Azure Multi Factor Authentication – Guest 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)*.*

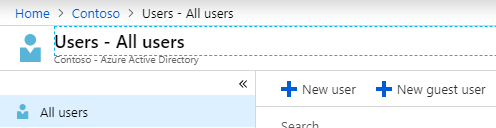
As I was writing the [Azure Multi Factor Authentication article](https://github.com/penblade/Tips/blob/master/Tips.AzureMultiFactorAuthentication/AzureMultiFactorAuthentication.docx) I initially started with a guest account. A guest account is any account not within your domain (microsoft.com and google.com are two separate domains). I was not getting the expected results at all no matter which MFA settings I made. Eventually I learned during my research that the guest accounts weren't maintained using the simple GUI interface by default. This article shares my confusing experience with guest accounts with a gentle nudge to learn more about Conditional Access to avoid this discrepancy in user experience.

# Requirements

1. Reference the requirements in [Azure Multi Factor Authentication article](https://github.com/penblade/Tips/blob/master/Tips.AzureMultiFactorAuthentication/AzureMultiFactorAuthentication.docx)
2. Create/Use an email account such as your personal account from a third-party like gmail.com
   1. Referenced as "guest" throughout this article

# 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. 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
   2. 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

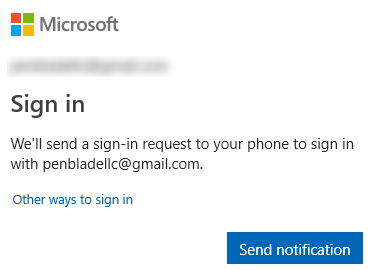
# MFA not working? Nope, user error

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.

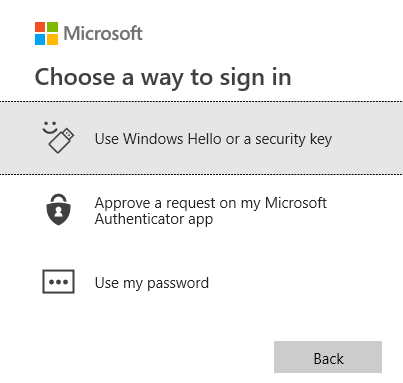
# Second-time Login as guest (without OAuth in url)

These are the options available on Edge.

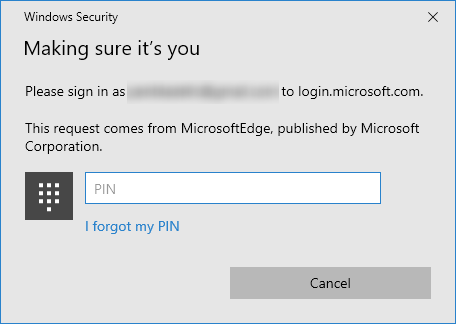
1. <https://account.activedirectory.windowsazure.com/>



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

# MFA doesn't apply to guest accounts by default

As I made adjustments to the MFA settings as noted in the previous article I found that none of the changes affected the guest account. While the guest account could be authenticated in multiple ways, I was never required to authenticate twice such as login with username password AND Microsoft Authenticator like I was with the domain account with MFA enabled.

Chris Lee mentioned that you could require MFA for a guest if you used Conditional Access that scoped to that guest. Attend [Chris Lee](https://dogfoodcon.com/speakers/#sz-speaker-17680ae9-5110-44dc-bd32-61b000e7cdd3)'s [DogFoodCon](https://dogfoodcon.com/) 2019 session [[Office 365] Establishing the Baseline Security for Microsoft 365](https://dogfoodcon.com/sessions/#sz-session-121065) to learn more about [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings).

# Conclusion

I have demonstrated the basic guest user experience and how the Azure Multi-Factor Authentication configuration does not affect the guest accounts. Next steps include learning [Conditional Access](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings), Device Trust, and Password Practices that you can learn more at DogFoodCon 2019.

Did you know that guest accounts by default aren't subjected to MFA settings like domain accounts? 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?