

Reader security, passwords, and login options

Last Modified on 09/24/2025 5:12 pm EDT

Learn about the settings for reader password expiration and complexity, Google login, and SSO login for readers.

Reader password security


If you're using reader accounts in any of your knowledge bases, you'll need to set up your **Reader Password Security**. This helps to determine:

- Whether readers will administer their own passwords or if one of your admins will manage them
- How many failed password attempts are allowed
- Whether **authors** can log in as readers
- If readers can only access your knowledge base from a specific list of IP addresses

These settings are account-wide across all of your knowledge bases, though you have some options to override them in individual knowledge bases.

To review and set up these settings:

1. Go to **Account > Readers**. The **Readers** page opens to the **Readers** tab.
2. Open the **Settings** tab.
3. Use the **Reader Password Security** section to adjust any settings you need. Options include:
 - a. **Password Management:** Choose whether you want your knowledge base admins to manage reader passwords or have readers manage their own. Self-administered passwords are the default password management option. We recommend self-administered passwords because few people have time to deal with forgotten password issues. This is an account-wide setting but can be overwritten on individual knowledge bases for accounts with multiple knowledge bases under **Security and access > Security settings**. Refer to [What's the difference between admin managed and self-administered reader passwords?](#) for more information.

**Related settings**

If you're using self-administered passwords, you'll also want to review the [Self-Administered Reader Options](#), the [Reader Welcome Email](#), and the [Reader Password Reset](#) email settings.
 - b. **Password Attempts:** By default, reader accounts are locked for 20 minutes following 3 unsuccessful attempts. If you'd like to allow unlimited password attempts, check the box to **Allow unlimited password attempts**.
 - c. **Author Logins:** Choose whether to allow KnowledgeOwl authors to log in as readers (recommended, on by default).
 - d. **Restricted IP Protection:** If your readers should all be on a VPN or on a specific range of IP addresses, add a comma-separated list of IP addresses here to enforce that restriction in addition to the **Default access** options in **Security and access > Security settings**.
 - e. **Case insensitive Logins:** If using admin managed passwords, choose whether or not you want the usernames to be case-sensitive.
4. Be sure to **Save** your changes.

What's the difference between admin managed and self-administered reader passwords?

You have two options for reader password management:

- **Self-administered Passwords:** Allow readers to administer their own passwords (default)
- **Managed Passwords:** Passwords can only be managed by KnowledgeOwl admins

Allowing readers to administer their own password also enables reader welcome emails, password reset emails, and reader signups. Emails are not sent for managed passwords.

To toggle between the password management options:

1. Go to **Security and access > Readers** (or **Account > Readers**).
2. Open the **Settings** tab.

3. The **Password Management** settings are the first option in the **Reader Password Security** section.

Self-administered passwords

To use this option, select **Allow readers to administer their own passwords**.



Valid emails only

You must have reader usernames that are valid email addresses for this option to work properly!

Self-administered passwords are set and reset by the reader themselves via email. When using self-administered passwords, readers are sent a welcome email containing a temporary password and will be asked to update their password when they first log in.

If a reader forgets or wants to reset their password, they can select **Reset Password** on the reader login page. This sends a temporary password to their email address to create a new password.

KnowledgeOwl admins can reset self-administered passwords either by sending a new temporary password or manually setting a temporary passwords; readers will be asked to update their password when they log in with the temporary one.

You can also customize [reader welcome](#) and [reader password reset emails](#) in the Readers **Settings** tab. Reader emails are account-wide so the same email is sent for all knowledge bases in an account.



Automatic welcome emails

When creating readers with self-administered passwords, readers will automatically be sent a welcome email with their temporary password when you add a single reader or create readers from a spreadsheet.

If you don't want the welcome email sent when you first create a new reader, choose **Managed Passwords**, create the readers with an admin password, and switch back to **Self-Administered Passwords**. The admin password will then be used as a temporary password; readers will be asked to update them when they log in.

