

Multi-Factor Authentication (MFA)

How to use this guide

The purpose of the guide is to provide a basic understanding of the benefits of MFA, as well as implementation considerations and options.

It is not intended to be an arduous read from front to back and can simply be referred to as and when needed.

Navigate easily by clicking on the sections above; and you'll find a full content overview on each page within the Guidance section.

If you are not sure where to start or whether your organisation might benefit from this guide, the action checklist on page 4 may help to identify where user access security needs strengthening.

Information has been provided with minimal use of technical terms so that it is accessible by management and any function of a business. However, should further understanding be required on any aspect of MFA, an IT specialist should be able to assist.

Executive summary

Often, it's only after an organisation has been hit by a cyber-attack or fraud incident that they start to take user access controls seriously, knowing that one of the root causes for the incident occurring was due to the lack of Multi-Factor Authentication (MFA) security.

Cyber and fraud incidents can often result in detrimental consequences for businesses on a financial, operational, and reputational level. At QBE, we endeavour to support businesses in proactively managing risks to avoid the distress that can come with a successful breach by unauthorised users. Our experience finds that many businesses are not aware that usernames and passwords on their own are *no longer sufficient* to protect user accounts with access to sensitive business or personal information. Using MFA, which is a baseline control, can protect these accounts and reduce the risk of a security breach and identify theft.

QBE has produced this MFA guide for any business or individual looking to understand MFA on a practical level. The guide also considers user access security benefits and risks from a stakeholder perspective, thereby also striving to help businesses protect against knock-on impacts from customers or suppliers that may fall victim to cyber-attacks.

Applying MFA everywhere should be a standard security activity for all businesses, large or small. This guide aims to help businesses navigate their MFA implementation journey.

Ultimately, it is essential that MFA deployment is planned and managed in such a way that balances highly effective security with an accessible user experience. Risk-based policies should be defined and used to determine MFA requirements. Effective engagement with users can support them in changing their login habits and create a more positive security culture across a business.

MFA should be implemented in the way that best suits your business security needs. This is likely to vary depending on each service, application, or device. If needed, seek the advice of specialists.



“The vast majority of cyber incidents; currently occurring at an alarming rate and affecting both companies and individuals, would not have occurred if MFA had been in extensive use.

Most cyber-attacks involve a preceding step where the attackers breach the defences of their victims by obtaining user passwords and using them for unauthorised access.”

Cyber Incident Response specialists,
STORM Guidance

Strengthening user access security

Don't wait to be a victim of cybercrime before you implement MFA. It is a crucial control that is often found to be missing, which can lead to being a key contributing factor to successful cyber-attacks and fraudulent activity.

This high-level checklist can be used as a guide to ensure critical controls for strengthening user access security for your business are implemented. You may wish to create more detailed checklists for the individual steps that may be required to achieve each of these actions for your business.

This checklist is available as a separate form to download [here](#).



For support with the above key actions, check out the rest of the guide and our [useful links](#).

Many of the useful links are from [ncsc.gov.uk](#), which has a wealth of guidance that is generally globally applicable.

Action checklist

Add a comment

- 1 Undertake a cyber resilience risk assessment to identify the critical assets, functions and all the access points to where sensitive data resides; and the MFA/user access control status for each of these.
- 2 Ensure the procurement process requires service providers to have minimum security standards, including MFA capabilities; and ensuring their systems are effectively protected.
- 3 Schedule regular reviews to ensure MFA is working effectively across the business, and new exposures have been sufficiently protected.
- 4 Ensure your organisation's password policy offers guidance on using strong, unique passwords for each access point or account.
- 5 Consider the use of password managers which can generate random strong passwords for users. Train your staff on how to make the best use of password managers.
- 6 Use risk-based policies to establish which triggers should alert relevant users, administrators, or management. e.g., where unauthorised access has been detected.
- 7 Ensure there is an established process to change passwords or replace MFA methods promptly if a user knows or suspects the password, other authentication method or account has been compromised.
- 8 Establish a clear and accessible reporting process, which staff and/or stakeholders are regularly made aware of, and encouraged to utilise.
- 9 Build and maintain a culture within your business where staff and stakeholders feel confident to speak up, especially in relation to security concerns or potential incidents.
- 10 Educate staff and customers to remain vigilant to social engineering scams and refrain from revealing any personal or security information.

What is authentication?

Firstly, let's go back to basics and understand the authentication process.

Authentication is a security process to confirm a user's identity before authorising access to a network, account, or system information.

A username or email address is often used to claim the user's identity, and then authentication is required to prove that identity. The most common form of authentication is a password, and a combination of a username and password is an example of Single-Factor Authentication (SFA), requiring only one check to prove the user's identity and in this case being a knowledge-based factor.

What is MFA?

