



USER MANUAL

Multi Factor Authentication and Password Policy

Version 1.1

NetVision Corporation

Disclaimer...!

This manual is proprietary to NetVision Corporation and no ownership rights are hereby transferred. No part of the manual shall be used, reproduced, translated, converted, adapted, communicated or transmitted by any means, for any commercial purpose, including without limitation, sale, resale, license, rental or lease, without the prior express written consent of NetVision Corporation.

This manual is for illustration purpose only. The information contained within this document is solely advisory, and should not be substituted for legal, financial or other professional advice. You should not rely on this information as absolute.

NetVision Corporation does not make any representations, warranties or guarantees, express or implied, as to the accuracy or completeness of the manual. Users must be aware that updates and amendments will be made from time to time to the application subsequently followed by the manual. The Functionality of the system will also depend on the modules activated for the client and their configurations as per their requirements & specifications.

All data (Company Names / Vessel Names / Crew Names etc) displayed on various screen shots are merely for illustration purpose. This is not actual data pertaining to any company. Any similarity or resemblance is merely coincidental.

Contents

Multi Factor Authentication (MFA) for Compas Users	3
Admin set-up.....	3
MFA Configuration	4
How to set-up Second Factor Authentication.....	7
Multi Factor Authentication (MFA) for Crew Members	10
Admin set-up for Crew Members	10
MFA Configuration for Crew Members.....	11
How to set-up Second Factor Authentication for Crew Members	12
How to emulate CSS Mobile like a mobile application	17
Password Policy	20

Multi Factor Authentication (MFA) for Compas Users

Multi-factor authentication (MFA) is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. In Compas, generally the first piece of information is the username & password for login which is authenticated by Compas. Along with this, a second piece of evidence based on Time-Based One Time Password (TOTP) can be set-up in Compas to enable users to gain access only after both these factors are authenticated respectively.

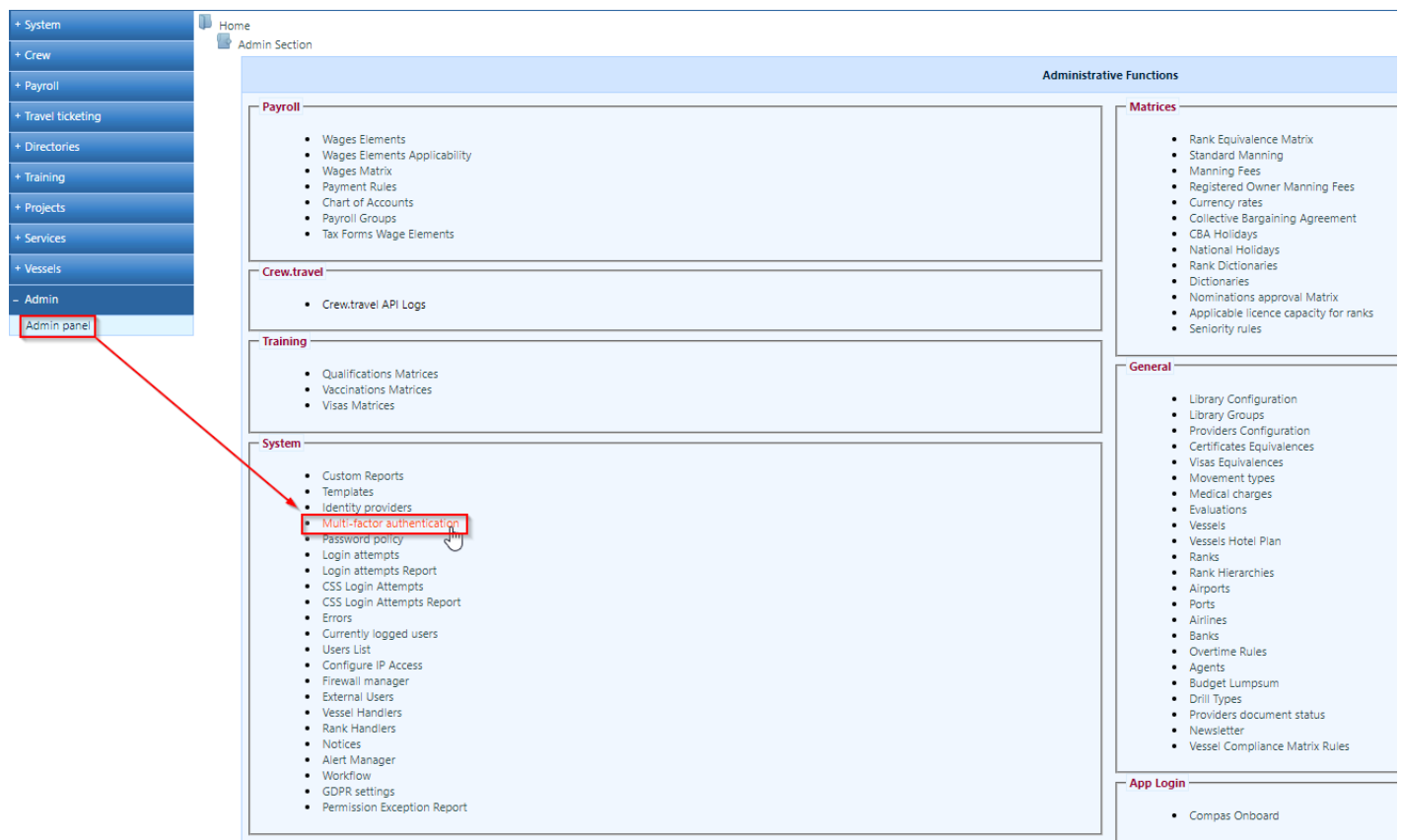
Clients already using another Identity Provider (IDP) such as Active Directory Federation Services (ADFS), can also setup MFA for their users. In this scenario, the first factor would be authenticated by the companies ADFS (Single Sign-On [SSO] if enabled) and then the user will be re-directed to a page where the second factor TOTP code will be required to be entered to gain access to Compas.

The following section provides details on how MFA can be set-up in Compas.

The functionality first needs to be enabled for clients and this can be enabled by NetVision upon request.

