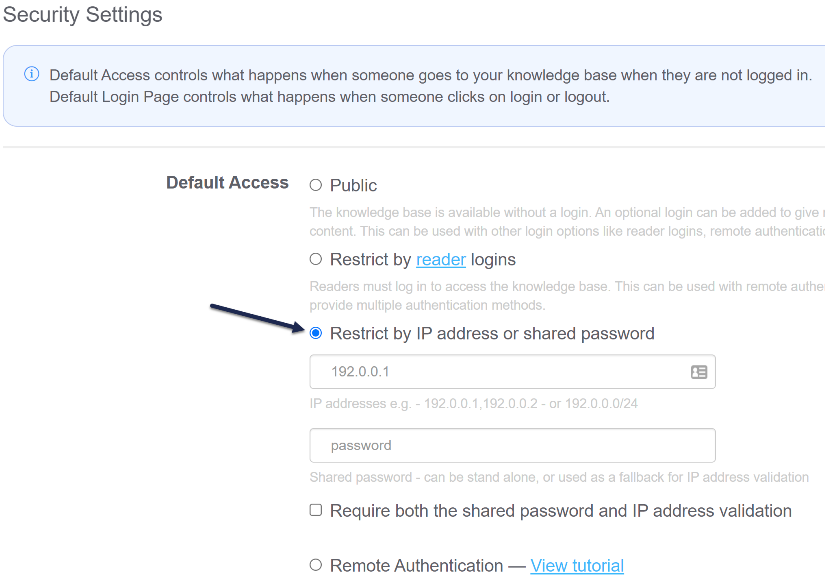
Restrict by IP address, shared passwords, reader logins, or a combination

Last Modified on 08/07/2024 3:01 pm EDT

The security settings under the Settings tab are mostly centered around the needs of private or internal knowledge bases. By default, your knowledge base will be visible to the public which means anyone can peruse your content. However, under **Settings > Security**, you have quite a few options.



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 r
content. This can be used with other login options like reader logins, remote authenticatio

○ Restrict by reader logins

Readers must log in to access the knowledge base. This can be used with remote authen
provide multiple authentication methods.

● Restrict by IP address or shared password

192.0.0.1

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

password

Shared password - can be stand alone, or used as a fallback for IP address validation

□ Require both the shared password and IP address validation

○ Remote Authentication — View tutorial

When would I use the different types of security?

Restrict by reader logins

Readers offer the most power in terms of authentication to your knowledge base. Essentially a reader is an individual login for each person or group whom you want to give access to your knowledge base. With this setting turned on, a person trying to access your knowledge base will be asked for a username and a password which we can then use to identify who they are. Once they log in, they will remain authenticated for 2 hours and can browse normally. If you select this option, you will need to set up readers under your profile > **Readers.**

You can also choose remote authentication, Salesforce SSO, or a SAML SSO integration to create readers using existing credentials.

Restrict by IP address

This setting is great for internal office knowledge bases. If you can track down the IP addresses that your office uses, you can paste the comma separated list into the box and ensure that no one trying to access your knowledge base from outside of your office can get in.

> You can also use the /24 subnet mask for a range of IP addresses; at this time, we only support the /24 subnet mask.

Restrict by shared password

This one is great if you need to restrict access to your knowledge base but you aren't sure of your office's IP addresses or if your readers are going to be spread out. Creating a single password that you can give to everyone will allow you to control who gets in but will allow for more flexibility.

IP-based Restriction OR Shared Password

You can also use the shared password setting in combination with the IP protection setting for even more flexibility. What this means is that while someone is in your office, on an approved IP address, they won't have to worry about logging in because they are accessing the knowledge base from an approved IP address. If they work from home one day though, they will be asked for the shared password to log in.

IP-based Restriction AND Shared Password

Need more security? You can select IP-based restriction as well as a shared password for a simplified two-factor authentication.