Multi-Factor Authentication (MFA) is a form of strong authentication that requires users to prove their identity via multiple pieces of evidence from independent sources, **using two or more factors of authentication**. The extra layers of authentication required by MFA provides a higher level of assurance about a user's identity and minimises the chances of unauthorised users gaining access to key accounts, systems, or critical data.

Two-Factor Authentication (2FA) requires two levels of credential verification to take place successfully before a user can be permitted access. 2FA is the most commonly used subset of MFA. However, 2FA, MFA and the term 'two-step verification' (2SV) are used interchangeably.

In this guide, we'll use the term MFA, as ultimately the key message is to ensure you are protecting key accounts and systems with more than single-factor security. For example, using a username and password, would be the **first** authentication factor. Then, **adding an extra factor or two**, such as a requirement for a fingerprint and/or a code from an authentication app, will increase security to MFA.

The MFA security process ensures better protection of both a user's personal information, as well as improving the security around the resources that can be accessed by authorised users.

Using two of the same type of authentication (e.g. something you know) is **not** two-factor; the factors must be different.

The next page explains the different factors.



What is MFA?

**This diagram briefly explains the three factors of authentication.
At least two different factors in any of these combinations constitutes MFA.**

Something you know

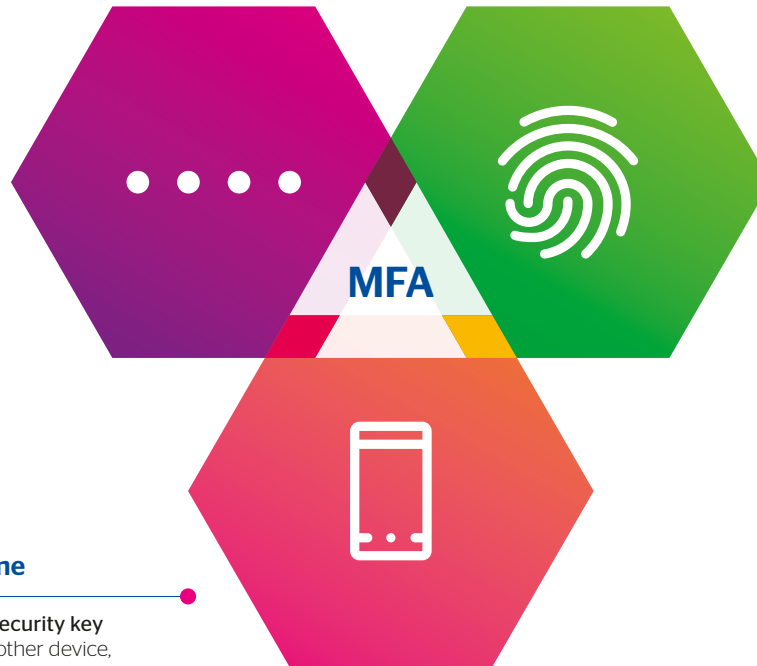
e.g. a password or PIN

Knowledge-based verification is most commonly used as part of MFA and is also the most vulnerable to security attacks. These can include a **password**, **personal identification number (PIN)**, a **security question**, or a **passphrase**.

Something you have

e.g. security key fob or smartphone

This involves something physical such as a **security key fob**, **smartcard**, **ATM card**, **smart phone**, or other device, that is in the possession of the rightful user. Often it requires the user to generate a one-time code to enter as evidence to verify their identity in order to gain access.



Something you are

e.g. fingerprint or voice recognition

Usually involves biometric methods to prove identity e.g. **fingerprint**, **facial** or **voice recognition**; or **retinal scan**. This is the strongest verification method, however it can result in failure if the user is impacted by an injury (e.g. to the eye, where a retinal scan is required for authentication).

Why is MFA important?

People are overloaded with the number of passwords they must manage, both in their personal life and in business. This overload has led to poor behaviours including using predictable passwords and reusing the same password or a variation of it across accounts. Attackers exploit these behaviours which can ultimately leave your business and personal activities vulnerable to attack.

Some of the common attack methods include:

- > **Brute-force attack:** Targeted attack where the attacker tries to infiltrate a user's account by using powerful tools to try many passwords;
- > **Password spraying:** Attackers attempt to try common passwords across a large volume of accounts;
- > **Social engineering including phishing:** Where individuals are manipulated into divulging confidential information, including passwords, that may be used for fraudulent purposes;
- > **Man-in-the-middle attack:** A fraudster (the 'man-in-the-middle') discreetly intercepts communications between a victim and a legitimate entity and deceives both parties to commit fraud or cybercrime;
- > **Credential stuffing:** Attackers exploit people's tendency to reuse username and password combinations, so once one valid combination is obtained, large scale attacks are delivered across many other accounts owned by the same user in attempt to gain unauthorised access;
- > **Keylogging:** A hacker is able to record every keystroke made by a user to obtain access to passwords or other personal information.

