LogonSafe

Setup Guide

Product Overview

Thank you for using LogonSafe! LogonSafe is the world's first (and only) password security system. LogonSafe stores ALL your passwords on your mobile device, so malicious actors with access to your computer can't access your "crown jewels". It also monitors all inputs in your web browser to ensure that you're not accidentally giving an attacker your passwords through a phishing attack.

App

The LogonSafe app is the "brains" of the LogonSafe service. Your passwords are securely stored in the app on your mobile device, and requires YOU to approve their use. This prevents attackers from stealing all your passwords as they can with other password managers.

Extension

The LogonSafe browser extension communicates with the app to allow you to easily access your credentials right from the login prompts where you need them.

Additionally, the extension sandboxes your input, ensuring that when you type passwords to secured sites, they are only ever used on those particular sites, and cannot be harvested by a phishing attack.

Setup / Admin

LogonSafe is designed for business. Everything you need to know is available through the Admin interface at https://console.LogonSafe.com. From this interface you can set Locked Passwords to prevent phishing attacks, you can see logs of recent logins and attempted phishing attacks, create/delete users, and all other administrative functions.

The setup wizard will walk you through the required steps, but the highlights are:

1. Configuring your billing and administrative users
2. Configuring users (if more than just you as the admin)
3. Configuring passwords to lock against phishing attacks in Locked Passwords.

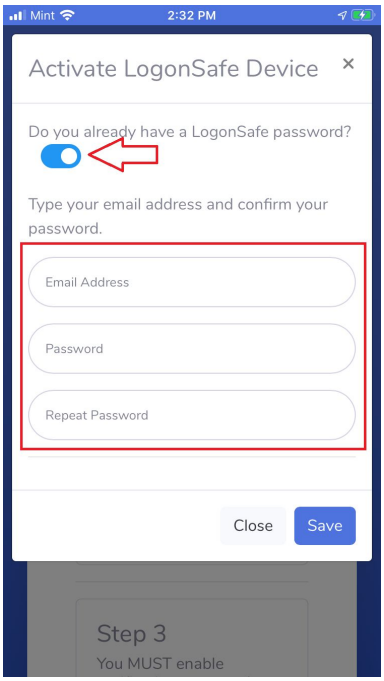
After you've completed these steps you'll want to first install the app (guide below) and then install the browser extension.

Importing passwords can take 10-15 minutes, and may require a restart of the app. Once the app is fully engaged you'll be able to take advantage of all the features in the browser extension.

Setup / App

The LogonSafe app will need to be installed by each of your employees. They can find it in their App Store (Android or iOS) by searching for “LogonSafe”.

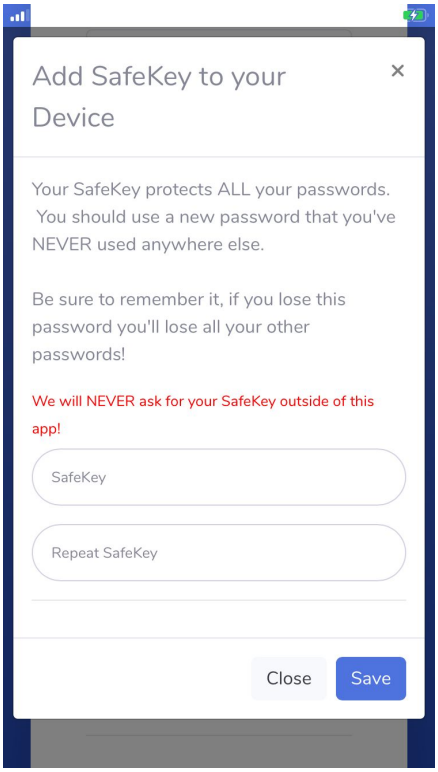
1. Use the App Store to search for “LogonSafe”
2. Install LogonSafe
3. Tap “Activate Account”
    a. If you’re an admin, be sure to click the toggle indicating that you already have an account



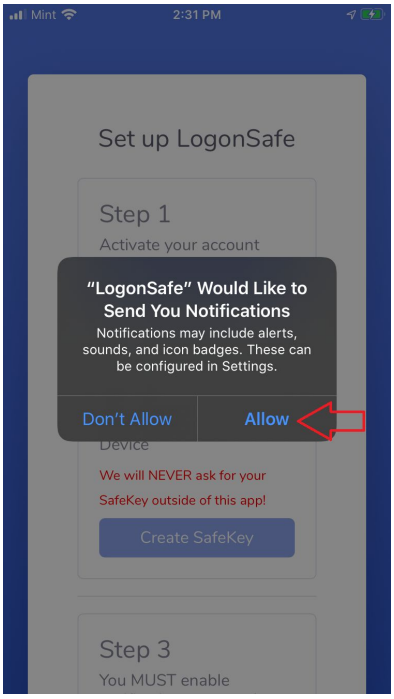
4. Otherwise use the Activation Code your IT Admin gave you during signup.