Managed passwords

To use this option, select **Passwords can only be managed by KnowledgeOwl admins**.

Managed passwords can only be set and reset by a KnowledgeOwl admin (an author with **Full Admin** or **Reader Admin** permissions). When using managed passwords, you'll need to give the reader their username and password through your own system. If the reader forgets their password, they'll need to contact you to retrieve or reset it. No welcome or password reset emails are sent for managed passwords; all reader communication occurs outside of KnowledgeOwl.

When creating readers with managed passwords, you will need to set the password in the **Admin Managed Password** field when [adding a single reader](#) or have a column with the passwords when [creating readers in bulk](#).

Account-wide password management

Reader settings are account-wide so the password management option will apply to all knowledge bases on an account by default. Self-administered passwords are the default option for password management.

Different password management for different knowledge bases

If you have multiple knowledge bases and you want to have one or more that don't use the account-wide password management, override the Global password management settings:

1. Go to **Security and access > Security settings**.
2. In the **Reader security options** section, update the **Global password management setting override** so it doesn't use the **Use global password management setting from the readers settings page**:
 - a. Select **Admins must manage reader passwords for this knowledge base** to use admin-managed passwords.
 - b. Select **Allow readers to administer their own passwords for this knowledge base** to use self-administered passwords.

Set up self-administered reader options

If you allow readers to administer their own passwords, you should review the **Self-Administered Reader Options** in **Account > Readers > Settings**.

Use these options to control:

- How frequently passwords expire
- If readers are allowed to reuse passwords
- If passwords need to meet specific validation/complexity rules
- If [reader signups](#) are allowed, and what the process looks like if they are

Review and change settings

To review and update these settings:

1. Go to **Account > Readers**. The **Readers** page opens to the **Readers** tab.
2. Open the **Settings** tab.
3. If the **Reader Password Security** section's **Password Management** option to **Allow readers to administer their own passwords** is selected, scroll down to the **Self-Administered Reader Options** section. Use the settings here to control the following password behavior:
 - **Password Expiration Interval:** Use this control to set whether reader passwords should expire and how frequently they should expire. When a reader's password expires, they're prompted to create a new password the next time they log in. Choose from these options:
 - **Never (default)**
 - **Every Month**
 - **Every 2 Months**
 - **Every 3 Months**
 - **Every 6 Months**
 - **Every Year**
 - **Repeat Password Limitations:** Use this control to set whether readers can reuse an existing password and/or how many previous passwords they can't reuse. Choose from these options:
 - **None (default)**
 - **Cannot use previous password**
 - **Cannot use previous 2 passwords**
 - **Cannot use previous 3 passwords**
 - **Cannot use previous 4 passwords**
 - **Cannot use previous 5 passwords**
4. **Custom Validation Rule:** Use this setting to enter regex to enforce your company's password requirements for complexity or format. You can find prewritten validation rules using your favorite search engine. Refer to [Regex for custom validation rules](#) for more help.
5. **Custom Validation Description:** This message will be displayed on the password reset screen if you have a custom validation rule. Use it to tell your reader about the rule so they can create a password that works.
6. **Auto-assign Group Rules:** If you are using group rules to [automatically assign your readers to groups](#), check this box to ensure that reader groups will update based on the rules each time a reader logs in. This allows you to create new rules and have it automatically applied to existing readers, but it will override any groups you might have set manually. Don't turn this option on if you're manually setting reader groups.
7. **Allow Google Sign In:** You can allow readers to sign up for and log in to your knowledge base with their Google account. Refer to [Allow Google log in for readers](#) for the additional steps to get Google Sign-in set up on your knowledge base.
8. **Reader Signups:** Add a [reader signup](#) link to your login page so readers can sign up on their own. By default, new readers will be added and a welcome email will be sent with a temporary password.
 - a. You can choose to require an admin approval before the welcome email is sent.
 - b. You can also set up notification emails to inform you of new reader signups or signup requests.
9. **Signup Notification Recipients:** If you're using [reader signups](#), add the email address(es) you'd like to be notified when a new reader signs up or requests access.
 - a. To add multiple addresses, use a comma-separated list, such as: `linus@knowledgeowl.com,owlbert@knowledgeowl.com` .
10. Be sure you **Save** your changes.

