



How do I give access to my CAPRA self-assessment?

Last Modified on 11/13/2025 1:48 pm EST

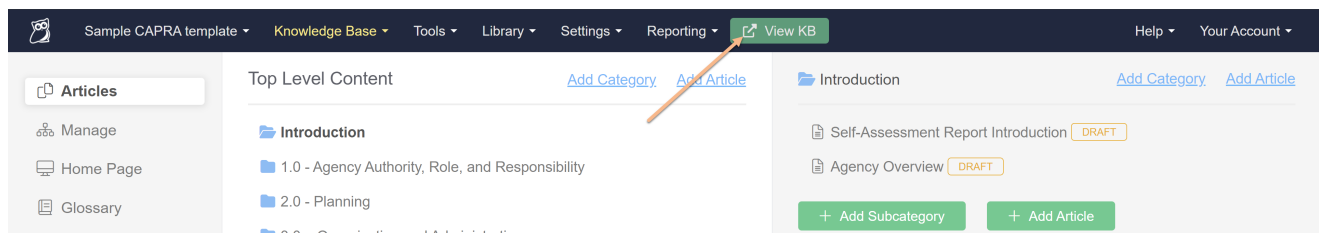
Learn how to give reviewers access to your self-assessment, and what security options are available.

Granting access to your self-assessment

To access your self-assessment, reviewers will need two things:

- The URL for your knowledge base
- A login of some kind

For the URL: you can see the URL for the knowledge base by clicking the **View KB** link in the top navigation:



To change the URL of your knowledge base, go to **Settings > Basic** and update the Sub-domain listed in the **Domain Settings** section.

For the login credentials: see the sections below. By default, your self-assessment knowledge base has been set up with a Shared Password, but there are other options available!

Default setting - shared password

By default, when our support team gives you the CAPRA accreditation knowledge base, anyone who accesses the knowledge base's URL and enters a single, shared password will be able to gain access.

You can see the shared password by going to **Settings > Security** and looking in the **Default Access** section at the top:

Sample CAPRA template Knowledge Base Library Settings Reporting View KB Help Your Account

Basic Security Search Style Article Ratings PDF Comments Subscriptions Widget

Security Settings

Default Access controls what happens when someone goes to your knowledge base when they are not logged in. Default Login Page controls what happens when someone clicks on login or logout.

Default Access

- Public
The knowledge base is available without a login. An optional login can be added to give readers access to restricted content. This can be used with other login options like reader logins, remote authentication, and SAML SSO.
- Restrict by [reader](#) logins
Readers must log in to access the knowledge base. This can be used with remote authentication and SAML SSO to provide multiple authentication methods.
- Restrict by IP address or shared password

IP addresses e.g. - 192.0.0.1, 192.0.0.2 - or 192.0.0.0/24

Shared password - can stand alone, or used as a fallback for IP address validation
- Require both the shared password and IP address validation
- Remote Authentication — [View tutorial](#)
Readers will be redirected to another website or application for authentication. This option requires a Remote Login URL. This can be used with reader logins and SAML SSO.

Default Login Page

- Reader Login Page
- Remote Auth Login URL
- SAML Login URL

Reader Options



To change the shared password, edit the password in the box above. Then click the **Save** button at the bottom of the screen.

If you'd prefer not to use a shared password, see the sections below for alternate security arrangements.

No login required (publicly available)

Some organizations prefer to remove the shared password from their self-assessment knowledge base, so that anyone with the URL can access it. If you'd like to make this change:

1. Go to **Security** and access > **Security settings**.
2. In the **Authentication settings** section, under **Content authentication**, select the radio button next to **Public**.
3. Be sure to **Save** your changes.

Once you save this change, anyone with the URL to your knowledge base can access it.

Individual reviewer accounts


Some organizations prefer to set up reviewers or teammates with their own individual accounts, rather than a shared password. This is a slightly higher level of security than the shared password, but it does require a little more setup at the beginning.

If you'd like to set up your knowledge base this way:

1. Go to **Settings > Security**.

2. In the **Default Access** section, select the option next to **Restrict by reader logins**.


Security Settings



Default Access controls what happens when someone goes to your knowledge base when they are not logged in. Default Login Page controls what happens when someone clicks on login or logout.

Default Access

Public
The knowledge base is available without a login. An optional login can be added to give readers access to restricted content. This can be used with other login options like reader logins, remote authentication, and SAML SSO.

 Restrict by [reader](#) logins
Readers must log in to access the knowledge base. This can be used with remote authentication and SAML SSO to provide multiple authentication methods.

Restrict by IP address or shared password

Remote Authentication — [View tutorial](#)
Readers will be redirected to another website or application for authentication. This option requires a Remote Login URL. This can be used with reader logins and SAML SSO.

Default Login Page

Reader Login Page

Remote Auth Login URL

SAML Login URL

Basic Authentication Enable designated readers to log in via basic access authentication
This feature is most commonly used to allow 3rd party tools to crawl the content of a private knowledge base

3. Click the **Save** button at the bottom of the screen.

This will lock the knowledge base down to require individual reader accounts.

Once you know who your reviewers are, you'll need to create each of them as a KnowledgeOwl reader, using their email address. To create a reader account:

1. In the upper right, click **Your Account**.

2. **Select Readers**.

3. This will take you to the **Readers index page**, where you can create add your reviewers one at a time using the **Add Single Reader** option, or upload a spreadsheet with all your reviewers to create all the accounts in bulk. The **Add Single Reader** option is the easiest, and that's what we recommend using here. See our general help documentation on [Creating a reader](#) for full step-by-step instructions.

Optionally, you can also allow reader sign-ups. This would let your reviewers "sign up" to your knowledge base so that they'd request access and enter most of their information directly. This might be a smoother way for you to get reviewers set up with accounts without having to know their email addresses initially. For CAPRA accreditation, if you want to [use reader sign-ups](#), we recommend:

- Requiring admin approval of sign-ups (outlined in steps 6 & 7 of the instructions linked above)
- Sending an email notification when a new reader signs up, sent directly to your own email address (outlined in steps 8 & 9 of the instructions linked above)

This ensures that random people aren't signing up and getting access to your accreditation, since you have to

approve them, but makes it easy for reviewers to sign up and for you to know once a reviewer has done so.
