Password Protecting an Environment

Development, staging, and production environments refer to common stages of software development where an application or system is deployed and operated in isolated environments. Access to the development and staging environments is usually restricted from public access as it is in these environments that new features, code changes, and updates are tested, built, and validated before they are published on the web in the production environment.

The Password Protection feature of Contentstack Launch allows you to enable access restrictions to your development and staging environments in Launch using the Basic Auth method in order to prevent them from being accessed by search engines and the public.

This document guides you through enabling and disabling password protection for your environments in Contentstack Launch.

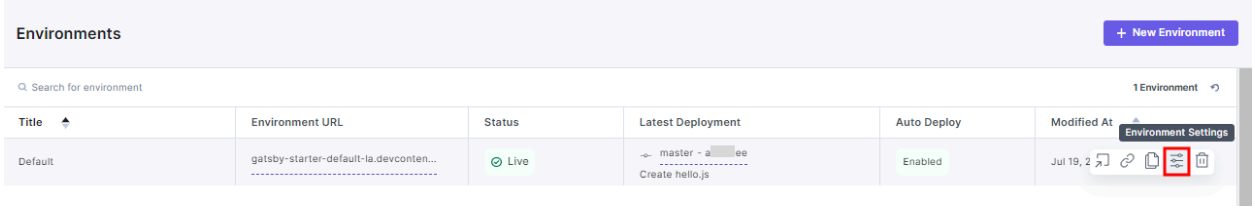
Prerequisites

1. Contentstack account
2. Access to Launch for your organization
3. A project already deployed in Launch

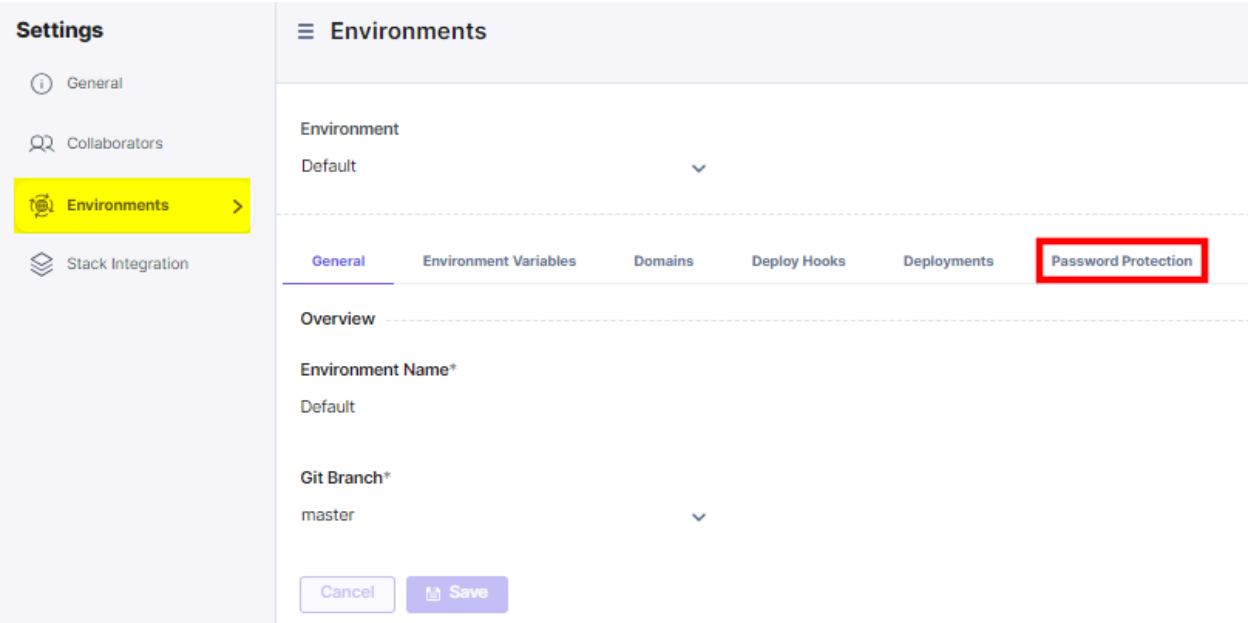
Enable Password Protection for your Environment

