Reader security, passwords, and login options

Last Modified on 01/07/2025 3:01 pm EST

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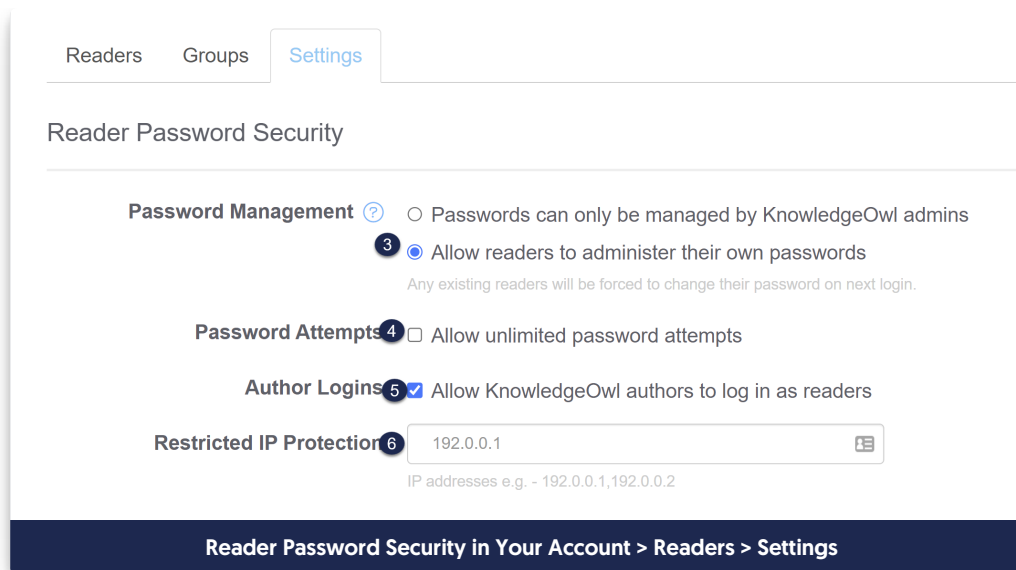
Reader password security

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 must be accessing 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. Click on your **profile icon/name** in the upper right.

2. Select **Readers** from the dropdown to access the Readers area of your account.

3. Open the **Settings** tab.

4. The Reader Password Security section will display at the top:

Reader Password Security in Your Account > Readers > Settings

5. **Password Management:** Choose whether you want to manage reader passwords or have them 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 **Settings > Security.** See **What's the difference between admin managed and self-administered reader passwords?** for more information.

> 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.

6. **Password Attempts:** Choose whether or not you want to allow unlimited password attempts. By default, reader accounts are locked for 20 minutes following 3 unsuccessful attempts.

7. **Author Logins:** Choose whether to allow KnowledgeOwl authors to log in as readers (recommended; on by default).

8. **Restricted IP Protection:** Optionally restrict reader logins to a specific IP address or list of IPs as a form of two-factor authentication (password AND IP address).

9. **Case insensitive Logins:** If using admin managed passwords, choose whether or not you want the usernames to be case-sensitive.

10. Click the **Save** button at the bottom of the screen 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 odesn'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 **Readers > Settings**.

These help determine:
- 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. Click on your **profile icon/name** in the upper right.

2. Select **Readers** from the dropdown to access the Readers area of your account.

3. Open the **Settings** tab.

4. If the box next to "Allow readers to administer their own passwords" is checked, scroll down to the **Self-Administered Reader Options** section:

Self-Administered Reader Options

⑤ Password Expiration Interval | Never ⌄ |

⑥ Repeat Password Limitations | None ⌄ |

⑦ Custom Validation Rule | ^(?=.*[a-zA-Z])(?=.*\d)[A-Za-z\d$@$!%*?&]{8,} |
Passwords will not be allowed that do not match the above regex

⑧ Custom Validation Description [   ]
Message will be displayed on password reset screen.

