Azure Multi-Factor Authentication – Domain Users

[*DogFoodCon*](https://dogfoodcon.com/) *2019 is October 3rd – 4th.* [*Chris Lee*](https://dogfoodcon.com/speakers/#sz-speaker-17680ae9-5110-44dc-bd32-61b000e7cdd3) *and* [*James Hopkins*](https://dogfoodcon.com/speakers/#sz-speaker-4d8e80d5-149b-463b-856a-2995a0684818) *will be presenting* [*[Office 365] Establishing the Baseline Security for Microsoft 365*](https://dogfoodcon.com/sessions/#sz-session-121065)*. I interviewed Chris Lee regarding their presentation and have included a summary at the end of this article.*

Businesses with sensitive information prevent most attempts to hack into an account via a username and password by introducing [Multi-Factor Authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication). The [typical forms of authentication methods](https://www.youtube.com/watch?v=dw-dTc69N3s) are a phone call, a text message, a notification in an authenticator app, or a verification code from an authenticator or hardware. I've use all of these methods to date. If you're a gamer like me you'll recognize the [Steam Guard Mobile Authenticator](https://play.google.com/store/apps/details?id=com.valvesoftware.android.steam.community&hl=en_US) and [Blizzard Authenticator](https://play.google.com/store/apps/details?id=com.blizzard.bma&hl=en_US). Perhaps you've setup [Google Authenticator](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US), [Duo Mobile](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=en_US), or [Microsoft Authenticator](https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US). These authenticators are available on the Google Play store and Apple App Stores.

Curious on how [Azure Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) works I reached out to [Chris Lee](https://www.linkedin.com/in/christopher-lee-32489a10/), Principal Consultant with [Improving](http://improving.com/), and he kindly setup a demo environment for me to learn. The demo is setup with Azure AD Premium P2. If you are interested in following along, I recommend working with your Azure administrators to setup a demo environment for you. While you could also try the free trial, Chris recommended the demo environment.

# Requirements

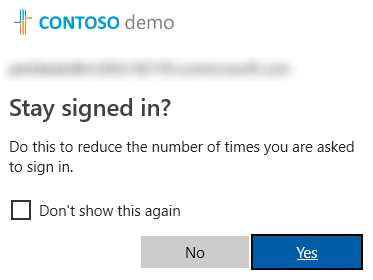
1. This demo environment was automatically provisioned via Microsoft partnership
   1. Alternatively, Chris recommended setting up [Enterprise Mobility + Security trial](https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security?rtc=1) if you don't have an existing environment
2. Create/Use an account with the domain of the demo environment
   1. Referenced as "domain user" throughout this article
3. Install [Microsoft Authenticator](https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US)
   1. I installed it on my Android phone via the Google Play store