Follow the steps below to enable password protection for your environment:

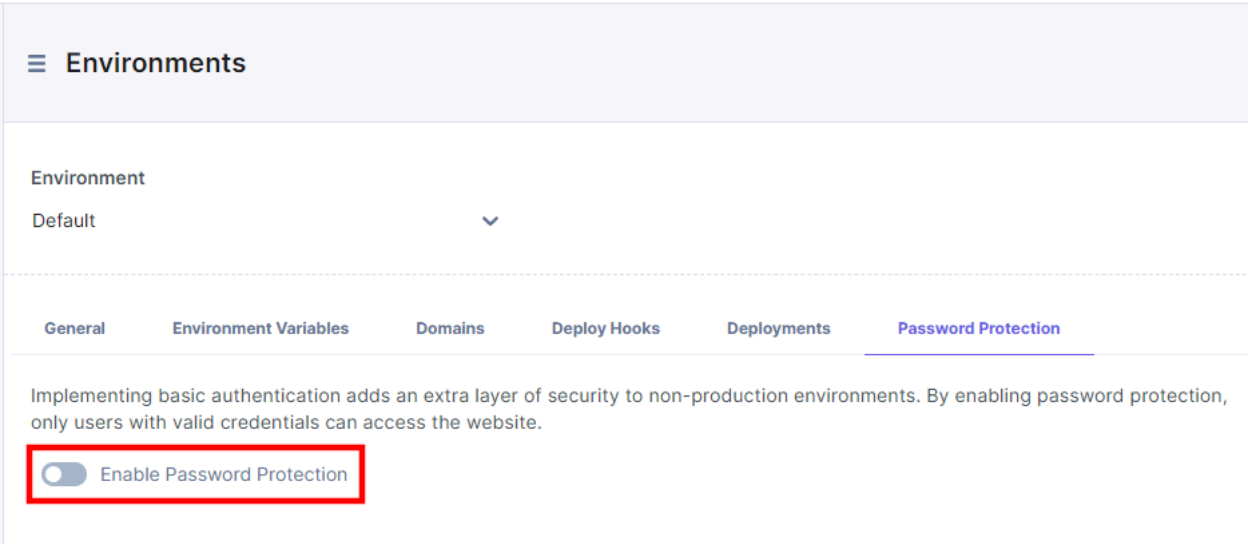
1. From the Launch landing page, click the project card to open your project.
2. In the Environments screen, hover over the environment for which you want to provide password protection, and click the Environment Settings icon.