Admin set-up







Once the MFA functionality has been enabled, the set-up can be completed under Admin > System > Multi-factor Authentication.



The screenshot displays the Compas Admin interface. On the left is a vertical navigation menu with options: System, Crew, Payroll, Travel ticketing, Directories, Training, Projects, Services, Vessels, Admin, and Admin panel. The 'Admin panel' option is highlighted with a red box, and a red arrow points from it to the 'Multi-factor authentication' option in the 'System' section of the main content area. The main content area is titled 'Administrative Functions' and is divided into four sections: Payroll, Crew.travel, Training, and System. The 'System' section is expanded, showing a list of options including Custom Reports, Templates, Identity providers, Multi-factor authentication (highlighted with a red box), Password policy, Login attempts, Login attempts Report, CSS Login Attempts, CSS Login Attempts Report, Errors, Currently logged users, Users List, Configure IP Access, Firewall manager, External Users, Vessel Handlers, Rank Handlers, Notices, Alert Manager, Workflow, GDPR settings, and Permission Exception Report. On the right side of the main content area, there are two additional sections: 'Matrices' and 'General'. The 'Matrices' section lists various matrices and dictionaries, while the 'General' section lists various configuration options. At the bottom right, there is a section titled 'App Login' with a single option: Compas Onboard.

Multi-factor authentication

Show MFA for ☒ Office users ☐ Crew

	Display name	Description	Type	Enabled	Sort
	TOTP OFF U	For office users	TOTP	<input checked="" type="checkbox"/>	 
	TOTP OFF 2	For office users2	TOTP	<input checked="" type="checkbox"/>	 



On the set-up screen, the Add (+) / Edit (pencil) icons will take us to the below MFA configuration section.

MFA Configuration

Multi-factor authentication

Edit TOTP provider

Display name

Compas MFA

Description

Compas MFA

Enabled

☒

Hashing algo.

Sha1

Digits

6

Time window (s)

30

Time correction (s)

0

Assign identity providers

Available

Azure login

None but the selected

All except the selected

Selected

Compas

Add all >>

Add selected >

< Remove selected

<< Remove all

Assign users

Available

admin - NetVision

None but the selected

All except the selected

Selected

admin - NetVision

Add all >>

Add selected >

< Remove selected

<< Remove all

Save

Cancel

Here, the Display name & Description are general information displayed on the MFAs Login Screen. The configuration has to be Enabled (checked) to be applicable. The other 4 settings are pre-configured for best compatibility and can be left as default (as follows) as these are the settings that most authenticator applications can work with.

User Manual #UM202002.01

www.netvisioncorporation.com

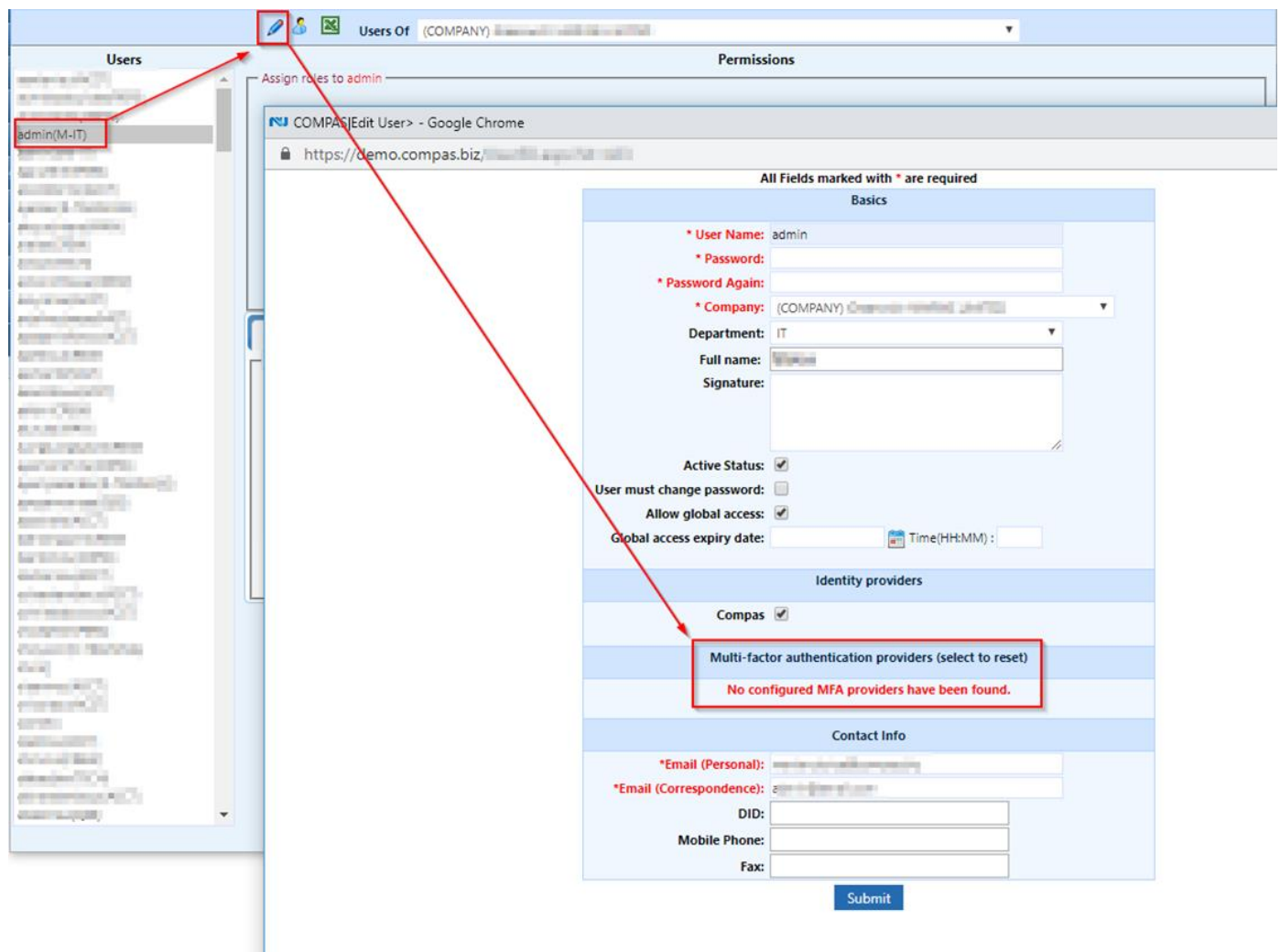
Page 4

- Hashing algo. = Sha1 (this is the Hashing Algorithm used for the TOTP generation)
- Digits = 6 (the length of the TOTP password to be generated for each access)
- Time window (s) = 30 (Lifetime of the generated codes)
- Time correction (s) = 0 (Offsets the local clock when it is considered for the generation of the TOTP code)

