**Prerequisites**

Each environment will have different requirements. Please view <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#prerequisites>

On the Azure PIM side, when rolling out for standard users global admin or authentication admin, conditional access admin, and office 365 admin is required. When rolling out to admins, global admin or privileged authentication admin, conditional access admin, and office 365 admin is required.

Azure AD P2

A break glass account with global administrator permissions

**Tips and tricks for planning a smooth implementation**

* Start with IT. This will give you time to gain information about the nuances of your environment. It is recommended to keep in IT for the first cycle (30 days in our example, explained below.)
* In smaller environments, it is recommended to work with individual users to train them on the product. If you don’t have the time to do that, it is recommended to either set up larger sessions or create detailed training.
* Encourage users to use the authenticator app! This is the easiest way to authenticate for most people but requires more initial set up.
* The authenticator app uses minimal data, typically less than 1 mb a month with frequent use (seen more for admins.)

**Enabling MFA**

**Step 1: Create a sign in risk policy. This will ensure that on unrecognized devices, users are always prompted for MFA.**

1. Open Azure AD <https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>
2. Click Groups
3. Click “new group”
4. Select Security group.
5. Name group. In this example, we call it “Sign-In Risk Policy”
6. Create group
7. When group has been created, click group name and notate the object ID. This will be used in later steps.
8. Create exclusion group – click groups
9. Click “new group”
10. Select Security group.
11. Name group. In this example, we call it “MFA Off Policy”
12. Put any service accounts, or break glass accounts in this group to start. Put all users in this group to start also.
13. Create group
14. When group has been created, click group name and notate the object ID. This will be used in later steps.
15. Go to “Identity Protection” <https://portal.azure.com/#blade/Microsoft_AAD_IAM/IdentityProtectionMenuBlade/Overview>
16. Click “Sign-in Risk Policy”
17. On the “users” option, select the “sign-in risk policy” group that was created above
18. For The sign in risk option, medium and above is recommended
19. On the assignments tab, choose “require multi-factor authentication”
20. On enforce policy, change the switch to on.

**Step 2: Turn on MFA**

1. Go to portal.office.com
2. Click “admin”
3. Click “settings”
4. Click “org settings”
5. On Services, click Modern Authentication
6. Make sure that it says “enable modern authentication.
7. Click Save
8. Go to conditional access https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/ConditionalAccessBlade/Policies
9. Click New policy
10. Select “users and groups”
11. On the “exclude” tab, choose “select users and groups”. Click the “users and groups” check box. Search for the sign-in risk policy group created earlier. Click Select
12. On the “exclude” tab, choose “select users and groups”. Click the “users and groups” check box. Search for the mfa off policy group created earlier. Click Select
13. Chose “include select cloud apps” chose the apps you would like to have mfa on. This will be unique to your organization and should include all applications that support modern authentication.
14. Do the same with the exclude tab. This should include all applications that only support legacy authentication.
15. On access controls, chose “require multi-factor authentication.”

**Step 3: Enable for users**

Before completing below steps, ensure you have the MSOnline module installed. This can be installed by running the below command in an elevated powershell window

Install-Module MSOnline

1. Save a csv on your c: drive with “upn” in the a1 slot. It will need to remain there.
2. Under upn, put the upns of the users you are turning on MFA for at that time.
3. Open the below script
4. $path =
5. $list = import-csv $path -ErrorAction Stop
6. connect-msolservice
7. ForEach ($users in $list)

{

$signinrisk = 'OBJECT ID HERE'

$nomfa = 'object id here'

$UserObjectID = (Get-MsolUser -UserPrincipalName $currentuser).objectid

remove-MsolGroupMember -groupObjectid $nomfa -GroupMemberObjectId $UserObjectID-GroupMemberType User -ErrorAction SilentlyContinue

add-MsolGroupMember -groupObjectid $signinrisk -GroupMemberObjectId $UserObjectID -GroupMemberType User -ErrorAction SilentlyContinue

}

1. Fill out the $path, $signinrisk, and $nomfa variables, with the path to your csv, the object id of the sign in risk policy group, and the object id of the no mfa group, respectively.