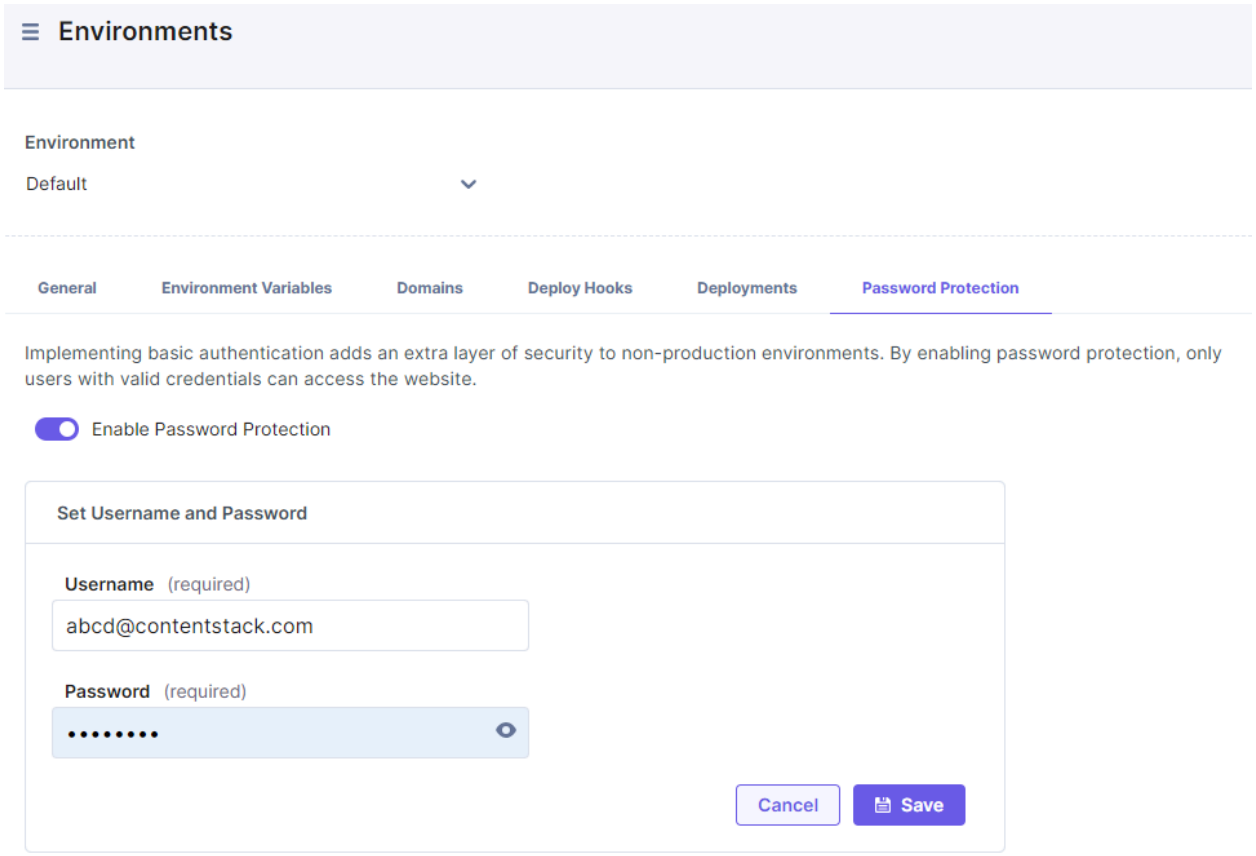
3. In Settings > Environments, click the Password Protection tab.



4. Click the Enable Password Protection toggle button to enable it.



5. Enter a username in the Username field and password in the Password field for your current environment, not exceeding 200 characters each.



Note: The username must not contain the colon (:) character.

6. Click the Save button.
   Note: The protection is specific to the selected environment. All domains within this environment will be automatically password protected.

You have now successfully enabled and set password protection for your environment.

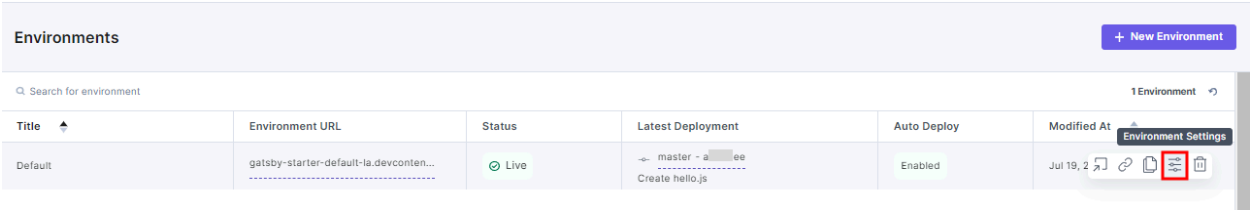
All visitors to the site or application hosted on this environment will be prompted to enter this username and password when they try to access the environment URL.

Best Practices: It is common that most modern web browsers cache Basic Auth credentials after they are successfully entered the first time. For this reason, and because the username and password set for each environment is shared for all users with whom you share these credentials, it is recommended that you change this password periodically (i.e., every three months).

