mobility U1; v

Reply all | v  
Wed 2/10/2016 1:34 PM

### Your group membership request was approved

Security group name: **Sales**  
Approved by: **EMS T2**

Business justification: **kindly add me to the group.**

[View Group Memberships](#) | [Privacy](#) | [Legal](#)

## Azure Reports

You can use Azure Active Directory's access and usage reports to gain visibility into the integrity and security of your organization's directory. With this information, a directory admin can better determine where possible security risks may lie so that they can adequately plan to mitigate those risks.

In the Azure Management Portal, reports are categorized in the following ways:

- Anomaly reports – Contain sign in events that we found to be anomalous. Our goal is to make you aware of such activity and enable you to be able to make a determination about whether an event is suspicious.
- Integrated Application reports – Provides insights into how cloud applications are being used in your organization. Azure Active Directory offers integration with thousands of cloud applications.
- Error reports – Indicate errors that may occur when provisioning accounts to external applications.
- User-specific reports – Display device/sign in activity data for a specific user.
- Activity logs – Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity.

## Report editions

Report	Free	Basic	Premium
Anomalous activity reports			
Sign ins from unknown sources	✓	✓	✓
Sign ins after multiple failures	✓	✓	✓
Sign ins from multiple geographies	✓	✓	✓
Sign ins from IP addresses with suspicious activity			✓
Sign ins from possibly infected devices			✓
Irregular sign in activity			✓
Users with anomalous sign in activity			✓
Users with leaked credentials			✓
Activity logs			
Audit report	✓	✓	✓
Password reset activity			✓

Password reset registration activity			✓
Self service groups activity			✓
Integrated applications			
Application usage			✓
Account provisioning activity	✓	✓	✓
Password rollover status			✓
Account provisioning errors	✓	✓	✓
Rights managment			
RMS usage			RMS Only
Most active RMS users			RMS Only
RMS device usage			RMS Only
RMS enabled application usage			RMS Only

In this section we will discover sample report: -

1. Select your directory and navigate to the **REPORTS** tab in the Azure Management Portal.
2. We will see the activity reports for this part, there is a lot reports can be discovered.
3. On the reports page, find the **ACTIVITY LOGS** section and click on the **PASSWORD RESET ACTIVITY** report.
4. On the confirmation dialog, click the **checkbox** next to it is acceptable for admins in my organization to view this data and then click the check mark in the lower right to **confirm**.
5. You will find that two people reset their passwords, one with **failed** status and the other is **succeeded** state.



Microsoft Azure | Check out the new portal | CREDIT STATUS | admin@MAQOV.onmicrosoft.com

### password reset activity

Provides a detailed view of password resets that occur in your organization.

FROM: 1/10/2016 TO: 2/10/2016  
SOURCE: Azure AD  
Data has been processed up to 2/10/2016 4:05:08 PM.

USER	ROLE	DATE AND TIME	METHOD(S) USED	RESULT	DETAILS
Mobility U1	User	2/10/2016 12:01:57 PM	Mobile Phone - Voice	Succeeded	User successfully reset pass...
Mobility U2	User	2/10/2016 11:53:07 AM	N/A	Failed	User's account has insuffici...

## Join Azure AD

In this section we see the new trend for join azure ad we will perform our test on windows 10 machine. Let us login to the machine it may be your new tablet and you need to use the cloud service anywhere. So let us start: -

We need to make sure that you enabled **Device Registration** on your Azure AD

1. Login to **Azure Portal**, select your **AAD**, select **configure** tab, scroll down to **devices**, **Users may join devices to Azure AD**, set it to **ALL**.

