Password Management Best Practices

Getting Started

How helpful was this page?

Unknown macro: 'rate'

Tell us what we can improve.

Save as PDF

this page has been moved to https://support.goalexandria.com/knowledge-base/password-management-best-practices/

Why security?

Each organization has unique security needs, so it is vital that your user team analyzes their situation and makes decisions on how to set up their distinct security goals.

Please take the time to go through our suggested best practices, and let our Customer Support Team know if you would like any consultation on them.

Alexandria is a secured program, meaning a username and password are always required to gain access to the service. It is imperative to plan for and have access redundancies in place for your Alexandria service.

Click the sections below to expand for more information.

General best practices

General best practices

- Don't share passwords.
- Don't use generic passwords or shared operator accounts. Each user should have their own unique username and password.
- Consider using a secure password management program to avoid forgetting your login info, and to avoid having your password in obvious places (like a post-it note on your desk).
- Keep your operating system, browsers, and COMPanion program up-to-date (if you are cloud hosted with us then you don't have to worry about the last one).
- ALWAYS add a valid and current email to an operator patron record so that the operator can recover their password if needed.
- Make sure to whitelist noreply@goalexandria.com, which is the email address any password reset emails will come from. This might need to be done by a district or facility IT team.
- Have a plan to access the district admin's password/email if they leave, or have a backup district admin user.

Login redundancies

- We recommend having two distinct highest level operators (District Administrator) for redundancies, in case one operator leaves, then the second operator can still access all areas of the program. These could be the District Librarian, Site or District Tech, or whoever has high-level responsibility over the library.
- Consider giving a backup, full-admin rights login to a person who is always onsite, like your principal IT technician. Even if they don't use Alexandria regularly, if you ever get locked out, someone can help. This can also be useful if someone is helping out as a librarian temporarily, but the permanent librarian is unavailable to help give them temporary access.
- A lot of this may depend on the size of your facility, and your administrative group should make a plan and policy for password and user management

Password Management Best Practices

Last .dateFormatter.formatDateTime($content.getLastModificationDate())

Creating a secure password

We recommend that you set a standard for secure passwords and train your team accordingly.

Here are some generally accepted password rules:

- It is not safe to use the same password on more than one site. If your password is hacked for one site, then it could be used to get into multiple sites. Reusing passwords is not secure.
- Create a password that is hard to guess, and doesn't contain personal information like your birthdate or phone number. A strong password should be easy for you to remember, but hard for anyone to guess or associate with you. Avoid using simple phrases, words, or patterns that are easy to guess.
- Remember that the longer a password is, the harder it is to hack.
- Follow these simple steps to keep your data (and yourself) safe.

Read more: Keep your data safe—Password Required!

Creating a new secure operator

Adding Operators is usually done by an admin, or someone who has greater security rights than the new operator being created.

Read through the step-by-step instructions for Adding Operators, or watch our training video below. **Be sure the operator has an EMAIL, maybe even TWO, so they can always recover their password!**

Recovering an operator login

There are two possible scenarios for recovering a login or getting back into Alexandria; if you have an operator record with an email attached to it, or if you do not. We will cover both below.

If you have access to the operator's email address, username, or barcode for password recovery:

When setting up an operator, ensure an email is entered. If an email was entered at the time of setup, the quickest way to recover an operator login is to:

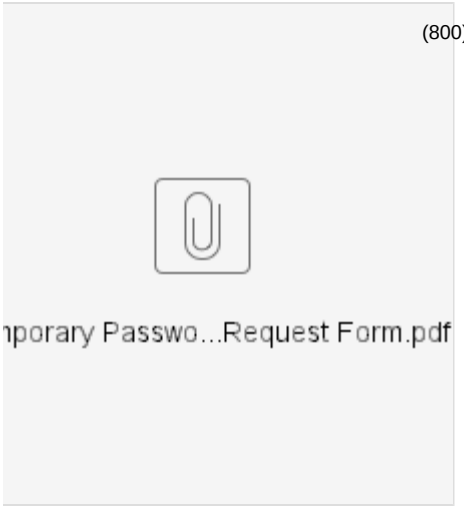
1. Go to the login page for Alexandria, and click the "Forgot your password?" button located below the username and password fields.
2. Enter the email, username, or barcode of the operator and click **SEND LINK**.
3. Once you receive the recovery link, follow the steps to update the password, within 24 hours of receiving the recovery link.