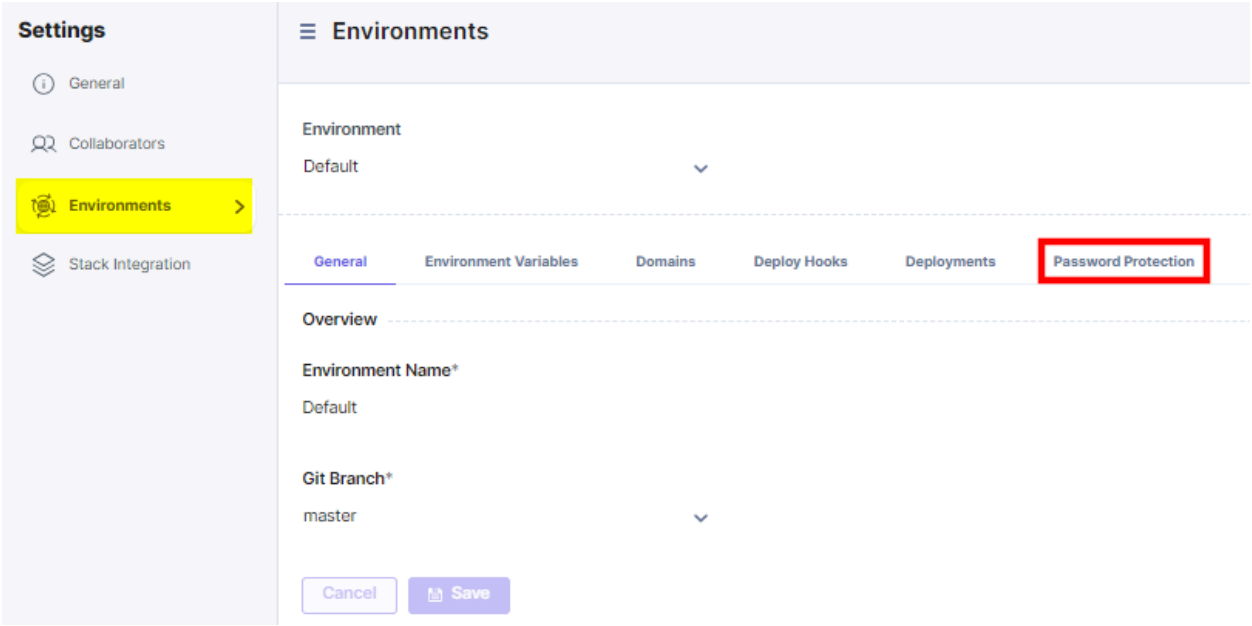
Disable Password Protection for your Environment

Follow the steps below to disable password protection for your environment:

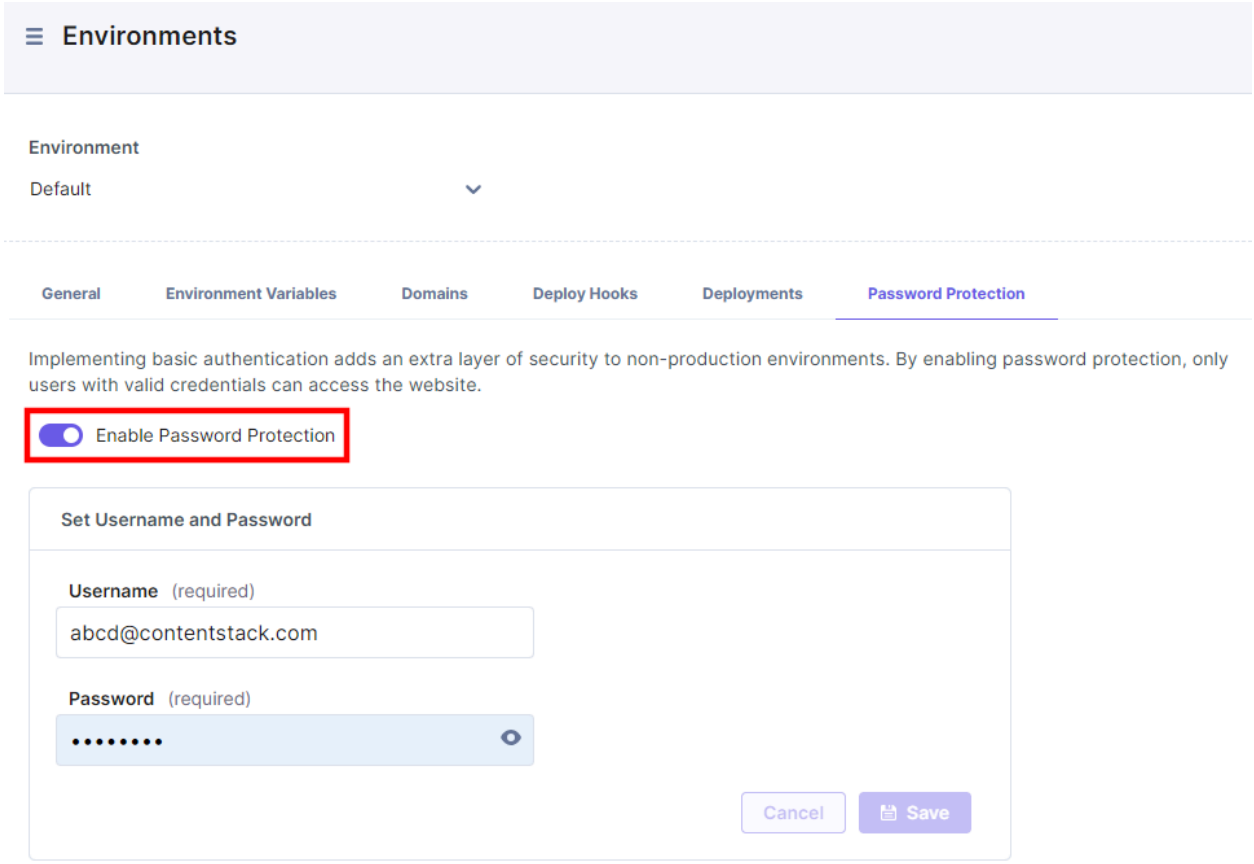
1. From the Launch landing page, click the project card to open your project.
2. In the Environments screen, hover over the environment for which you want to disable password protection and click the Environment Settings icon.