These are just some of the reasons why the "Something you KNOW" factor can be most vulnerable. If the same password is applied to many different accounts, a breach on one account can mean that other accounts using the same password are also easily compromised.

Implementing multi-factor authentication will prevent hackers from gaining access to your accounts even if your password is guessed or stolen. The extra layer of protection that MFA offers ensures your account is more secure and drastically reduces the chances of fraud, data loss or identity theft.

"Passwords on their own (a form of SFA) are virtually useless as a security mechanism to protect your accounts. MFA should now be the minimum standard of security and vendors who do not provide it should not be trusted with your data."

Neil Hare-Brown, STORM Guidance

Case examples

Cyber-attacks and incidents in the press have been highlighting the issue for many years now, revealing that all firms, even major corporates, are falling victim due to their lack of user access controls.

Deloitte

In 2016 - 17, Deloitte's global email server (on the Cloud) was compromised by a hacker due to an administrator's account requiring only a single password. No MFA meant the hacker had unrestricted access to all areas!

British Airways

In 2018, British Airways was subject to a cyber-attack where a significant amount of personal data related to customers and staff was accessed, along with usernames, passwords, and PINs.

The ICO found that MFA had not been applied to protect employee or third-party accounts - a security measure which could have mitigated the risk of attackers accessing the BA network.

Criminal law firm

A ransomware attack which encrypted the firm's client data as well as back-ups, resulted in the personal data being no longer accessible to the firm, and a loss of confidentiality.

The UK ICO highlighted that one of the key vulnerabilities contributing to the success of this attack was a **lack of MFA** required for remote access to the firm's network.

The ICO's decision to issue the firm with a fine of almost £100,000 in March 2022, **highlights the importance it places on user access security controls such as MFA to protect sensitive data.**

"The [Information] Commissioner believes that the use of MFA was a comparably low-cost preventative measure which should have been implemented..."

To this day many firms are not recognising the significant benefit of this relatively simple control. All firms, small and large need to make it a priority to review their critical systems and user access security levels, and ensure MFA is enabled appropriately.

Where is MFA required?


Ultimately, MFA should be applied everywhere where you are accessing personal or corporate data. This includes devices, applications, online/cloud services, and remote access to networks for all staff. In short, everywhere you use a password you should use MFA.

When starting your programme to ensure MFA is ubiquitous, priority should be applied based on where the most critical assets/sensitive data reside. Start with administrative accounts that have the most extensive access to systems and data.

Businesses should undertake a cyber resilience risk assessment to identify their critical assets, functions and where sensitive information resides, and all the access points to that data. This will help determine which accounts or systems need to be reviewed first to ensure effective user access security controls are in place, and whether MFA has been applied, needs to be applied, or in cases where it is not possible, a further review undertaken on how to ensure other layers of protection make unauthorised access extremely difficult.

MFA is relatively simple for a solutions provider to implement. Therefore, if they do not provide MFA, it should lead you to question their ability to fully support such a solution and to seriously consider changing to a service provider that does offer MFA.

Your cyber resilience risk assessment should consider all key areas that may be exposed to the potential of unauthorised access. For some organisations this may mean applying MFA within their internal networks as well, to address the insider threat as well as the external threats.

 **Conditional access policies** can be used to define which access control requirements should apply for which users, and in which circumstances. For example, if a user is on the corporate network on their registered device, the policy can allow that user to access applications and accounts via regular SFA; but if they switch to accessing the network via a remote device, they are required to pass MFA checks.

Conditional access policy decisions will need to be assessed, applied, and managed effectively to ensure user access privileges are not exploited.

Remote access to your business network

There are a few ways that businesses can set up remote access to their networks. Some are more secure than others and it is important that your IT support team/individual discusses the options and security risks and benefits of each with your management.

Virtual Private Network (VPN)

A significantly high proportion of network attacks occur through unauthorised access via remote access. Once remote access is hijacked by cybercriminals, they steal data and drop ransomware and other types of malware to wreak havoc on their victims.

It is therefore vital that remote access using Remote Desktop Protocol (RDP) and any other methods are secured with multiple layers of protection.

One such layer is the use of a Virtual Private Network (VPN) which offers a secure channel between the user's computer and their company or other legitimate network. However due to the many reasons mentioned earlier on the vulnerability of passwords, it is critical that VPNs are also secured with MFA.

Additionally, using VPNs with origin authentication (being able to trust the origin of the entity that establishes a VPN) using private certificates can provide this valuable security protection.

VPN solutions should be managed like any other software, with timely patching to ensure they are not subject to vulnerabilities.

