myILMS

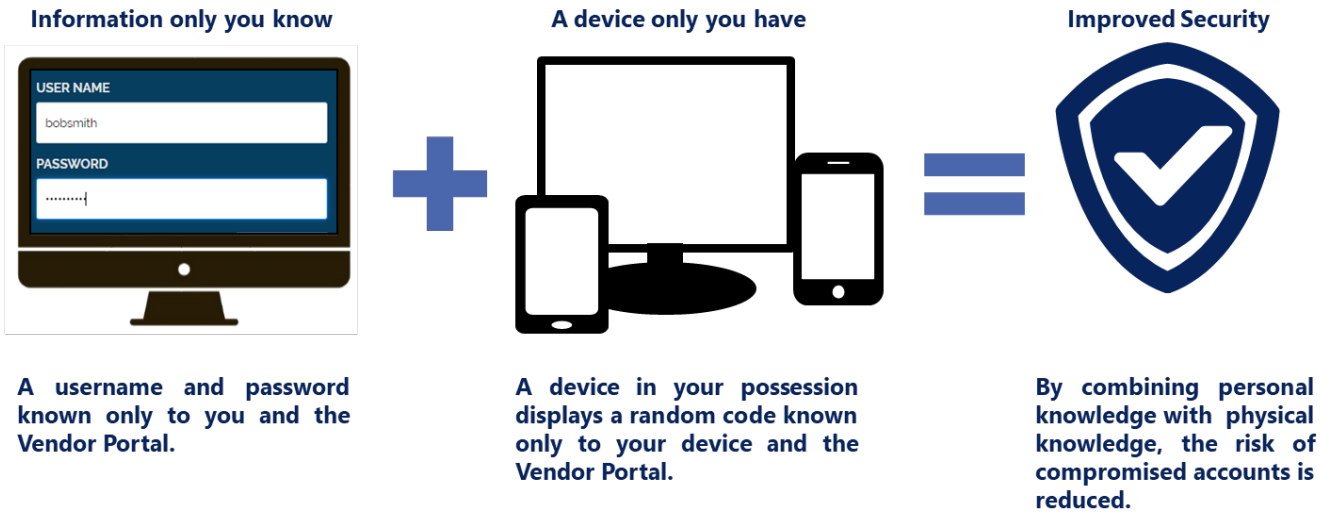
logistics for diplomacy

Multifactor Authentication

Multifactor Authentication

OVERVIEW

- Multifactor Authentication (MFA) is an extra layer of security designed to help authenticate a user's identity every time they log in to the Procurement Portal. It is required for ServiceNow systems to satisfy the Department's Identification and Authentication control requirements.
  - MFA applications are free to use.
  - MFA does not require internet or cell tower connectivity to function.



Multifactor Authentication

USER SPECIFIC NEEDS

Multiple platforms are currently available for users within ServiceNow, based on their MFA preferences and access to authentication devices.

For users with a smart phone… Google Authenticator is a great MFA tool that is developed with a smartphone app that users can download directly to their personal devices. Each login attempt will notify users of an attempt which can be approved via an in app notification. Note, a smartphone is required for setup.

For users who do not have a smart phone… Authy is an alternative that offers setup that does not require a smartphone, and provides alternatives to an app verification method. Authy provides desktop methods and added security for shared public devices.

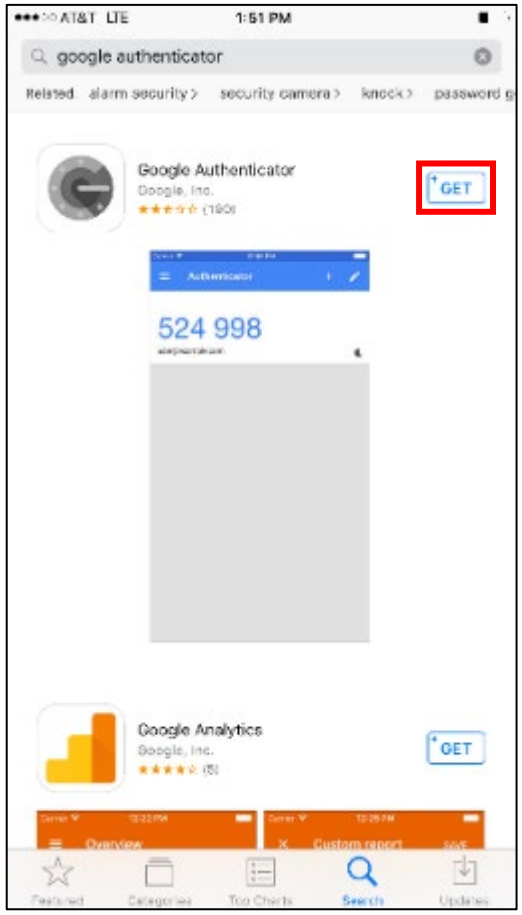
For users who do not have a phone… WinAuth provides users with a setup method to completely bypass setup with a phone. This method is simple and easy to use for users who will be using only a desktop device

myILMS
logistics for diplomacy

Google Authenticator

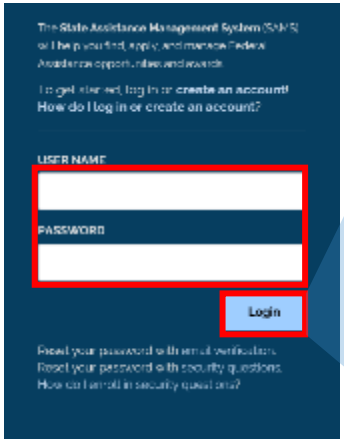
Google Authenticator
SETUP

Google Authenticator setup is performed with a smart device. The following instructions are for iOS, however, MFA with Google Authenticator is possible with Android and other mobile software.



1. Download the **Google Authenticator** app to a smart device. Note that **Google Authenticator** is a free app that will not charge your account.