**If you need to turn off mfa for a user for any reason:**

1. Save a csv on your c: drive with “upn” in the a1 slot. It will need to remain there.
2. Under upn, put the upns of the users you are turning on MFA for at that time.
3. Open the below script

$path =

$list = import-csv $path -ErrorAction Stop

connect-msolservice

ForEach ($users in $list)

{

$signinrisk = 'OBJECT ID HERE'

$nomfa = 'object id here'

$UserObjectID = (Get-MsolUser -UserPrincipalName $currentuser).objectid

add-MsolGroupMember -groupObjectid $nomfa -GroupMemberObjectId $UserObjectID-GroupMemberType User -ErrorAction SilentlyContinue

remove-MsolGroupMember -groupObjectid $signinrisk -GroupMemberObjectId $UserObjectID -GroupMemberType User -ErrorAction SilentlyContinue

}

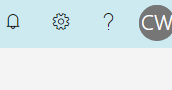
1. Fill out the $path, $signinrisk, and $nomfa variables, with the path to your csv, the object id of the sign in risk policy group, and the object id of the no mfa group, respectively.

Please note that this just switches back what group the user is a member of.

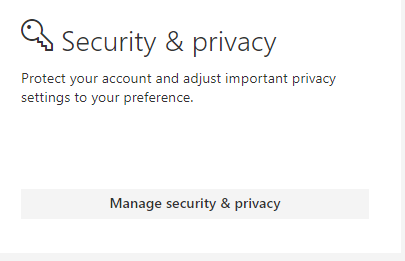
**MFA Troubleshooting guide (helpful for service desk)**

**I’m having issues setting up MFA**

1. Navigate to portal.office.com
2. Click on your initials/photo in the top right-hand corner of the screen.



1. Click Manage Security and Privacy



1. Click additional security verification



1. Click update your phone numbers used for account security



1. Choose verification method
   1. Notify me through app is the recommended option. This uses minimal data (less that .01 mb a month.) It also works far more smoothly.
      1. On phone. Go to the app store and download “authenticator app” by Microsoft. The logo looks like the below picture.



* + 1. Open app. Allow pictures and notifications.
    2. On computer – click set up authenticator



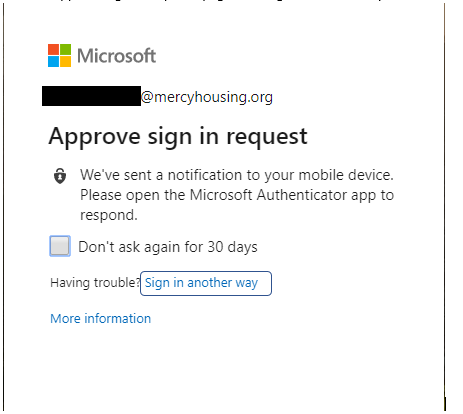
* + 1. A QR code will appear.
    2. On phone – say no to personal account, and Microsoft account. Say yes to work or school account.
    3. The camera will open. Scan the QR code that is on the computer screen.
    4. Click next on computer with 6 digits appears in app on phone.
    5. Click approve when notification appears on phone
    6. Click save on computer if the option is available. (this doesn’t always happen. If it doesn’t move to testing stage)
    7. Click approve on phone if another notification appears
  1. If a user would like to have their desk phone or their cell phone set up for calls.
     1. DO NOT click call my office phone. The number will not be able to be edited and must be formatted correctly in Active directory for this to work.
     2. Check the box by authentication phone. Ensure the country is set to United States.
     3. Type in the phone number.
     4. A test will start. Have the user answer the phone and hit pound when asked to.
     5. It is highly recommended for users to set up an alternate authentication phone for days that they forget their cell, or work from home.
  2. Text code
     1. Check the box by authentication phone. Ensure the country is set to United States.
     2. Type in the phone number.
     3. A code will be sent to the authentication phone to verify it. Have the user type in the code.

1. Test with user that desktop apps are working.

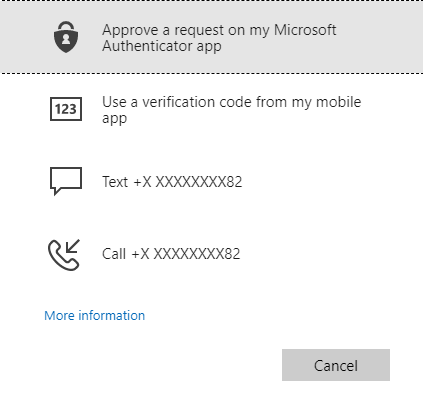
**I don’t have my primary Authentication with me**

**If the user has a new cell phone and the app isn’t working:**

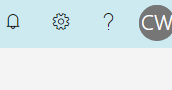
1. On the “approve sign in request” page, click sign in another way



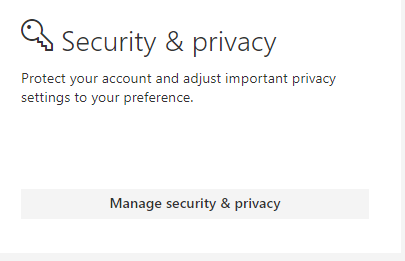
1. Have the user click text or call to receive a code or phone call to sign in.