Cloud application access

Companies are moving corporate data from on premise servers onto the cloud, due to the flexibility it offers from a business continuity perspective and the 'work from anywhere' aspect.

Although the security in many cloud services is often superior to anything a small organisation can organise for themselves, if the access to those services is a password alone, this can introduce a significant vulnerability to the confidentiality, integrity, and availability of the organisational data.

In recent years, there has been an increasing number of attacks on cloud services, using techniques to steal user's passwords to access their accounts. In 2019, Microsoft reported that there are over 300 million fraudulent sign-in attempts to their cloud services every day.

To prevent unauthorised access and reduce the risk of a breach on data stored and processed by cloud-based solutions, it is crucial these applications are fully secured with requirements for MFA, privileged account access, access management controls and monitoring access attempts.

When sourcing cloud service providers, or procuring cloud-based applications, ensure your business only selects those service providers that support MFA for access on all user accounts. If MFA is not an available option or easy to integrate into the service, then alternative options should be sourced.

Online accounts for business purposes

Where possible, turn on MFA for all accounts that are accessible over the internet. Ensure that all business-critical applications or accounts with personal or confidential data, are protected by MFA.

If the online service doesn't offer MFA, ask for this security feature to be provided or consider alternative options that offer what experts agree should be the baseline level of security that MFA offers. The demand for MFA and customers choosing alternative providers that offer MFA will help to raise awareness of cyber risks, and support improvements in online security.

Your organisation's Acceptable Use Policy (AUP) should prohibit staff from accessing web-based accounts (e.g., shopping, email, social media etc) on corporate network devices unless such access uses MFA. It is a common problem that users often use the same password for all their online accounts, both business and personal. Your AUP should also mandate use of MFA on personal accounts to counter the threat that passwords protecting business accounts might be revealed via insecure personal accounts.

Network administrator accounts or privileged access accounts

Any privileged access or administrative accounts used for managing hardware and software networks, and conditional access controls are prime targets for attackers looking for access into a business network.

These accounts should be identified, and clearly distinguished from typical user accounts. Strong security controls should be applied with MFA being a principal requirement for accessing such privileged accounts.

Access to administrator accounts should only be assigned to authorised staff members who undertake roles involving system access control or other privileged rights related to accessing sensitive data. Such accounts should be separate from accounts assigned to the same users for non-administrative work.

Similarly, any accounts assigned to third parties for support or other reasons, should also be protected with MFA.

Regular review and monitoring of such administrative/privileged accounts across the organisation's systems and the supply chain will ensure least privilege access status is up to date and applied. This can also protect against insider threat.

Most services will provide specific guidelines on how to protect these critical accounts that are more vulnerable to attack. E.g. Microsoft 365 has step-by-step guidance on protecting privileged accounts - see our [useful links](#).

Password Managers

A Password Manager (PM) application is a software solution that acts as a secure repository for user account credentials. It is especially useful for users who need to manage many different accounts on different platforms. PMs can be installed on desktops, laptops, and mobile devices.



The LastPass report findings on the left prove that users need to be better educated on user access controls, taking advantage of secure password management solutions.

PMs can vary to meet different requirements, but most will be able to auto-generate highly secure passwords that should be impossible to guess. It is crucial to select a PM that has reputable security credentials and stores passwords in an encrypted database that is synchronised online or has a secure backup feature which prevents unintentional loss and easy recovery of account credentials.

Don't forget to ensure that MFA is always enabled to protect access to each PM in use. Most PMs offer MFA by default, so ensure this requirement features on your selection criteria when deciding which PM(s) to authorise for use within your business.

Bring Your Own Device (BYOD)

In today's hybrid working environments, it's more common for staff to use their personal devices to access corporate accounts. This requires businesses to have BYOD policies in place, and it is recommended that these policies are regularly reviewed and shared with staff to ensure security requirements are continuously met.

MFA can benefit businesses, where employees are permitted to use their own device to access corporate networks or accounts. Personal devices may be at greater risk of being exposed to open wi-fi networks, as well as having vulnerable online accounts accessed only via password, which if breached could risk hackers being able to access corporate accounts. All staff should be made aware of the risks to which they may be exposed, and educated on mobile device security.

It is vital that BYOD does not represent the weak link in the chain of your security, and so access to such devices should also be protected with MFA. The good news is that many mobile devices have inbuilt features that can simply be enabled. Examples include PIN or passcode working together with fingerprint and face recognition.

Support and train those staff using BYOD to ensure MFA is applied for access to all accounts and applications from their device, and to minimise the risk of corporate data being compromised.

Single Sign On (SSO)

Some organisations may already be using a Single Sign On (SSO) solution, and management or users may not even realise they are using authenticated access to applications or the cloud, because it has been integrated into their provider's (e.g., Microsoft) authenticated SSO, so that needs to be considered in assessments and security requirement discussions.