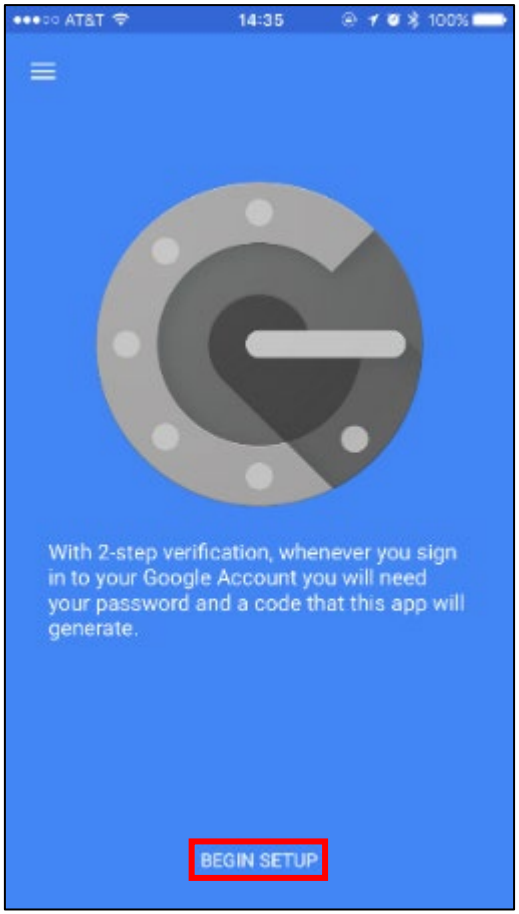
2. **Log in** to the Invoice Submission Portal using the username and password provided via email during account creation.

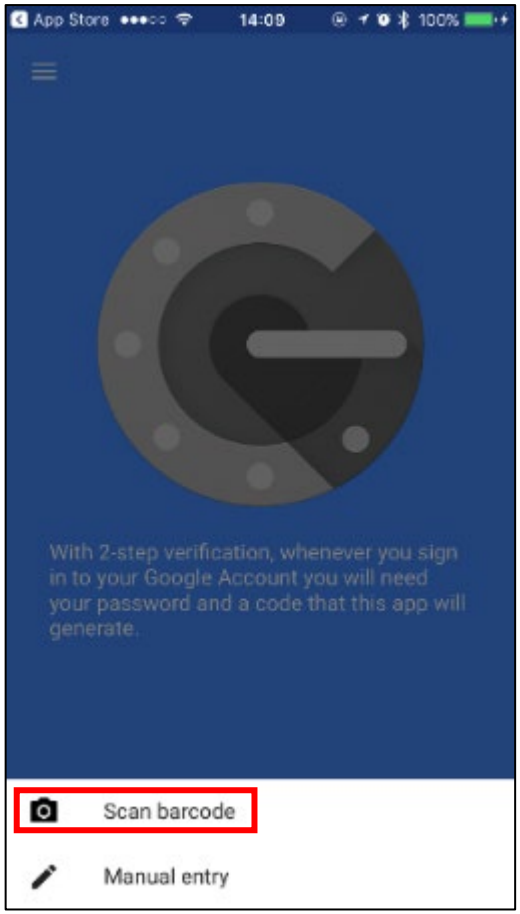


3. The **Enable multi-factor authentication** page will load.

Google Authenticator
SETUP

It is recommended to set up MFA with a smart device like a smartphone or tablet that will be reliably available when logging into the Invoice Submission Portal.



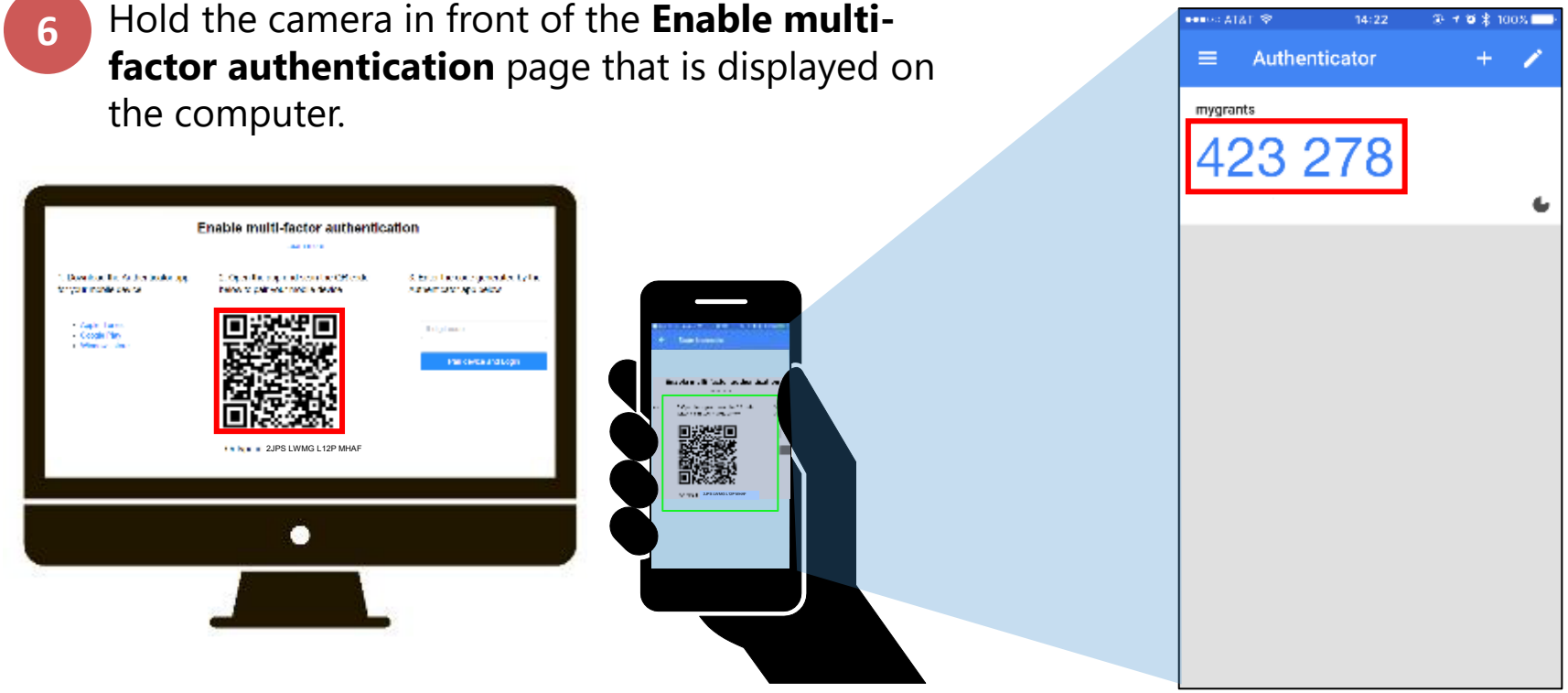


4 Tap **BEGIN SETUP**.

5 Tap **Scan Barcode**. The Google Authenticator app will activate the smart device's camera.

Google Authenticator
SETUP

6 Hold the camera in front of the **Enable multi-factor authentication** page that is displayed on the computer.



7 Use the light green box projected on the smart device screen to center the **QR code** and scan it.

8 When the smart device recognizes the **QR code** displayed on the computer screen, the **Google Authenticator** app will automatically generate an **authentication code**.