# First-time Login as domain user

1. <https://account.activedirectory.windowsazure.com/>

# 

1. I entered my password and clicked "Sign in"

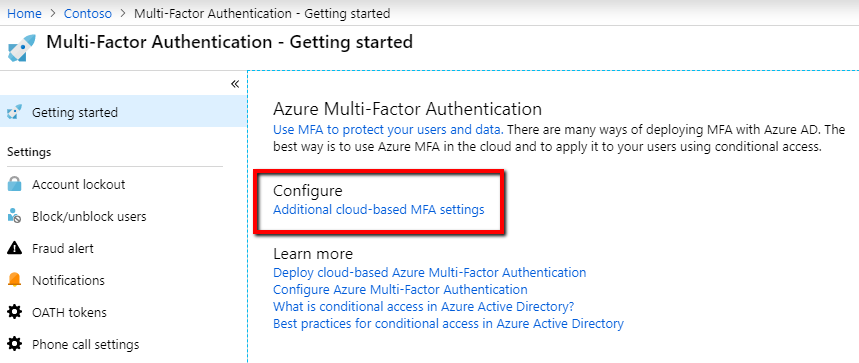


1. For these tests, I clicked "No"
2. And I'm signed in… hmm MFA isn't setup

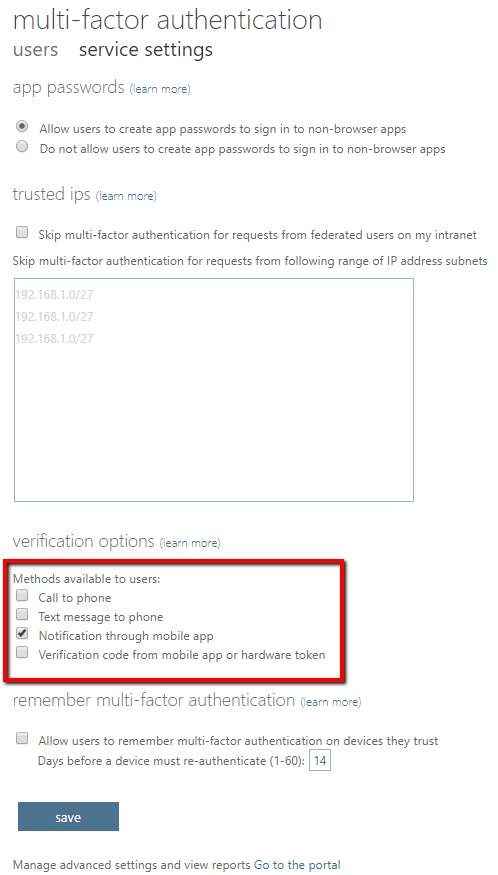
# Setup MFA

The MFA settings allow you to manage account lockout, block/unblock users, and many other settings. Let's change the MFA to only allow Notification through mobile app. These settings affect all accounts within the Active Directory and B2B.

1. <https://portal.azure.com>
2. Login as an administrator
3. Azure Active Directory > MFA



1. Under Configure > click "Additional cloud-based MFA setting"
   1. Check "Notification through mobile app" and uncheck the other "Methods available to users" > Save
      1. Race condition to be aware of
         1. Domain user enters their username and password and clicks "Sign in"
         2. Administrator saves any of these changes
         3. Domain user clicks the "Next" button
         4. Expected behavior: Domain user sees the options that were just saved
         5. Actual behavior: Domain user see the original options

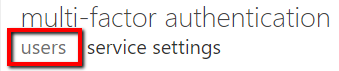


Ok, so MFA was already setup with "Text message to phone", "Notification through mobile app", and "Verification code from mobile app or hardware token" and now I've limited it to just "Notification through mobile app", but I still don't see any requirements for MFA. It's almost like MFA was not enabled for my account.

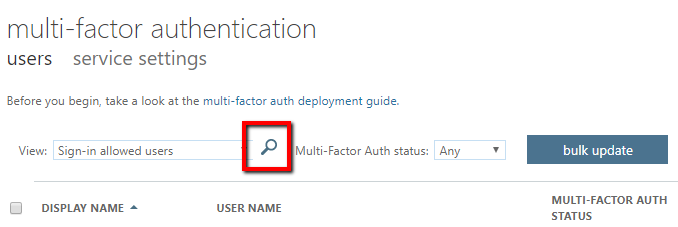
# Enable MFA for an account

So yeah, my account needed MFA enabled. It's not obvious, but in the MFA page there are two tabs "users" and "service settings". By default, when you follow the previous steps you open into the "service settings" tab.

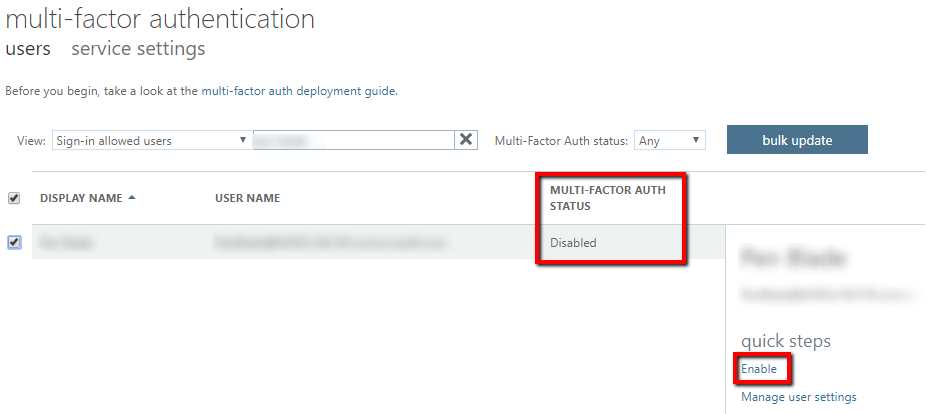
1. Click the "users" tab



1. Click the search icon (magnifying glass)



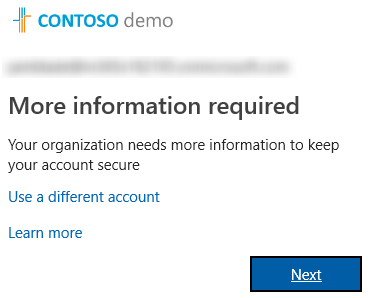
1. Search for your domain user
2. Yep, my account had MFA disabled, so under "quick steps" click the "Enable" link



