AXLR8 Multifactor Authentication for Public sector Request Tracker

This document explains the designs AXLR8 are using for increasing user authentication demands in the public sector systems. Similar processes are used in some commercial systems depending upon the user population and sensitivity of the data. This can be at login or even individual transaction level – for example biometric check in for remote workers.

Contents

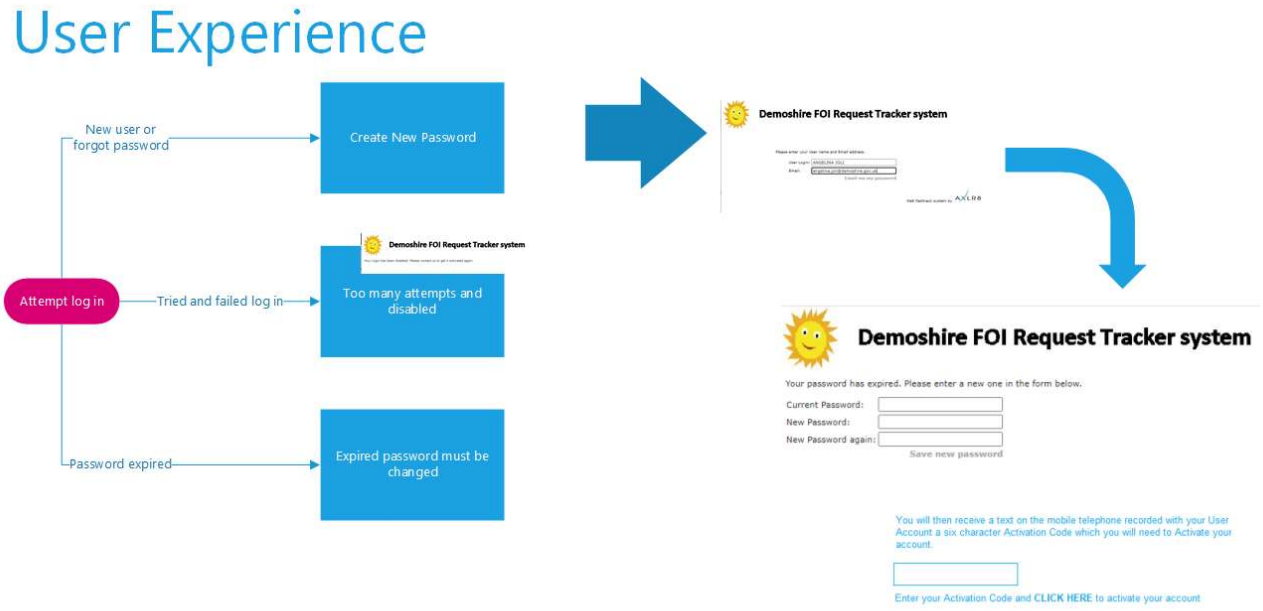
Version	Author	date	Change
1.0	ERM	02/03/2020	AXLR8s:34491
2.0	ERM	02/04/2022	AXLR8s:37270

1 Requirement

At any point a user may become untrusted for the system. At that point their account is disabled. In order to continue, they may (or may not) be forced to reset their password but must authenticate by a second or other method. Usually, this means using another device such as their phone. The goals include The goal is to reauthenticate the user and shut down access to a password that has somehow become known to another person.

1. **Password times out**
   The period is client dependent. Common examples are after, 60, 90, 180 or 360 days or not at all.
2. **Too many password attempts**
   Again, this varies between organisations but is typically set somewhere between 3 and 15 depending upon the application sensitvity.
3. **Passage of time between logins**
   After X days (X to be directed by the client) from the last log in, they must use 2FA
4. **Access from a new machine/ location**
   This happens when the user attempts access when
   a. there is no cookie present
   b. accessing from a new IP address compared to last time (not withstanding that users may be restricted to certain IP addresses)
5. **User wishes to create a new or reset the password**.
   This may be because they have forgotten the password or they believe it is compromised or simply feel they need to change it more frequently than demanded by the system. In this case the account is disabled after they have received a temporary password and have used it to gain access to create, and have created a new password.

