**THE VALUE OF MULTI-FACTOR AUTHENTICATION – GET YOUR STORY RIGHT!**

I’ve tried something different last night. To write the story of Multi-factor authentication and bring the relation in the eco-system of Microsoft. Everything is connected. I would love a comment, share or a reply to see if this content is valuable for you! Thanks, Jasper

**Creating the modern workplace! – Vision**

* **Increase mobility**: People are working from home. From clients and during travel. In regard to collaboration, 98% of information workers collaborate or communicate with someone else at work on a weekly basis.
* **Improve security and compliance.** Most of the time there is no control of data compliance in the current on-premise environment. Security systems are complex and static without growing or proven improvements. Start with a Zero Trust model. Start with protection of your people.
* Find more **topics**I’ve written in my [previous article.](https://jasperbernaers.com/the-value-of-microsoft-365-e3-or-e5/)

**What is Multi-Factor Authentication – To know**

* Something you **know**, typically a password or a pincode.
* Something you **have**, such as a trusted device that is not easily duplicated, like a phone or hardware key/token.
* Something you **are**– biometrics like a fingerprint or face scan.

**Cybersecurity Reference Architecture – The Cybersecurity vision to integrate deeply in Microsoft tech**

Whoooaww, that’s a extreme reflex for doing our MFA implementation!! **IS IT? Dear customer, colleagues**. is it? **I don’t think so**. We need to see and understand that the small parts (Micro) are connected to the big parts. (Macro) Identity & Access management in crucial. Identity is the first step, is the bases, the baseline. **We need to invest in the whole Cybersecurity frame and we need to start with the basics.**

Next to the macro view of this Cybersecurity Reference architecture we need to dare to question the identity providers we have integrated in our current environment.

Graphical user interface, application

Description automatically generated

**Foundation Infrastructure – The not so interesting part**

The only way is up. Starting with your foundation. **1. Networking**  
**2.** **Identity**is the first investment **before**you ‘**grow**‘ to **workloads and scenario’s**.

A picture containing chart

Description automatically generated

**Identity is a fundamental part of the workplace – The attack surface**

As you can see in this figure all security mechanisms are built on the fundamentals of Identity Management. What can you protect IF you’re not able to enable MFA? It has his reasons. There are numbers out there to make you aware of this. We will come to that, later in this article.

Graphical user interface, application

Description automatically generated

**Cloud Architecture Identity – MFA is part of something**

Understanding identity management in the eco-system of Microsoft’s Identity management **system**is crucial to find the place where Multi-factor authentication (MFA) belongs. User Accounts – Identity management – Azure Active Directory – Azure/Microsoft365

Diagram

Description automatically generated

**Self-Service Password Reset – To help the people**

Give people in your organization the ability to get some good because they ‘need’ to do [MFA](https://jasperbernaers.com/the-multi-factor-authentication-struggle-and-the-solution/). This will ask people of your organization to change their password when there is a threshold higher or above the risk level. It will decrease the IT workload and more import **it will make your customers happy.** By the way, it’s very easy to configure go to [Azure AD](https://portal.azure.com/#blade/Microsoft_AAD_IAM/) – [Password Reset](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/PasswordReset) – [Authentication Methods.](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/PasswordReset)

Graphical user interface, text, application, email

Description automatically generated

**Force a password change when assuming breach – To prevent breaches AND decrease IT tickets**

Go to [Identity Protection](https://portal.azure.com/#blade/Microsoft_AAD_IAM/IdentityProtectionMenuBlade/UserPolicy) in [Microsoft Azure](https://portal.azure.com/). Select your assignment. All users. Conditions. Select your requirement. And select Require Passwords Change. This will ask people of this organization to change their password when the threshold is at or above the risk level.

Did you know that: IT administrators can enable sign-in risk as a condition in multiple [conditional access](https://jasperbernaers.com/tag/conditional-access/)policies outside [identity protection](https://jasperbernaers.com/tag/identityprotection/).  
In case you don’t have MFA enrolled before this ‘risk policy’ – your account will be locked.

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

**Azure AD Conditional Access – To make it easier**

[Conditional Access](https://jasperbernaers.com/tag/conditional-access/) is a solution used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. [Conditional Access](https://jasperbernaers.com/tag/conditional-access/) is at the heart of the new identity driven control plane.