Make sure to whitelist noreply@goalexandria.com

If the operator DOES NOT have an email attached to their record in Alexandria:

The steps for recovering a login in this case can be a lengthy process and customers will be required to speak with the COMPanion Support team and confirm their identity and role. Due to security considerations and requirements, COMPanion Corporation and the COMPanion Support Team withhold the right to deny or approve password requests at any time.

This is why it is important to maintain and manage access to your service. If you do not have access to the operator's email address, username, or barcode for whom you wish to recover or reset a password (or if the operator did *not* have a valid email in their record), then you will need to speak with a member of the COMPanion Support Team. Their contact info is:



If approved, a Support Team member will then issue a temporary password that is good for 24 hours.

With this temporary password, you can log in to Alexandria and follow these steps to reset the password:

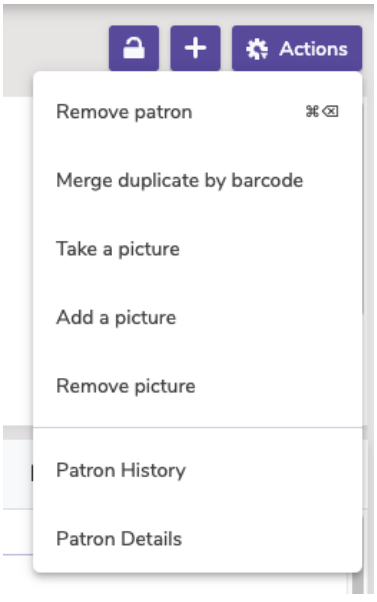
Go to Patrons and select Advanced Search to bring up the patron profile with the login credentials and permissions. Once the patron record is displayed, click the Lock icon to unlock the record. Go to the Access tab and enter a new password, then click Save.

> Please also be aware that our 24 hour temporary password does give the logged-in-user **highest access** to the program. It is wise to be sensitive with whom you are sharing these temporary credentials.

See also: Reset Patron Username and Password

> The Approval process for temporary password issuance can be lengthy due to the detailed review requirements. This can take up to 2 or more business days processing based on the verification of the person requesting, and release of the temporary passwords.

Switching out a leaving librarian for a new one



If you have a librarian who is retired, or one that has already left, you will want to remove their access to Alexandria. You might also be adding a new librarian as an operator to your Alexandria. Here are the steps to do that.

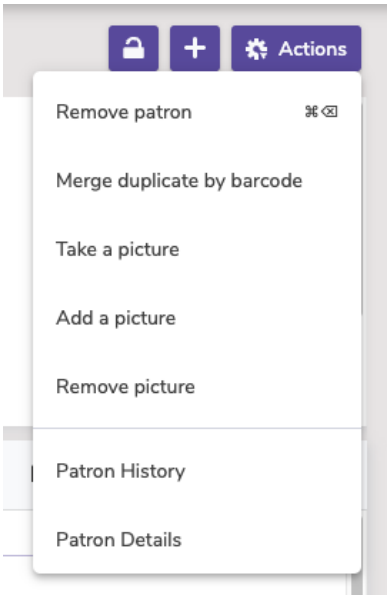
To remove an operator:

Go to **Patrons** and select **Advanced Search** to locate the record of the librarian who is leaving. Unlock the record and go to the actions menu and choose **Remove Patron**, then select **Yes, Remove**.

To create a new librarian, see the section above for creating a new secure operator or see Adding Operators.

Cleaning up unneeded operators

COMPanion suggests regular audits of who has operator access to Alexandria, and if old operators should be removed. There are multiple security group levels; all may need to be cleaned up.



To clean up your operators:

Run the Operator Summary report to generate a list of your operators to review.

Go to **Patrons** and click **Advanced Search** to find all operators with login credentials. Click the **Access** dropdown, then **Security**.

First, select the District Administrator option and click Search. Review the list of operator patron records and determine which need to be removed.

Click to highlight the operator you want to remove and click the **Lock** icon to unlock the record. Go to the **Actions** button next to the lock and choose **Remove Patron**, then select **Yes, Remove**.

Repeat these steps for all operators you need to remove.

If needed, repeat these same steps for any other security group levels (other than the **Patron** level), such as **Library Administrator**, **Librarian**, and **Library Staff**.