The User experience process is shown here.



2 Definitions

Most meanings are self-explanatory but it is important to distinguish between user accounts and contact (client, applicant) accounts. In this paper we are specifically referring to user accounts. A similar system may be purchased for client accounts if you use a client portal or file download facility.

Word	Meaning
User	HQ or office admin person working for the AXLR8 Client or a member of field or mobile staff working for the client with an employee or subcontractor log in. They will have been vetted and employed under some form of contract with your business. They will be granted different rights to data by a Super User
Joint User	We discourage this practice but it is common practice in some organisations to allow more than one user to sign in to the same account. For example, two people might sign into an account called "Traffic Service Team". This could be for a number of reasons. It could be a job share or a team who share out the tasks. It is often associated with a shared email address.
Super User	A *Super User* is someone who has been allocated User Admin rights and hence has the highest level of access to the system. This is by definition. They can grant (or revoke) any rights to any *User* including themselves.
Contact	This refers to an applicant, client or other person who has some limited customer or pre-employment access. They may have agreed to little more than an initial acceptance that they have read and understood your privacy policy as it applies to information you may request from them and perhaps some statement of limitations of liability for mistakes in content. Examples include clients who wish to see data you have collected on their behalf or job applicants who have registered to complete an application journey.
Robot	Certain facilities are automated or may be anonymous ad hence need an automated process to provide them. In this case, you may see login from "WEBENTRY" "TRIGGERSENDER" or other robotic users in the audit logs along with any changes they have made in the system. Even though their user accounts are disabled, they could be used by a hacker somehow and we are looking at some way a human could identify that any system access they have is indeed that user and not some other person using their account.

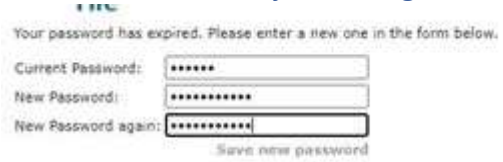
3 User Experience

The trade-off between security and operational efficiency and costs is important to review as security practice evolves to meet new risks.
As listed above, the user may have their account disabled and have to authenticate themselves for specific reasons. For very high security applications we could extend this to every login. In some commercial applications face recordings and biometric data must be taken (for example to ensure proof of presence).

3.1 User logging in and has disabled their account from failed login attempts.

After they pass the 2FA challenge, they get a link to go back to the login page so they can try to login again.

3.2 User who has just changed their password.



On updating the password.

If you have the Text SMS Option installed at you authority, then the number will be sent to the mobile of the user which is stored on the
After they pass the 2FA challenge, it will auto log them in.

3.3 User who is challenged for a second form of authentication for some other reason

You can set the challenge to require the user to authenticate themselves in some other way when they do know their password and do not need to reset it. Your system I just checking occasionally.

3.3.1 New access point (machine or location)

A common practice is to detect a suspicious change of access and ask the user to authenticate by some other method just in case.

Log in from a new machine	Text, call, other authentication methods	This could be by MAC address detection or a cookie with a certificate on the "Usual" machine.
Log in from a new location	Text, call, other authentication methods	IP address (but we know these can be spoofed
Not on VPN?	See above.	May be prevented altogether

3.3.2 Time forces a 2FA

on a time out so that users have to use a second or third form of authentication every 30 or 90 days. This period of time (referred to as X days because you choose what X is) is not the same as the forced password reset time.

3.3.3 Every login 2FA

You can ask them to authenticate themselves by telephone or text or some other form of authentication, every time they sign in.
This might be the case if the users are accessing highly secure information or if they are a Super User, for example.

In all the above cases, the manual method of authentication is as secure as the SMS (AKA Text messages) form of 2FA. However, the manual effort on your part will be reduced when it is automated via SMS. The manual 2FA and automatic 2FA are compared below in section 4.3.

4 Admin Process

This manual method is cost effective if you only have a few users in your organisation. It is included free so long as we do not have to create unusual bespoke custom user deactivation paths.
This version is the "ask us" provider – i.e. the person who is trying to login has to contact a Super User to get the activation code. If you have been granted Super User status, then when they contact you (probably telephone), you can discuss how they prove that they are who they say they are.

