SurePassID Authenticator Guide

SurePassID Authentication Server 2025

© 2013-2025 SurePassID, Corp. All rights reserved. Protected by patents pending. SurePassID, the SurePassID logo and design, and Secure SSO are registered trademarks or trademarks of SurePassID, Corp. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

SurePassID, Corp.

360 Central Avenue

First Central Tower

Suite 800

St. Petersburg, FL 33701

USA

+1 (888) 200-8144

www.surepassid.com

Introduction

This technical guide explains how to use the SurePassID Mobile Authenticator app to generate One-Time Passwords (OTPs) compatible with the SurePassID Authentication Server.

The SurePassID Authentication Server provides strong authentication for online identities and aims to reduce identity theft risks such as phishing. It is designed to meet requirements for secure authentication while also seeking to simplify usage and lower deployment and management costs.

Prerequisites

Before you start

Complete the following steps before configuring SurePassID Authenticator to work with SurePassID Authentication Server:

- You will need an Android or iOS capable device such as a mobile phone or tablet.
- Open and configure a SurePassID Authentication Server account. If you have not already done so, open an account at www.surepassid.com.

What is SurePassID Authenticator?

The SurePassID Authenticator is a mobile application that acts as a container for storing SurePassID mobile security tokens. SurePassID Authenticator can store the following tokens:

- One Time Passcode - Each SurePassID Authenticator token is a software equivalent of a physical two-factor hardware authentication token. The user enters this token to gain access to a system.
- Push Tokens – The SurePassID Authenticator will prompt the user to approve access to a system with a phishing resistant platform/transport authenticator (token).

The SurePassID Authenticator offers the following advantages over traditional hardware tokens:

- The SurePassID Authenticator can hold an almost unlimited number of SurePassID Authenticator tokens.
- The SurePassID Authenitcator supports phishing resistant push authentication for third party systems and non-web based systems.
- In addition to QR codes for SurePassID Authenticator token activations, SurePassID Authenticator supports over-the-air provisioning of SurePassID Authenticator tokens with a single click, increasing user satisfaction and eliminating security flaws inherent with QR codes.
- Supports legacy mobile security tokens like Google Authenticator, Authy, etc.
- No need to carry additional hardware tokens - just your phone.
- SurePassID Authenticator tokens can be created instantaneously and electronically distributed to your users. Conversely, traditional hardware tokens must be sent to individual users.

- SurePassID Authenticator tokens are software and as such they are inherently less costly than traditional hardware tokens. Perfect for budget constrained companies.
- SurePassID Authenticator tokens can be delivered to users in a matter of minutes. Hardware tokens can often require a set of operational procedures for the distribution of physical corporate assets.

Using SurePassID Authenticator involves the following steps:

1. Adding a SurePassID Authenticator token to the user's SurePassID account
2. Installing the SurePassID Authenticator application on the user's mobile device
3. Activating the SurePassID Authenticator token on the user's mobile device
4. Verifying the SurePassID Authenticator token is setup correctly

