Azure Multi-Factor Authentication

[*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.

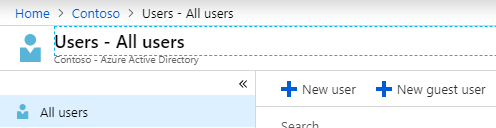
Curious on how [Azure Multi-Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks) works I reached out to [Chris Lee](https://www.linkedin.com/in/christopher-lee-32489a10/), Principal Consultant with [Improving](http://improving.com/), and 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. Demo environment setup by an Azure administrator in your corporation.
   1. [Office 365 dev/test environment](https://docs.microsoft.com/en-us/office365/enterprise/office-365-dev-test-environment)
   2. [Multi-factor authentication for your Office 365 dev/test environment](https://docs.microsoft.com/en-us/office365/enterprise/multi-factor-authentication-for-your-office-365-dev-test-environment)
   3. We won't actual work with Office 365 for this article, so there may be simpler demo setups that would work just as well
2. 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

# Create a guest user for testing MFA

1. Login to <https://portal.azure.com> as the administrator account provided for the demo
2. Azure Active Directory > (Manage) Users > (All users) + New guest user
   1. If you have an email address within the domain you can create a New user account
   2. The guest user account is a great way to grant access to limited company resources without managing their account or passwords within the corporate AD
   3. Learn more about the "[Properties of an Active Directory B2B collaboration user](https://docs.microsoft.com/en-us/azure/active-directory/b2b/user-properties)"



1. I entered my personal email address and saved
   1. I'll refer to this as the guest email address going forward to help distinguish it between the administrator account used to change settings.

# First-time Login as guest (with OAuth in url)

1. I received an email with the invitation to the CONTOSO demo with a link
2. I opened the CONTOSO link in a different browser so I could have the administrator account opened at the same time
3. I logged in with the guest email address and password
   1. Again the CONTOSO Azure portal does not maintain the password
4. There was no requirement for MFA, because the link included an OAuth 2.0 entry/token for OpenIDConnect
   1. Read more about how to "[Authorize access to web applications using OpenID Connect and Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-openid-connect-code)"
   2. This is done intentionally since you were already authenticated by the administrator sending the invite
5. Sign out

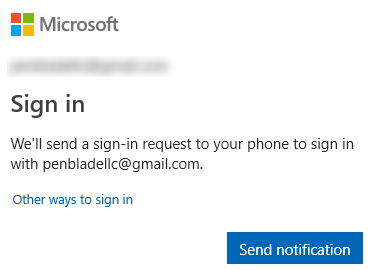
# MFA not working? Nope, user error

Warning: I made the mistake of bookmarking the link from the email to login. Since it had the OAuth 2.0 entry/token in the url as mentioned earlier I kept bypassing the MFA. Instead you should bookmark the links provided by the administrator or for this demo I extracted the base redirect url.

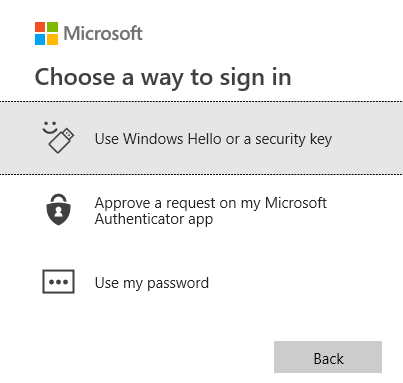
# Second-time Login as guest (without OAuth in url)

These are the options available on Edge.

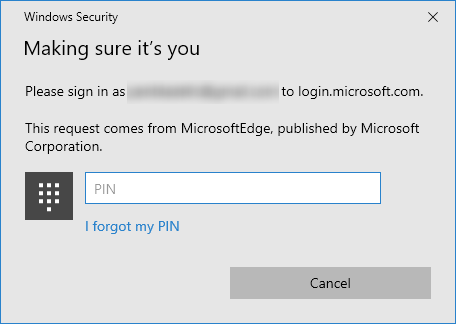
1. <https://account.activedirectory.windowsazure.com/>



1. Send notification worked the same as the Microsoft Authenticator step below
2. Click "Other ways to sign in"



1. Options:
   1. Interestingly, if you have Windows 10 and are logged in with the guest email address and setup with quick login via a pin, then you can enter your login pin to login



* 1. Approve a request on my Microsoft Authenticator app
     1. I got a Microsoft Authenticator notification on my phone, I clicked approve, and on my desktop I was now logged into the site
     2. When my phone was locked I would also be required to enter my lock screen password/pin/pattern/swipe
  2. Use my password
     1. I was able to login to the site with my password without any other authentication