SSO can offer an effective user experience for staff as they are generally only required to login once, to be authenticated across multiple applications and services. It is therefore recommended that MFA is used where the user initially accesses systems protected by SSO. This is crucially important as whilst SSO certainly makes it easier for users by avoiding having to remember multiple passwords, it also means if an attacker manages to compromise one account, they may have easy access to other accounts and systems too.

SSO should therefore be implemented to require MFA upon initial user login; and then configured so that it is only required in specific scenarios such as where a new device is trying to access an application under an SSO account, or other unusual circumstances where there is a potential for unauthorised access.

Summary



Ultimately, broad application of MFA is recommended for initial access across your entire business operations and IT infrastructure to minimise cyber risk. MFA should be used for all user access to online accounts not protected with SSO.

Stakeholder risks

Most 'Business Email Compromise' (BEC) attacks are successful because of a phishing message received by a staff member, from a trusted stakeholder whose mailbox has already been hijacked, most likely because they were not using MFA. This may be a client, a supplier, another professional party or even a colleague. Criminals propagate further phishing messages from such hijacked mailboxes in the hope that new victims (using SFA) can be easily targeted for fraud and further propagation.

Therefore, it is important to apply MFA on your own systems, in case your business falls victim to an attack such as simply clicking a link on a phishing email purportedly from a trusted stakeholder. But it is just as important and reasonable to expect those with whom you interact to also implement effective safeguards such as MFA.

Responsible procurement: Protecting your business

Organisations should make it part of their procurement policy to expect minimum security requirements from suppliers/service providers. Many types of suppliers, in particular IT Service Providers (ITSPs) and Managed Service Providers (MSPs) are prime targets by cybercriminals due to their role and access to many customer networks. If a hacker gained access to a service provider's systems, their customers; including your business, are highly exposed to the resulting impact of a cyber-attack.

Any service providers you use should have effective cyber security controls on their own systems, including MFA to prevent any security incidents that could impact your business, as their customer.

If service providers do not offer or apply MFA sufficiently, then re-consider onboarding or continuing your contract with them until they meet your security standards, advising them that the security of your information is a critical requirement for your business.

Communicating with customers

How and whether you support your clients or customers with understanding cyber risks and security controls will depend on your industry, profession or how you interact with them.

Where online interactions or high value transactions are taking place, it is crucial that customers are aware of the risks because a breach of their security may expose your business to a cyber-attack. Using a secure customer communications portal is often more effective than email communications. Such portals also offer many other advantages to businesses and their customer relationships. Where this is not possible, educate your customers on baseline cyber security hygiene and most importantly encourage them to enable MFA on their accounts to protect themselves and your business.

Various channels can be used to deliver these messages, including providing and directing customers to guidance that may reside on your website, communications portal or shared early in your engagement. Aside from protecting your business from your customers' online security habits, your customers may appreciate your support and guidance on this important topic, which may strengthen your customer relations and business reputation.

A guidance template that can be adapted and shared with customers is available in our [useful links](#).

How MFA can be implemented

Many service providers and vendors of sites, portals, apps, and devices now offer some form of MFA, and many popular sites also offer guides explaining how to set up MFA on your account. Some of which are included in our [useful links](#).

If you need to implement MFA across the business, then first investigate the options available to enable MFA across the enterprise.

To enable for specific end users, check account settings or user profile to see whether MFA or 2FA is an available option on your devices and accounts. If it is, follow the necessary steps to implement MFA immediately where possible (or discuss with your IT team/consultant as needed).

The common types of MFA are described on the following page, along with information on some of the benefits and vulnerabilities that should be considered during the selection and implementation process.

The authentication options available for each service being used, will determine which additional factor/s can be added as a requirement to the initial authentication factor (commonly a username and password). In some cases where it is not straightforward, or a number of additional authentication options are available, it may be beneficial to seek the advice of IT specialists or the service provider.

Be aware that cyber criminals will continue to find ways to gain unauthorised access. When selecting authentication methods, be mindful of some of the known tactics used to bypass MFA. For example, it is recommended that push notifications and approval requests are disabled as these expose users to **MFA fatigue attacks**. This is where a hacker with stolen credentials sends multiple approval requests in hope that the user may authorise their request inadvertently or out of frustration.



Common types of MFA

A trusted device



- > A user possesses a specific device (e.g., a company computer/laptop) to prove they are who they say they are.
- > Organisations can configure cloud services to only accept authentication attempts from within their trusted enterprise networks, ensuring that users can only authenticate if they are either directly connected to that trusted network or have remote access to it over a virtual private network (VPN).
- > In addition, or as an alternative to using a VPN, remote workers would be able to access online services only on trusted devices that are managed by the organisation.