The “Assign identity providers” section and the “Assign users” section should be configured with the required users who will login to Compas using various IDPs selected according to company requirements. This section is designed similar to other eligibility configuration screens in Compas following an inclusive / exclusive selection design for ease of maintenance.

The above sample configuration screen (for reference only) would imply that users who login by using only Compas username & password (the list as per selected users) will require the second factor for authentication to gain access.

Once this configuration is saved, the next time the user logs-in into Compas, she / he will be required to set-up her / his second factor for authentication. The steps for same have been listed under the section “How to set-up Second Factor Authentication”. Until this is done, the users profile screen will look as follows.



Once the Second Factor Authentication set-up for the user has been completed, her / his user profile screen will look as follows.

The screenshot shows the Netvision user management interface. On the left, a list of users is shown, with 'admin(M-IT)' highlighted. A red box around the 'Edit User' icon (a person with a pencil) in the top navigation bar has a red arrow pointing to the 'Edit User' form. The form is titled 'COMPAS|Edit User - Google Chrome' and shows the URL 'https://demo.compas.biz'. The form has a section for 'Basics' with fields for User Name (admin), Password, Password Again, Company (COMPANY), Department (IT), Full name, and Signature. There are checkboxes for Active Status, User must change password, and Allow global access. Below this is a section for 'Identity providers' with a checkbox for 'Compas' and a section for 'Multi-factor authentication providers (select to reset)' which includes a checkbox for 'Compas MFA'. A red box highlights the 'Compas MFA' checkbox. The bottom section is 'Contact Info'.

If the user has lost her / his device providing the Second Factor Authentication, the Admin can simply check (select) the configured MFA provider (Compas MFA in the above sample) and save the user profile.

This will reset the Second Factor Authentication settings for the user and the user will be required to re-setup the same upon next login (using the same steps as prescribed in the section “How to set-up Second Factor Authentication”).

The Admin can also reset the Second Factor Authentication settings for the user from the below screen by simply selecting the user and clicking on the Reset button.

Multi-factor authentication

The screenshot shows the 'Multi-factor authentication' settings interface. At the top, there is a table with columns: Display name, Description, Type, Enabled, and Sort. The first row is 'Compas MFA' with a green background. A red box highlights the 'Reset user' icon (a person with a red X) and a red arrow points to the 'Reset MFA user settings for "Compas MFA"' dialog box. The dialog box has a 'User to reset' dropdown set to 'admin' and 'Reset' and 'Cancel' buttons. A red box highlights the 'Reset' button.

How to set-up Second Factor Authentication

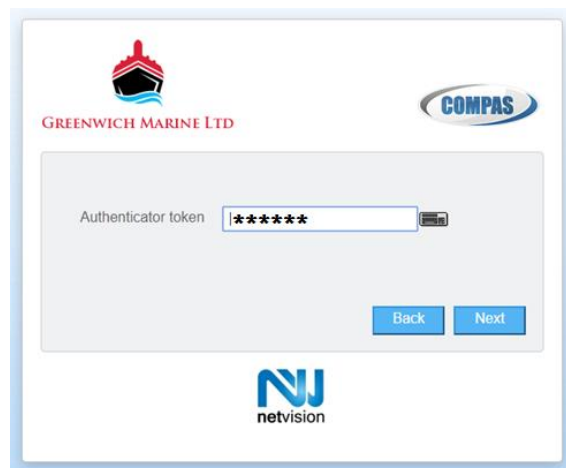
Once a user account has been configured to require a second factor authentication, the user will need to follow the below steps upon first log-in.

Firstly, the user will require a device which will provide the second factor authentication, the handiest device one can use would be a smartphone. On the smartphone, download an Authenticator application, the most common ones used are Google Authenticator or Microsoft Authenticator.




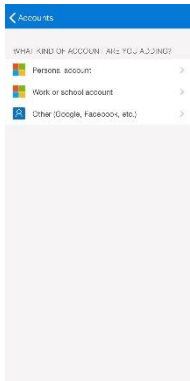


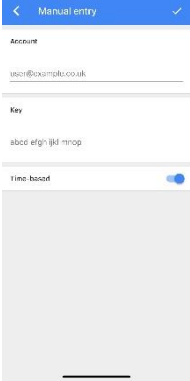
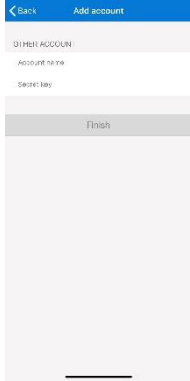
Now proceed to login into Compas. Once the initial credentials are verified, the system will provide a screen as below to complete the second factor authentication setup.

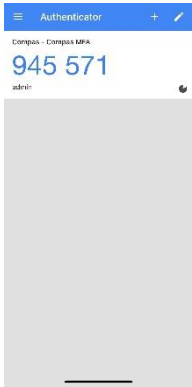
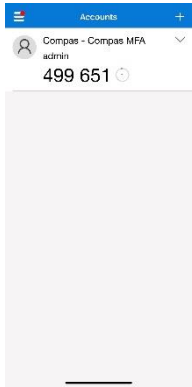




User can simply launch the Authenticator Application on the smartphone and scan the QR Code provided on the screen. Alternatively, user can also manually enter the manual configuration code provided. Once the Authenticator application is set-up, the code generated will be required to be entered as Authentication Token to complete the set-up. This code (regenerated as per time frequency configured) will also be required for every login into Compas.