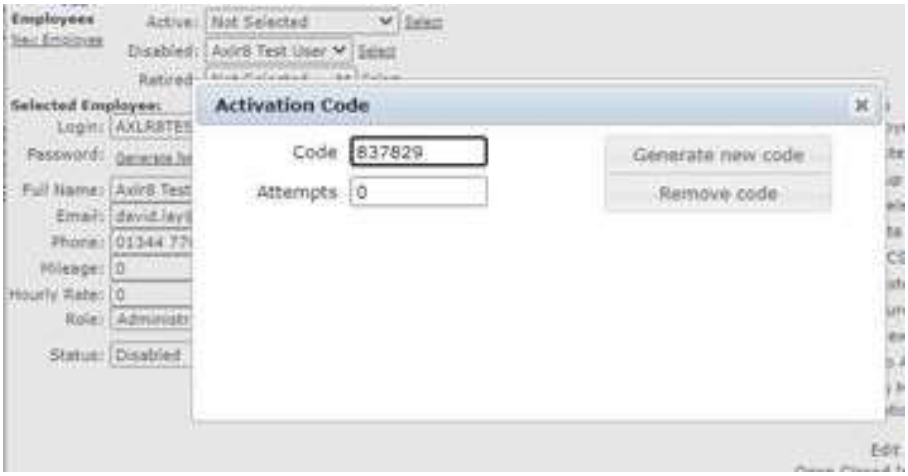
On the right is the *User Admin* screen for seeing what the activation code is, generating a new one and removing the code if needed.

A *Super User* may check the User's account and re-enable it on the telephone or may send them the six-character code.

They also have the ability to reset the password or disable the account fully if it is a rogue ex-employee.

Lastly, they can check the correct cell phone number is in the "Phone" field.

User admin screen for seeing what the activation code is, generating a new one and removing the code if needed.
The Admin is able to create a new code if the old one has expired.
The user can now be given this code.



4.1 Automatic Authentication with no human intervention

The method is familiar to many of us. Instead of calling to obtain to ask for reactivation, a random code (in our case six characters, alpha numeric) is generated and sent by SMS message to the user.

4.2 Costs of implementation using SMS messages

If the cost of implementing this is justified by the amount of manual work your team needs to do in order to deal with deactivated user accounts, then we can automate the system at a small price around £475 plus

VAT for the first year and £145 per year, thereafter. This assumes a reasonable use policy of no more than 1000 SMS text credits used.
AXLR8 customise a message and create a trigger to deal with different situations, and the cost of setting up an integration with the AXLR8 SMS buyers' club account. If your organisation already has a chosen text supplier, we can integrate that but it requires the Managed Account described in the text pricing below.

4.3 Manual authentication compared to automatic authentication

If your re-activations are infrequent then do not bother. Let them call up the office. This has the advantage that an ex-employee where the employer has forgotten to or has not fully deactivated their account, may get back into the system. At least if they call the office, the Super User or member of staff taking the message for the Super User will have a chance of picking this up. Alternatively, they will realise they have been caught and hang up the call.
If you have several hundred field staff or clients, then you should consider automation.
https://www.axlr8.com/Files/AXLR8SMSPricing2020.pdf
https://www.axlr8.com/Files/AXLR8_SMS_Messaging_ManualV3.1.pdf
NB a text credit is roughly a 160 char text. So, 200 chars would be two credits. For the purposes of MFA, you should use no more than one credit per text and hopefully only 6 or 8 chars.

4.4 SMS compared to other forms of authentication

There are other methods available as options in addition to the manual and SMS methods mentioned above. Examples include:

- Google authenticate (expected 2023
- AXLR8 Chat (expected 2023)

However, you have to assess that the vast majority of your user base carries a smart phone. SMS (text) messaging is still more reliable and commonplace – and often faster.
The exception would be if your user population have internet but no mobile phone signal which happens in some WFH organisations in more rural areas.
However, they will probably have a land line and a text can be sent to most landlines and will be read by an automated speaker.