The trusted device being used to access the account service, becomes the additional factor.

A known or trusted account

Phone call or SMS-based MFA

- > The service sends an SMS message containing a single-use code, or makes a voice call reading out a code to the phone number registered for that user.
- > Vulnerabilities include:
 - > hackers cloning chips in a mobile phone enabling them to intercept messages. If a hacker has access to a user's account password, they could intercept the user's phone to retrieve the authentication code via SMS too.
 - > SIM swap attacks, where hackers convince phone service providers to transfer a victim's phone number over to their own phone, so they would receive any authentication codes.

Email-based MFA

- > The service will email a single-use code to a registered email address. **The email account used should be protected by MFA for the authentication process to be most effective.**
- > Services that send a code for the user to type in is preferable to a clickable link, as it can be difficult for a user to distinguish between a legitimate email and a phishing attack.

These MFA techniques are often least secure; however, they still offer a significant advantage over not using any form of MFA. It is recommended that if alternatives to telephone or email-based MFA are available, those should be implemented.

A physically separate security key or token



- > A user has a separate physical security key or token that proves they are who they say they are.
- > Some types will require the user to unlock them before use, others just require proof of possession.
- > Examples include Smartcards, online banking tokens and USB keys that are unlocked by a PIN code, and chip-and-PIN card readers which generate a single-use code each time a user logs in.
- > **Added benefit:** physical security keys often validate domain names before codes are generated, making it difficult for hackers to intercept via fake domains.

Often physical keys are seen as the most secure form of MFA; however, they may be more costly.

Authenticator apps on trusted devices



- > An authenticator app can generate time limited one-time codes once it has been set up with sites or accounts that need to be accessed securely.
- > A generic authenticator app can work with many services.
- > Some accounts or sites have their own bespoke authenticator code generator apps which can also be authorised to a trusted device.
- > **Added benefit:** the constantly changing codes can be used for authentication even without an Internet connection.

- > Some apps can receive push notifications prompting users to confirm or deny that they are currently trying to log into a named service. **However, these are susceptible to MFA fatigue attacks, so this method should be avoided or disabled if possible.**

Select your authenticator apps carefully, ensuring that they securely synchronise the user accounts to the cloud or alternative backup, so that the authenticators can be easily recovered if devices are lost or damaged.

Is MFA required for every access attempt?

MFA is unlikely to be required every time a user attempts to access a service, however there will be crucial occasions where it will be recommended or required, based on the assessed risk.

Conditional access policies mentioned previously can help to govern access to services or accounts so that MFA is only required in scenarios that might be classed as high risk or unusual to the norm for that user. These might include:

- > **Logging onto a service using a device that the user has not used before.** Most MFA approaches will be able to track devices that have been previously used, and therefore remembers the device used to re-enter a site/account by the same user. It may be necessary to opt into the service by selecting a 'remember my device' option.
- > **Logging onto a service that has a higher impact if it's compromised,** such as an email account or online banking.
- > **When performing high risk actions,** such as changing a password or transferring money.

- > **When the authentication has been determined as high risk,** such as the connection coming from a different part of the world than is normal for that user.
- > **For administrators,** both at login and to confirm certain actions such as resetting user passwords, deleting accounts, or disabling MFA.

Conditional access reduces the number of prompts for MFA, enabling you to set up requirements for MFA only when necessary and helping to reduce the friction for user adoption. Applying relevant conditional access policies is important to avoid the potential risk of users unconsciously approving prompts and falling victim to phishing attacks, because they are continuously prompted to apply MFA for every access attempt.

What is required for an effective implementation of MFA?

Implementation of MFA should not be an action that is left purely with IT teams or consultants to consider or deliver on.

Management teams or senior managers within the business should understand:

- > why their business might be at risk of a cyber incident or fraud;
- > the controls they have in place to protect against unauthorised access; and
- > where they might be exposed.

It is important for internal managers to understand why vital safeguards, such as MFA are needed. Proactive engagement with ITSPs, MSPs or IT managers is essential, and it may be necessary for IT experts to explain the potential consequences of failing to implement baseline security such as MFA. This will enable top management in businesses to have a transparent view of why MFA implementation is required to protect their critical assets, and in turn should raise awareness of cyber security across their staff and stakeholders, and create an open and cyber resilient culture.

An effective MFA implementation plan will prioritise high risk targets such as privileged users of administrative accounts, and should involve senior management early in the roll out.

Some organisations may not need a detailed roll out plan, however the approach will be determined by the complexity or volume of user accounts and systems involved. For example, larger companies are likely to benefit from a phased roll out of MFA with priority assigned to the most critical functions and administrative accounts.

Top management buy-in is valuable in all cases for a smooth transition to users accepting MFA as standard practice. In addition, the easier you can make it for your staff and end users by considering the most secure and convenient methods of MFA to deploy, and applying relevant conditional access policies, the smoother the implementation and change acceptance phases will be.