Google Authenticator
SETUP

9 Return to the **Enable multi-factor authentication** page on the computer. Type the **authentication code**, without spaces, into the **authentication code** field.

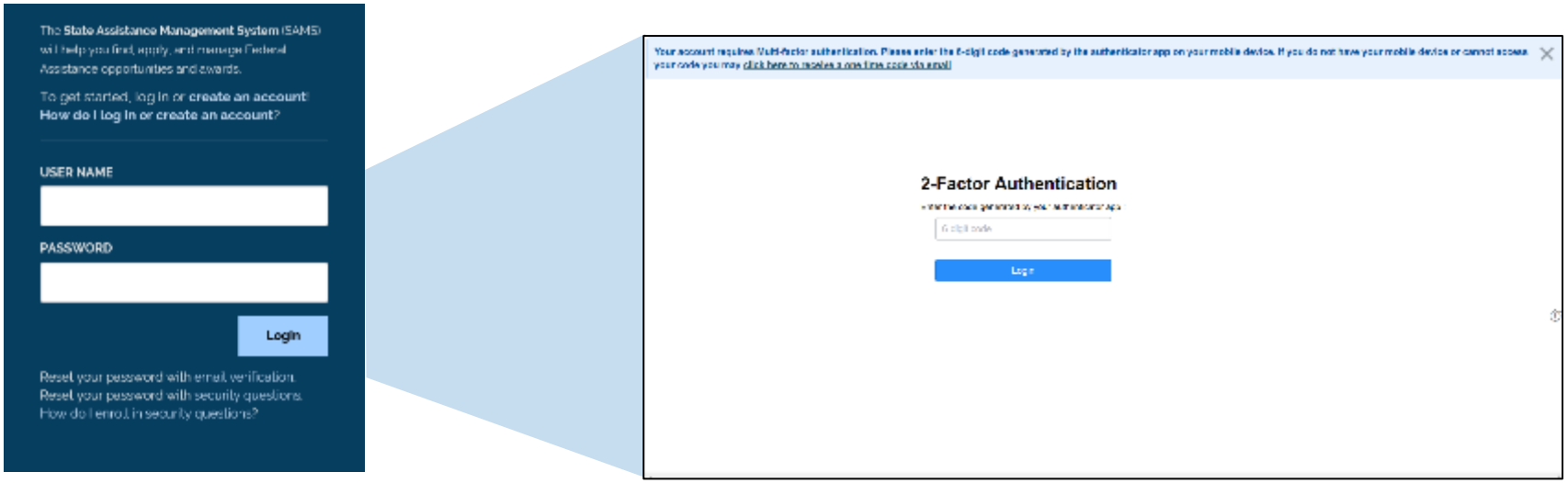
10 Click **Pair device and Login**.

Note: This ends the one-time setup for Google Authenticator. For subsequent logins, only user verification is required.

Google Authenticator
LOGGING IN

MFA is required every time a user logs into the Invoice Submission Portal. Each account must only be accessed by the user registered to the account.

1 Log in to the Procurement Portal. The Procurement Portal will now display a **2-Factor Authentication** page.

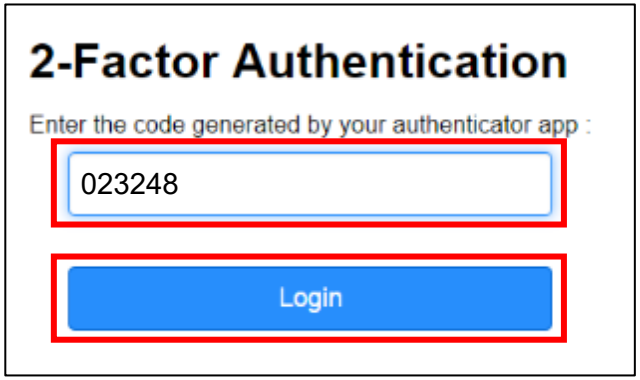


2 Open the **Google Authenticator** app.

Google Authenticator
LOGGING IN

3 Upon opening, the **Google Authenticator** app will automatically generate an **authentication code** under the heading “mygrants”.

4 On the Invoice Submission Portal **2-Factor Authentication** page, type the **authentication code** (without spaces) in the **authentication code** field.



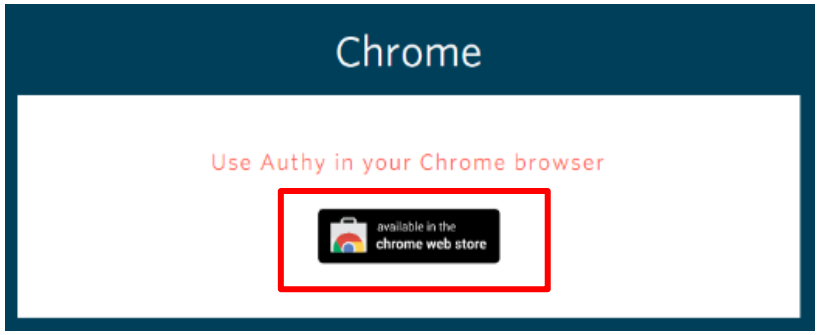
5 Click **Login**.