⑨ Auto-Assign Group Rules ☐ Override reader groups based on rule logic on each login

⑩ Allow Google Sign In ☐ Allow readers to log in using their Google account
To use, additional information is required for each knowledge base. Go to Settings → Security and fill out the Google integration settings.

⑪ Reader Signups ☐ Allow people to sign up to become a reader
☐ Require a KnowledgeOwl admin to approve new reader access
☐ Send a notification email when a new reader signs up

⑫ Signup Notification Recipients | john@email.com,jane@email.com |
For multiple email addresses, use a comma separated list.

⑬ **Save**

5. **Password Expiration Interval:** Should reader passwords expire? And if so, how frequently should they expire? This setting determines how frequently reader passwords will expire, forcing readers to choose new passwords. The options are:

   ○ **Never (default)**

   ○ **Every Month**

   ○ **Every 2 Months**

   ○ **Every 3 Months**

   ○ **Every 6 Months**

   ○ **Every Year**

6. **Repeat Password Limitations:** Can readers reuse an existing password? This setting lets you choose whether and how to limit password reuse when resetting passwords. The options are:

   - **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**

7. **Custom Validation Rule:** Do you have company password requirements for complexity or format that you'd like to enforce? Use this setting to create your own password validation using RegEx. You can find prewritten validation rules using your favorite search engine. Refer to Regex for custom validation rules for more help.

8. **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.

9. **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. **Do not choose this option if you are manually setting reader groups.**

10. **Allow Google Sign In:** You can allow readers to sign up for and log in to your knowledge base with their Google account. See Allow Google log in for readers for the additional steps to get Google Sign-in set up on your knowledge base.

11. **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.

12. **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.`

13. **Click the Save button.**

Regex for custom validation rules

By default, KnowledgeOwl does not enforce any password validation. You may wish to add rules forcing readers to use more complex passwords (for example, enforce a mixture of upper and lower case, numbers, and symbols). You can do this by entering a regex rule in the **Custom Validation Rule** field.

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**).

This means that 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, see if any of these examples meet your requirements. You can always **contact us** for more help.

Password rules	Regex	Modifications
Password must: • Be eight characters or more • Include at least one each of: number, symbol, lowercase letter, uppercase letter • Not contain whitespace	^(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%^&+=])(?=\S+$).{8,}$	• If you want to remove or add permitted symbols, change the contents of [@#$%^&+=] • If you want to change the character limit (for example, you want 12 as a minimum length, rather than eight), change the number in {8,}
Password must be eight characters or more. It can contain any characters apart from whitespace	^(?=\S+$).{8,}$	Change the 8 to any other number to alter the length restriction
Password must be between 12 and 24 characters long. It can contain any characters apart from whitespace	^(?=\S+$).{12,24}$	• Change the 12 to another number to alter the minimum length • Change the 24 to another number to alter the maximum length

Password rules	Regex	Modifications
Password must: • Be 16 characters or more • Include at least one each of: lowercase letter, uppercase letter • Not contain whitespace	^(?=.*[a-z])(?=.*[A-Z])(?=\S+$).{16,}$	**Change the 16 to any other number to alter the length restriction**
Password must: • Be between 12 and 128 characters. • Contain three out of four of: number, symbol, lowercase letter, uppercase letter • Have no more than two of the same character in a row	^(?:(?=.*\d)(?=.*[A-Z])(?=.*[a-z])|(?=.*\d)(?=.*[^A-Za-z0-9])(?=.*[a-z])|(?=.*[^A-Za-z0-9])(?=.*[A-Z])(?=.*[a-z])|(?=.*\d)(?=.*[A-Z])(?=.*[^A-Za-z0-9]))(?!.*(.)\1{2,})[A-Za-z0-9!~<>,;:_=?*+#."&§%°()|\[\]\-\$\^\@\/]{12,128}$	

A detailed example

It's fine to just use any of the examples from the list above, but if you want to learn a bit more about what they are doing and how regex works, here is a detailed explanation of one of the examples.

```
^(?=.*[0-9])(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%^&+=])(?=\S+$).{8,}$
```

