When users cannot log in: Instructions for AXLR8 Super Users.

Password security is becoming stronger. Therefore, some of your users will face barriers to accessing your systems including the one you have purchased from AXLR8.

Quick fixes

The quick solutions are generally (in order of the frequency we meet them):

User behaviour	**What to do about it**
Forgot password (includes typing the wrong case e.g. "ABCD1234" instead of "AbCd1234")	They should go through the password reset process. It sends them a temporary login and instructions on how to create a new secure password. A Super User can also kick off this password reset process.
Too many false login attempts	The users account will be disabled. A Super User needs to go to their User Admin area, select that user and take their account from the "disabled" to the "active" list. Don't forget to check they are still legitimate users!
Not received password reset email	The email with the reset password instructions has probably gone into their spam folder.* The user must check their spam folder, retrieve the mail and follow the instructions.
User forgot login name (includes typing it wrong such as "JOHN SMITH" when it is actually "JOHNSMITH" without a space)	They can use the user name reminder process. You can send them the correct user name and explain the importance of typing it exactly.

**If all go to spam, then your DKIM and SPF records a may not be set up correctly and you may need to ask assistance of whoever manages your DNS. AXLR8 can re-supply the correct values for these.*

The above should solve it (and probably similar problems from any system you may use from any supplier). If not, your Super User should follow the steps on the next page with your user (client, field staff, etc.) in order to resolve the matter.

We are happy to help your Super User but cannot support high volumes of end users directly.

Diagnosing Login problems

Sometimes Users cannot log in to a portal and you will need to run through these steps to diagnose why before contacting AXLR8.

Login problems rare for most AXLR8 clients. For example, we have clients with many thousands of active users who have no issues for several years. After a new app launch a very high-volume client may have perhaps two or three such problems in a month.

Try these steps:

1. Do they have the right link or app?
    a. Ask them what they are attempting to log into and make sure it is the intended web page or that they have downloaded the correct app to their device. Sometimes users are not even on the right website so you need to eliminate that right up front.
    b. Once you have eliminated this possibility, jump to step 2.
    c. Occasionally, you may be told by a user that they are on the right page but they may have made a mistake so check they see what you expect if you suspect this rather than get to further steps down the process and have to come back and check this again! In some rare cases, you may need them to read or copy the URL or send you a screenshot to be sure.
2. Have they made so many log in attempts that they have been locked out?
    a. Ask them if that error message shows on their log in screen. The number of login attempts varies from system to system. 10 is a common number in a commercial environment but some government clients allow only three.
    b. Check their User Admin (or ask a Super User to do so if you do not have Super User authority). If they are a valid user, set them back to the live users list.
    c. Make sure there is not a reason (retired, resigned, etc.) that they should not log in.
    d. Find them in the list of disabled users and re-enable their account
3. Do they have the right username and password?
    a. You (or a Super User) can tell them the username. Make sure it is exactly correct and they are typing it correctly. Perhaps email it to them so they can copy and paste it. Common errors include.
        i. Adding a space or removing a required space,
        ii. Typing s similar looking character (such as the number 1 instead of the letters “l” or “I” (lower case L, or upper case i) or a zero instead of the letter “O”).
    b. Ask them to reset their password or send them a password reset email from within User Admin (if you have authority, else, ask someone who is a Super User for your company).
    c. Check if there are any characters in the user name or password that may have come from a foreign keyboard. It is rare for this to be a problem as we have dealt with many over the years and written code to accept them.
4. If they (or you) have initiated the password reset mechanism then they should receive an email. If they do not then:

   a. Is the password reset email stuck in their spam folder? (Obviously they should check, retrieve it and follow through with the rest instructions)
   b. Has it bounced back (it should come from an email which you can receive replies upon so that you can specifically check those email addresses are valid? NB if you do not deal with bounced emails, then your business domain may be banned as a sender which can lead to blocked receipt for many partner email services. (Don't let this happen as it is time consuming for you to get your email domain taken off the "naughty list".)
   c. Is their User Admin email present and correct in order that the email can go to them with the rest of the instructions?

5. If they have received the email for the password reset, and it still does not allow them to create a new password, you may
   a. have they accurately typed or copied and pasted the temporary password? Common typographical errors include copying and pasting a leading or following space with the temporary rest password.
   b. Have they reset the password and then been distracted and forgotten it or mistyped it once again? This is especially easy to do on a smartphone! In this case they should go through the rest password process again and make a note of the password on their phone. PC so they have an accurate record.
6. If you have got his far and they still cannot log in, you have several options
   a. We find that users, with the best of intentions provide information that is inaccurate sometimes. (For example, they cannot actually see the font on their 'phone or are frustrated by technology generally or too busy to take the care required to go through what can sometimes be a trying security procedure.)
      i. Go back through the previous steps with them checking more thoroughly. For example, you may have trusted them when they said they had the right login at step 1 but you could ask them what it was and maybe get a screenshot. Commonly, people think they are on the "login" page but they message actually says "password reset".
   b. If you are a Super User, you could, with their permission, substitute your email for theirs in User Admin and go through the password reset process. Then you can see if you can log in. Then you can make sure it is their issue and not a bug in your system (which is unlikely as most others will have successfully logged in).
      i. Obviously, don't forget to reverse the email back to theirs afterwards (I tend to copy and paste it onto a Notepad temporarily so I can paste it back later and paste it into an email to check they actually receive that email).
      ii. Also, make sure you do not go deeper into their account dialogues and agree to terms and conditions or anything like that. Logging in should be enough. Remember the login will be audited

Any other issues

If the above fails, call AXLR8 and we will run through the process with you and see if there is some, as yet unforeseen, bug or system problem. We will need lots of detail like the phone model if it is an app and any operating system, browser version or other relevant platform / environment settings

Future Security features

Security is only going to be increased. We try to make it as simple for your end users as possible.

These notes will be updated for 2FA (two forms of authentication). When your system is updated to work with 2FA, you will get a pass code which will allow you to activate your newly created password. The way 2FA works is to send this via another medium as a double check you are receiving it and not just someone who has access to one of your accounts. You will almost certainly be familiar with this but your users may not be so you will need to launch it in a planned way.

The 2FA process will include a pass code sent to a separate device or via a separate mechanism such as text to your phone or Google Authenticate will mean that, following your reset password there will message asking for the code. You will find that it is accessible on that second medium (for example you may have received a text with it.)