TORQUE
SOFTWARE

LIGHTHOUSE AUTHENTICATION BEST PRACTICE

LIGHTHOUSE BY TORQUE SOFTWARE

LOGGING INTO LIGHTHOUSE

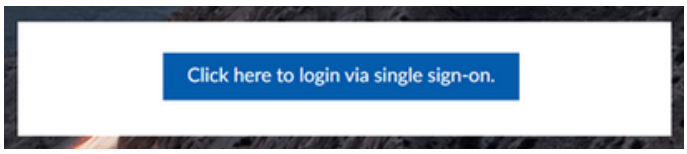
LOGGINING INTO LIGHTHOUSE

Lighthouse offers three different logon options:

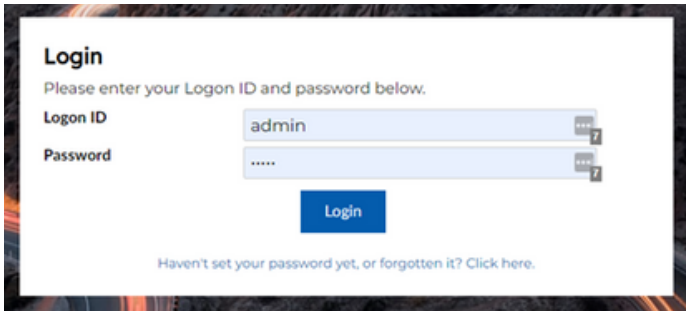
1. Single sign-on (SSO)
2. Entering you Logon ID & Password
3. A hybrid authentication which uses both SSO and Logon ID & Password.

Wherever possible, option 1 (SSO) should be used to log into Lighthouse as it uses enterprise level authentication including multi-factor login options. Logon ID & Password is not a best practice authentication method as it only uses a single factor login - we recommend disabling this login functionality where possible.

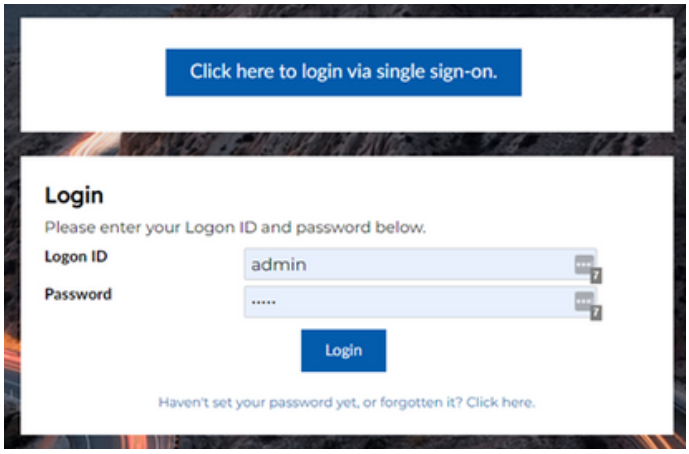
1



2



3



SINGLE SIGN-ON (SSO)

SSO

At Torque Software, we recommend using SSO where possible. SSO is securely configured for each organisation so staff can use their existing corporate login credentials to gain access to their Lighthouse instance.

If accessing Lighthouse through SSO, there are a few different ways this can be achieved. At a minimum, Lighthouse users can gain SSO access via the following platforms:

1. AZURE AD

Azure AD SSO automatically signs users into their Lighthouse Instance via their corporate login details, regardless of their location.

If you are an existing Lighthouse User with Azure AD enabled, you can access your Lighthouse instance here: https://azuresso.lighthouse.torque.software/Login

2. VANGUARD

VANguard is another secure SSO login option. Developed by the Department of Industry, Science, Energy & resources, VANguard assists Australian, state and local governments to deploy cost effective and secure authentication solutions when opting to log in via SSO.

TORQUE OPTIONS

At Torque Software, we can offer cross-over options, such as a mix of proprietary, VANguard, Azure AD SSO and logon ID & password all at the same time. However, for best practice, we recommend that organisations use Azure AD for SSO.

Click here to login via single sign-on.

SSO NOT POSSIBLE?

LOGGING INTO LIGHTHOUSE

Where SSO is not possible in your organisation, we strongly recommend reviewing the security settings in your Lighthouse instance to maximise protection.

To access the security settings in Lighthouse, follow these steps:

1. Log into Lighthouse
2. Select the 'cog icon'
3. Select 'Administration'
4. Select 'System'
5. Select the 'Security' tab.

For recommendations about which settings to select/enable in Lighthouse, see page 5 which outlines this information. We have also included some 'Torque Tips' in the boxes below. Please keep these in mind when updating your system settings.

