


Yellowfin UI Security Settings

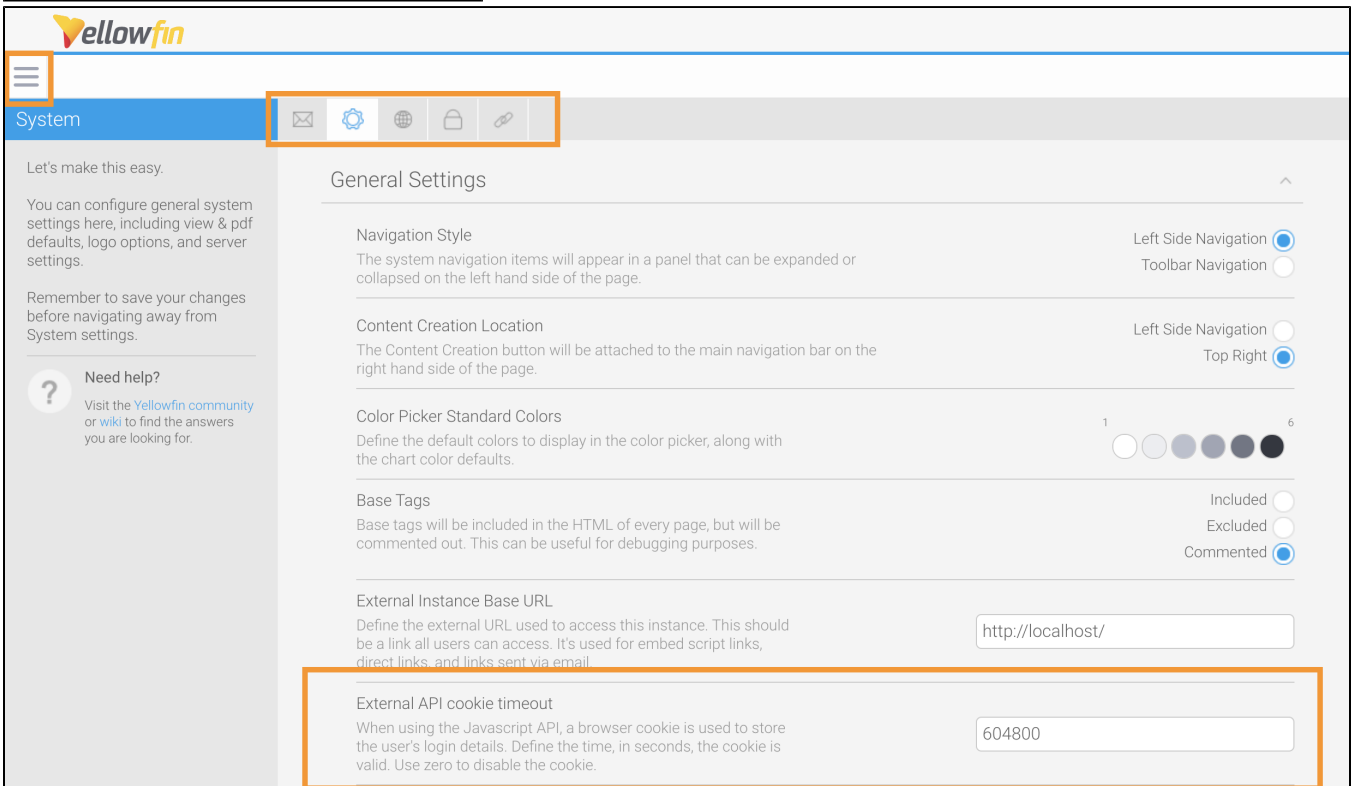
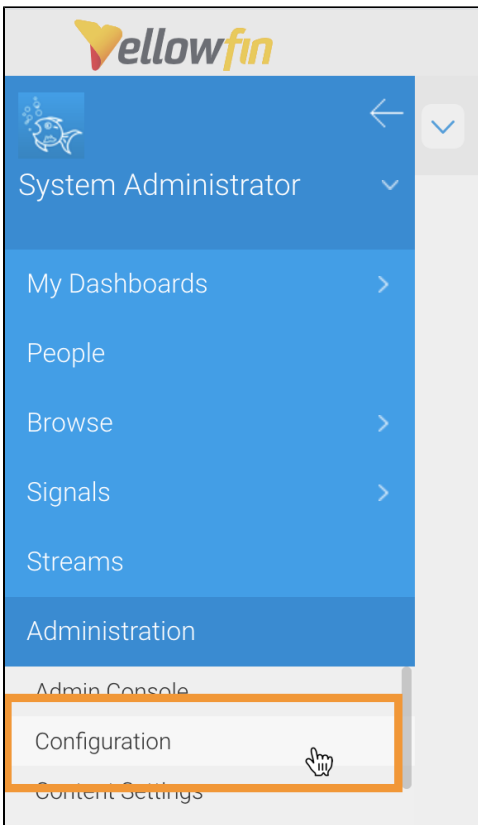
- [Overview](#)
- [External API cookie timeout](#)
- [Password settings](#)
- [Disable quick logon](#)
- [Yellowfin tools with security impacts](#)
- [Deployment and Hardening Guide](#)

