CENTRE FOR CYBERSECURITY BELGIUM

# MULTI-FACTOR AUTHENTICATION (MFA): A GUIDE FOR ORGANISATIONS

## UNDERSTANDING AND IMPLEMENTING MFA FOR BETTER IT SECURITY

Centre for Cybersecurity Belgium
*Under the authority of the Prime Minister*

# Table of Contents

# 1. Introduction

**When it comes to securing your accounts, you have probably heard of Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). Two-Factor Authentication is a security approach requiring to present two factors for authentication for accessing an account. Multi-Factor authentication (MFA) requires to present two or more pieces of evidences, or factors, for authentication. So while 2FA involves two steps of verification, MFA takes it a step further by incorporating multiple authentication methods.**

**This simple yet robust solution adds an extra layer of protection by requiring you to provide two or more forms of identification. Even if someone knows your password, enabling MFA prevents unauthorised access to your accounts. It is highly recommended that you enable MFA wherever possible due to its simplicity and enhanced safety. The importance of 2FA and MFA for organisations, public or private, cannot be overstated. Cyber threats, including ransomware attacks, data breaches, and intrusions, pose significant risks. Statistics show that a significant percentage of ransomware attacks could be prevented by implementing MFA. A lot of these attacks could be prevented with robust authentication measures. By adding multiple layers of security, MFA makes it much harder for cybercriminals to gain access to sensitive data, thus reducing the likelihood of data breaches and other cyber threats.**

**In this guide, we will walk you through the basics of MFA and provide practical advice on how to implement it within your organisation. We will also discuss real-world examples and offer tips to help you avoid common pitfalls when deploying MFA solutions. By the end of this guide, you will have a better understanding of MFA and how to effectively utilise it to protect your organisation's sensitive information. In our Cyberfundamentals Framework, we also clearly highlight the critical role of strong authentication measures in safeguarding your organization's digital assets.**

# 2. What is Multi-Factor Authentication and why is it important?

Simply put, MFA involves using an additional code or confirmation alongside your password to securely access an account or system. With MFA, you need to provide a password and a token or biometric data to access information, greatly reducing the risk of unauthorised access. By requiring multiple forms of authentication, MFA greatly enhance the security of your organisation and **reduce the risk of unauthorised access to sensitive information or systems**.

To securely access your account, it is necessary to provide proof of your identity. This can be achieved through the utilisation of three methods or factors:

- something only you know (your password or PIN number);
- something only you have access to (your phone or token); or
- something that is a part of you (your fingerprint, face, iris, etc.).

Implementing MFA on an organisational level means that employees and any other user who requires access to your resources are required to provide more than one form of authentication to access corporate systems, networks, and sensitive information and applications. MFA can be implemented across a range of applications and systems, such as email, VPNs, cloud-based services, and internal networks.

MFA is becoming increasingly important in today's business environment, where cyber threats are becoming more sophisticated and frequent. For example, a phishing attack that tricks a user into divulging their password would be less effective against **an MFA-enabled system**, as the attacker would also need to provide the token or biometric data to gain access. Similarly, a brute-force attack that tries multiple password combinations would be much less effective against an MFA-enabled system, as the attacker would also need to provide the additional form of authentication.

In addition to **improving security**, implementing MFA can also help **organisations comply with legal and regulatory requirements** (e.g., GDPR, NIS2) for strong authentication measures. MFA can also help ensure business continuity by preventing or mitigating the impact of security breaches, allowing organisations to continue operating with minimal disruption.

## 3. Multi-Factor Authentication: a critical security measure for organisations

While MFA has traditionally been associated with large enterprises, it is now becoming **more accessible and affordable** for organisations of all sizes. Additionally, some MFA solutions are available as a **subscription service**, which can help organisations manage costs more effectively by paying only for what they need. In terms of complexity, MFA solutions are becoming increasingly **user-friendly** and **easier to implement**, with many providers offering simple plug-and-play options that require minimal configuration.

Some MFA solutions even integrate with existing access management systems, making it easier for organisations to adopt **without major changes to their existing infrastructure**, such as Active Directory or LDAP. Both LDAP and Active Directory are used for authentication and authorisation, allowing organisations to control user access to systems, applications, and data. By integrating MFA solutions with LDAP or Active Directory, organisations can enhance their security posture and protect against cyber threats, without the need for a complete overhaul of their existing infrastructure. By prioritising MFA as **a critical security measure**, organisations can ensure that they are taking proactive steps to protect their business and their customers' sensitive information. Overall, organisations can implement MFA to enhance their security posture and reduce the risk of unauthorised access to sensitive information or systems.