Regex for custom validation rules

KnowledgeOwl doesn't automatically enforce any password validation, but you can use the **Custom Validation Rule** field to force readers to use more complex passwords (for example, enforce a mixture of upper and lower case, numbers, and symbols).

What is regex?

Regex is a common abbreviation of 'regular expressions'. Regular expressions are "a sequence of characters that specifies a *search pattern*. Usually such patterns are used by string-searching algorithms for "find" or "find and replace" operations on strings, or for input validation" (from [Wikipedia - Regular expression](#)).

KnowledgeOwl takes the regex you provide and uses it to check that the password the reader creates matches your requirements.

Regex password rule examples

Regex can be very powerful, and can look very complicated. Don't panic! If you're stuck, check if any of these examples meet your requirements. You can always [contact us](#) for more help:


Password rules	Regex
<div>Password must:</div> <ul style="list-style-type: none">• Be eight characters or more• Include at least one each of: number, symbol, lowercase letter, uppercase letter• Not contain whitespace	<div>^(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(?=.*[@#\$\$%^&+=])(?=\S+\$).{8,}\$</div>
<div>Password must be eight characters or more. It can contain any characters apart from whitespace</div>	<div>^(?=\S+\$).{8,}\$</div>
<div>Password must be between 12 and 24 characters long. It can contain any characters apart from whitespace</div>	<div>^(?=\S+\$).{12,24}\$</div>
<div>Password must:</div> <ul style="list-style-type: none">• Be 16 characters or more• Include at least one each of: lowercase letter, uppercase letter• Not contain whitespace	<div>^(?=.*[a-z])(?=.*[A-Z])(?=\S+\$).{16,}\$</div>

My Knowledge Base Login

Username:

Password:

[Reset Password](#)

 Sign in with Google

[Don't have a login? Click here to sign up.](#)

KnowledgeOwl Reader Login page with Google Sign-in enabled

To enable this option, you'll need to configure some things in Google Cloud Platform APIs & Services and in KnowledgeOwl.

In Google Cloud Platform, you'll need:

- A new project
- An OAuth consent form
- OAuth credentials

In KnowledgeOwl, you'll need access to:

- Settings > Security
- Your Account > Readers

Step 1: Create a Google Cloud Platform project (Google)

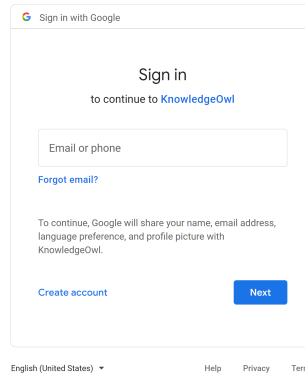
You must have a Google Cloud Platform project in order to complete the rest of the steps in this tutorial.

1. In Google Cloud Platform, go to [Google credentials settings](#) to open APIs & Services in Google Cloud Platform.
2. Click the option to **Create Project**.
3. Give your project a name (we recommend using the name of your knowledge base or "KnowledgeOwl" as the project name).
4. Add an organization and location (if appropriate).

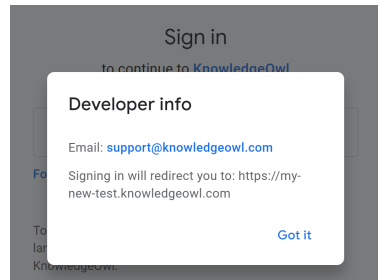
Step 2: Set up your Google Project's OAuth Consent Screen (Google)

Google requires an OAuth consent screen. For more details, see [Google Cloud Platform Console Help's instructions for Setting up your OAuth consent screen](#). We cover this only at a high level. Set up your OAuth consent screen by clicking the **Configure Consent Screen** button.