Overview

The Yellowfin user interface ships with some quick wins regarding security. The most important ones are listed below, but do spend time becoming more familiar with the administration tools. There is a full section on the Yellowfin wiki dedicated to [administering Yellowfin](#).


External API cookie timeout

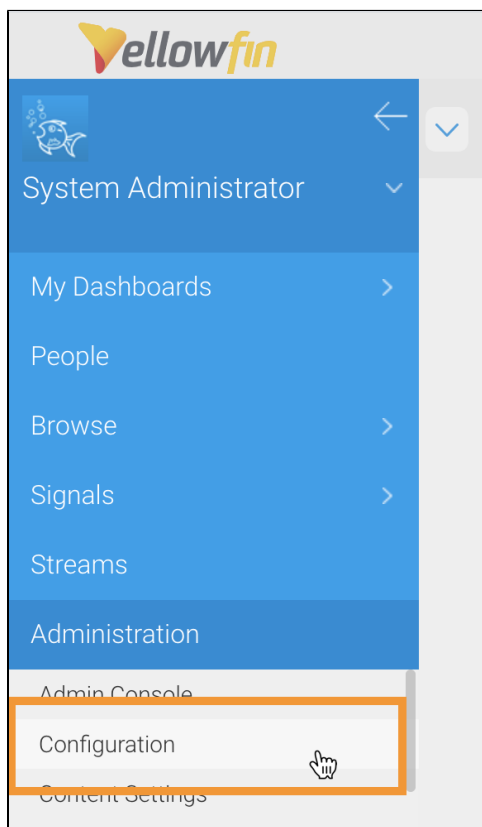
If you plan to embed content using the JavaScript API, decide the acceptable timeout length for this cookie. This can be changed from the burger bun menu  on the left, under **Administration > Configuration > System** (Gear icon) > **General Settings**.