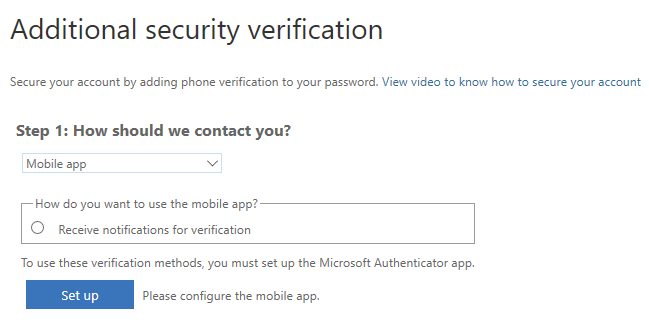
1. The "About enabling multi-factor auth" modal opens > "enable multi-factor auth"
   1. [Deployment guide](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted) link
   2. [MFA Setup](https://aka.ms/MFASetup) link
2. Click "close" and verify that the MFA status for the domain account is now "Enabled"
3. If you click "Manage user settings" you can perform the following tasks for the user
   1. Require selected users to provide contact methods again
   2. Delete all existing app passwords generated by the selected users
   3. Restore multi-factor authentication on all remembered devices

# Second-time Login as domain user

1. <https://account.activedirectory.windowsazure.com/>
2. Login as the domain user with the email address and password like we did earlier
3. Now we're prompted to enter more information > click "Next"
   1. "Use a different account" redirects back to the login page as expected
   2. "Learn more" opens a document to "[Troubleshoot common two-factor verification problems](https://docs.microsoft.com/en-us/azure/active-directory/user-help/multi-factor-authentication-end-user-troubleshoot)"



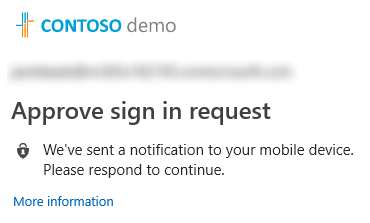
1. Since we limited the options to just the Mobile app we only see that option
   1. "[Manage your two-factor verification method settings](https://docs.microsoft.com/en-us/azure/active-directory/user-help/multi-factor-authentication-end-user-manage-settings)" includes screenshots and instructions of the other methods
   2. "[View video to know how to secure your account](https://www.youtube.com/watch?v=uWbkLuI4g30)"
2. Select "Receive notifications for verification" > Click "Set up" > Open the Microsoft Authenticator on your phone and scan in the bar code
   1. "[Manage your two-factor verification method settings](https://docs.microsoft.com/en-us/azure/active-directory/user-help/multi-factor-authentication-end-user-manage-settings)" includes screenshots and instructions



1. The next set of instructions ask if you want to store an app code, click "Done"
2. Now I'm signed in, but do I have to do this every time? Nope, that's a one-time deal unless you reset your desired MFA method

# Third times a charm

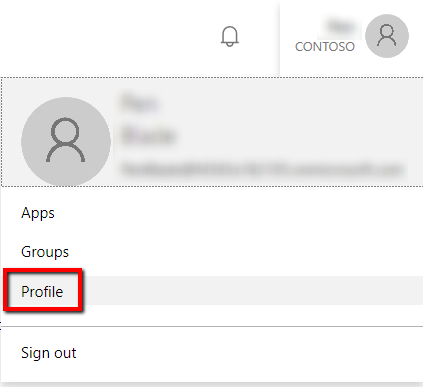
1. <https://account.activedirectory.windowsazure.com/>
2. Login as the domain user with the email address and password like we did earlier
3. Now we're prompted with a request to "Approve sign in request"
4. On my phone I click the notification and click Approve on the request
5. I'm signed in and ready to go



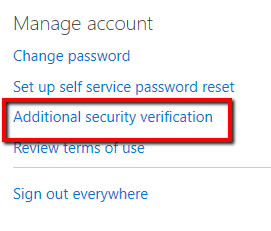
# Self-Service

While an administrator can reset your MFA configuration so you can choose a different authentication method, it would be great to have the option to do it yourself.