myILMS
logistics for diplomacy

Authy

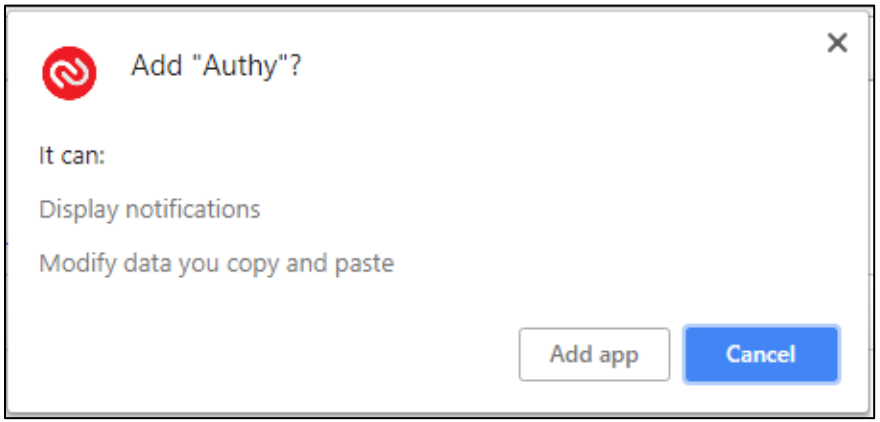
Authy
SETUP

Authy setup is performed with a smart device, Google Chrome Browser Extension, or a desktop app. The following instructions are for the Chrome Extension.



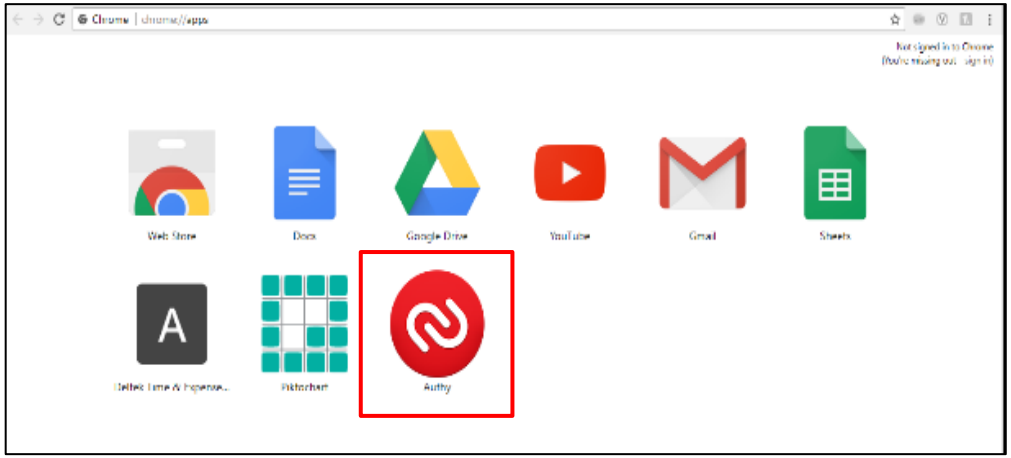
1. Open Google Chrome and go to https://authy.com/download. Click the **chrome** icon.
2. Click **Add To Chrome**.

3. Click **Add app** in the pop-up window.

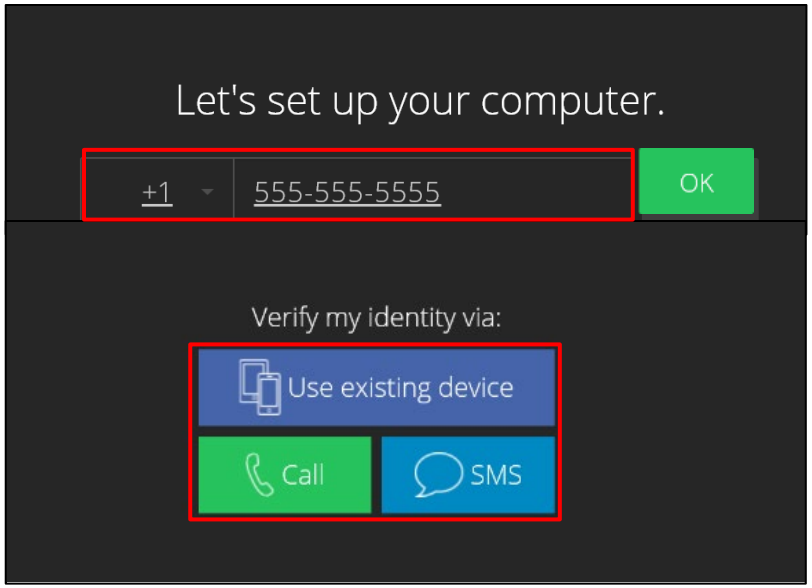


Authy
SETUP

4 Click the **Authy** icon in Google Chrome.



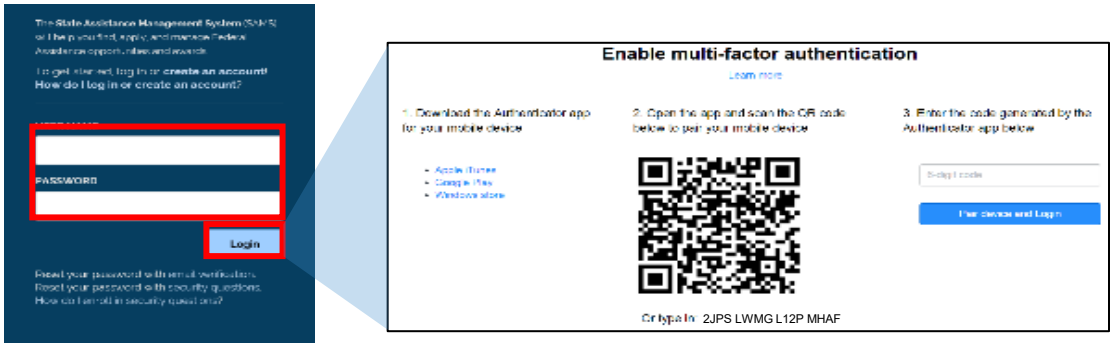
5 Select a country code, enter a phone number and click **OK**.



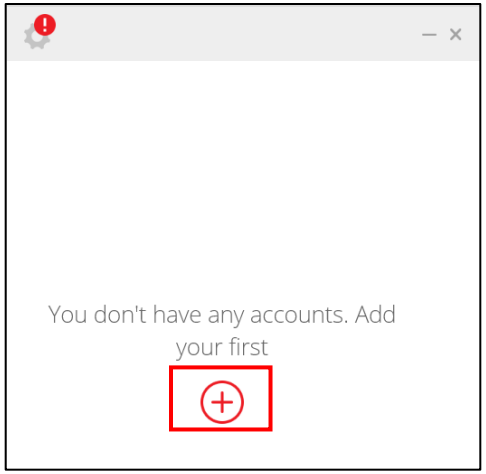
6 **Verify** the users identity by selecting to receive a verification code through one of the listed methods.