Adding a SurePassID Authenticator token to a User Account

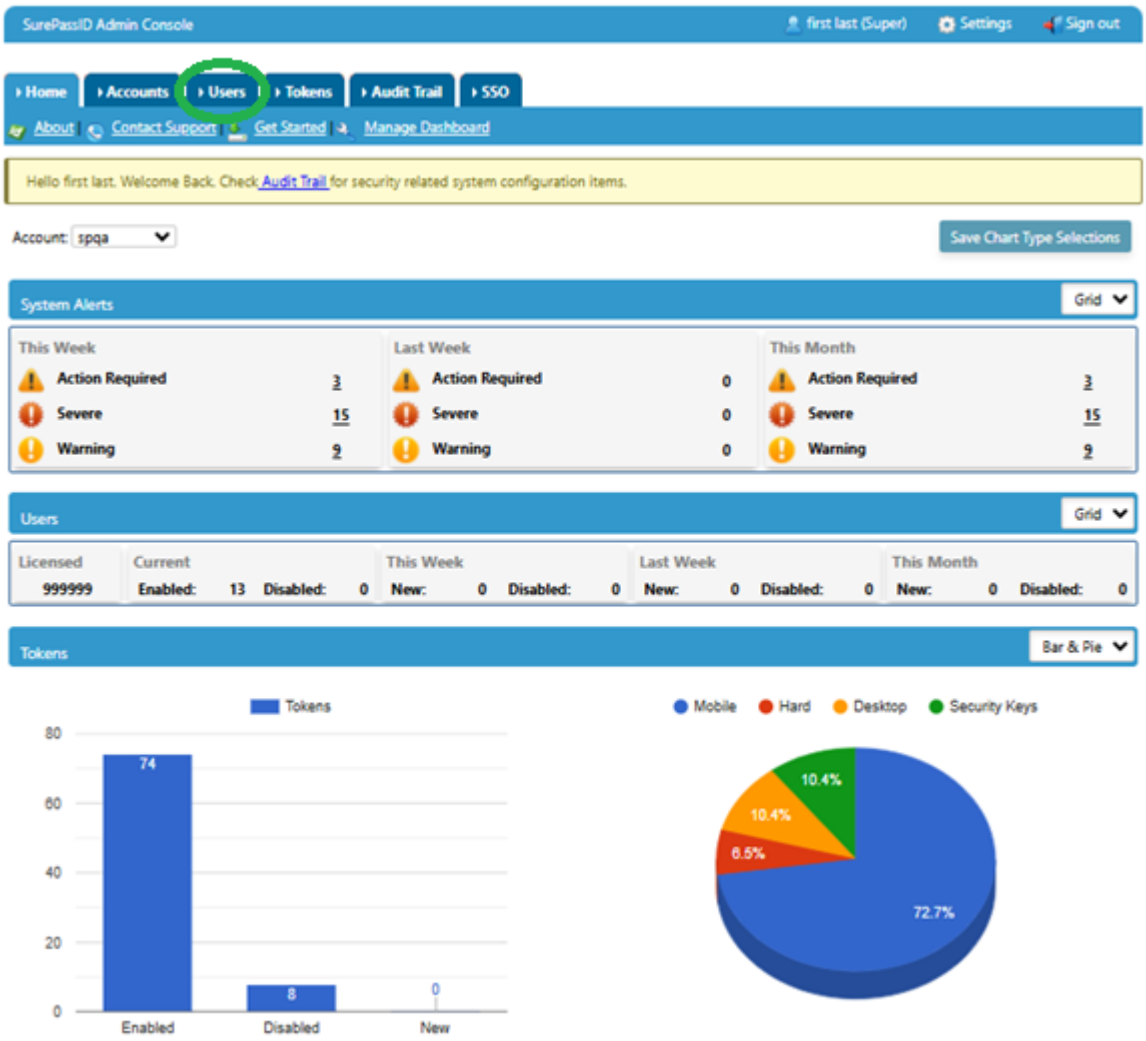
There are a few ways you can add a SurePassID Authenticator token to a SurePassID user account:

1. Manual – Add a SurePassID Authenticator to each user account one at a time. Best for doing some limited testing or on an ad-hoc basis.
2. Quick Link – You direct users to the SurePassID Activate web app and they can install the SurePassID Authenticator on their mobile device and activate their SurePassID Authenticator token.
3. SurePassID API – Use the SurePassID API to create SurePassID Authenticator tokens from your existing corporate intranet or IT application and assign them to users.
4. User Import – When you import users into SurePassID you have the system automatically create tokens for each user and send them a link to the activation page.
5. ServicePass – End-user self-service portal to create, activate and disable SurePassID Authenticator tokens.

This document only describes the Manual method. The other methods are beyond the scope of this document.

To add a SurePassID Authenticator manually, follow these steps.