With MFA as **a critical security measure**, organisations can ensure that they are taking proactive steps to protect their business and their customers' sensitive information. Overall, organisations can implement MFA to enhance their security posture and reduce the risk of unauthorised access to sensitive information or systems.

Why just using a password is no longer enough:

- Passwords can be easily guessed, especially if they are simple and easy to remember. This is why many attackers use brute-force and password spraying attacks, where they try to guess a password by testing many combinations until they get it right.
- Passwords can be reused across multiple accounts, which means that if one password is compromised, attackers can use it to gain access to other accounts as well. This is known as password reuse, and it is a common problem that makes password-only authentication less secure.

Passwords can be **stolen through phishing attacks or malware**. Attackers can send fake emails or messages that appear to be from a legitimate source, tricking users into giving away their login credentials. Similarly, malware can be used to steal passwords directly from a user's device.

Due to these weaknesses, **a password-only approach can be exploited in various ways**. For instance, attackers can use stolen or guessed passwords to gain access to an organisation's sensitive data or systems. They can also use password cracking tools to break weak passwords, and then use the same passwords to access other accounts. In summary, the weaknesses of passwords make them vulnerable to exploitation, which is why implementing MFA) is crucial to enhance security.

## 4. How to implement Multi-Factor Authentication at work?

In practice, implementing MFA for organisations involves 4 steps to ensure that the rollout is effective and secure, identifying, choosing, planning and implementing .

The first step is to **identify which systems and applications require MFA**, as well as which types of authentication are most appropriate. Access to confidential data should be secured via MFA.

The second step is to **choose an MFA solution that is appropriate for your organisation's needs and budget**. It is important for organisations to consider factors such as ease of use, scalability and cost when choosing an MFA solution. You should also choose a solution that is compatible with the existing systems and applications that your organisation uses, and to consider the security risks and threats that your organisation faces.

Here are some specific examples that organisations can consider when choosing an MFA solution:

- **SMS-based MFA**: This is a option that sends a one-time code to the user's phone via text message. The user then enters the code to complete the authentication process.
- **Software-based MFA**: This is an option that typically uses a mobile app or desktop software to generate a one-time code. Some examples of software-based MFA include Google Authenticator and Microsoft Authenticator.
- **Hardware-based MFA**: This is an option that typically involves a physical token, such as a smart card or USB device, which generates a one-time code. Hardware-based MFA can be more expensive and less flexible than other options but may be appropriate for organisations that require a higher level of security.
- **Biometric MFA**: This uses biometric data, such as fingerprints or facial recognition, to authenticate users. Biometric MFA can be more convenient and secure than other options but may require specialised hardware or software and can be more expensive.

The third step is to **plan the rollout of the MFA solution**. This is important to ensure that the rollout is effective and does not disrupt business operations. Organisations should also consider elements such as user training, communication and support when planning the rollout. It is important to communicate the benefits of MFA to users and to provide training on how to use the MFA solution properly.

The final step is to **implement the MFA solution**. This involves configuring the MFA solution to work with the systems and applications that require it. Organisations should also provide ongoing support to users to ensure that the MFA solution is used properly and to troubleshoot any issues that may arise.

Enhancing cybersecurity can often seem like a daunting and complex task, especially with limited resources and budgets. However, implementing MFA can be a quick and effective way to significantly enhance your security posture. This additional layer of security greatly reduces the risk of unauthorised access, as it makes it much more difficult for attackers to bypass traditional password-based security measures. MFA can be easy to implement, with many providers offering user-friendly solutions. By implementing it, organisations can quickly improve their security posture, protect their sensitive data, and increase customer trust, all while staying within their budgets and resources.

