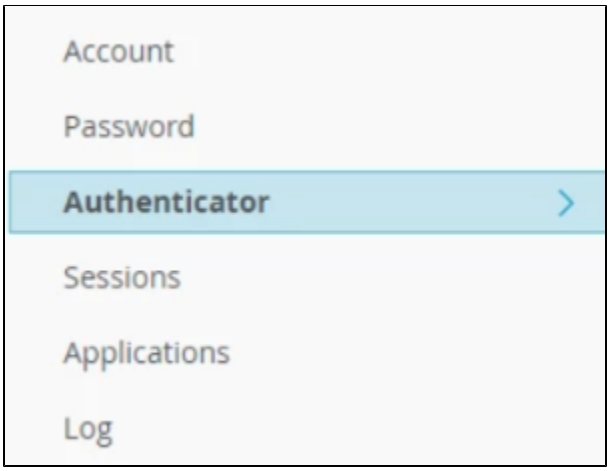
Two-Factor Authentication

For additional security, you can configure two-factor authentication (TFA) with a free authenticator application like Authy.

> Two-factor authentication exceeds standard security practices by requiring more than a username and password for login access. The authenticator software generates a token that expires within 60 seconds. This token provides the additional layer of authentication required for login.

To configure two-factor authentication:

1. Log in to security.litmus.cloud.
2. Select **Authenticator** in your profile.

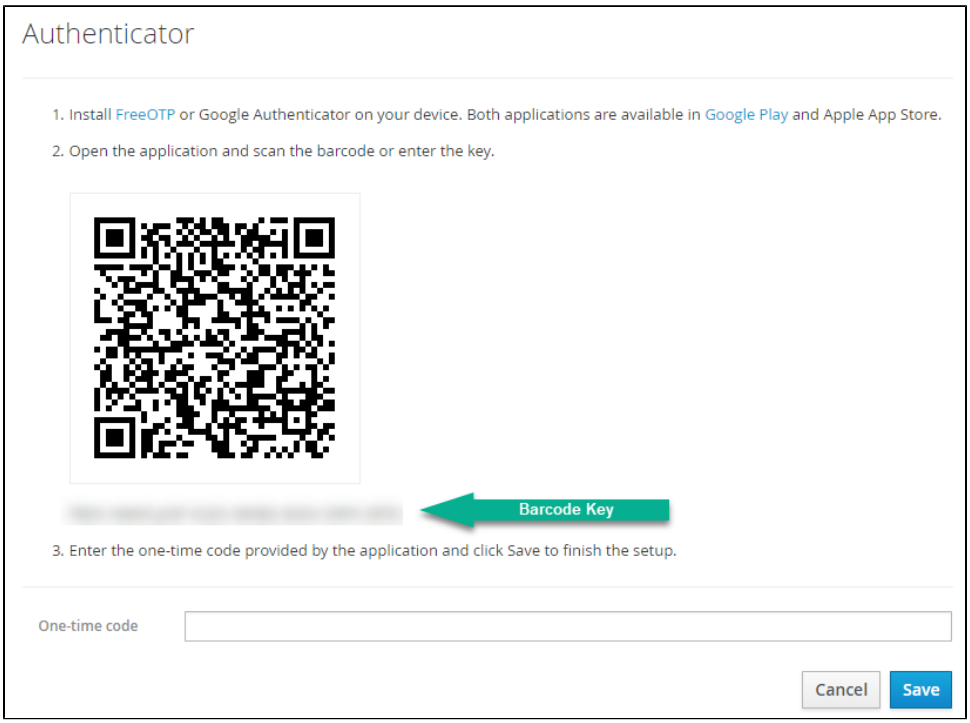


3. Download and install an authenticator on your smart phone from the Google Play or Apple App store.

> **Authenticator Applications**
>
> FreeOTP
>
> Google Authenticator
>
> Authy
>
> **Note**: These applications do not require internet access to generate a one-time code.

4. Open the authentication application on your smart phone.

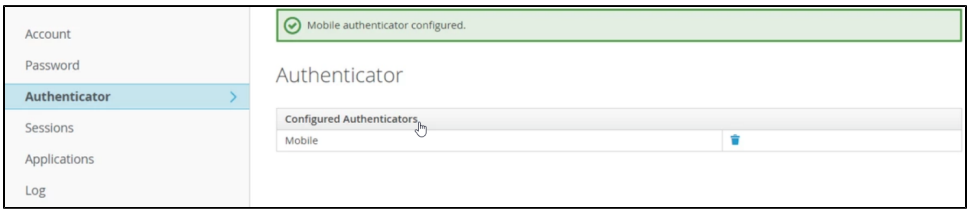
5. Scan the barcode (or enter the key) displayed on the LoopCloud Authenticator dialog.



> The authenticator application generates a 6-digit random number code.

6. In the LoopCloud Authenticator dialog, enter the one-time code generated by the application.
7. Click **Save** to complete the authentication configuration.

> Once you configure the authenticator, you will see a confirmation message.



- Once you set up two-factor authentication, you will need to use the authenticator application to access your account after entering your username and password.
- After you enter the username and password, the login will direct you to a screen to enter the one-time code generated by the application.