Do not close the Authy window at this time.

7 **Log in** to the Invoice Submission Portal using the username and password provided via email during account creation.

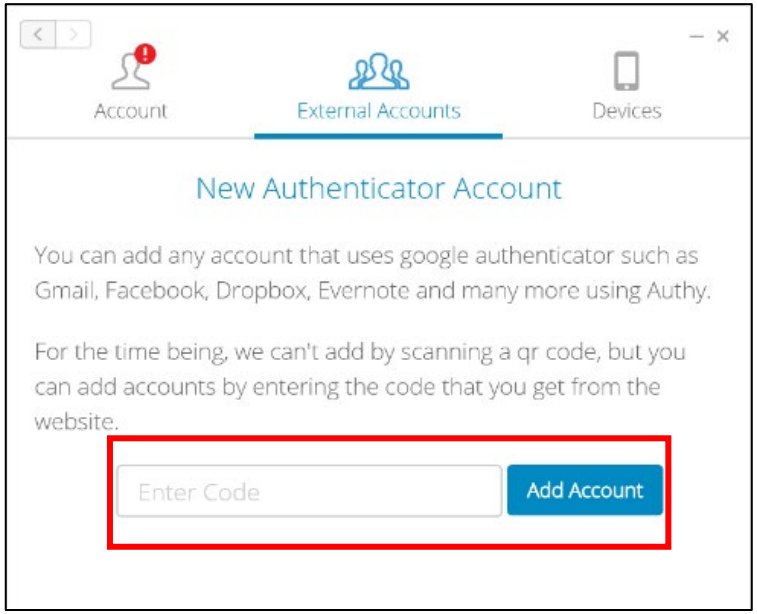


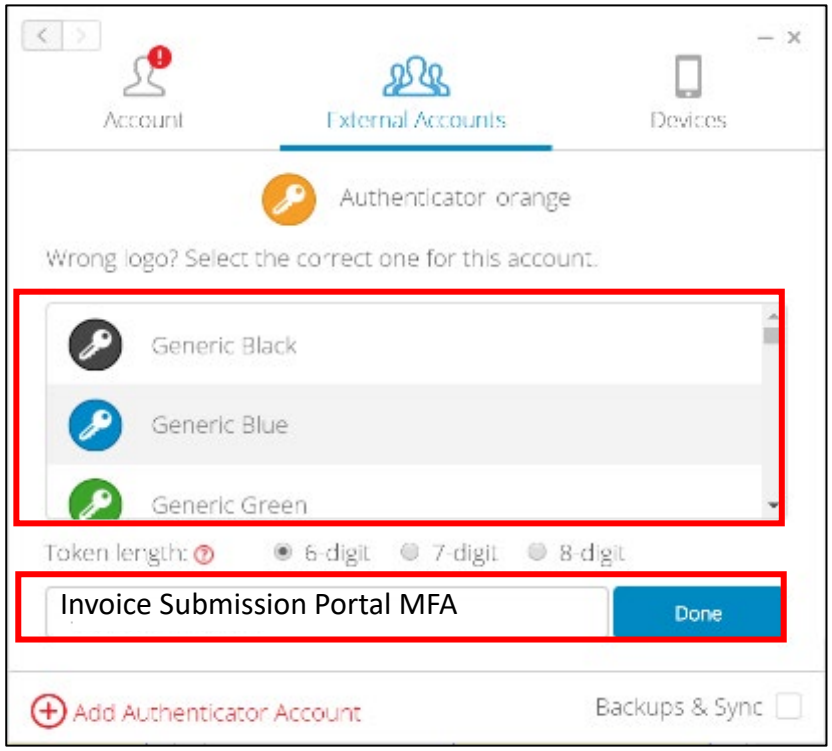
8 Copy the unique code on the **Enable multi-factor authentication** page. Return to the Authy Window.



9 Click the **plus icon** on to add an account.

10 Paste the code from the **Enable multi-factor authentication** page into the **Enter Code** field and click **Add Account**.





11 Select a color icon, and enter **"Invoice Submission Portal MFA"** into the text box.

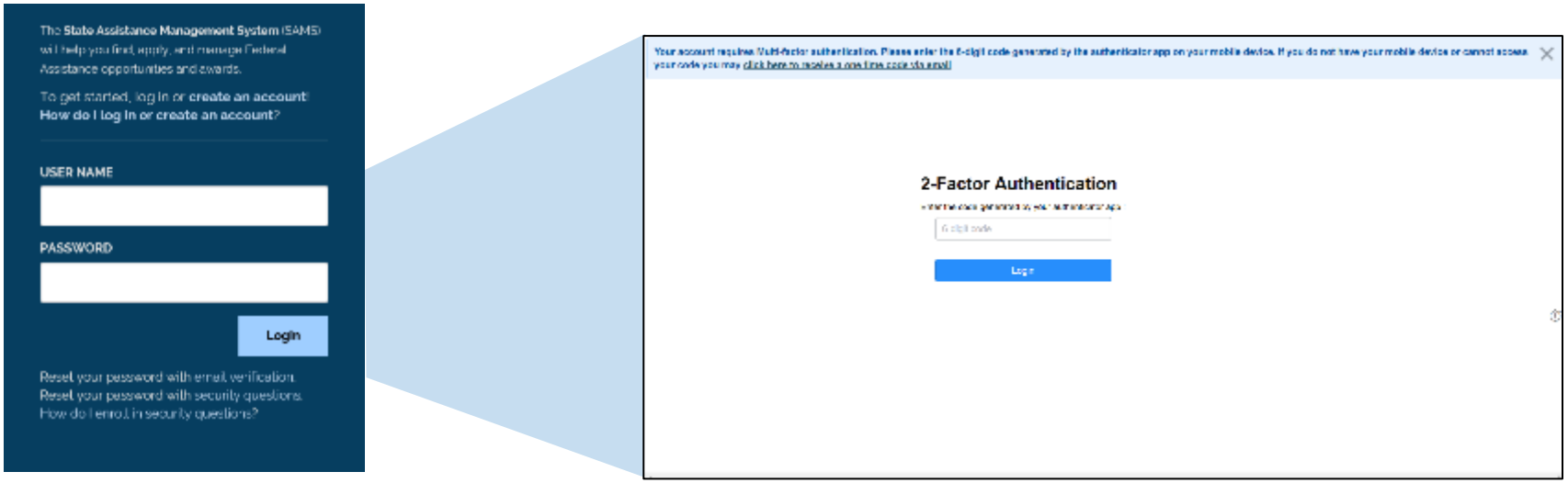
12 Click **Done**.