Sample steps to add second factor authentication using Google Authenticator / Microsoft Authenticator on smartphone.

	Google Authenticator 	Microsoft Authenticator 
<p>Step 1: Add Account</p> <p>For Microsoft Authenticator: select Other (Google, Facebook etc.) type of account.</p>		
<p>Step 2: Scan the QR Code</p>		
<p>Alternate Step 2: Manual Entry of Authentication Set-up Code</p> <p>The Account could be entered as required (to be shown as on the main screen of the authenticator application to identify the Compas application).</p>		

<p>Step 3: The Authenticator application on your smartphone will now generate a new unique code every time the application is used. This code will be valid for 30 seconds (as per set-up done by your Admin) and will be required to be entered as Authentication Token to complete the set-up and also upon every login into Compas</p>		
<p>Step 4: Complete Authentication setup by entering the Code and clicking on Next.</p>		

Multi Factor Authentication (MFA) for Crew Members

Multi-factor authentication (MFA) is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. In Compas, generally the first piece of information is the username & password for login which is authenticated by Compas. Along with this, a second piece of evidence based on Time-Based One Time Password (TOTP) can be set-up in Compas to enable users to gain access only after both these factors are authenticated respectively.

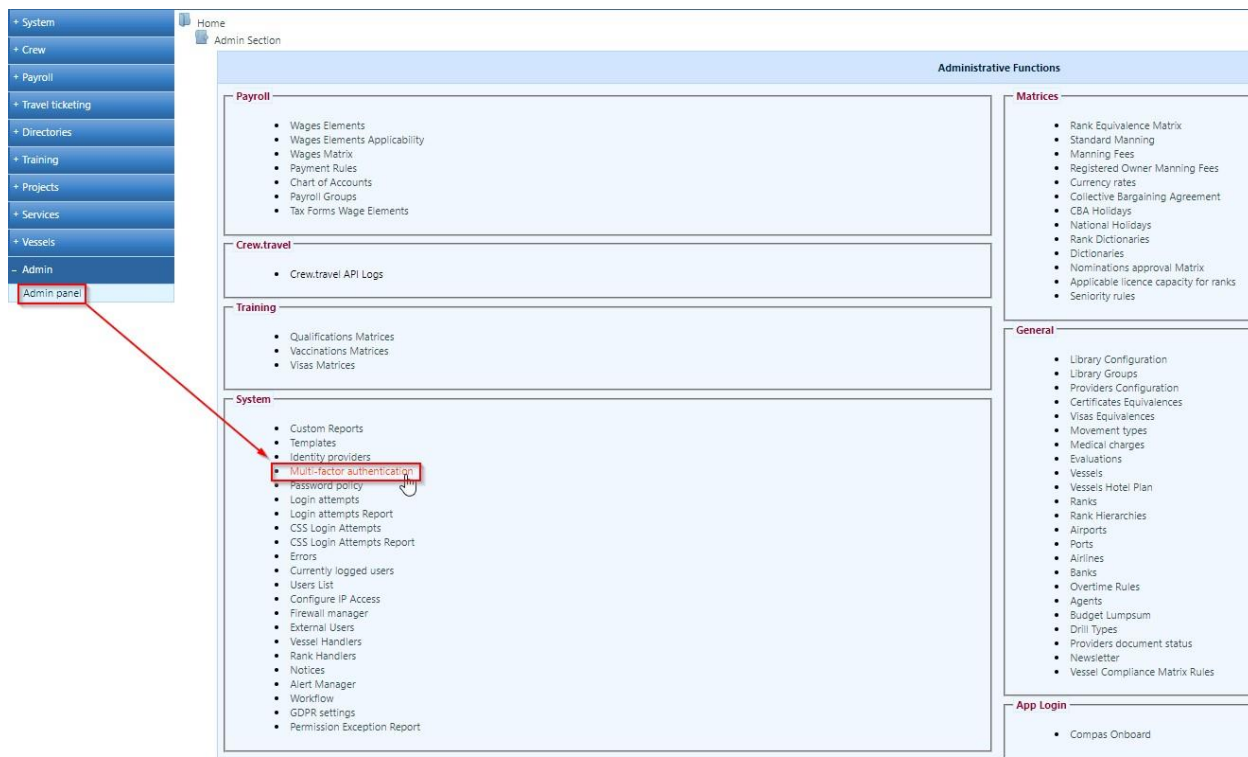
Clients already using another Identity Provider (IDP) such as Active Directory Federation Services (ADFS), can also setup MFA for their users. In this scenario, the first factor would be authenticated by the companies ADFS (Single Sign-On [SSO] if enabled) and then the user will be re-directed to a page where the second factor TOTP code will be required to be entered to gain access to Compas.

The following section provides details on how MFA can be set-up in Compas.

The functionality first needs to be enabled for clients and this can be enabled by NetVision upon request.





Admin set-up for Crew Members

Once the MFA functionality has been enabled, the set-up can be completed under Admin > System > Multifactor Authentication.



Multi-factor authentication

Show MFA for: ☐ Office users ☒ Crew

	Display name	Description	Type	Enabled	Sort
  	TOTP crew	TOTP crew	TOTP	<input checked="" type="checkbox"/>	

On the set-up screen, the Add (+) / Edit (pencil) icons will take us to the below MFA configuration section.

MFA Configuration for Crew Members

Multi-factor authentication

Edit TOTP provider for Crew

Display name: TOTP CREW

Description: MFA 1 CREW

Enabled: ☒

Hashing algo: Sha1

Digits: 6

Time window (s): 30

Time correction (s): 0

Assign users

None but the selected
All except the selected

Available

Crew Name - Surname

Add all >>

Add selected >

< Remove selected

<< Remove all

Selected

Save Cancel

Here, the Display name & Description are general information displayed on the MFAs Login Screen. The configuration has to be Enabled (checked) to be applicable. The other 4 settings are pre-configured for best compatibility and can be left as default (as follows) as these are the settings that most authenticator applications can work with.