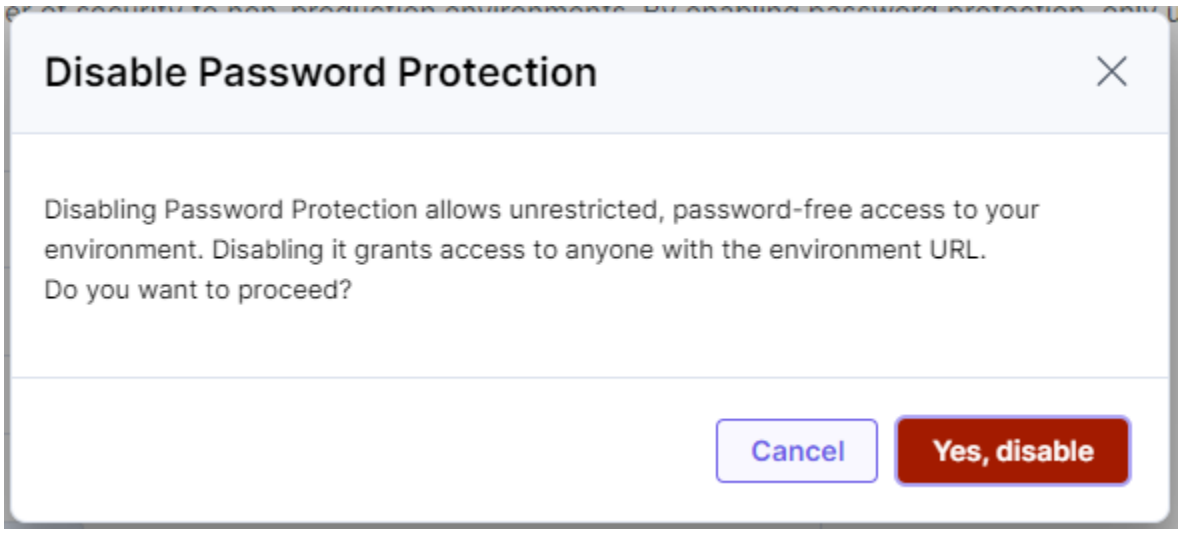
3. In Settings > Environments, click the Password Protection tab.



4. Click the Enable Password Protection toggle button again to disable the password protection.



5. Click the Yes, disable button.



You have now successfully disabled password protection for your environment. This allows anyone with the environment URL to access your environment.