Note: This ends the one-time setup for Authy. For subsequent logins, only user verification is required.

Authy
LOGGING IN

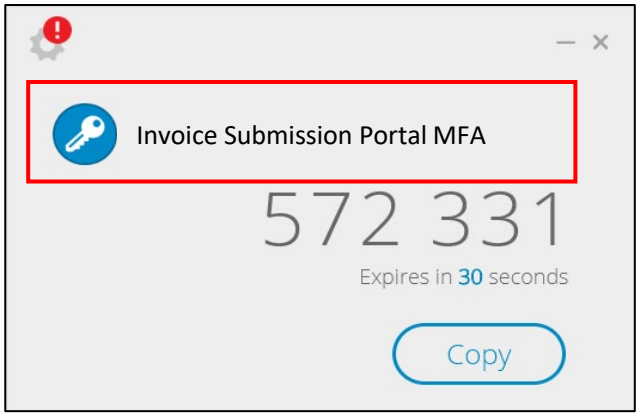
MFA is required every time a user logs into the Invoice Submission Portal. Each account must only be accessed by the user registered to the account.

1 Log in to the Procurement Portal. The Procurement Portal will now display a **2-Factor Authentication** page.

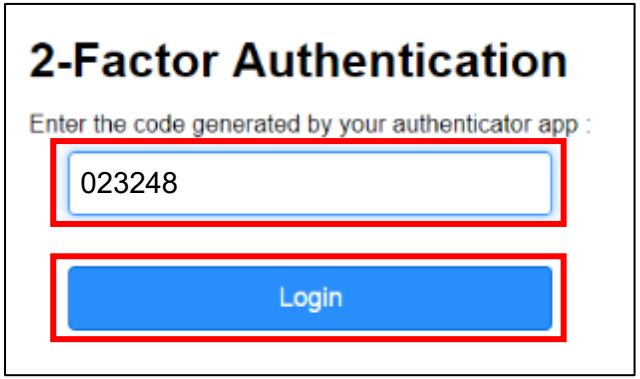


2 Open the **Google Authenticator** app.

3 Upon opening, **Authy** will automatically generate an **authentication code** under the heading "Invoice Submission Portal MFA".



4 On the Procurement Portal **2-Factor Authentication** page, type the **authentication code** (without spaces) in the **authentication code** field.



5 Click **Login**.

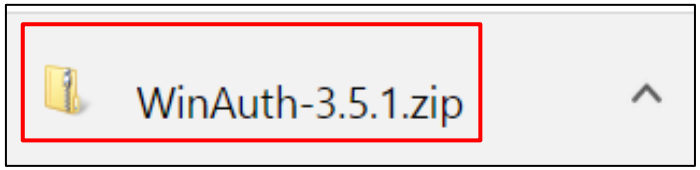
myILMS
logistics for diplomacy

WinAuth

WinAuth
SETUP

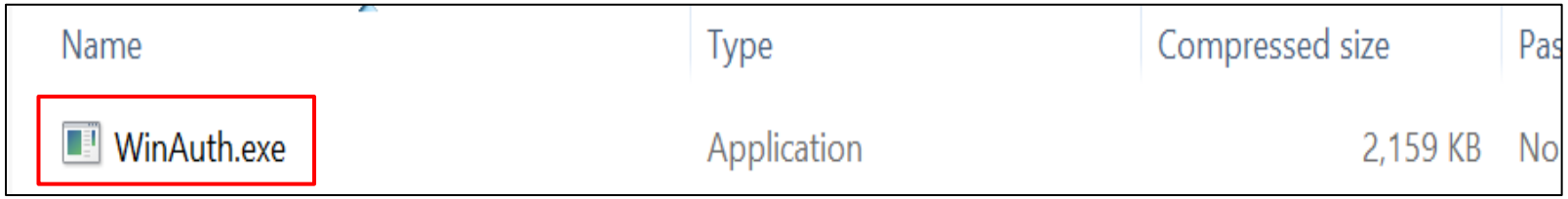
WinAuth setup is performed on a user's desktop.

1. Download the **WinAuth** to your desktop by opening a browser and navigating to https://winauth.github.io/winauth/download.html. Click on the latest version of **WinAuth** to download it.



2. Click on the **zip folder** after it appears in the Downloads folder in.

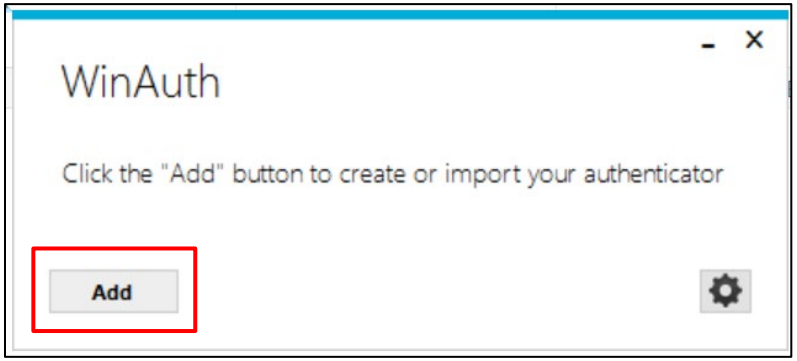
3. Once the folder is opened, **double click** the WinAuth.exe file.