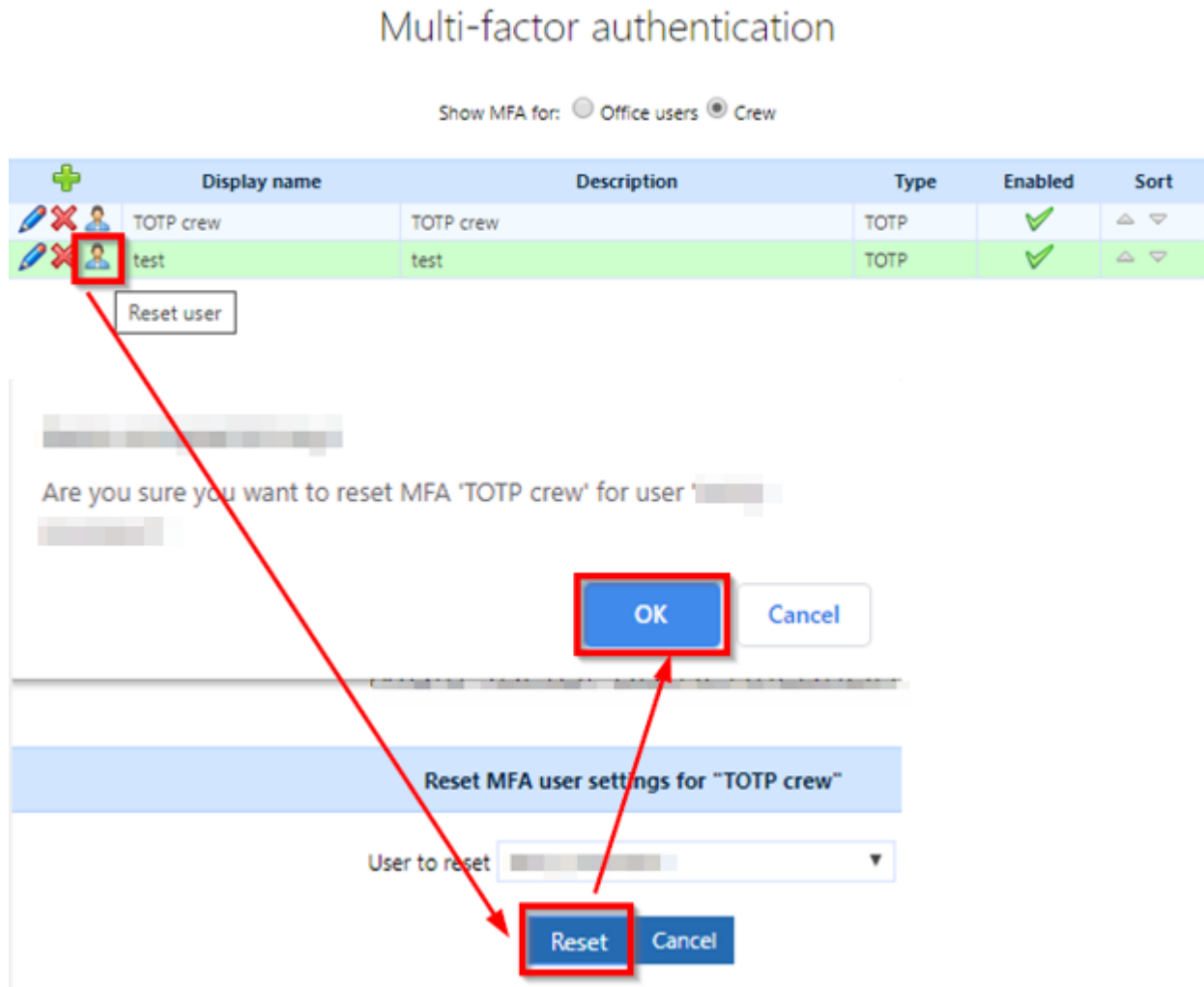
- Hashing algo. = Sha1 (this is the Hashing Algorithm used for the TOTP generation)
- Digits = 6 (the length of the TOTP password to be generated for each access)
- Time window (s) = 30 (Lifetime of the generated codes)
- Time correction (s) = 0 (Offsets the local clock when it is considered for the generation of the TOTP code)

The “Assign users” section should be configured with the required crew who will login to Compas Onboard / Crew Self Service using various IDPs selected according to company requirements. This section is designed similar to other eligibility configuration screens in Compas following an inclusive / exclusive selection design for ease of maintenance.

The above sample configuration screen (for reference only) would imply that crew members who login by using only Compas username & password (the list as per selected users) will require the second factor for authentication to gain access.

Once this configuration is saved, the next time the crew member logs-in into Compas, she / he will be required to set-up her / his second factor for authentication. The steps for same have been listed under the section “How to set-up Second Factor Authentication”.

If the crew member has lost the device providing the Second Factor Authentication, the Admin can reset the Second Factor Authentication settings for the crew member from the below screen by simply selecting the crew member and clicking on the Reset button.



This will reset the Second Factor Authentication settings for the crew member and she / he will be required to re-setup the same upon next login (using the same steps as prescribed in the section “How to set-up Second Factor Authentication”).

How to set-up Second Factor Authentication for Crew Members

Once a crew account has been configured to require a second factor authentication, the crew will need to follow the below steps upon first log-in.

Firstly, the crew will require a device which will provide the second factor authentication, the handiest device one can use would be a smartphone. On the smartphone, download an Authenticator application, the most common ones used are Google Authenticator or Microsoft Authenticator.

Now proceed to login into Compas OnBoard or Crew Self Service. The URLs for these applications would be as follows (as a sample).

Compas Onboard: demo.compas.biz/compasonboard

Crew Self Service (Web): demo.compas.biz

Crew Self Service (Mobile): demo.compas.biz/cssmobile

The actual URL for the client will be as per the clients Live Compas URL followed by “/compasonboard” or “/cssmobile” where applicable. For Crew Self Service Web version, no additional URL input is required, the system will automatically identify the person logging-in as a crew member and redirect the user to the appropriate application.