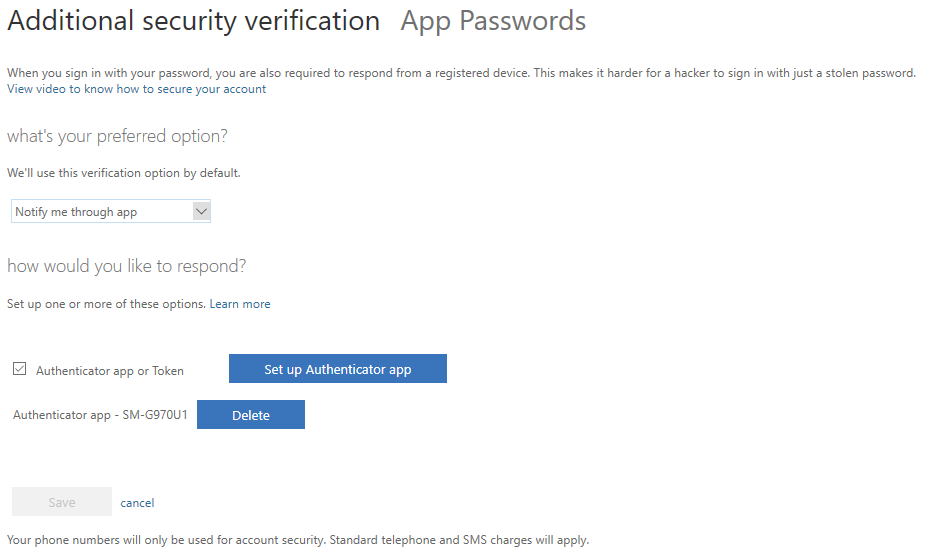
1. <https://account.activedirectory.windowsazure.com/>
2. Sign in, approve, you're in
3. Click your profile picture > Profile



1. Click "Additional security verification"



1. Change your MFA options
   1. You're limited to what the administrator configured in MFA, but it's nice to reset the options you have control over and may save a call to the support desk



# Resources

* [Azure Multi-Factor Authentication (MFA): From Configuration to Implementation - Azure Training](https://www.youtube.com/watch?v=dw-dTc69N3s)
* [What is conditional access? | Azure Active Directory](https://www.youtube.com/watch?v=ffMAw2IVO7A)
* [Ensure all your users have strong passwords with Azure Active Directory Password - THR3047](https://www.youtube.com/watch?v=iasTx-AAwdA)
  + This video included some scary metrics.
* [Configure Azure Multi-Factor Authentication settings](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings)

# DogFoodCon 2019

[DogFoodCon](https://dogfoodcon.com/) 2019 is October 3rd – 4th. [Chris Lee](https://dogfoodcon.com/speakers/#sz-speaker-17680ae9-5110-44dc-bd32-61b000e7cdd3) and [James Hopkins](https://dogfoodcon.com/speakers/#sz-speaker-4d8e80d5-149b-463b-856a-2995a0684818) will be presenting [[Office 365] Establishing the Baseline Security for Microsoft 365](https://dogfoodcon.com/sessions/#sz-session-121065). Chris was well spoken, very informed, and he has a passion for security and helping others. He eagerly setup a demo environment for me to learn and test MFA at my convenience and can't thank him enough.

Chris Lee has been working with Microsoft 365 (M365) since its inception. He's been working with the Microsoft cloud from the beginning when it was called Business Productivity Online Suite (BPOS) which evolved into Office 365 which is a small part of M365. While most of his time has been devoted to Enterprise Mobility + Security he has plenty of experience with the other components as well.

Azure Multi-Factor Authentication is great start to setting up your baseline security. I've shown a small sample of the user experience and a how you can enable/disable the authentication methods. This session focuses solely on Microsoft security, so the target audience is anyone who has started or plan on using Microsoft cloud productivity solutions.

By attending their session you'll learn the following:

1. Enterprise Mobility + Security E3 and Azure AD Premium P2
2. Azure Multi-Factor Authentication
3. Conditional Access
4. Device Trust
5. Password Practices

|  |  |
| --- | --- |
| [Chris Lee](https://dogfoodcon.com/speakers/#sz-speaker-17680ae9-5110-44dc-bd32-61b000e7cdd3) | Special thanks to [Improving](http://improving.com/)[Insight Digital Innovation's Twitter Page](https://twitter.com/improving) [Jeff McKenzie's LinkedIn Profile](https://www.linkedin.com/company/improving-enterprises/) |

# Conclusion

I have demonstrated the basic domain user experience when using Azure Multi-Factor Authentication and how to change which authentication methods are enabled. Next steps include learning [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview), Device Trust, and Password Practices that you can learn more at DogFoodCon 2019.

What are your thoughts about MFA? Are you an Azure administrator just learning MFA? Are you a domain user taking a peek behind the curtains to learn how your IT handles MFA? What has been your experience with MFA as an administrator or domain user?