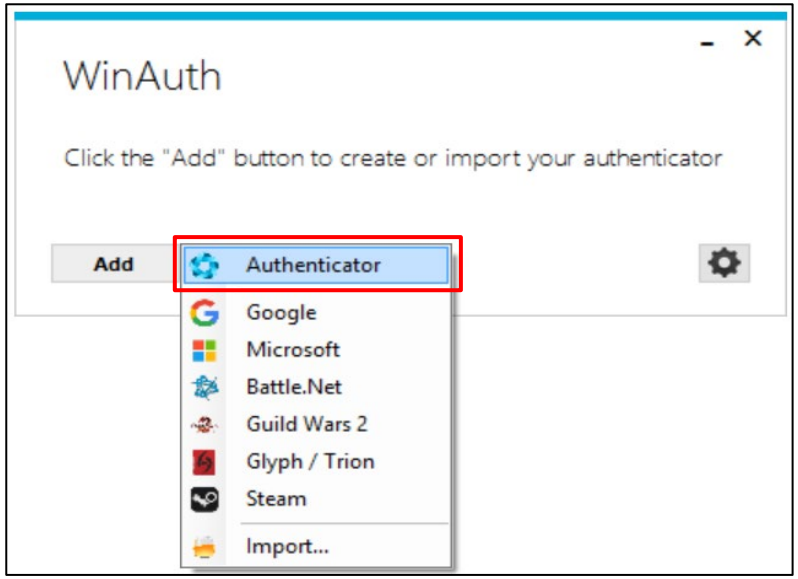
WinAuth
SETUP

myILMS

4 Click the **Add** button in the WinAuth window.



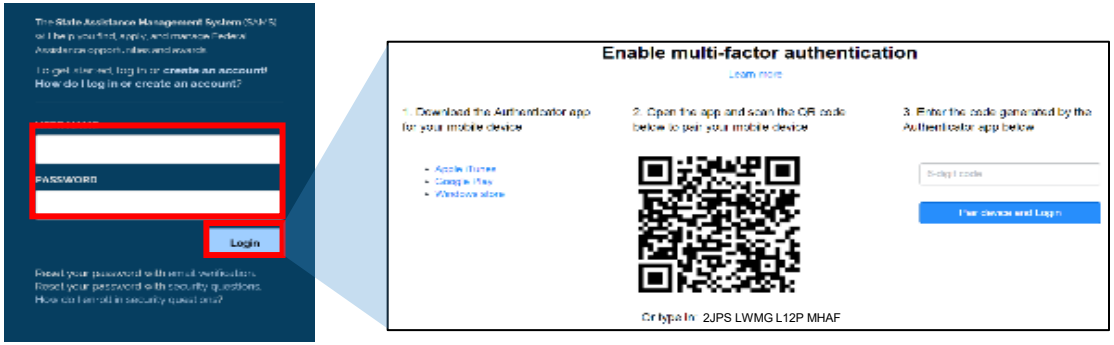
5 Select **Authenticator** from the Add dropdown menu.



6 In the **Name** field, type "Invoice Submission Portal MFA".

Do **not** close the WinAuth window at this time.

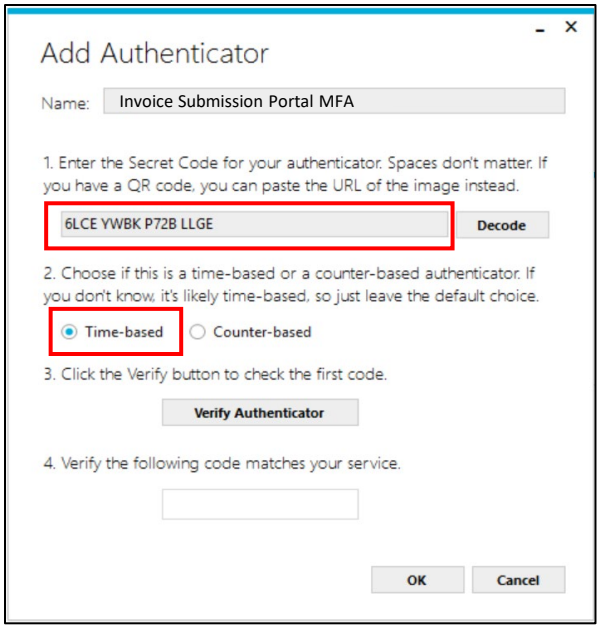
7 **Log in** to the Invoice Submission Portal using the username and password provided via email during account creation.



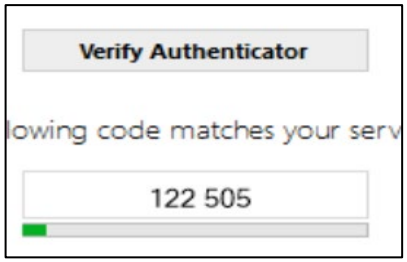
8 On the **Enable multi-factor authentication** page, copy the unique code. Then return to the **WinAuth** window.

9 Paste the unique code from the **Enable multi-factor authentication** page into the **Secret Code** field. Be sure to select "Time-Based".

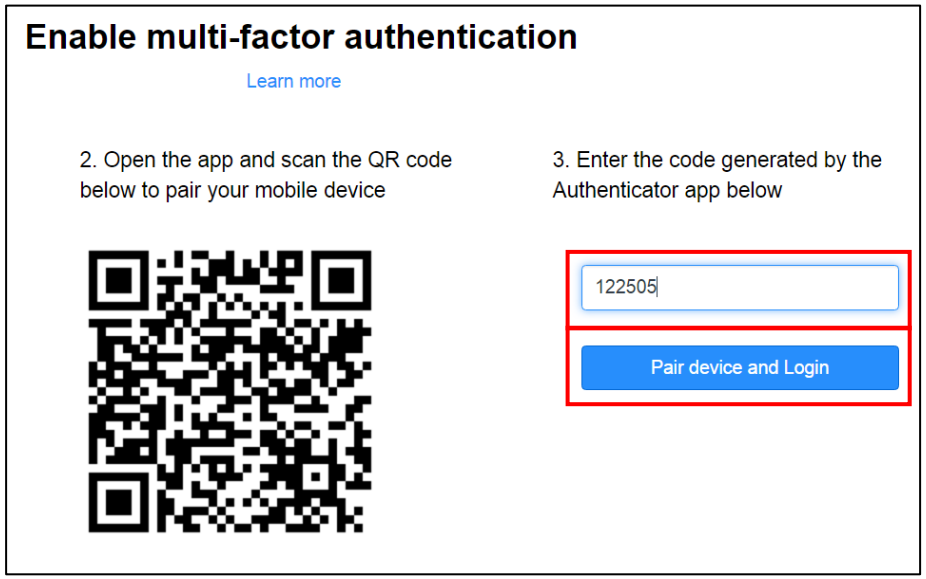
10 Click **Verify Authenticator**.