## 4.1 MULTI-FACTOR AUTHENTHICATION ON APPLICATION LEVEL

MFA can be implemented across a range of applications and systems, such as email, VPNs, cloud-based services, and internal networks. The most commonly used services offer a form of multi-factor verification and have a short instruction page. You can find a few here:

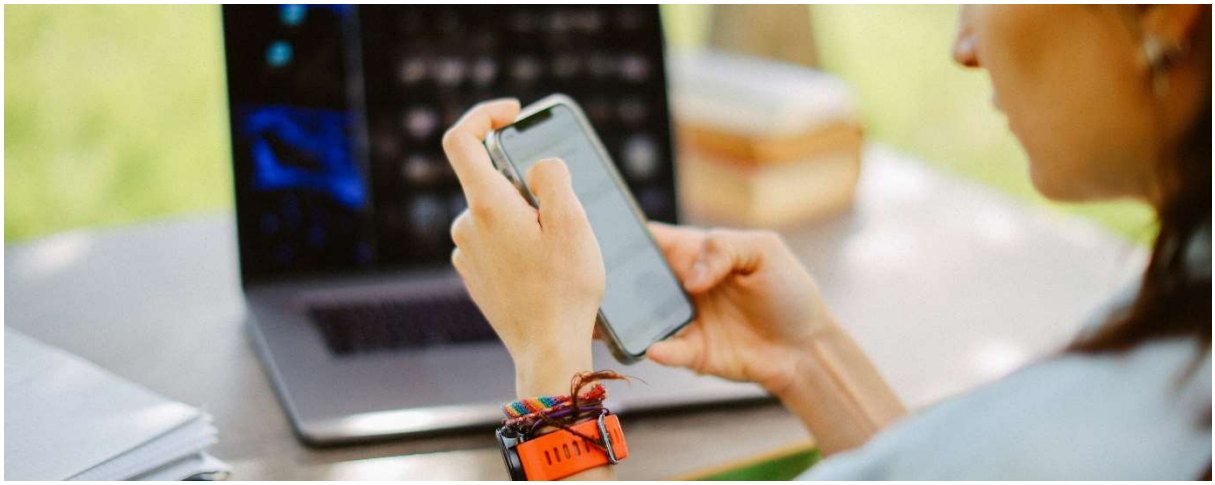
- Dropbox
- Google
- LinkedIn
- Microsoft
- Skype
- WhatsApp
- Yahoo

For more concrete examples, we refer you to the following article: Two Factor Authentication, is it difficult to use?

## 4.2 MULTI-FACTOR AUTHENTICATION ON REMOTE ACCESS

Remote access refers to the ability of users or processes acting on their behalf to **connect** to an organisational information system **through external networks such as the Internet**. It is commonly facilitated by technologies such as encrypted Virtual Private Networks (VPNs) to ensure the confidentiality and integrity of the communication. Implementing secure remote access involves establishing strict usage restrictions, configuration requirements, and authorization protocols before allowing such connections. This ensures that only authorized users can access the system remotely, thereby safeguarding the system from potential external threats.

In the context of remote access, the importance of MFA cannot be overstated. A password alone, no matter how complex, can still be cracked, guessed, or phished by determined cyber criminals. By implementing MFA, businesses can **add an extra layer of security to their remote access protocols**, ensuring that only authorized users can access their systems.



## 4.3 KEY CONSIDERATIONS WHEN CHOOSING AN MFA SOLUTION

Before choosing an MFA solution, make syre to keep in mind these key considerations:

- **Security**: choose a secure MFA tools that aligns with security standards and best practices;
- **Compatibility**: make sure to choose an MFA tool that is compatible with the existing system and infrastructure within your organisation (e.g., OS version) and that can be easily integrated with your organisation authentication framework (e.g., Active directory);
- **Deployment**: Consider an MFA tool that will provide security and easier to deploy within your organisation environment and the level of support needed;
- **Cost** : Evaluate the cost of the resource needed for the implementation of MFA such as maintenance, licencing fees etc; and
- **Authentication options** : it is best to choose an MFA tool that offers a variety of authentication options in order to offer flexibility for users to choose the authentication factors based on their preferences and needs.

Below are some examples of setting up Multi-factor Authentication within your organisation using most common authentication application. These are general guidelines and may not be applicable to your organisation needs, or specifics might change according to your environment.

## 4.4 IMPLEMENTING MFA IN AZURE CLOUD

**Step 1: Azure Active Directory (pre-requisite)**

In order to use Microsoft authenticator app, your organisation needs to have an Azure AD (Active Directory) account.

**Step 2: Enable MFA**

Every edition of Azure AD includes Azure AD Multi-Factor Authentication. No additional license is needed for a registration campaign. This can be done in the Azure portal by going to Azure Active Directory > Security > MFA.

**Step 3: Choose authentication methods**

Microsoft authenticator supports a range of authentication methods, such as push notifications, one-time passcodes.