1. Navigate to portal.office.com
2. Click on your initials/photo in the top right-hand corner of the screen.



1. Click Manage Security and Privacy



1. Click additional security verification



1. Click update your phone numbers used for account security



1. Below set up authenticator app, remove the old cell phone instance by clicking delete.



1. On phone. Go to the app store and download “authenticator app” by Microsoft. The logo looks like the below.



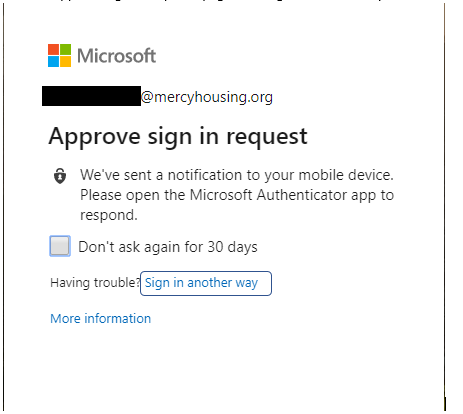
1. Open app. Allow pictures and notifications.
2. On computer – click set up authenticator



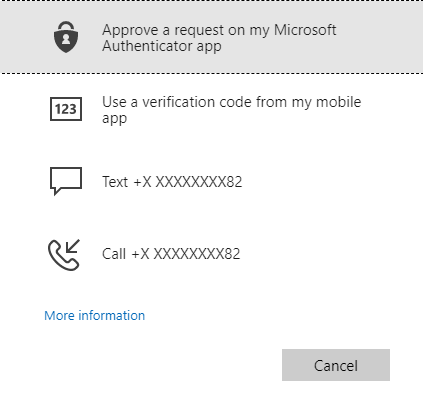
1. A QR code will appear.
2. On phone – say no to personal account, and Microsoft account. Say yes to work or school account.
3. The camera will open. Scan the QR code that is on the computer screen.
4. Click next on computer with 6 digits appears in app on phone.
5. Click approve when notification appears on phone
6. Click save on computer if the option is available. (this doesn’t always happen. If it doesn’t move to testing stage)
7. Click approve on phone if another notification appears

**If user forgot cell phone/is working at a different location than usual/at home:**

1.On the “approve sign in request” page, click sign in another way



2. See if one of the options is the user’s office phone. If it is, click call. User will receive call on office phone to authenticate.



3. If the office phone is unavailable, MFA will need to be turned off. Please contact someone authorized to do so.

4. Help user through setting up an alternate authentication method. Here however, you will not pull down the drop down as that will change the primary, you will simply check the box to the left of the decided method.

**Email isn’t working on my phone since turning on MFA**

1. Verify that the user is using the Outlook app and not the native mail app. Sometimes this is confusing do to the fact that people think they are the same thing. To ensure you are communicating this correctly, please ask what it says below the app icon when they go to open it.
2. If a user does not want to use the Outlook app, please nicely inform them that the Outlook app is the only supported Microsoft solution, and therefore the only solution that Mercy is able to support. If the user would still like assistance with setting up the native mail app you are welcome to try to assist, but please be clear that it doesn’t always function as expected.
   1. For both Android and iPhone users, please have them delete the account from the settings app.
   2. Click add account
   3. Add account as you normally would.
   4. If a user is not using the authenticator app, this will not work correctly. They will need to be very quick switching between the apps to grab a 6 digit code.

**Anything from Office Suite (Including OneDrive) isn’t functioning since turning on MFA/ “Right now this device cannot get to your organizations resources.”**

1. On property machines
   1. Log into device enrollment manager
   2. Sync policies
   3. Reboot
   4. Log into user account
   5. Try logging in again. If this doesn’t work, try step 2
2. TPM reset.
   1. Log out of user account
   2. Log into the computer as yourself
   3. Open Device manager
   4. Navigate to “Security Devices”



* 1. Expand “Security Devices”
  2. Right click “Trusted Platform Module 2.0” and click “uninstall device.”
  3. Reboot computer
  4. Log in as user
  5. Open Device Manager
  6. Navigate to “security devices”
  7. Right click “security devices”
  8. Select “scan for hardware changes”
  9. TPM 2.0 should appear as a device under security devices. If it does, open the effected Office application again.
  10. Sign back into Office if SSO doesn’t automatically force a logon after this change.
  11. Test the previously effected apps.