- **^** tells us that we must match the pattern from the start of the line. For example, **^a** means to look for 'a' at the start of the line. It matches the 'a' in 'abc', but not in 'bca'.
- **(?=)** creates a positive lookahead. This means that it matches something followed by something else. For example, **h(?=o)** matches an 'h' followed by an 'o'. So it matches the 'h' in 'hoot' but not in 'hype'. In our example it's a bit more complicated, as we have chained multiple positive lookaheads together, and added some special characters.
- **.** matches any single character, and ***** tells us to match the previous token any number for times (from zero up). So **.*** means match any number of single characters. By itself this is meaningless: **.*** would match any phrase. In the context of our example, it means that the restriction that follows it (the bit in square brackets) can be preceded by any number of any other characters. For example, given the regex **.*[0-9]**, we'll match 'owl23', 'lotsOfOwls36', 'owlsWithSomeSymbols$48', and so on.
- **[]** ranges in square brackets match a single character in that range. For example, by itself **[0-9]** matches each number in '123owl456'. In our example, **[@#$%^&+=]** provides a list of symbols readers can use in their password.
- **\S** matches any non-whitespace character, and **+** tells us to match the previous character any number of times (from one up - so there has to be at least one character). **$** indicates the end of a line. To take one of our previous example phrases, 'abc', **c$** matches the 'c' at the end, in the same way that **^a** matches the 'a' at the beginning. In the context of our example, **\S+$** is there to ensure there are no whitespace characters in the password.
- **{8,}** tells us to match the preceding character (in this case, ., which matches any single character), eight or

more times. In other words, there must be at least eight characters in the line for it to match. This means if you want a 12 character minimum length, you can change the 8 to 12.

Tips for creating your own regex rule

- **Start the rule with ^. This ensures we look for a password that matches your rule right from the start of the phrase that the reader enters.**
- **Include (?=\S+$) to ensure readers can't create passwords containing whitespace.**
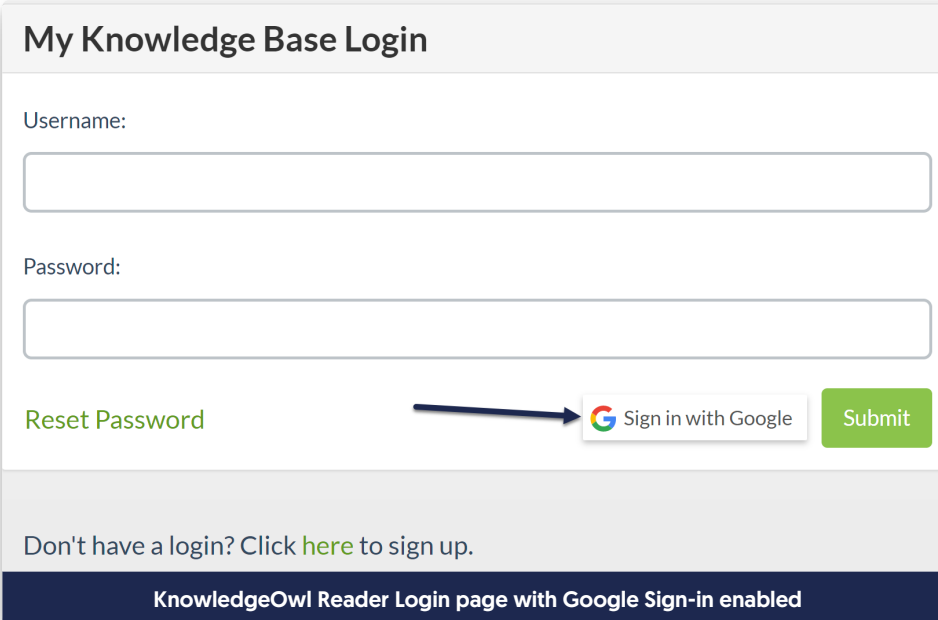- **Be aware that KnowledgeOwl uses PCRE (PHP) regex.**