User engagement and education

Introduce the concept of MFA as early as possible to staff members, and any stakeholders that will be impacted by the implementation of MFA. Engaging users in the implementation process will reduce the chances of acceptance issues, that can result in delays to the roll out. Ensure users understand what MFA is, the benefits of adding an extra step of security to access key systems and accounts, and what will be required of them.

Various channels can be used to inform and engage with users. The ability for clear communications both ways should be created so users have a route to ask questions or raise concerns.

The goal is for businesses to achieve optimum security by offering MFA options that are convenient and do not disrupt a user's productivity. However, users should have the clear understanding that the additional MFA control is a crucial requirement and is less inconvenient than it would be to deal with the impact of a security breach.

Businesses can also address the inconvenience argument by considering implementing single sign-on (SSO) alongside MFA, so that the number of times users are prompted for MFA is reduced, providing easy access to multiple applications via the same device.

Training and awareness

Training and awareness activities are crucial to ensure everyone is comfortable with the new processes, and to identify if the MFA roll-out needs to make any considerations for areas or individuals that may need additional support.

Cybercriminals will no doubt attempt new tricks to defeat MFA security. This is already evident with the development

of MFA fatigue attacks mentioned earlier; and reverse proxy phishing tools enabling man-in-the-middle attacks where MFA tokens are stolen. It is therefore essential that regular cybersecurity training is provided to staff raising awareness on the latest scams, social engineering tactics and ways to remain secure. Phishing simulation tests can be used to create real life scenarios and ensure all staff are vigilant, and such exercises can help to identify areas where further education is required.

Users should also be regularly reminded of methods for reporting issues, via various channels, with top management encouraging a speak-up culture, and leading with a security focused mindset.

Make it easy for staff to report any concerns or suspicions related to data or account access, misplaced devices, or potential breaches. Reporting procedures should be easily accessible, clear, and straightforward.

Post implementation

Following implementation or phases of implementation, tests should be carried out to ensure MFA has been applied effectively where required, and users have been able to successfully apply MFA to access the relevant accounts or applications. In addition, effective monitoring systems should be activated to trigger any misuse or unusual activity.

Logging and monitoring

Monitoring access is important to detect cases where MFA may be bypassed. For example, if an individual's authentication factor has been stolen; or if sufficient security support processes are not in place enabling fraudsters to impersonate a user and replace or reset their authentication factors.

Effective monitoring and detection tools can help to highlight unusual activity. These may alert you when login attempts using MFA have failed, or if login attempts have been made via a different device or geographic location to the usual. In some cases, accounts are configured to alert users each time entry is made into an account, so that the user can report any unexpected activity. It is important that users are aware of when they will receive notifications, and ensure they aren't falling into a junk mailbox, as these alerts will help to detect unauthorised access, so that measures can then be taken to respond effectively.

All platforms where users authenticate (using any method) should have logging suitably configured to support continuous monitoring of who is accessing which service or account, when and with what credentials, as well as all administrative activities. Logging of security-related events can be vital to identifying and preventing unauthorised access. The availability of such logging should be a mandatory security requirement when considering any vendor-provided services.

Regularly review critical assets and accounts along with access rights, and in particular privileged access levels. This is essential to ensure access controls are being applied at all access points to sensitive information, and that least privilege access status is up to date for all users.



Reporting processes

If a user can reset an account without appropriate access factors, then remember that an unauthorised user or criminal will also be able to reset it. Therefore, have clear processes in place to enable users to report issues, and verify their identity to ensure they are who they say they are, before enabling them to reset or replace their authentication factor.

Make it easy for staff and/or stakeholders to report any issues or suspicions related to data or account access, misplaced devices, or potential breaches. Reporting procedures should be easily accessible, clear, and straightforward.

Regular reminders of key information such as reporting issues with MFA or raising concerns related to data security should be made available via various channels, with top management encouraging a speak-up culture, and leading with a security-focused mindset.

Some countries have national reporting services available for organisations or individuals to report suspicious emails, phishing attacks, or other attack vectors. For example, the UK's National Cyber Security Centre has a Suspicious Email Reporting Service (SERS), which was launched in April 2020, and as of September 2022, 14 million scams have been reported via this service; and 100,000 scams have been removed across 184,000 URLs.

This type of public cyber awareness and reporting campaign can make a huge difference in the fight against cybercriminals for individuals, businesses, and society as a whole. Businesses should aim to also support this drive by regularly reminding their staff and stakeholders of the risks of cyber and fraud, offering effective user access options, and reinforcing the benefits of good security and reporting practices.

