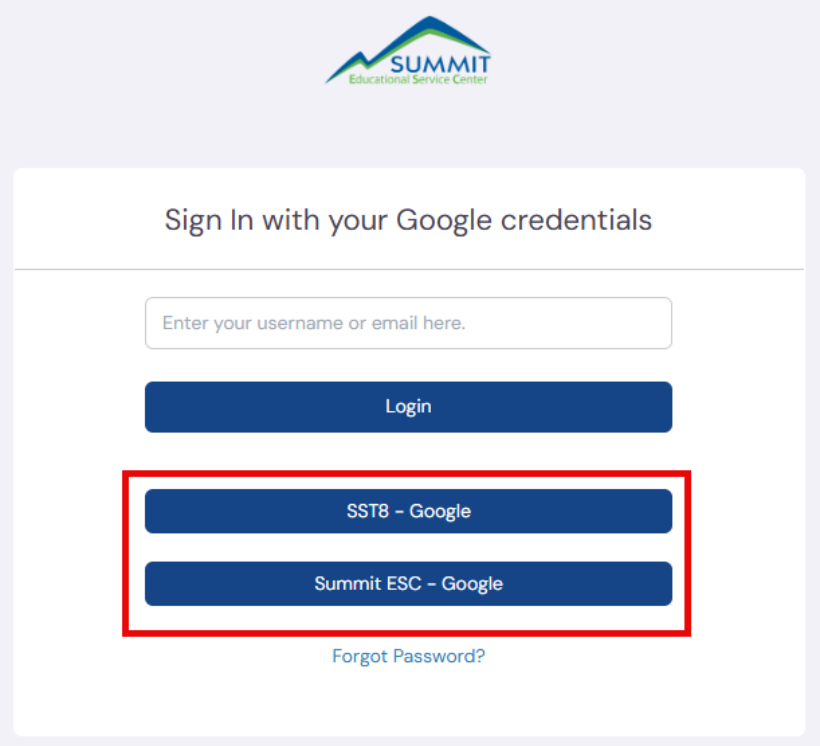
# Setting Up Your Mini-Orange Account

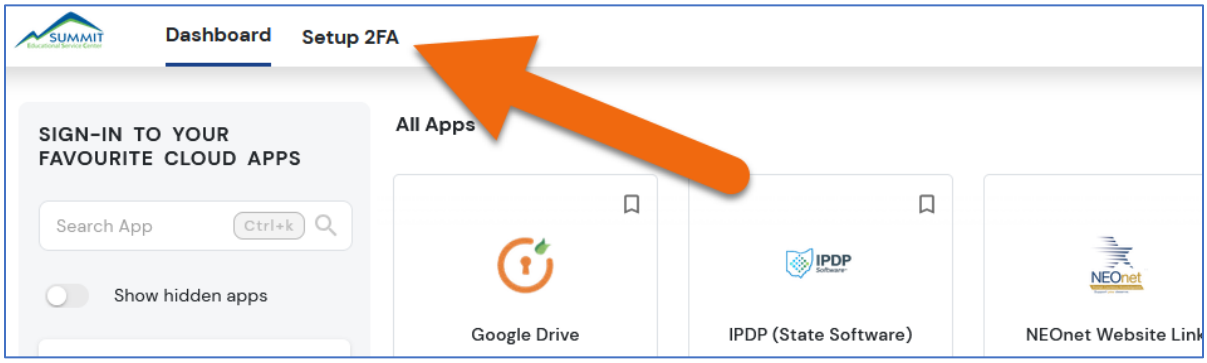
## What You Need to Do

Log into the Mini-Orange Portal and establish your choice of 2FA.

1. Browse to [https://neonet-su.xecurify.com/moas/login](https://neonet-su.xecurify.com/moas/login) and click the appropriate **Google** button to login with your Google account. (Summit ESC or SST8 depending on which Google account you have)