multi-factor authentication

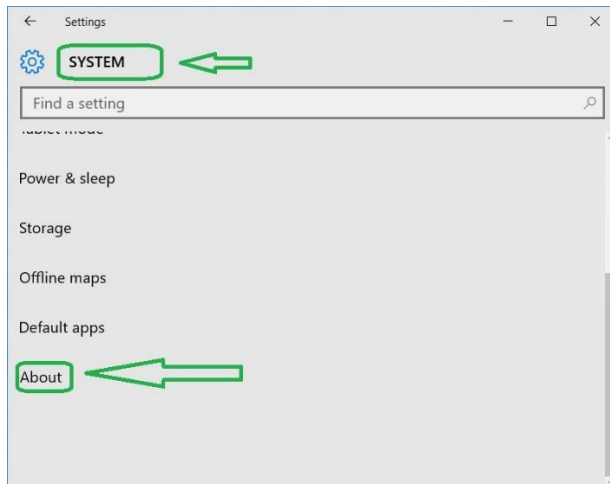
Manage service settings

devices

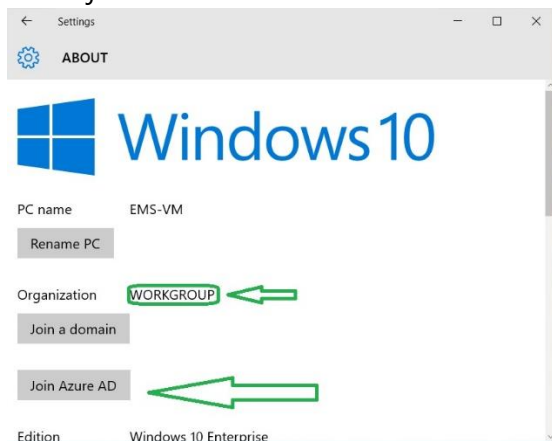
USERS MAY JOIN DEVICES TO AZURE AD: **ALL** | SELECTED | NONE

on the other hand let us swap to your pc or your tablet.

1. Login to the new machine with your local credentials, got to **settings**, **about**.

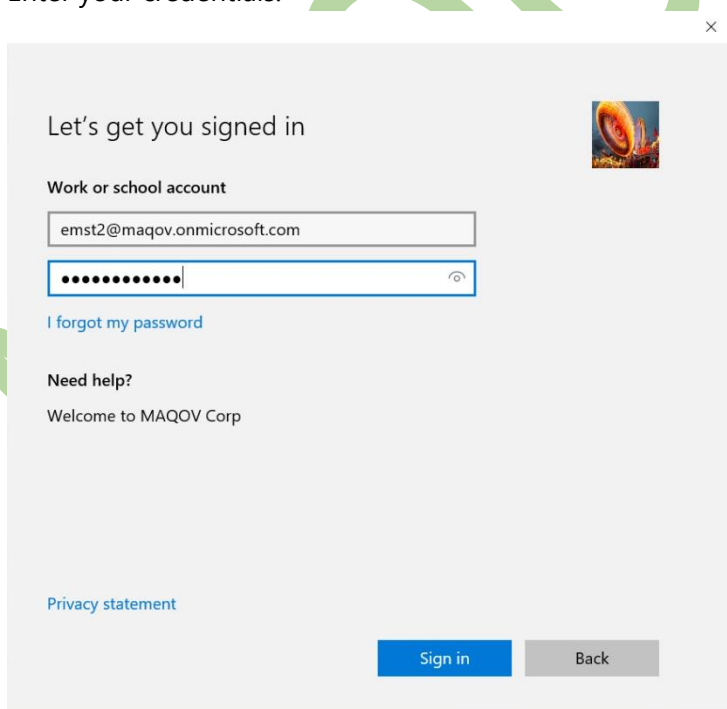


2. Select join azure AD.



3. On what happens next, click Next.

4. Enter your credentials.



5. On **Make sure this is your organization**, click **join**.

Make sure this is your organization

## Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC.  
Is this the right organization?