1. Click the **Configure Consent Screen** button.
2. Select a **User Type**.
 - External lets any user with a Google account sign up; Internal restricts to users within your Google Cloud Organization. You must make a selection here before you can complete configuration. External does require additional verification, not covered by this guide.
3. On the OAuth consent screen, in the **App information** section, at minimum, these fields are required:
 - **App name**: This is displayed in the "Sign in to continue to [app name]" portion of the Google login process and in the "To continue, Google will share....with [app name]." In our screenshot, we've used "KnowledgeOwl" and you can see where it displays:



- o **User support email:** In the Google login process, if you click on the hyperlinked App name, this is the email address that is displayed in the Developer info box that appears. Here, we've used our support email address:

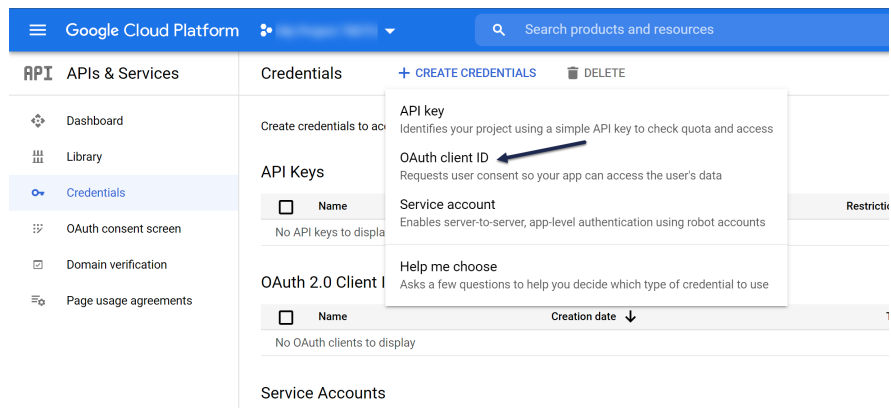


4. On the OAuth consent screen, in the **Developer contact information**, add an email address. This is not displayed anywhere--Google uses it to notify you of changes.
5. Add other fields in various sections as appropriate for your configuration.
6. Click **Save and Continue**.
7. Set the **Scopes** for your consent screen. See Google's documentation for guidance here.
8. Click **Save and Continue**.
9. *Optional:* If you're doing an External User Type, you'll be prompted to add any **Test users**. (We do recommend using these if you're testing an External User Type.)
10. Once you're done, Google generally displays a Summary page.

Step 3: Set up the OAuth client credentials (Google + KO)

In this step, you'll copy redirect URLs from KnowledgeOwl into your Google Cloud Platform project.

1. In Google Cloud Platform, go to **Credentials**. (This is generally always present in a menu on the left, at the time this documentation was written.)
2. At the top, click the **+ Create Credentials** button.
3. Select the option to create an **OAuth client ID**.



4. For **Application type**, select "Web application."

5. Enter "KnowledgeOwl" as the name.

[←](#) Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
KnowledgeOwl

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

6. In the **Authorized redirect URIs**, you'll paste in some information from KnowledgeOwl:

a. In KnowledgeOwl, go to **Security and access > Security settings**.

b. Go to the **Reader sign ins using Google** section at the bottom of the page:



c. Copy the **Google login redirect URL** and add it as an **Authorized redirect URI** in Google Cloud Platform.

d. Copy the KnowledgeOwl **Google signup redirect URL** and add it as an **Authorized redirect URI** in Google Cloud Platform:

