Enabling and Enforcing 2FA/MFA

To boost the security of an account in the Client Portal, it is strongly recommended that 2 Factor Authentication (2FA/MFA) is utilised by the end user. This article covers the different options available for how to implement 2FA on the Portal including:

- 1. Optional this is where the MM user chooses not to enforce the use of 2FA on the Portal but the end user can choose to enable it themselves
- 2. Enforced (case by case) this is where the MM user chooses to enforce the requirement for 2FA on an individual matter
- 3. Enforced (all new Matters) this is where the administrator has set that 2FA is enforced by default on all new matters created

1. Optional 2FA

By default, all end users of the Portal can enable 2FA on their account, regardless of whether it is enforced by the MM user. To enable 2FA via the Portal:

1.1. Open the Portal settings

To enable 2FA, after logging in, the Portal user needs to click the menu button in the top right corner and then select **Setup 2FA**



1.2. Confirm

The user will then be asked to confirm that they want to set up 2FA and that they will need to use an authentication app on their mobile device such as Google Authenticator. They need to click Continue in order to proceed with the setup.

Google Authenticator is but one option - the user can use other MFA authenticators such as Authy, Microsoft Authenticator, Lastpass Authenticator etc.

d	Setup Two-Factor Authentication
	To setup two-factor authentication you will be required to setup an authentication app (such as Google Authenticator) by following the steps provided. Do you wish to continue?
	Continue Cancel

1.3. Scan the QR

Next they will need to scan the displayed QR Code using their mobile device. This will generate a code on their Authenticator device.

If they can't scan the code, they can click the "Can't scan the QR code link" which will display the code as an alpha numeric code that can be typed/copied in to the Authenticator.

Two Factor Authentication Setup
Scan the QR code with your app
To help protect your account, please use an authenticator app (such as Google Authenticator) to scan this QR code and set up 2FA
Contact us if you need assistance
Can't scan the QR Code?
Enter the 6-digit code from your app
After scanning the QR code image, the app will display a 6-digit code that you can enter below
Verification Code
Help Cancel Verify

1.4. Enter the 6-Digit Code

The Authenticator app will now generate a 6 digit code which must be entered in to the Verification Code field. Then click **Verify.**

Enter the 6-digit code from your app									
After scorning the QR code in you	mage, the ap u can enter b	pp will display a 6-digit code that below							
	Verification Code								
Help	Cancel	Verify							

A The verification codes are time sensitive. They usually change every 30 seconds and may need to be re-entered if the timer has expired.

1.5. Completion

If successful, the user will be returned to the main portal page. Next time they login they will need to enter the 2FA code from the authenticator

Two Factor Authentication	
Complete logging in with your authenticator app	
Please enter 6 digit code provided by the authenticator app	
Please enter 6 digit code provided by the authenticator app Verification Code	

2. Enforced 2FA - Case by Case

If you want to ensure that a client is using 2FA on the Portal, you can enforce this requirement via the Portal Control Panel for the matter.

Note: You must be running version 8.8.3.4 or higher to have access to this functionality.

2.1. Open the Progress tab

First open the Matter and then go to the Progress tab and (assuming the Portal has been activated), click on the Portal button.

File Notes Acc	ounts Progress	Documents		@ 🗾 🖬 👸 🛃 Active					
:h: (Search Progress Item / Task, Required From) 🔹 Advanced 🚳 🔋 Portal 🗗 🗖									
em / Task		Requir d From	Due Date	Responsibility equested/ Commenced Done By					

2.2. Click Account Details

After the Portal Control Panel opens, click on the **Account Details** button and then select **MFA Requirement**



2.3. Set Enforce option

Now set the **Enforce MFA Requirement** slider to Yes to enforce 2FA on the Portal for this client.

2	Portal MFA Control - FLEMRO.21.0001	_ = X	
ia y	Enforce MFA Requirement		:d
	Reset MFA		
			c
		Close	
		Close	

You will be prompted to confirm. Click Yes to proceed.

Change MFA		×
You are about to change the	MFA for the clier	nt. Proceed?
	Yes	No

2.4. Complete

You can then click **Close** on the MFA Control. The next time the client logs in to the Portal, they will be required to set up 2FA before they can access the main page of their portal (see Step 1.3 above)



3. Enforce for All New Matters

If you want to have the MFA requirements enforced for all new matters, this can be set in the system preferences.

A Note that this setting does not affect existing matters with active Portals. To enforce MFA for these users you will need to use option 2 above.

3.1. Open System Preferences

In the top menu of MM, go to Tools > Administrative > Preferences

File Sched	ules Tools	Help	BETA Feedba	ck					
New I	Green Tem Arch	Setup Guid r Setup Guid plate Setup nive	le de) Guide	ew Fl	Filenotes	All FNs	Capture	Tasks	Accou
	Adm Bato Con Mat Scar Upd	Inistrative h Data Impo flict Check ter Manage Document late	ort ment		Detect/Fix Miss Preferences Reset Bank Rei Reset Client Di Reset Filenote Reset General Reset Passwor Reset User Log Reset User Log	sing Directorie conciliation an etail Locks Locks Ledger Lock d gin Count ase	ed Bank Staten	nent Locks	
					Restore Fileno Settings	tes			

3.2. Open Portal Preferences

After the System Preferences window opens, navigate to the Portal tab

Preferences												
Program-Leve	el Use	r Permissions	Report Pe	missions	User Pref	ferences	eLodge	e				
Accounts	Dept	Email Captu	ire Emails	Filenotes	Files	Firm	Letters	Logins	Misc	Open File	Portal	Question
Pertal Dat	-ile - D		D		5 40							
Fortal De	alis P	ortal Email 1	Portal Emai	2 Portal	Email 3	Portal Er	nail 4 S	SMS I	erms and	d Privacy		

3.3. Set Multi Factor Authentication Requirement

Now set the MFA Enforced by Default slider, located at the bottom of the window, to Yes

ss of the Ounce	O RMA				
	0				
hentication					
A enforced by default	on all new matters				
t	thentication A enforced by default	thentication A enforced by default on all new matters	A enforced by default on all new matters	thentication A enforced by default on all new matters	A enforced by default on all new matters

3.4. Save & Close

Now click **Save & Close** to finalise and save these changes. This will result in new matters by default having "Enforce MFA" enabled.

Default Contact Details Show the name, email address and phone number of the	IA () Manager () Clerk	
Multi Factor Authentication		
	Exit Without Saving Save & Exit	