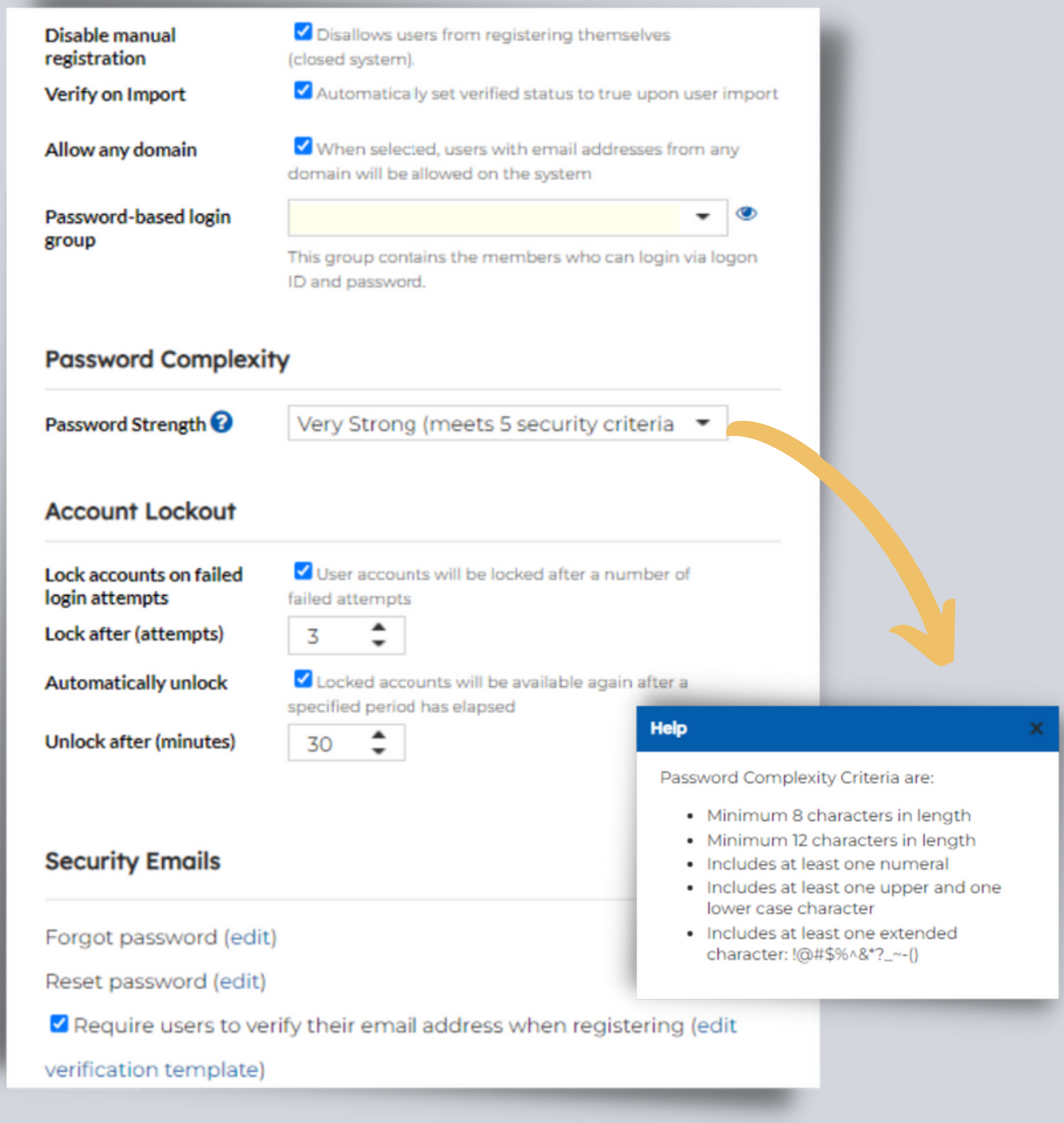
TORQUE TIPS

1. Have a high level of password strength (refer to the screenshot below regarding 'password strength criteria').

2. Select accounts to lock after the smallest number of attempts you deem acceptable. If accounts do lock, select to either unlock accounts manually or, if you'd like to let accounts automatically unlock, set the unlock period to be as long as acceptable (e.g. 30 minutes).

3. If using SSO in conjunction with Logon ID & Password, best practice is to put all users who can't use SSO into a group and then nominate that group in the 'Password-based login group' setting. This will ensure all users not in this group can only login via SSO, increasing security.

PASSWORD SECURITY SETTINGS



1300 795 581

6/43 Comrie Street
Wanniassa ACT 2903

info@torquesoftware.com.au

TORQUE
SOFTWARE