# Browser Differences

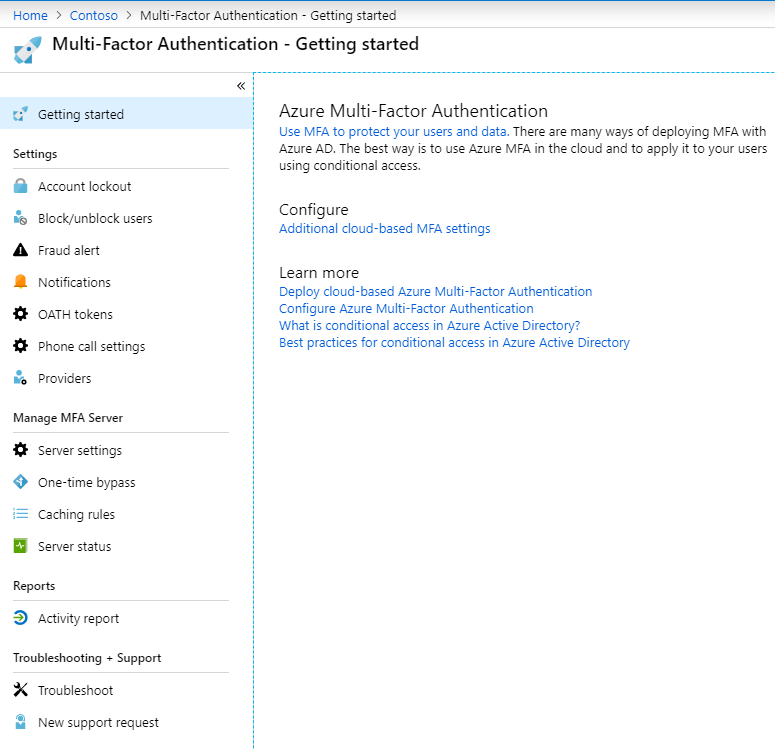
I was surprised the Chrome did not support all of the features listed

1. Edge/Firefox
   1. Send Notification (Microsoft Authenticator)
   2. Windows Hello (pin) or Security Key
   3. Microsoft Authenticator
   4. Use my password
2. Internet Explorer 11 (IE11)/Chrome
   1. Send Notification (Microsoft Authenticator)
   2. Use my password

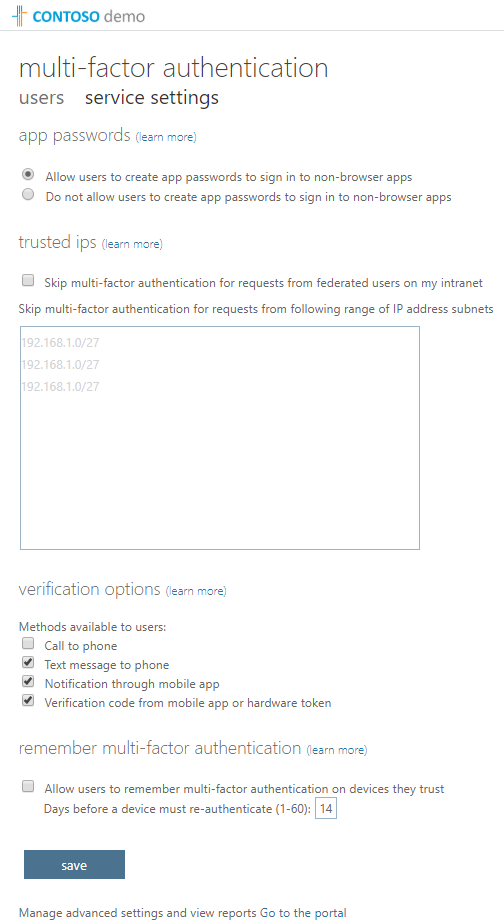
# Setup MFA

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. Azure Active Directory > MFA



1. Under Configure > click "Additional cloud-based MFA setting"
2. Check "Notification through mobile app" and uncheck the other "Methods available to users" >
3. Save



1. When you repeat the login steps you'll only see the "Send Notification" and Microsoft Authenticator options

# Next Steps

My experience with MFA is that I have to enter my username and password followed by a second authentication method such as clicking approve in Microsoft Authenticator from my phone. This is where [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview) comes in.

# 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 guest user experience when using Azure Multi-Factor Authentication and how to change which authentication methods are enabled. Next steps include learning Conditional Access, Device Trust, and Password Practices that you can learn more at DogFoodCon 2019.

What are your thoughts about MFA? We're you surprised by the browser support as I was? Did you know you could use your Windows 10 pin as an authentication method?