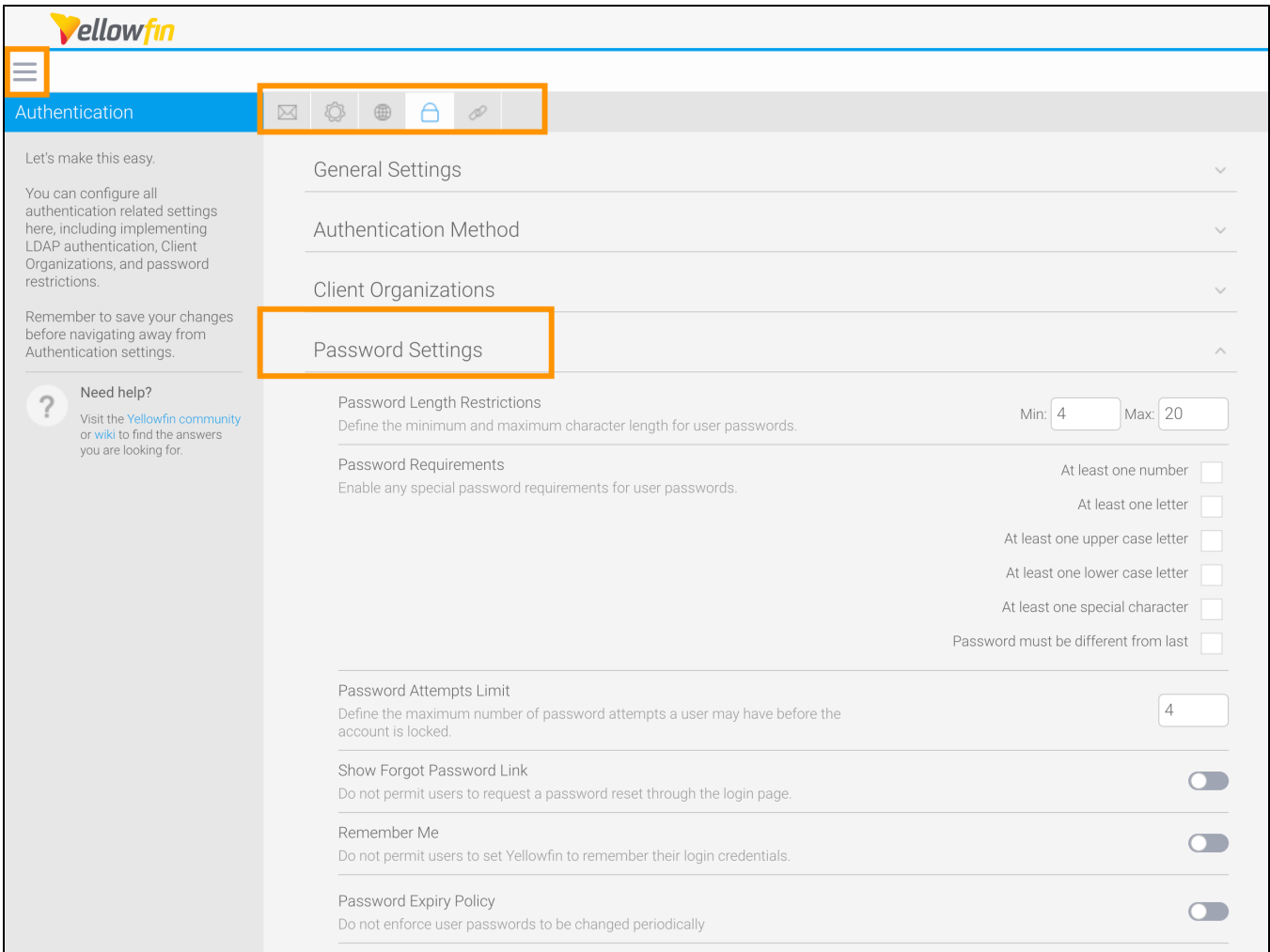


[top](#)

Password settings

Configure your password settings to meet your organizational requirements from the burger bun menu  on the left, under **Administration > Configuration > Authentication** (padlock icon) > **Password Settings**.





yellowfin

Authentication

Let's make this easy.

You can configure all authentication related settings here, including implementing LDAP authentication, Client Organizations, and password restrictions.

Remember to save your changes before navigating away from Authentication settings.

Need help?
Visit the [Yellowfin community](#) or [wiki](#) to find the answers you are looking for.

General Settings

Authentication Method

Client Organizations

Password Settings

Password Length Restrictions
Define the minimum and maximum character length for user passwords. Min: Max:

Password Requirements
Enable any special password requirements for user passwords.

At least one number ☐

At least one letter ☐

At least one upper case letter ☐

At least one lower case letter ☐

At least one special character ☐

Password must be different from last ☐

Password Attempts Limit
Define the maximum number of password attempts a user may have before the account is locked.

Show Forgot Password Link
Do not permit users to request a password reset through the login page. ☒

Remember Me
Do not permit users to set Yellowfin to remember their login credentials. ☒

Password Expiry Policy
Do not enforce user passwords to be changed periodically. ☒

[top](#)

Disable quick logon

Yellowfin offers a quick logon feature that allows users to easily log back in without entering their credentials, over roughly a 12-hour window. In environments requiring strict authentication mechanisms, this may not be desirable. To disable this, run the following SQL against the Yellowfin configuration database and restart the service.

```
UPDATE Configuration SET ConfigData='NO' WHERE ConfigCode='LOGONCOOKIE';
```

[top](#)

Yellowfin tools with security impacts

Yellowfin Tool	Description
Code Mode	Code Mode allows content creators to write their own JavaScript. This should be provided to select trusted developers only, and content should be periodically audited to validate the content.
JavaScript Charts	JavaScript Charts provides similar functionality to above, but at a report level. This feature should be treated similarly to above if in use.
Plugin Manager	The plugin manager allows users to upload custom plugins into Yellowfin. Access to this functionality should only be granted for the highest-level administrator and should include a manual code review of any custom plugins.
Freehand SQL	Freehand SQL in calculated fields, views, or reports allows content creators to manually query a data source. Keep in mind that from a security perspective, this feature is like running queries directly against an RDBMS in the context of the data source user.

Deployment and Hardening Guide

[Back to the Overview](#)

- [General Security Infrastructure Considerations](#)
- [Application Server Security](#)
- [Yellowfin UI Security Settings](#)

[top](#)