Authorized redirect URIs ⓘ

For use with requests from a web server

URIs *

https://my-new-test.knowledgeowl.com/docs/google-auth

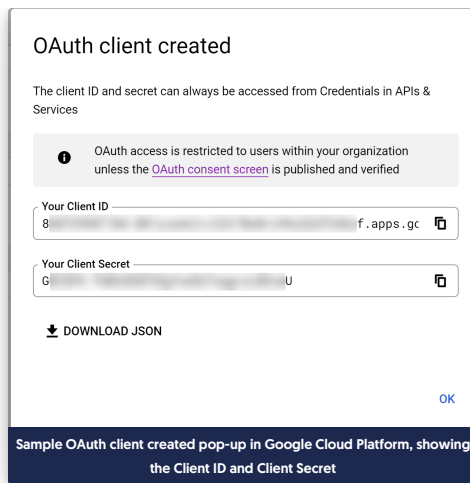
https://my-new-test.knowledgeowl.com/docs/google-signup

[+ ADD URI](#)

[CREATE](#) [CANCEL](#)

7. Once you've added both authorized redirect URIs in Google Cloud Platform, select the **Create** option there to finish creating your credentials.

8. This will display the OAuth Client ID and Secret you need in the next step!



Step 4: Add your Google Cloud Platform Client ID and Secret (KO + Google)

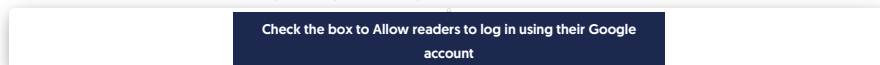
In this step, you'll copy the OAuth Client ID and OAuth Secret generated above into KnowledgeOwl.

1. In KnowledgeOwl, go to **Security and access > Security settings**.
2. Go to the **Reader sign ins using Google** section at the bottom of the page.
3. Paste your **Client ID** from Google Cloud Platform into the **Google API client ID** field.
4. Paste your **Client Secret** from Google Cloud Platform into the **Google API secret** field.
5. **Save** your KnowledgeOwl Security settings.

Step 5: Turn on Google login for readers (KO)

With all of the configuration done, you can now enable Google login for readers in KnowledgeOwl! To do so:

1. Go to **Security and access > Readers (or Account > Readers)**.
2. Open the **Settings** tab.
3. In the **Self-Administered Reader Options** section, find the **Allow Google Sign In** heading.
4. Check the box to **Allow readers to log in using their Google account**:



5. *Optional:* to allow readers to sign up for access to your knowledge base, you'll need to check the **Reader Signups** box to **Allow people to sign up to become a reader**. Refer to [Using reader signups](#) for more details on reader signup options.
6. **Save** your changes.

Your Reader Login page now displays a **Sign in with Google** button. If you've enabled reader sign-ups, the reader sign-up link will display below the login section:

Allow readers to log in through SSO

Do you already have a Single Sign-On provider? You can set up a SAML/SSO integration to allow your readers to login using

those same credentials.

Review the configuration options available at [Single Sign-On \(SSO\)](#).

Help readers reset their passwords

If you use self-administered reader passwords, readers should be able to reset their password without your help, using the **Reset password** link on the login page. You can [Set up self-administered reader options](#) to configure things like password expiry.

Refer to [What's the difference between admin managed and self-administered reader passwords?](#) to learn more about the different types of reader password management.

To manually reset a reader's password:

1. Go to **Account > Readers**. The **Readers** page opens to the **Readers** tab.
 2. Select the reader whose password you want to reset.
 3. Follow the steps for your reader password management type:
 - For self-administered readers:
 1. Select **Reset Self-Administered Password**.
 2. Choose either:
 - **Email reader a randomly generated temporary password:** This has the same effect as the reader going through the password reset process.
 - **Assign a custom temporary password:** When you select this option, KnowledgeOwl shows a **Temporary Password** field, allowing you to enter a temporary password of your choice. When you use this option, KnowledgeOwl does not automatically send an email with the new password. You must email the password to the reader.
 - For admin-managed readers, enter a new password in the **Admin Managed Password** field.
 4. Select **Save** to apply your changes.
-