* **Keep user**accounts **safe**by requiring strong authentication based on location and risks.
* **Keep data safe** by only allowing **managed devices**.
* Meet compliance requirements.
* Create **simple policies**for **everyone**– not for groups, departments – **make it simple!**
* **Your**modular **dreams**…

Diagram

Description automatically generated

Diagram

Description automatically generated

**What if MFA fails like it did before? – Probably won’t**

* [**MFA**](https://jasperbernaers.com/tag/multi-factor-authentication/)**failed 2 times?** Less than 4 hours? Ever? Compared to **your**on-premise environment?
* We like to kill [MFA](https://jasperbernaers.com/tag/multi-factor-authentication/)implementations because we don’t like it **but we still want more security**. DO IT. If security is a priority, you can fix this technically.**What if that’s the real problem?**
* **What if**you did not have MFA and are breached? OR leave MFA enabled and still be in control of your data.
* **What if**[MFA](https://jasperbernaers.com/tag/multi-factor-authentication/) failed and you had your devices and identities connected to your modern workplace because it was not a side-project and part of a strategic decision and were able to work when the service fails for some hours?
* **The reflex should to be prevent:**Like a [break glass account](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access) in case of a problematic situation.
* Next to that **write up a document** that **describes**the **action requires**in case of **MFA authentication problems**. **High risk user**will get a unique passwords, **low risk users**may authenticate without password change. Risky users with medium risk and higher will get a password change.

**The standard pitch doesn’t work – So stop telling this**

* [99,9%](https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/) compromised accounts did not have MFA.
* Next to this fact the [50 accounts on 10.000 people](https://www.forbes.com/sites/zakdoffman/2020/04/30/us-issues-new-microsoft-security-alert-for-millions-of-office-365-users/#61cc86a64169) that will be breached according the numbers of Microsoft is more and more understandable.
* [Your Pa$$word doesn’t matter](https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984)
* You can do internal [phishing attacks](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide) and see that people are entering their passwords. It’s a fact. What’s the point of knowing again if it’s already known? *Any fool can know, the point is to understand.* Albert E.

These stories are well-known but will not trigger changes. Do’s & don’ts are judging. Don’t work on the ‘facts’. Work on the **value** and **support**and **simplicity**of **modern technology**. **GIVE** to the people. Don’t take things away.



**MFA is included in all licenses – It has been changed since a long time**

Basic MFA is included in all Office 365 and Microsoft 365 licenses. It does not mean conditional access or other related features are included. [Reference](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-of-versions).

**Passwordless authentication – To give to the people**

Enablement of Passwordless authentication will activate authentication without a password – isn’t this great? Enablement of password Authentication in Azure AD is easy. Go to Azure [Active Directory](https://portal.azure.com/) – [Security](https://portal.azure.com/#blade/Microsoft_AAD_IAM/SecurityMenuBlade/GettingStarted) – [Authentication methods | Authentication method policy (Preview)](https://portal.azure.com/#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods) – Enable.

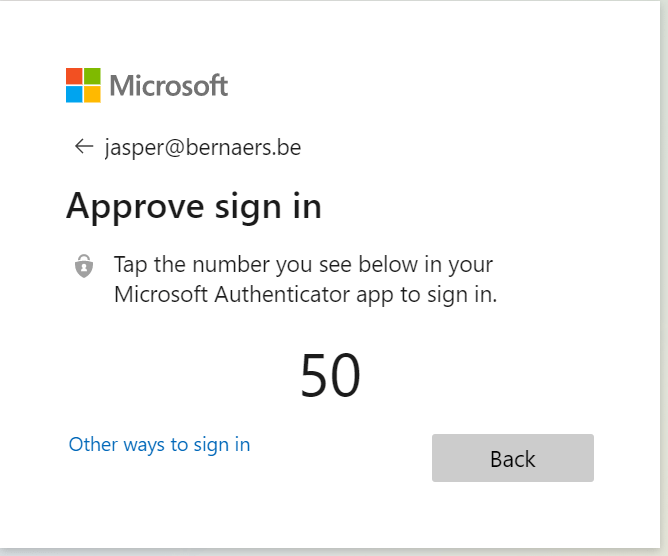
Passwordless authentication is a feature that let us rethink our current MFA solution IF it’s not running in the cloud or third-party. As you can see the integration is deeper and deeper here.