5. Tap “Create SafeKey”

Your SafeKey is what encrypts your credentials. This should NOT be the same as your account password, but SHOULD be easy to remember and type.

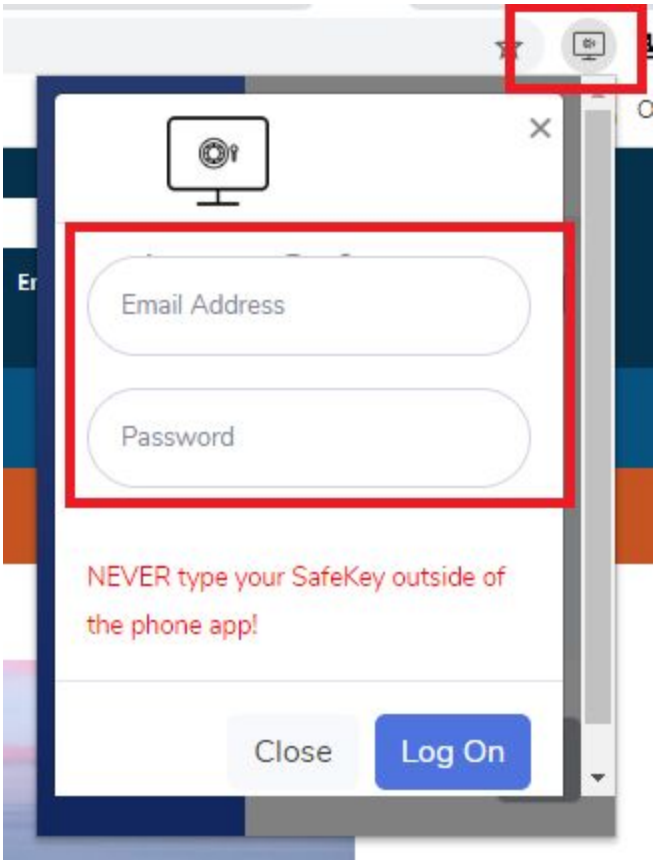


6. Ensure you select “Allow” for push notifications in order for the app to communicate with your browser plugin



Setup / Extension

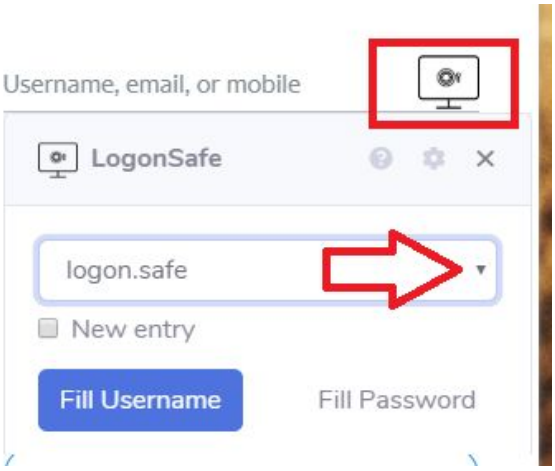
Currently, we only support Google Chrome and the new version of Edge, but we will have Firefox next. Customer demand will indicate IE support (please let me know what your preference is!).

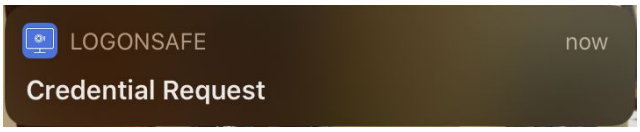
1. Go to the Chrome Browser Extension page: https://chrome.google.com/webstore/detail/logonsafe/eogndjobhgnfjnmpejnlmpbcfhlmnmdk (NOTE: you cannot search for it, please ONLY use this link)
2. Click "Add to Chrome"
3. Once installed, accept all the various security permissions (yes, we need all those permissions. No we will NEVER track you :-)).
4. Once Installed, Click the LogonSafe icon next to your URL bar and use your username and password (NOT your SafeKey) to log in.
   a. 

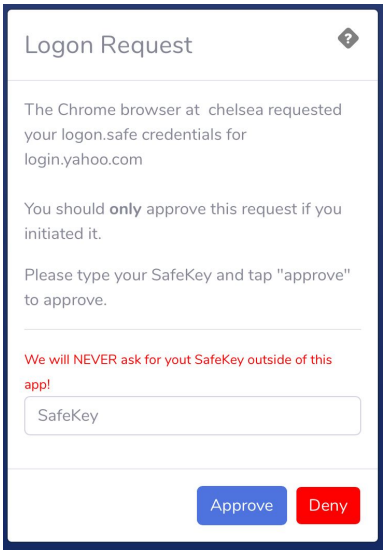
5. All Done! You can import your credentials from other services, or just add them as used.