Learning more

If you want to dive in and really learn regex, here are a few tips to get you started:

- **Be aware different programming languages can have slightly different flavors of regex. If you're already familiar with/using a particular language, it's worth looking for regex tutorials specific to that language.**
- **regex101 is a handy site that allows you to try out Regex rules against example words and phrases. When testing regex for use in KnowledgeOwl, select PCRE2 (PHP >= 7.3) under FLAVOR.**

Allow Google log in for readers

You can allow readers to sign up for and log in to your knowledge base with their Google account.

My Knowledge Base Login

Username:

Password:

Reset Password   →   G Sign in with Google   Submit

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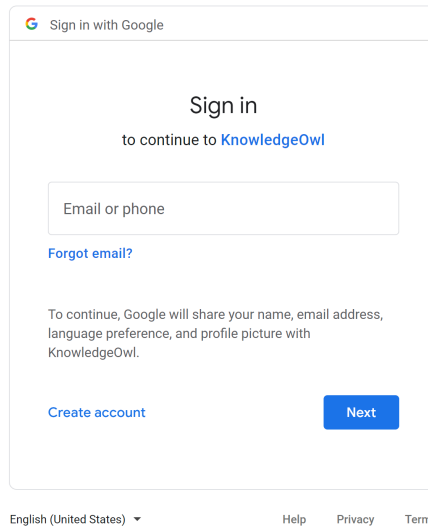
- **User support email**: In the Google login process, if you click on the hyperlinked App name, this is the email address that is displayed in the Developer info box that appears. Here, we've used our support email address:
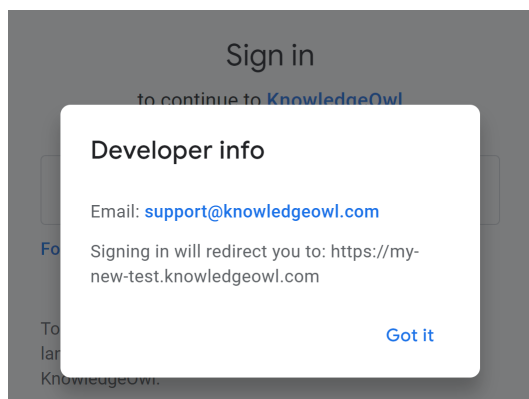

4. On the OAuth consent screen, in the **Developer contact information**, add an email address. This is not displayed anywhere--Google uses it to notify you of changes.

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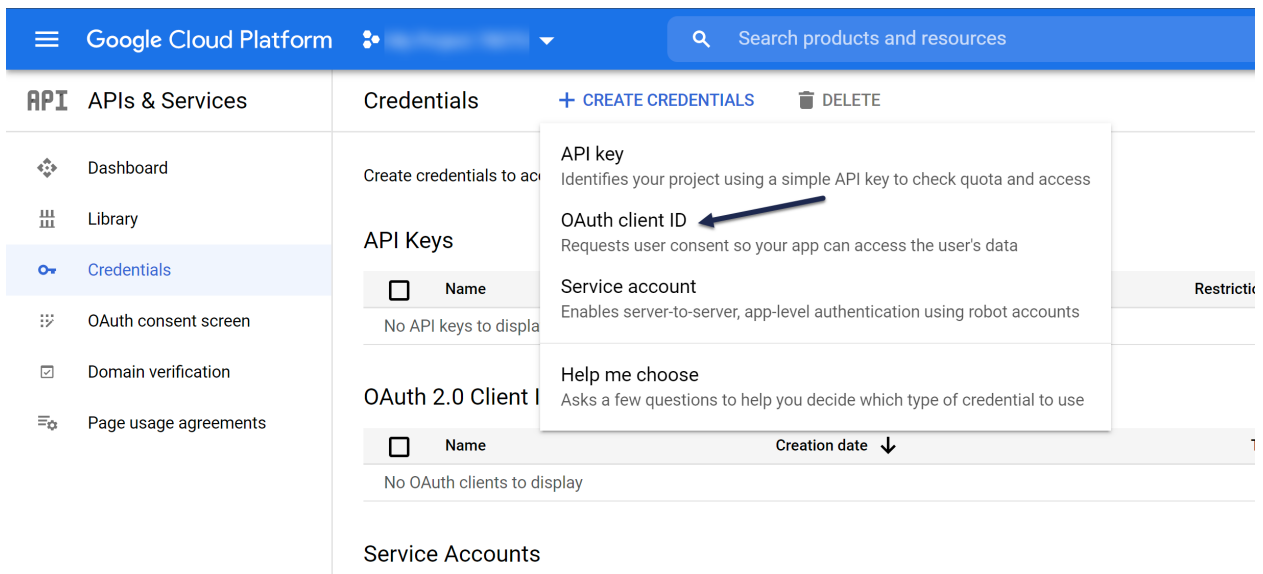
4. For **Application type,** select "Web application."