**Step 4: Configure policies**

This step allows your organisation to determine which user are required to use MFA, which authentication methods can be used and when the MFA is required (e.g., specific application).

This can be determined using one of these policies:

- *MFA Registration Policy*: Users will need to be enabled for notification through mobile application.
- *Authentication Methods Policy*: Users will need to be enabled for the Authenticator app and the Authentication mode set to Any or Push.

**Step 5: Set up Microsoft authenticator**

Once MFA is enabled and policies are configured, instruction for setting up Microsoft authentication can be communicated to users via email or using your organisation internal communication platforms (e.g., intranet).

For more guidance refer to :

- Nudge users to set up Microsoft Authenticator - Microsoft Entra | Microsoft Learn
- Configure the MFA registration policy - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

## 4.5 IMPLEMENTING MFA IN GOOGLE CLOUD

**Step 1: Google Cloud account (pre-requisite)**

In order to use Google Authenticator, your organisation need to have a google cloud account for MFA deployment.

**Step 2: set up 2 steps verification**

Enable 2 step verification using the Google Admin Console:

Menu > Security> Authentication > 2-step verification.

**Step 3: choose authentication method**

Google authenticator support a range of authentication methods for 2 steps verification such as Google authenticator app ( for android version 4.4 and up), security keys, Google prompt, text message, or phone call and backup codes.

**Step 4: Configure policies**

Determine which user are required to use MFA. To apply the setting to everyone, leave the top organisational unit selected. Otherwise, select a child organisational unit or a configuration group and check the Allow users to turn on 2-Step Verification box.

To enforce MFA for all users or the selected group enable the enforcement option.

**Step 5: Enrol 2-step verification**

Provide user with instruction for setting up google authenticator via email or the or using your organisations' internal communication platforms.

For more guidance refer to : Deploy 2-Step Verification - Google Workspace Admin Help

## 4.6 IMPLEMENTING MFA IN CUSTOM APPS USING ITSME

**Step 1: Register for itsme MFA services**

Your organisation needs to be registered for itsme MFA services in order to enable MFA using itsme application and create an account on the itsme administration portal allowing your organisation to manage MFA setting and view usage statistics.

**Step 2: choose the authentication method**

The available authentication methods in itsme are based on at least the combination something the user has such as their smartphone and the installed itsme application, and user's biometrics such as fingerprint or Face ID and or something the user knows (e.g., PIN code).

**Step 3: Configure policies**

Navigate the policy setting in the administration portal and determine the rules that will determine when itsme MFA is required, exception and setup notification in case of failed login attempts.

**Step 4: Enrol itsme MFA**

Provide user with instruction for setting up itsme via email or using your organisation internal communication platforms.

For more guidance refer to : General information - Documentation - Onboarding (belgianmobileid.be)

## 4.7 AUTHENTICATOR APPLICATIONS

An authenticator app is an application used to generate time-based one-time passwords (TOTPS) for multi-factor authentication. It helps users secure their accounts by providing a second layer of verification

- Authy
- Google Authenticator
- Microsoft Authenticator
- Okta Verify

# 5. Considerations for Multi-Factor Authentication configuration and user support

**Policies configuration:**

- Determine the allowed  authentication method that is provided by the chosen authentication application and compatible with your organisation environment and user needs.
- It is recommended to apply MFA authentication for all user and application specially while working remotely. During this process, the administrator must specify for which user, group and application the MFA is applicable, define criteria for exceptions and ensure the appropriate controls are in place.
- Integrate MFA with the available ystem within your organisation such as Active directory to ensure that MFA is enforced for all application and system, provide high security while ensuring a good user experience by using a single set of user credentials.

**User support:**

After Policies configuration and MFA enforcement, users will not be able to authenticate to the system, if applicable, without Enabling MFA. Your organisation need to ensure that the users are provided with the appropriate support by:

- Clearly communicate the enrolment process of MFA and provide user with guidelines on how to set up the authentication app within their mobile devices using your organisation communication tools such as email and intranet.
- Organise training sessions for users to increase awareness regarding MFA, its purpose and how it can be used.
- Provide ongoing support, contacts where users can ask for assistance on the implementation.
- Keep users up to date regarding and change or update on the policies of the MFA and applicability.