Connecting to: MAQOV.onmicrosoft.com

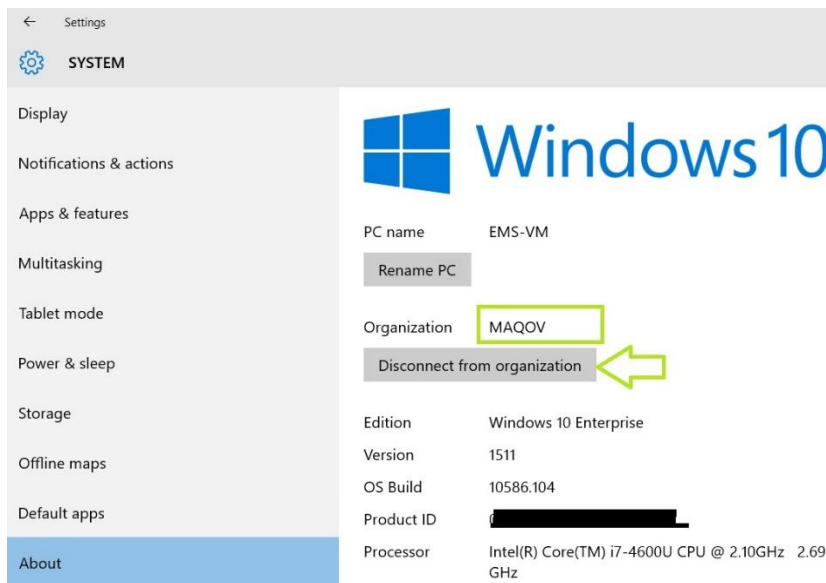
User name: EMST2@MAQOV.onmicrosoft.com

User type: Administrator

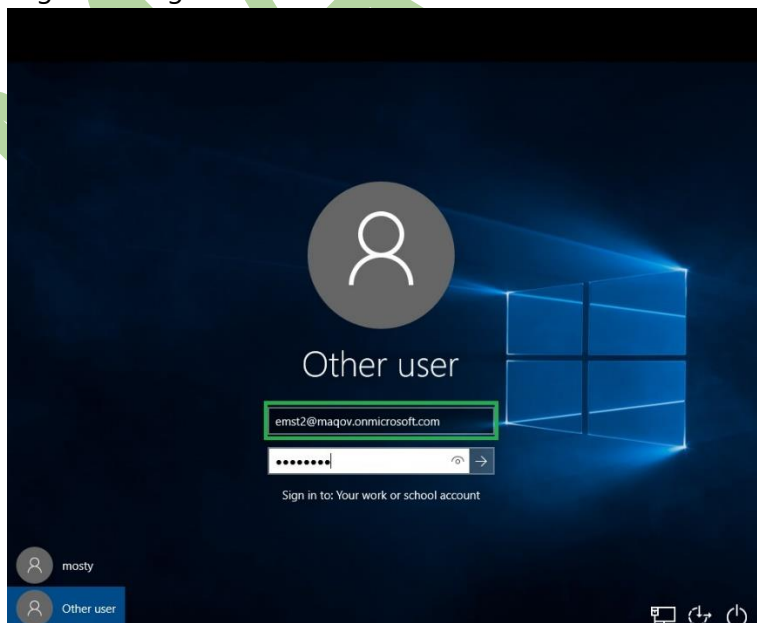
Cancel

Join

- Verify that your device joined Azure AD, go back to Settings, about and see Organization, in our case it is "MAQOV".

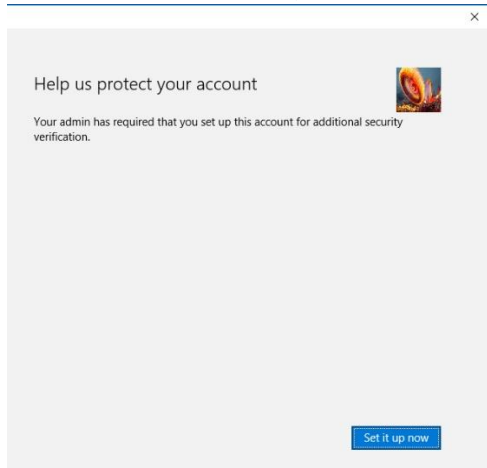


- Sign out or restart your pc/tablet.
- Login to using azure ad credentials.

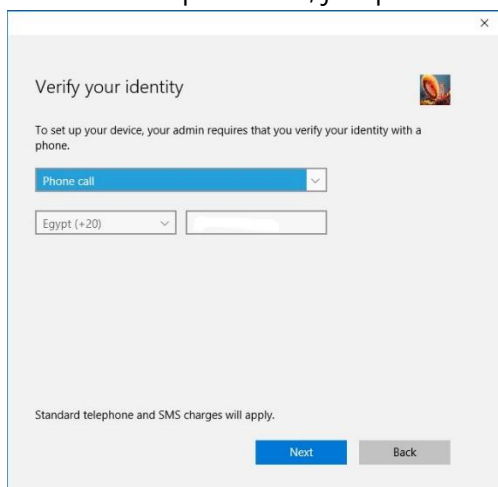


- You will prompt to setup a simple login pin, **create PIN**.

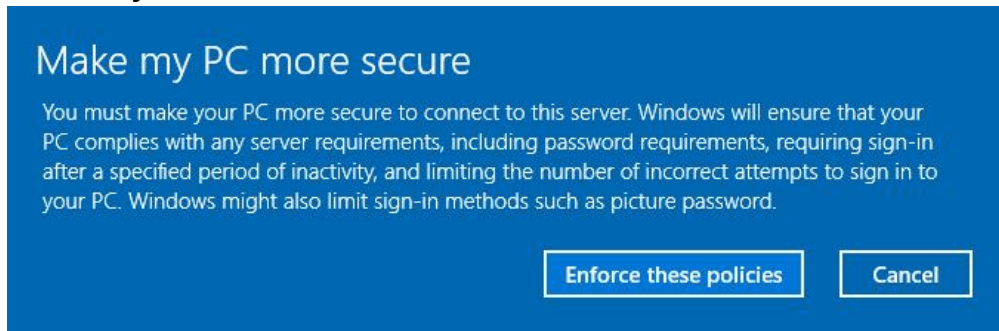
10. On **help us to protect your account**, click **Set it up Now**.