5. Enter "KnowledgeOwl" as the name.

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:

> The Reader sign ins using Google section of the Security settings 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
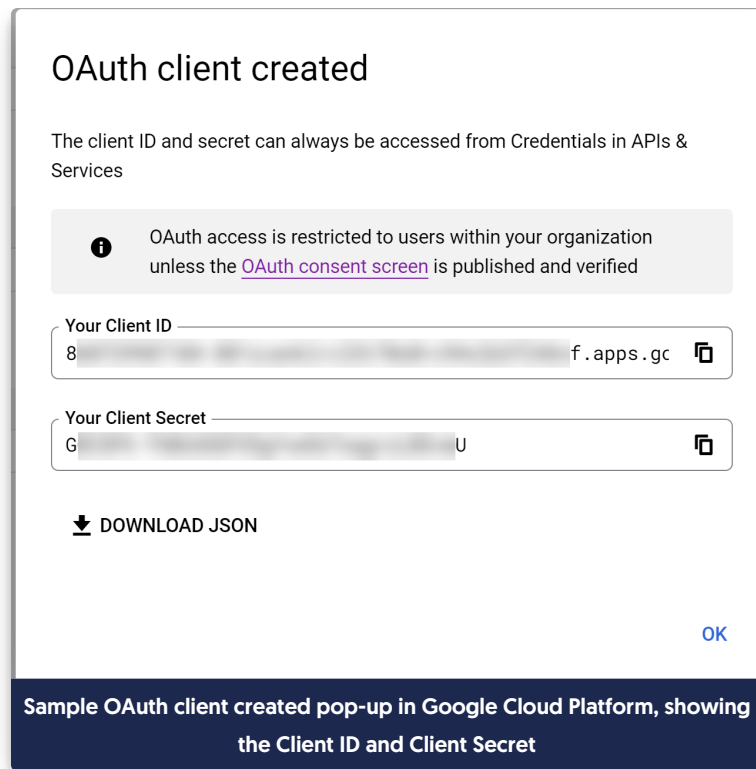
https://my-new-test.knowledgeowl.com/docs/google-signup

＋ 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!

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

ⓘ OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified

Your Client ID
8███████████████████████████████████████f.apps.gc ⧉

Your Client Secret
G███████████████████████████████U ⧉

⬇ DOWNLOAD JSON

OK

Sample OAuth client created pop-up in Google Cloud Platform, showing the Client ID and Client Secret

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**:

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:

My Knowledge Base Login

Username:

Password:

Reset Password   G Sign in with Google   Submit

Don't have a login? Click here to sign up.

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.

If you need to manually reset a reader's password:

1. Click on your **profile icon/name** in the upper right.

2. Select **Readers** from the dropdown to access the Readers area of your account.

3. Select the reader.

4. 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, 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.

5. Select **Save** to apply your changes.