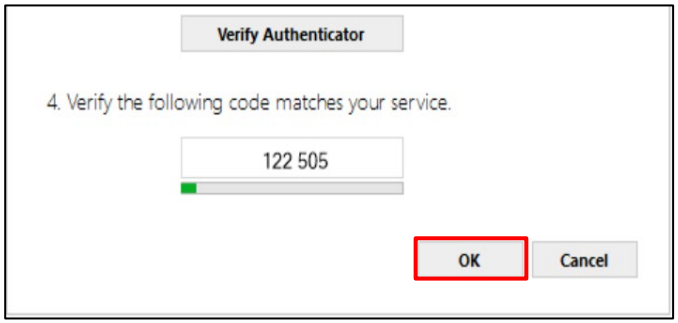
11 **Copy** the six-digit authentication code that generated.



Note, each code is only valid for 30 seconds.



12 Return to the Invoice Submission Portal multi-factor authentication page. Type the authentication code (no spaces) and click **Pair device and Login**.



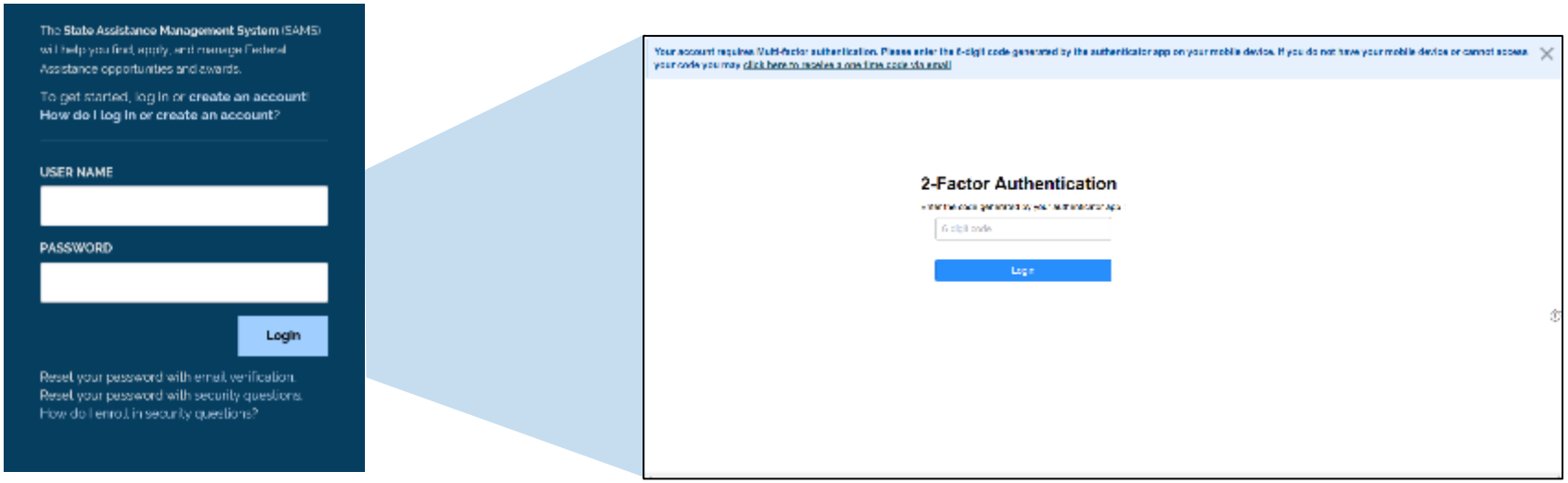
13 Return to the WinAuth page and click **OK**.

Note: This ends the one time setup for WinAuth. For subsequent logins, only user verification is required.

WinAuth
LOGGING IN

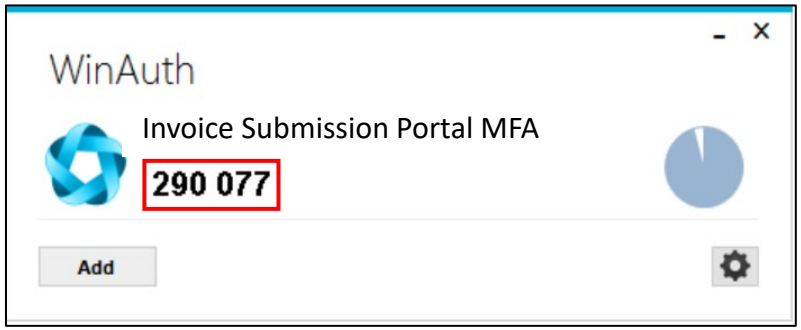
MFA is required every time a user logs into the Invoice Submission Portal. Each account must only be accessed by the user registered to the account.

1. Log in to the Procurement Portal. The Procurement Portal will now display a **2-Factor Authentication** page.

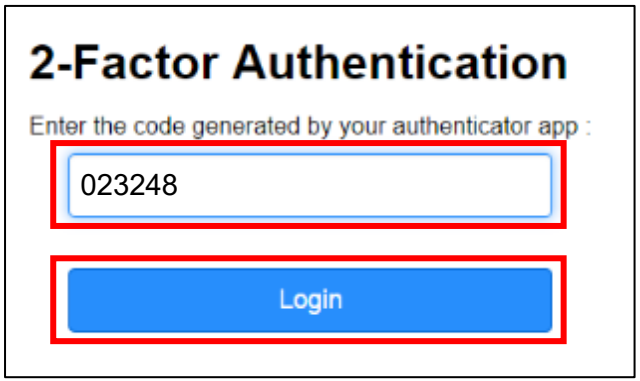


2. Open the **Google Authenticator** app.

3 Upon opening, **WinAuth** will automatically generate an **authentication code** under the heading "Invoice Submission Portal MFA".



4 On the Invoice Submission Portal **2-Factor Authentication** page, type the **authentication code** (without spaces) in the **authentication code** field.



5 Click **Login**.