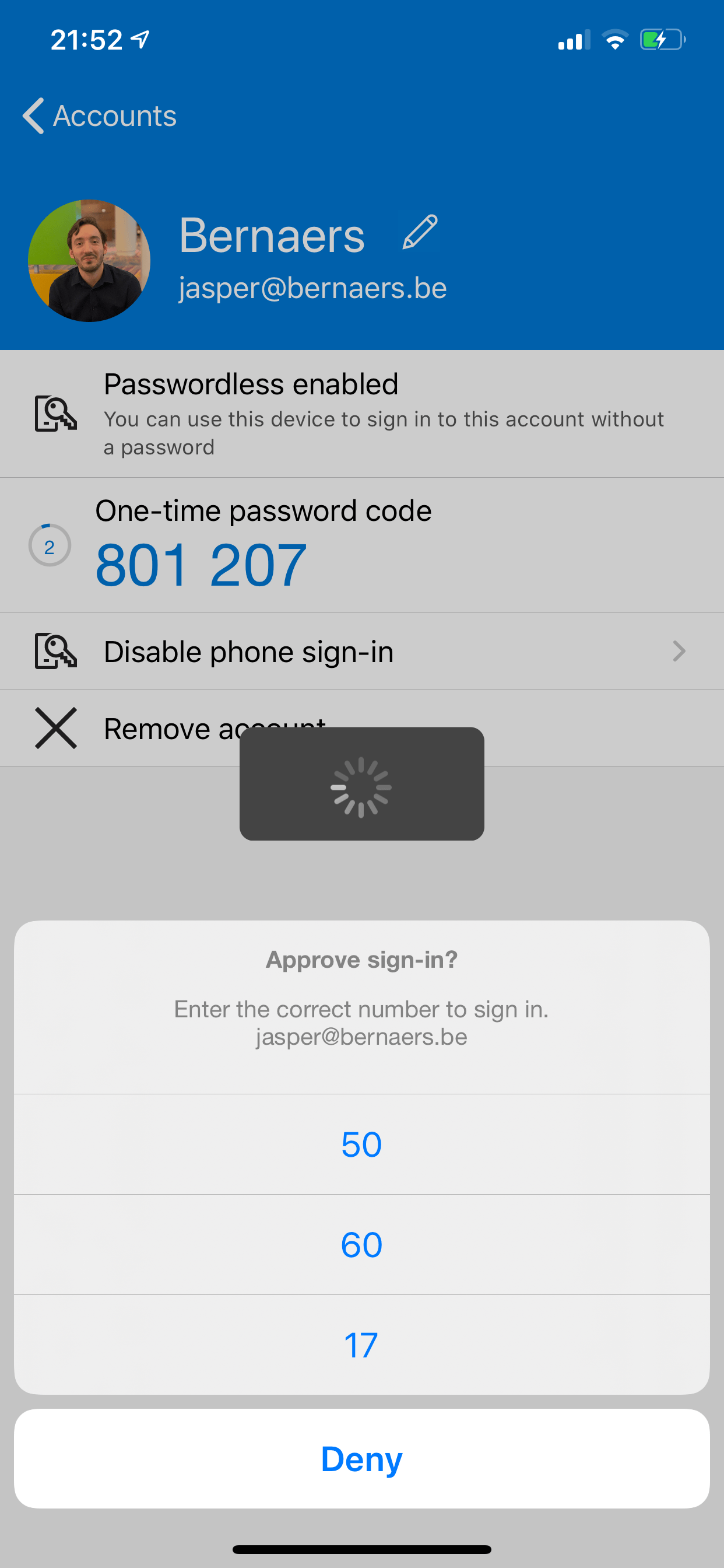
Graphical user interface, text, application

Description automatically generated

**The MFA Experience – It isn’t bad at all**

The mobile experience shows 3 sign-in code’s to validate the sign-in. Your code needs to be validated. and you don’t need to enter the password.





**Combined MFA and password reset registration – To make the onboarding smooth**

Microsoft has announced that the combined security information registration is now generally available (GA). This new experience makes it easy for users to register for [Multi-Factor Authentication (MFA)](https://jasperbernaers.com/tag/multi-factor-authentication/) and [Self-Service Password Reset (SSPR)](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment) in a simple step-by-step process.

**Adoption and change management – To make everyone happy except the sponsor**

Make standards that are understandable for everyone, not only of the IT organization. Communicate MFA announcement and changes before the change – not after. Keep track of the change record. Explain very well how you’re using ‘standards’ in your organization. Put the guidelines on a place where all procedures are located. Communicate over multiple platforms. Make it about the end-user. Help end-users. It’s all about experience! And you are in control!

Published on the [#WorldPasswordDay](https://twitter.com/search?q=%23WorldPasswordDay&src=typed_query) – Stay Save!