A crew member can login into Compas Onboard application only if the crew member is currently onboard a vessel.

A crew member can login into Crew Self Service only if the crew member is Active with the company. Once the initial credentials are verified, the system will provide a screen as below to complete the second factor authentication setup.



GREENWICH MARINE LTD

COMPAS

The initial configuration is required.

1. Open your authenticator App. [Need an App?](#)

2. Add an account and scan the QR code.

3. Enter the code generated by the App.

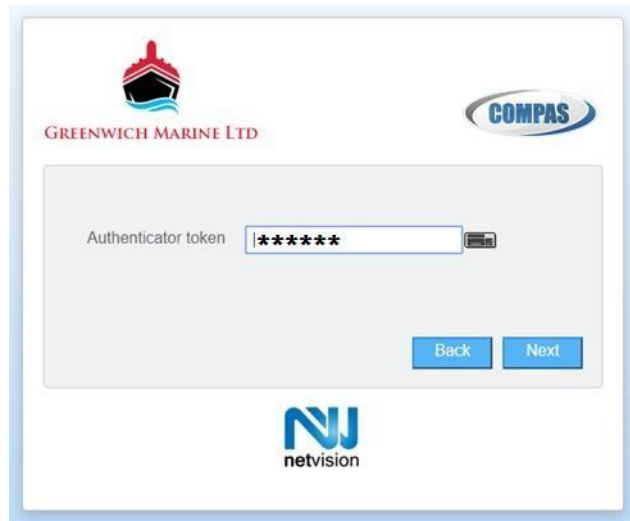
Your manual configuration code is [Sample Manual Configuration Code](#)

Authenticator token

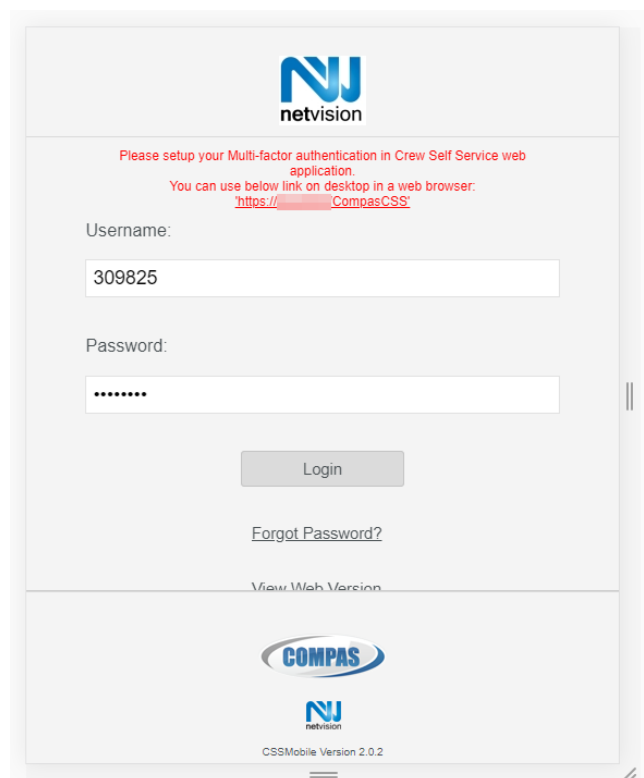
Back Next

netvision

Crew can simply launch the Authenticator Application on the smartphone and scan the QR Code on the screen provided. Alternatively, crew member can also manually enter the manual configuration code provided. Once the Authenticator application is set-up, the code generated will be required to be entered as Authentication Token to complete the set-up. This code (regenerated as per time frequency configured) will also be required for every login into Compas applications.



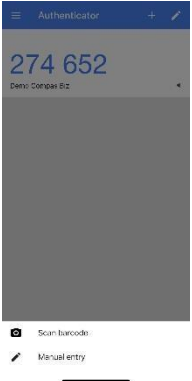



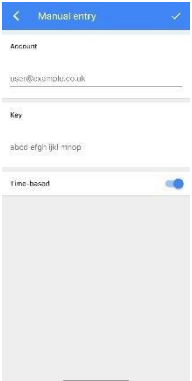



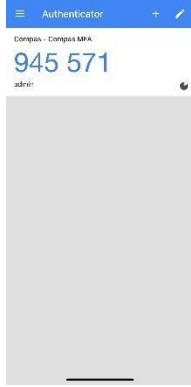
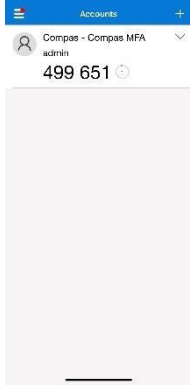


If the crew member intends to set-up the 2nd factor authentication via the Crew Self Service, then the crew member will be required to do so using the CSS Web version. Without this, the crew member will not be allowed to login on the CSS Mobile application. The crew member will get a prompt on the login screen as follows.



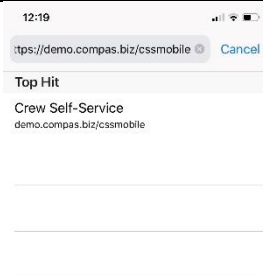
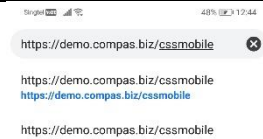

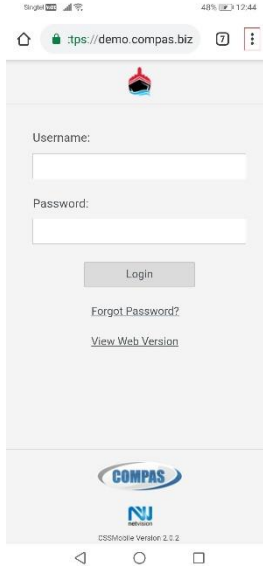
Once the configuration is made, crew can login in CSS mobile as normal and the 2nd factor authentication will be required to gain access.

Sample steps to add second factor authentication using Google Authenticator / Microsoft Authenticator on smartphone.

