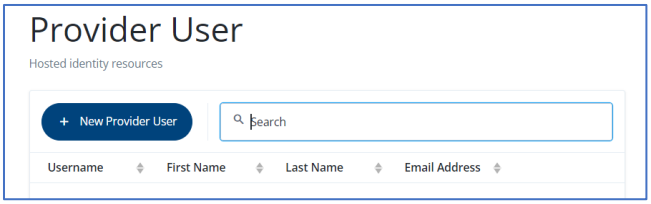
ProviderCONNECT
User Maintenance Guide
For Local Administrators (LA)

Local administrators (LAs) should maintain their back-up local administrators, any additional LAs, and general users (GUs) they have set up in the ProviderCONNECT Portal Dashboard. The LA will register additional GUs of the system only for users who have a responsibility to be in the portal. To access Local Administrator responsibilities and user set up (welcome packet), please click LOCAL ADMINISTRATOR AND WELCOME PACKET. **When members of the organization no longer need access to the portal, the LA must delete that user account**.

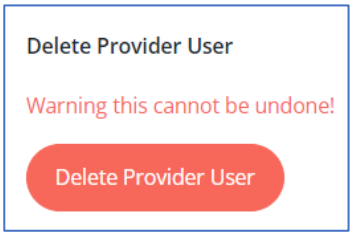
Deleting a General User from the System

Login to the Portal Dashboard and follow these steps:

1. Click on the left navigation bar marked "Provider User."
2. Enter the user's first name in the search bar and press ENTER.



3. Click on the username in the list you wish to delete. Details of that user will populate. Read the details to ensure this is the user you wish to delete.
4. At the bottom of the screen, click on the "Delete Provider User" button. You will be asked, "Are you sure you want to delete this provider user?"
5. Click "Delete" to confirm and execute the action.

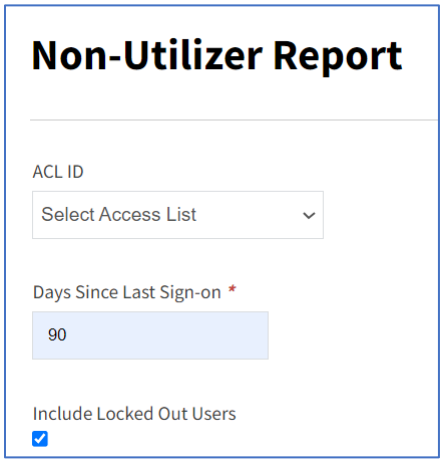


Revalidation

Users are regulated by an automated system that will prompt them to revalidate their login after 90 days for all users. When they attempt to login after being inactive for 90+ days, the system will prompt them to reset their password.

User Auditing

The purpose of auditing users is to ensure that all inactive user accounts have been appropriately deleted or reinstated. Local Administrators should perform an audit of their users every 90 days, or more often. To do this, Partners has provided your organization with a "Non-Utilizer Report" in ProviderCONNECT under the Office Management category in "Reports." Once the report name is selected, use the dropdown list under ACL ID and select your organization. Fill in "Days Since Last Sign-on" and check "Include Locked Out Users."



The query will return the report to your screen to view or download. Once you leave the screen, you can find the report again in your Document Manager (this may take up to 30 minutes). When the report is available, go through each inactive user and determine:

a. If the user is no longer with the practice, then immediately delete the account as described above.
b. If the user is still with the practice but hasn't logged in from the time the account was opened and 90 days has passed, determine if that user really needs the account – delete the account if necessary. Users should only be given accounts with the need to be in the portal.
c. If the user is still with the practice and it has determined that their account is still needed, that user will need to reset their password if 90 days has passed from their last login.

Provisioning

All users are granted general user permissions once they are in the portal. Local administrators have user maintenance privileges that can be found in the Portal Dashboard, allowing them to add or delete users and assign back-up local administrators.