egress

CJSM Multi-Factor Authentication

User Guidance

V1.0

Confidentiality statement

This document contains information confidential and proprietary to Egress Software Technologies. It shall not be disclosed in whole or part by the recipient to any third party or to any employees other than those who have a need to know such information. It shall not be duplicated or used by the recipient for any purpose other than to evaluate Egress Software Technologies products and services.

No part of this document may be reproduced, distributed, stored in a database or retrieval system, or transmitted in any form or by any means, without the exclusive and written permission of Egress Software Technologies. No liability is assumed for damages resulting from the use of the information contained herein.

Copyright notice

Contents

1 What is Multi-Factor Authentication (MFA)?

MFA is an additional layer of security that requires the user to provide two or more verification factors to gain access to a resource such as an application or online account. This means that should your password ever become compromised it would still not be possible to access your account due to the fact the malicious third-party would not (or should not) have access to this secondary piece of authentication information.

As part of our continued efforts to enhance the security of CJSM, Multi-Factor Authentication (MFA) has been enforced on your organisation. This step has been taken to ensure your CJSM accounts cannot be misused.

MFA is a widely accepted industry best practice for securing access to online digital services. It is advised by the National Cyber Security Centre, that MFA should be adopted in support of online account security. CJSM have implemented this feature to enhance account security and better protect our community.

2 Mobile MFA

Mobile MFA refers to the ability to generated timed single use authentication codes on a mobile device. These codes are generated and stored in an MFA application on your device.

2.1 Setting up your device for MFA

You can download authenticator apps on the iPhone and Android App Stores; just search for AUTHENTICATOR or TOTP.

Alternatively, if you contact your organisation's IT helpdesk, there might already be an approved application that you can download.

Once the authenticator app has been downloaded and installed on your mobile device you are ready to enrol in Mobile MFA.

2.2 Complete MFA enrolment

1. Upon your first login to CJSM, you will be directed to the MFA enrolment page.
2. Read the instructions in Step 1 to download a suitable authenticator application on your mobile device if not done already.
3. Launch the MFA application downloaded in step 1 and scan the QR code or copy the MFA secret code located on the CJSM MFA enrolment page.
4. Once the authenticator app is configured, it will generate a 6-digit code that refreshes every 30 seconds. To complete the setup, enter the 6-digit code from the app into the CJSM MFA enrolment page and press 'Submit'
5. A pop-up will be displayed advising you successfully enrolled and will then be automatically signed out of your account for this to take effect.

If you receive an error message saying the code is invalid, please:

- Ensure that you are entering the code with sufficient time remaining before it refreshes.
- Check that you do not have multiple CJSM entries in your authenticator app. If you do have multiple entries and are not sure which is valid, please delete the entries from your authenticator app, refresh the CJSM MFA enrolment page to generate a new QR code/MFA secret and follow the above process again.

3 Email MFA

For certain users, mobile MFA will not be an option. If you can't use mobile MFA, please select 'Email MFA' to have a time-based one-time password sent to your verified non-secure email address.

3.1 Issues receiving the MFA email

Email codes are single use, expire after 15 minutes and will always come from noreply@system.cjsm.net. If the email hasn't arrived in your inbox, please check your junk folder, and mark the email as safe.

We are aware of issues in the past where users with either a Hotmail or BT Internet domain have failed to receive emails from noreply@system.cjsm.net. If you hold one of these domains, and have failed to receive your email MFA code, you should add noreply@system.cjsm.net as a 'Safe Sender' within your respective email client and generate a fresh code.

3.2 Complete MFA enrolment

1. Upon your next login to CJSM, you will be directed to the MFA enrolment page. If you can't use an authenticator app, please select 'use email MFA instead' listed in Step 2.
2. Follow the instructions listed and click 'Send code' to have a six-digit code sent to your registered non-secure email address. If the email hasn't arrived in your inbox, please check your junk folder and mark the email as safe.
3. To complete the setup, enter the 6-digit code that you receive into the CJSM MFA enrolment page and press 'Submit'.
4. A pop-up will be displayed advising you successfully enrolled.

If you receive an error message saying the code is invalid, please:

- Ensure that you are entering the code within 15 minutes. If the code expires a new one will need to be generated. If multiple codes have been generated, the most recent will need to be used. The code will always consist of six numbers, please enter exactly as it is shown on the email.

Egress Software Technologies Ltd

Egress provides human layer security – helping users receive, manage and share sensitive data to meet compliance requirements and drive business productivity.

Egress' award-winning platform makes sure emails and files are delivered to the correct recipient, encrypts and protects sensitive data, and provides compliance auditing and reporting.

www.cjsm.net

cjsm.helpdesk@egress.com

0207 604 5598

@EgressSoftware