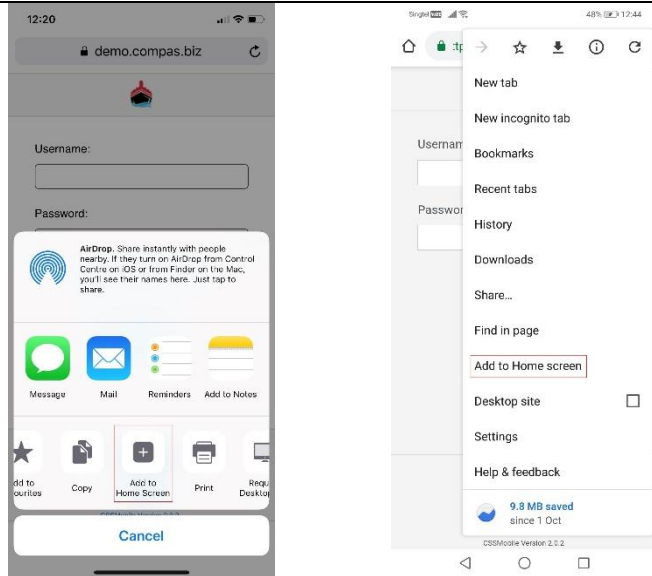
	Google Authenticator 	Microsoft Authenticator 
<p>Step 1: Add Account</p> <p>For Microsoft Authenticator: select Other (Google, Facebook etc.) type of account.</p>		
<p>Step 2: Scan the QR Code</p>		
<p>Alternate Step 2: Manual Entry of Authentication Set-up Code</p> <p>The Account could be entered as required (to be shown as on the main screen of the authenticator application to identify the Compas application).</p>		

<p>Step 3: The Authenticator application on your smartphone will now generate a new unique code every time the application is used. This code will be valid for 30 seconds (as per set-up done by your Admin) and will be required to be entered as Authentication Token to complete the set-up and also upon every login into Compas</p>		
<p>Step 4: Complete Authentication setup by entering the Code and clicking on Next.</p>		

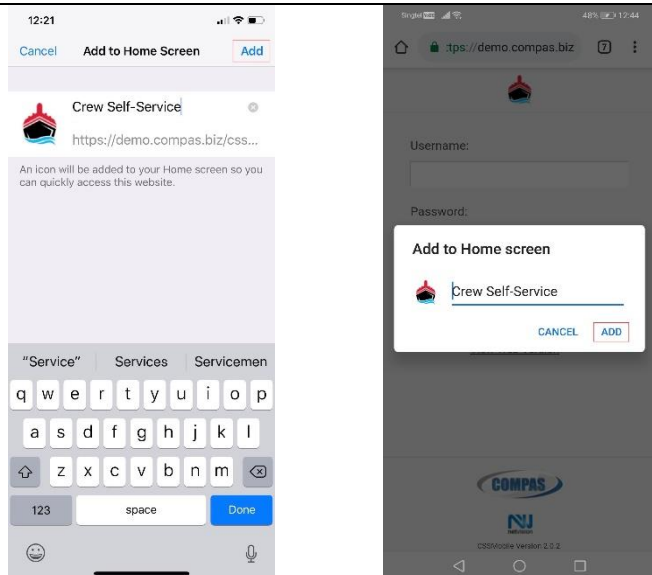
How to emulate CSS Mobile like a mobile application

	iOS	Android
<p>Step 1.</p> <ul style="list-style-type: none"> For mobile devices having iOS as operating system <p>Open Safari and enter Compas CSS Mobile URL (example https://demo.compas.biz/cssmobile)</p> <ul style="list-style-type: none"> For mobile devices having Android as operating system <p>Open Chrome and enter Compas CSS Mobile URL (example https://demo.compas.biz/cssmobile)</p>		
<p>Step 2. You will be directed to the Login screen</p> <p>Step 3.</p> <ul style="list-style-type: none"> For mobile devices having iOS as operating system <p>Use the Share icon on the tool bar</p> <ul style="list-style-type: none"> For mobile devices having Android as operating system <p>Use the Menu icon (3 vertical dots)</p>		

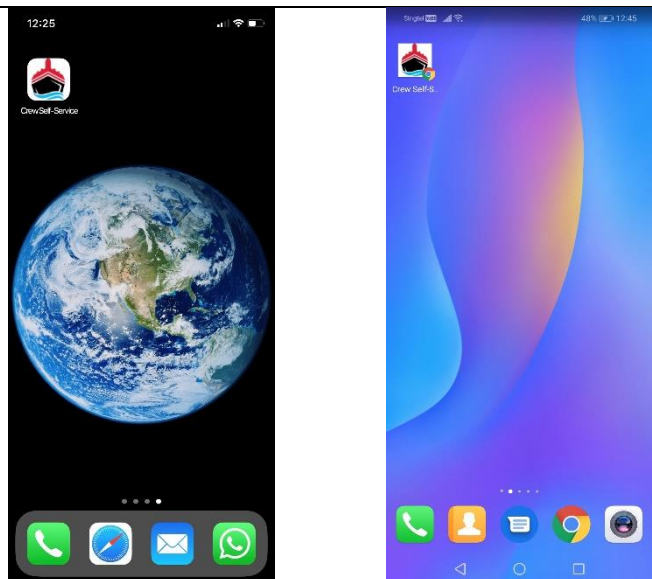
Step 4. On the menu options, chose Add to Home Screen



Step 5. Enter desired name for the home screen shortcut and tap on Add to save



Step 6. The shortcut is added to the home screen



Step 7. When used, the website is launched in full screen mode like an application

Password Policy

Password policy for Compas users/Crew Members can be maintained under Admin > System > Password policy. This policy will be applicable for all users, system wide.

