Multi-Factor Authentication from CSL

What is Multi-Factor Authentication (MFA)?

MFA is an authentication process that requires two methods to verify the identity of a user, strengthening the access security of a system.

This form of authentication protects against phishing, social engineering and password brute-force attacks. Moreover, it has the capability to secure logins from attackers exploiting weak or stolen credentials.

Why is MFA important?

MFA is a vital part of a *zero-trust security model*. In order to protect sensitive data, users requesting access to data must confirm they are who they say they are. MFA ensures protection against many security threats that target user passwords and accounts, such as those mentioned above.

If a remote attacker can tap into a computer via a user's internet connection, they could gain access to the user's password, along with a second form of authentication, if both are delivered over the same channel.

Remote attackers can't attempt to steal a user's identity (in order to gain unauthorised access to information stored in applications) without that individual's physical device.

By integrating MFA, attackers will be unable to access private accounts without possessing a user's physical device needed to complete the second factor.

What type of MFA does CSL use?

CSL uses time-factor authentication, sometimes referred to as Time-Based One Time Password (TOTP). The TOTP MFA method generates a code in time-based intervals that the user must enter in order to gain access. The passcode generated by the authenticators, or SMS/email, expires after a certain period and a new one will be generated the next time a user logs into their account. TOTP is part of the Open Authentication (OAUTH) security architecture.

CSL DualCom Ltd
Building 4, Croxley Park
Hatters Lane, Watford
WD18 8YF, United Kingdom

T +44 (0) 1895 474 474
E sales@csl-group.com
W www.csl-group.com
@CSLGroupLtd

Registered in England No. 03155883
CSL2024V1 13042021

CSL has implemented time-factor authentication with OTP, email and SMS. Here is a list of commonly used authenticators approved by CSL:

- Free OTP
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile
- IBM Security Verify

How does it work?

1. Enter your username and password on CSL Live as usual.
2. Receive a code from your Authenticator App, programme, email or SMS.
3. Enter the code in CSL Live.
4. You are now securely logged in.

Which industries use MFA?

End-point security is rapidly becoming an important concern for many industries. Regardless of which applications users are accessing, protecting credentials is paramount to ensuring the security of the wider business.

Retail

Now the nation's largest employing industry, remote attacks have become dominant in the sector and difficult to prevent. Additionally, security solutions are becoming increasingly important for retail as information technology adjusts to a perimeter-less environment. MFA provides peace of mind for companies within retail – allowing them to authenticate the identities of users accessing their networks through remote desktops and personal mobile devices.

Banking

Banks use MFA to protect against the many hacking attempts made on both their own internal and as their customer's systems. MFA has helped many large banks improve their resiliency against such attacks.

It has become paramount for all banks to know which users and devices are accessing their systems at any given time. MFA allows the Banking industry to secure remote devices and authenticate every login attempt.

Social Media

Social media platforms and agencies use MFA to protect the personal data of billions of users worldwide. Companies, such as Facebook, use an authentication to shield their developers from hacking attempts when working on the company's internal networks.

MFA also makes security easier for social media companies by simplifying the access process for developers. Cloud-based MFA solution protects developers, and users in turn, by eliminating the need for hardware and software installation.

Government

Current IT developments are challenging government agencies to implement rapid changes to their infrastructure, as they look to accommodate the shift to cloud and mobile.

MFA technology assists government agencies as they put forward zero-trust policies for the millions of users who need access.

FAQs

What if a user has lost or replaced their mobile device?

MFA relies on users to have a device with which to authenticate. If that smartphone or laptop is lost, stolen or replaced, users can self-enrol a new device by resetting their password via CSL Live. This feature can also be used if the user purchases a new phone or laptop to register MFA on their new device. Wherever a user is in the world and whatever technology they are using, their information will be secure.

Can I set up MFA on multiple devices?

Yes, you can set up MFA on multiple devices – MFA lets you link multiple devices to your account.

My chosen authenticator isn't on the list, is it OK to use?

CSL have tested and approved those listed in this document. We recommend that you use these authenticators in order to ensure reliability and accessibility of your CSL Live account.

I can't use an authenticator App, what are my other options?

We've developed backup options of SMS and email in case you cannot use an authenticator app for whatever reason. Simply select the SMS or email option when the system prompts you for a one-time code. All SMS/emails have an expiry time of 60 seconds.

How can I find out more?

For more information on MFA standard practices and guidelines please click on the links below.

National Cyber Security Centre

National Institute of Standards and Technology