List of abbreviations

2FA	Two-Factor Authentication	PIN	Personal Identification Number
AUP	Acceptable Use Policy	PM	Password Managers
BEC	Business Email Compromise	RDP	Remote Desktop Protocol
BYOD	Bring Your Own Device	SERS	Suspicious Email Reporting Service
GDPR	General Data Protection Regulation	SFA	Single-Factor Authentication
ICO	Information Commissioner's Office	SIM	Subscriber Identity Module (commonly known in the format of a SIM card)
IT	Information Technology	SMS	Short Message Service (also known as Text Messaging Service)
ITSP	Information Technology Service Provider	SSO	Single Sign On
MFA	Multi-Factor Authentication	URL	Uniform Resource Locator (also known as internet/web address)
MSP	Managed Service Provider	USB	Universal Serial Bus (common forms include USB sticks, keys, drives, cables)
NCSC	National Cyber Security Centre	VPN	Virtual Private Network

Useful links and references

QBE templates

Strengthening user access security checklist [↗](#)

Fraud prevention guidance to share with your customers [↗](#)

Acceptable usage policy for ICT facilities [↗](#)

Cloud service provider considerations checklist [↗](#)

IT outsourcing assurance checklist [↗](#)

A broad suite of templates addressing various business risk issues are available and regularly added [here](#) [↗](#)

Tools for checking and reporting

Email and phone data breach checker [↗](#)

Reporting suspicious emails and phishing scams (UK) [↗](#)

Guidance for enabling MFA on popular services

Microsoft 365 [↗](#)

Microsoft 365 Privileged Accounts [↗](#)

Salesforce [↗](#)

Google [↗](#)

Zoom [↗](#)

LinkedIn [↗](#)

DocuSign [↗](#)

Common email accounts [↗](#)

Social media services [↗](#)

StopThinkConnect [↗](#) originates from the USA but includes several global services and websites with links advising users on how to activate MFA

Password strategies and MFA guidance

MFA for online services [↗](#)

Password administration for system owners [↗](#)

Password policy [↗](#)

Password manager guidance [↗](#)

Top tips for staying secure online [↗](#)

Effective implementation [↗](#)
(blog by Microsoft)

Cyber security insights

QBE Cyber [↗](#)

NCSC weekly threat reports [↗](#)

Storm Guidance [↗](#)

IASME [↗](#)

Acknowledgements

We thank Neil Hare-Brown at [STORM Guidance](#) for his review and contributions to this MFA guide.

The wealth of knowledge and guidance available on [ncsc.gov.uk](#), and insights from [IASME](#), have helped in creating this guide.

Contacts

Jaini Gudhka
Senior Risk Manager
QBE Risk Solutions
jaini.gudhka@uk.qbe.com

Deborah O’Riordan
Practice Leader
QBE Risk Solutions
deborah.oriordan@uk.qbe.com

QBE European Operations

30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
QBEurope.com

QBE European Operations is a trading name of QBE UK Limited, QBE Underwriting Limited and QBE Europe SA/NV. QBE UK Limited and QBE Underwriting Limited are both authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. QBE Europe SA/NV is authorised by the National Bank of Belgium under licence number 3093.

These publications have been produced by QBE UK Ltd (“QUK”). QUK is a member of the QBE Insurance Group (“QBE Group”). Readership of these documents does not create an insurer-client, or other business or legal relationship. These publications provide information and guidance to help you to understand and manage risk within your organisation. To the extent that any legal or regulatory references are made, this is not the same as legal advice.

These documents do not purport to provide a definitive statement of the law and are not intended to replace, nor may they be relied upon as a substitute for, specific legal or other professional advice. QUK has acted in good faith to provide accurate publications. However, QUK and the QBE Group do not make any warranties or representations of any kind about the contents of these publications, the accuracy or timeliness of their contents, or the information or explanations given. You are recommended to take your own steps to verify the information and to obtain legal or other professional advice as appropriate. For the avoidance of doubt, nothing in these publications disappplies or amends any duties owed by a client of QUK or any member of the QBE Group in connection with the formation of contracts of insurance, whether contractual in nature or by operation of applicable law.

QUK and the QBE Group have no obligation to update these documents or any information contained within them. To the fullest extent permitted by law, QUK and the QBE Group disclaim any responsibility or liability for any loss or damage suffered or cost incurred by you or by any other person arising out of or in connection with you or any other person’s reliance on these publications or on the information contained within them and for any omissions or inaccuracies.

QBE UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority and has its registered offices at 30 Fenchurch Street, London EC3M 3BD. You may use and adapt the contents of these publications for your own internal business purposes. Please acknowledge the source of these materials as follows: “Material taken from QBE Risk Solutions Template Documents and reproduced with QBE’s permission. © QBE UK Limited 2022. Not for further publication.”

© QBE UK Limited 2022.