Password Policy for Office Users

Home
Admin Section
Password policy

Password policy

Show policy for: ☒ Office users ☐ Crew

Setting	Value
Minimum password length:	4
Password expires after # days:	200
Disable account after # failed login attempts:	5
Enable users to request new passwords:	<input type="checkbox"/>
Disable password change requests after # failed attempts to activate new password:	3
Password must contain numbers:	<input type="checkbox"/>
Password must contain mixed upper/lower case:	<input type="checkbox"/>
Password must contain special characters:	<input type="checkbox"/>
Password cannot contain user name:	<input type="checkbox"/>
Number of unique passwords before an old password can be reused:	0

Reset Save

Password Policy for Crew

Home
Admin Section
Password policy

Password policy

Show policy for: ☐ Office users ☒ Crew

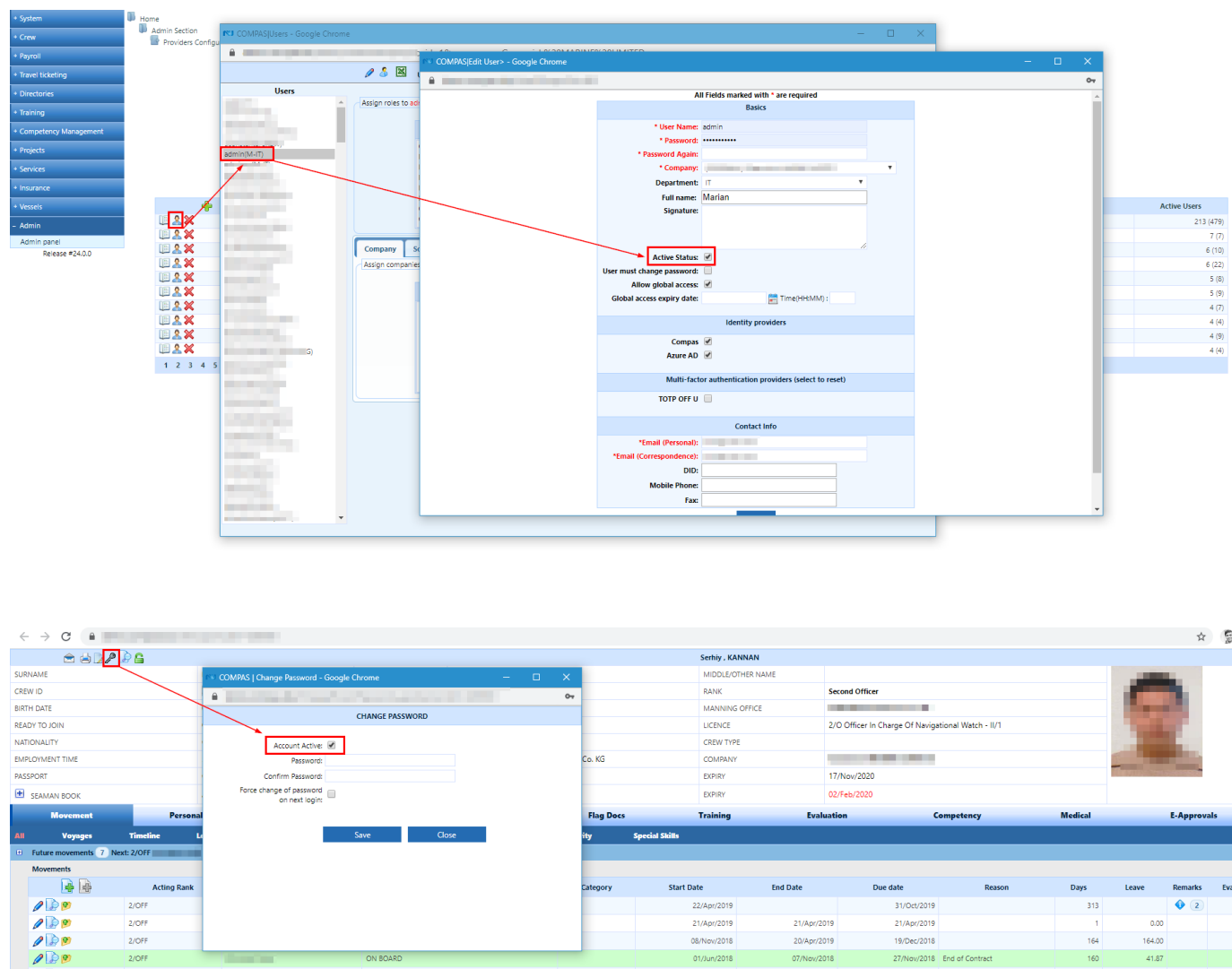
Setting	Value
Minimum password length:	1
Password expires after # days:	90
Disable account after # failed login attempts:	5
Enable users to request new passwords:	<input checked="" type="checkbox"/>
Disable password change requests after # failed attempts to activate new password:	10
Password must contain numbers:	<input type="checkbox"/>
Password must contain mixed upper/lower case:	<input type="checkbox"/>
Password must contain special characters:	<input type="checkbox"/>
Password cannot contain user name:	<input type="checkbox"/>
Number of unique passwords before an old password can be reused:	0

Reset Save

The Reset button will set all the parameters to system default values. User needs to ensure to Save the profile after making desired changes to any parameters.

The “Disable account after # failed attempts” will reactivate the account of the user / crew member and remove the “Active” check from the users / crew members account profile. This needs to be re-checked to activate the users / crew members account on the screens below. Here, the Admin can also set a new password for the user / crew member, and the new password can be communicated to the user / crew member to assist with login. The Admin user can also check (select) the “user must change password” /

“Force change of password on next login”. This will force the user / crew member to set a new password upon next login.



The image displays two screenshots from the COMPAS system interface. The top screenshot shows the 'Users' management screen with a list of users on the left and a detailed user profile on the right. A red box highlights the 'Active Status' checkbox, which is checked. A red arrow points from this checkbox to the 'CHANGE PASSWORD' dialog box in the bottom screenshot. The bottom screenshot shows the 'CHANGE PASSWORD' dialog box with a red box around the 'Account Active' checkbox, which is also checked. The dialog box includes fields for 'Password' and 'Confirm Password', and a checkbox for 'Force change of password on next login'. The background of the bottom screenshot shows a user profile for 'Serhiy, KANNAN' with various details and a table of movements.

For users / crew members using the “Forgot Password” utility, will be required to enter the “Personal” email address as maintained in the system to confirm their identity and upon successful validation, they will be sent the reset password link via email to their “Personal” email with instructions to reset their password.