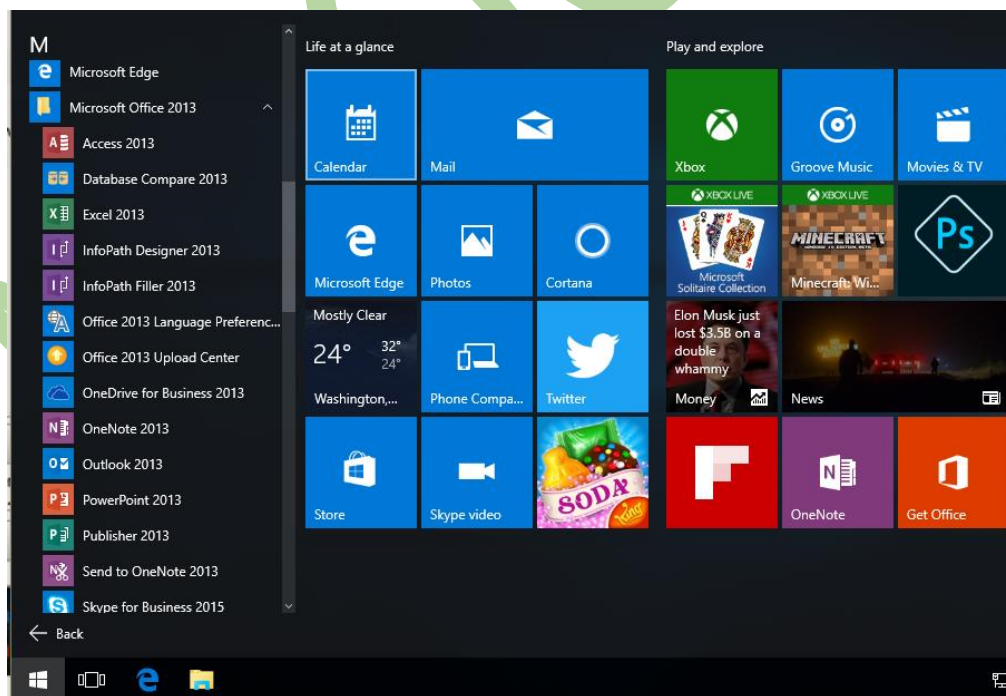
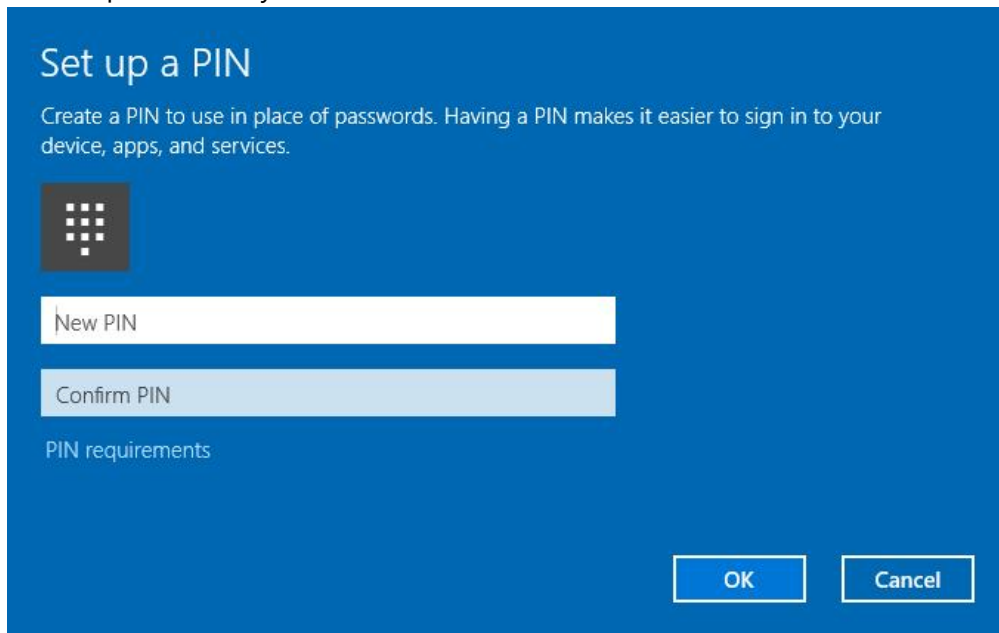
11. On Verify your Identity, select your preferred method of verification, for example phone call, you will receive a new phone call, just press bounce key '#'.  
MASSACHUSETTS



12. On **Make your PC More Secure** Press, **Enforce these Policies**.



13. On Setup PIN, enter your PIN, click **OK**.



Some notes, I found after signing in to the PC.

- The user that cloud joins the device to Azure AD will be added to the local Administrators group.
- Other users from you Azure AD can also use the device – they will not get admin rights though