# 6. Potential problems or barriers

## 6.1 LOSS OF CONNECTIVITY

It is important to have a backup plan in place for what to do if users are unable to authenticate using MFA in case of loss of connectivity, loss of the MFA-enabled device or are unable to authenticate using the primary method (e.g., blocked GSM number, changed email). This may include:

- Providing **backup authentication method** such as a secondary phone number or email address.
- Use **alternative authentication methods** that do not rely on connectivity (e.g., physical tokens, smart cards).
- **Temporary disable** MFA for a specific user or group of users. This should only be done as last resort. The MFA should be reactivated once the problem is resolved.

Additionally, an operation support guide should be defined including step-by-step instructions for how to troubleshoot the issue, who to contact for support, and how to ensure that your organisation's data remains secure during the outage.

## 6.2 FACTORS TO CONSIDER WHEN CHOOSING AN MFA METHOD

When it comes to choosing a Multi-factor Authentication method, it is important to consider the type of MFA that suits your organisation needs the best. One of the commonly used MFA methods is the use of an authentication app. While this method is convenient and secure, it is important to keep in mind that all users need a smartphone to use it. This can be a potential issue for **organisations that do not provide its employees with organisation's smartphone** or for **employees who do not have a smartphone**,or **don't want to install** the application on their personal smartphone or have limited access to one. In such cases, it may be necessary to consider alternative MFA methods, such as a physical security token or a text message-based system, to ensure that all users can access the systems securely. Therefore, it is crucial to **weigh the pros and cons** of different MFA methods before making a decision, and secure that the chosen method is accessible to all users.

## 6.3 MFA AND BYOD

Personal devices such as smartphones used for work purposes may not be compatible with your organisation's chosen MFA method, making it difficult to **enforce MFA in a Bring Your Own Device (BYOD) environment** and ensure a consistent MFA implementation across all the devices in a formal and correct way.

Therefore, your organisation should consider using a mobile device management (MDM) to manage user personal devices used for work purposes and ensure that these devices are properly secured and compliant with your organisation's security policies.

Additionally, organisation security policies should be applied to:

- ensure that **minimum security requirements** are implemented in users' devices (e.g., type of operating system, requirements for keeping the device up to date with security patches, configurations, etc.).
- communicate the importance of MFA and **the risk associated with using personal devices** for work purposes. They should be communicated to all organisation's employees to raise awareness on how to protect the personal devices used for work purposes.
- Support with **clear guidelines** should be provided to users to properly configure their devices for use with MFA and procedures on how and where to report in case of security incident related to BYOD.
- Limit remote access. Your organisation should also consider **segmenting access** to its data and application based on the risk level and requiring MFA whenever it is feasible and specially for high-risk data and applications and remote access.

In conclusion, implementing **MFA in BYOD environment** should be considered an essential security measure as employee's devices may not meet the same security standards as organisation-owned devices.

# 7. Key considerations for secure MFA usage

When using MFA to add an extra layer of protection and enhance security, it is important to be vigilant and mindful of certain considerations :

- **Ensure device security**: Implement security updates and patches for your MFA application, operating systems and software versions installed on your devices as soon as they are available to address potential vulnerabilities.
- **Mindful interaction**: if you choose push up notification as your second factor of authentication  it is important to remain vigilant and avoid mindlessly accepting notification without reviewing the content. Always take time to read the notification before taking action.
- **Use a strong password/ paraphrase:** Additionally to MFA, use a strong and long password or  a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security, with lower- and upper-case characters, possibly also numbers and special characters and avoid obvious, such as “password”, sequences of letters or numbers and personal information.
- **Use official platforms:** When downloading MFA applications, use trusted official app stores such as google Play Stores for Android or the Apple App Store for IOS devices to ensure the authenticity and the integrity of the application reducing the risk of downloading malicious software.

# 8. References

## 8.1 CYBERFUNDAMENTALS

This appendix links to the relevant Basic cyberfundamentals requirements associated with Multi-Factor Authentication (MFA), offering a detailed reference to support the implementation and management of MFA in our cybersecurity framework.

- **PR.AC-3**: **Remote access is managed.**

  **Key Measure:** The organisation's networks when accessed remotely shall be secured, **including through multi-factor authentication (MFA)**.

## 8.2 SAFEONWEB (@WORK)

Protect accounts with multi-factor authentication | Safeonweb@work

A strong password to protect valuable information | Safeonweb@work

Access policy | Safeonweb@work

Use two-factor authentication | Safeonweb

Two Factor Authentication, is it difficult to use? | Safeonweb