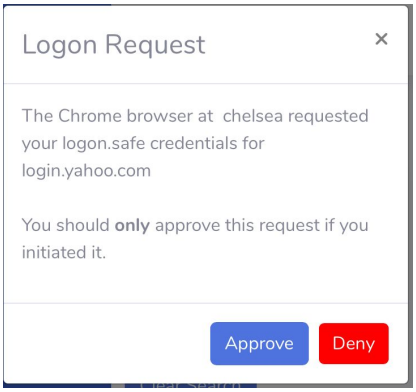
Use the service

The service itself should be fairly self-explanatory, especially if you've used a password manager before. The main difference revolves around our patent-pending process to store and access our credentials.

1. When you want to access your stored credentials, click the LogonSafe icon on the input field
    a. If we have credentials, the prompt that appears will display all of them in a drop-down menu.
    b. 

2. Usernames will fill instantly, but when you request a password, it will send a push notification to your device and the browser waits for a response.
3. On your phone
    a. Tap the notice on your home screen
        i. 

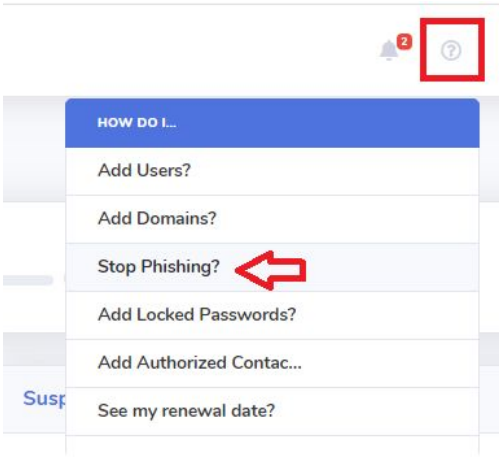
        ii. Then type your SafeKey into the approval modal
        iii. 

    b. OR - If you're already signed in to the app, simply click the "Approve button on the approval pop up.
        i. 

The other key difference is our patent-pending process for sandboxing user input to prevent against phishing scams.

LogonSafe monitors user inputs on EVERY website, in order to ensure that no website can trick your users into typing specific passwords where they do not belong.

In order for LogonSafe to prevent a password from being phished, you'll need to create a Locked Password. This essentially tells the LogonSafe app which sites to protect with the anti-phishing service. For instance, you may want to add banks, email/cloud office services, etc.

1. Log in to https://console.LogonSafe.com
2. To add a password to the anti-phishing service:
    a. Click the question mark to bring down the help menu
    b. Then "Stop Phishing"
    c. 

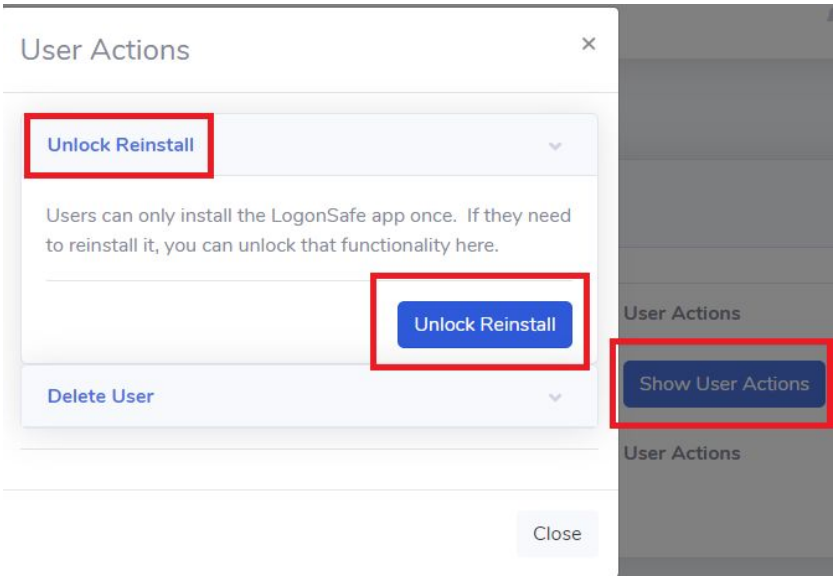
And you can follow these steps to whitelist sites if you ever need to prevent the anti-phishing from monitoring inputs:

1. Log in to https://console.LogonSafe.com
2. To whitelist a site from the anti-phishing protection:
    a. Click “AntiPhishing Whitelist” on the left
    b. Type the hostname into the “website” field and click “add”
    c. 

To disable any antiphishing entries, use the toggle next to them in the list below the new entry.

Finally, our roadmap for the future of LogonSafe requires that there only be one “primary device” (i.e. your cell phone) at a time. In order to ensure that, the account Admin has to approve reinstallations after the first one. So, if you get a new phone (or when the beta ends), you’ll need to approve the reinstall to a new device before you install LogonSafe to it.

1. Log in to https://console.LogonSafe.com
2. Click “Users/Domains” in the left menu
    a. Click “Show User Actions” next to the user you want to interact with
    b. Click “Unlock Reinstall”
    c. Click the “Unlock Reinstall” button in the drop down.
    d.



That’s it!

Thank you for your business and for being a part of the LogonSafe family!