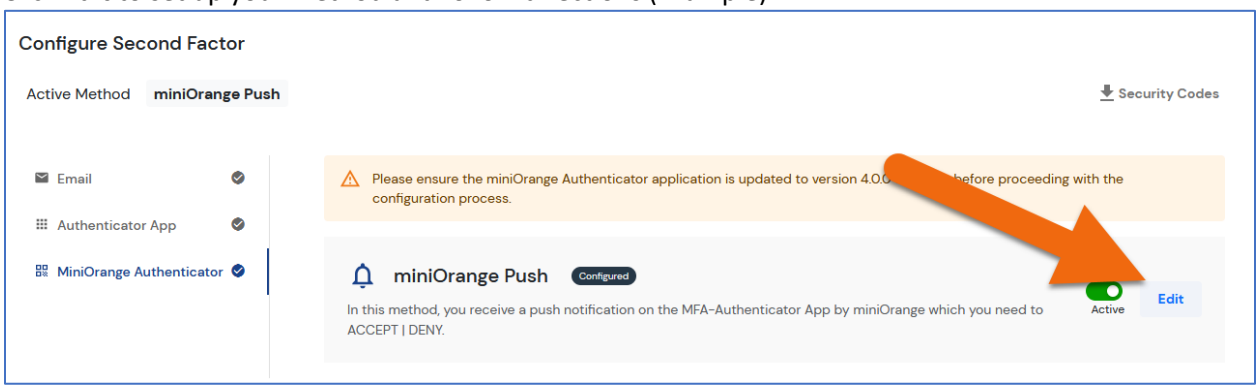



2. Click **Setup 2FA** at the top of the screen

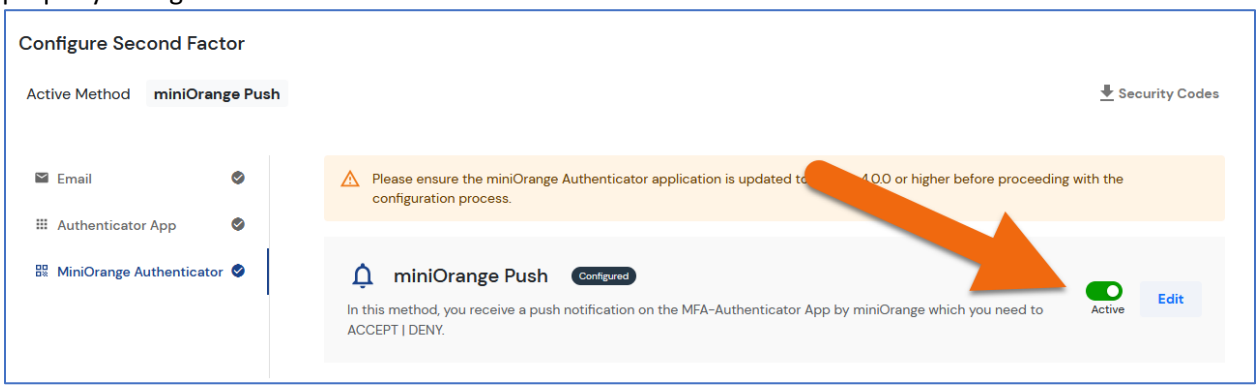



3. **Choose** one or more methods of authentication that you prefer
    1. The Mini-Orange Authenticator app is recommended
    2. But if you want to use either the Google or Microsoft Authenticator apps you are welcome to do so.
    3. If you don't want to use an app, you can choose to have it email you a one-time-code.

4. Click **Edit** to set up your method and follow directions (Example)




5. Turn ON the method by clicking the gray "Inactive" slider to make it Green. Or it may become **Active** once properly configured.




You do not need to do anything else.

As we connect more applications to our Mini-Orange accounts, we will automatically publish those applications to your Mini-Orange Dashboard!

---

## ABOUT MINI-ORANGE

**What Is Mini-Orange?**
Mini-Orange is a cybersecurity company specializing in Identity and Access Management (IAM) solutions, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), and adaptive authentication. It provides secure, cloud-based, and on-premise access to applications, protecting user identities for over 25,000 customers.

**Why are we using Mini-Orange?**
Mini-Orange is one of the top solutions available to tie together many of your logins into a single unified and protected service. This means that rather than having separate usernames and passwords for many of your work-related applications, you can have ONE that handles it all for you. Because your identity is protected behind Mini-Orange's security it is much harder for your identity to be stolen. And if that still happens, you can change just this one password, and it will control the other connected accounts for you.

Security *and* convenience? Win-Win

---

# ABOUT 2FA

**What Is Two-Factor Authentication (2FA)?**
Two-factor authentication (or two-step authentication) is an important security measure that adds a second layer of protection in addition to your password. Adding this additional security layer makes it much harder for hackers to break into your accounts. 2FA is essential to web security because it immediately neutralizes the risks associated with compromised passwords. If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access: without approval at the second factor, a password alone is useless

**Why are we establishing 2FA?**

- Since personal data is visible in many different applications, we are required to take steps to secure access to our accounts.
- Insurance providers are **requiring** districts to have 2FA for cyber-security coverage.
- The simplest and least expensive way to provide 2FA service to our employees is to authenticate through the user's smartphone through an Auth App, text, email and/or phone call.