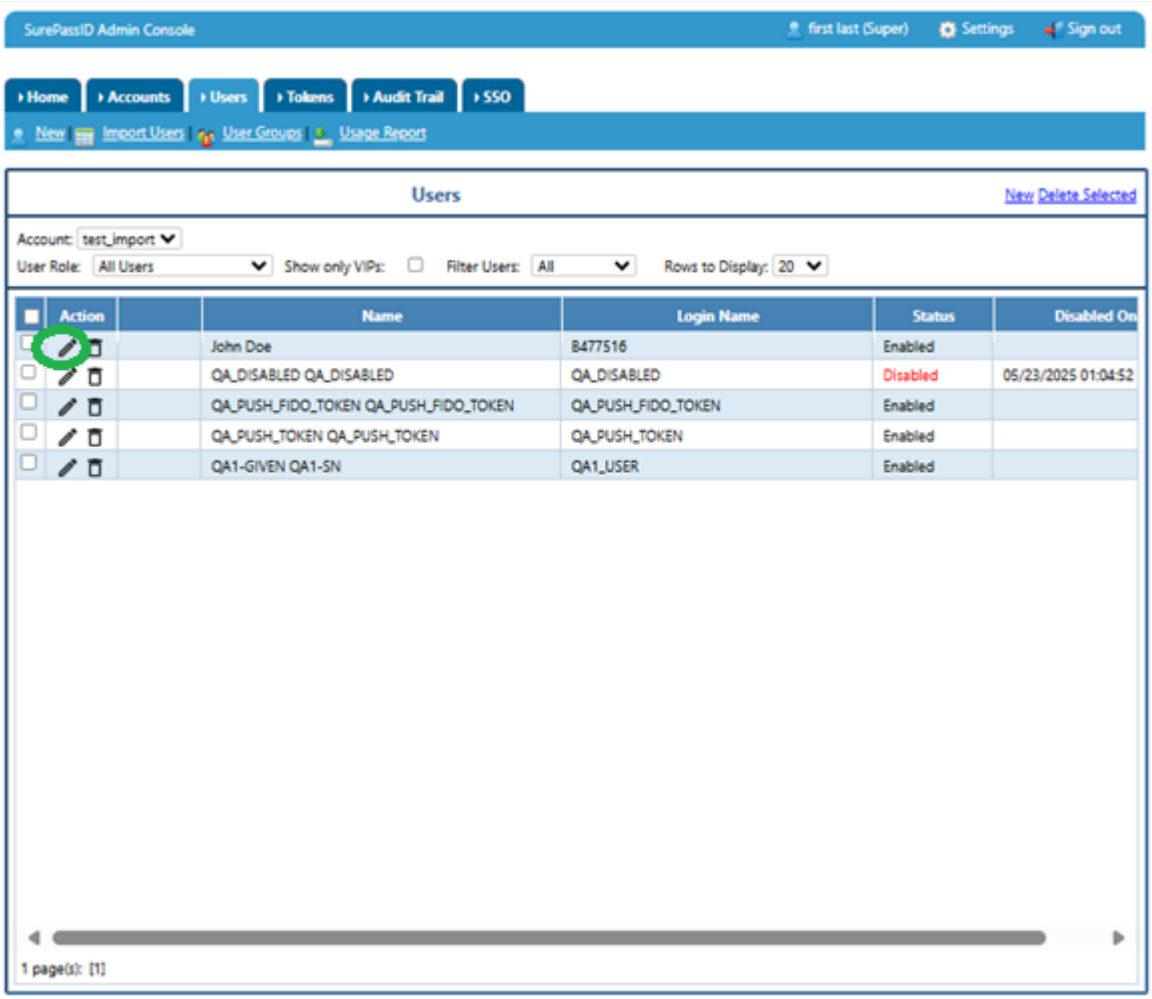
Log in to your SurePassID account. After logging into your account, select the **Users** tab as shown below.



HINT: Alternatively, you can use the **Tokens** folder to add an existing SurePassID Authenticator token and then assign it to an existing user.

HINT: To add many users art once, use the SurePassID User import. For additional instructions on this, please refer to the SurePassID Administrators Guide.

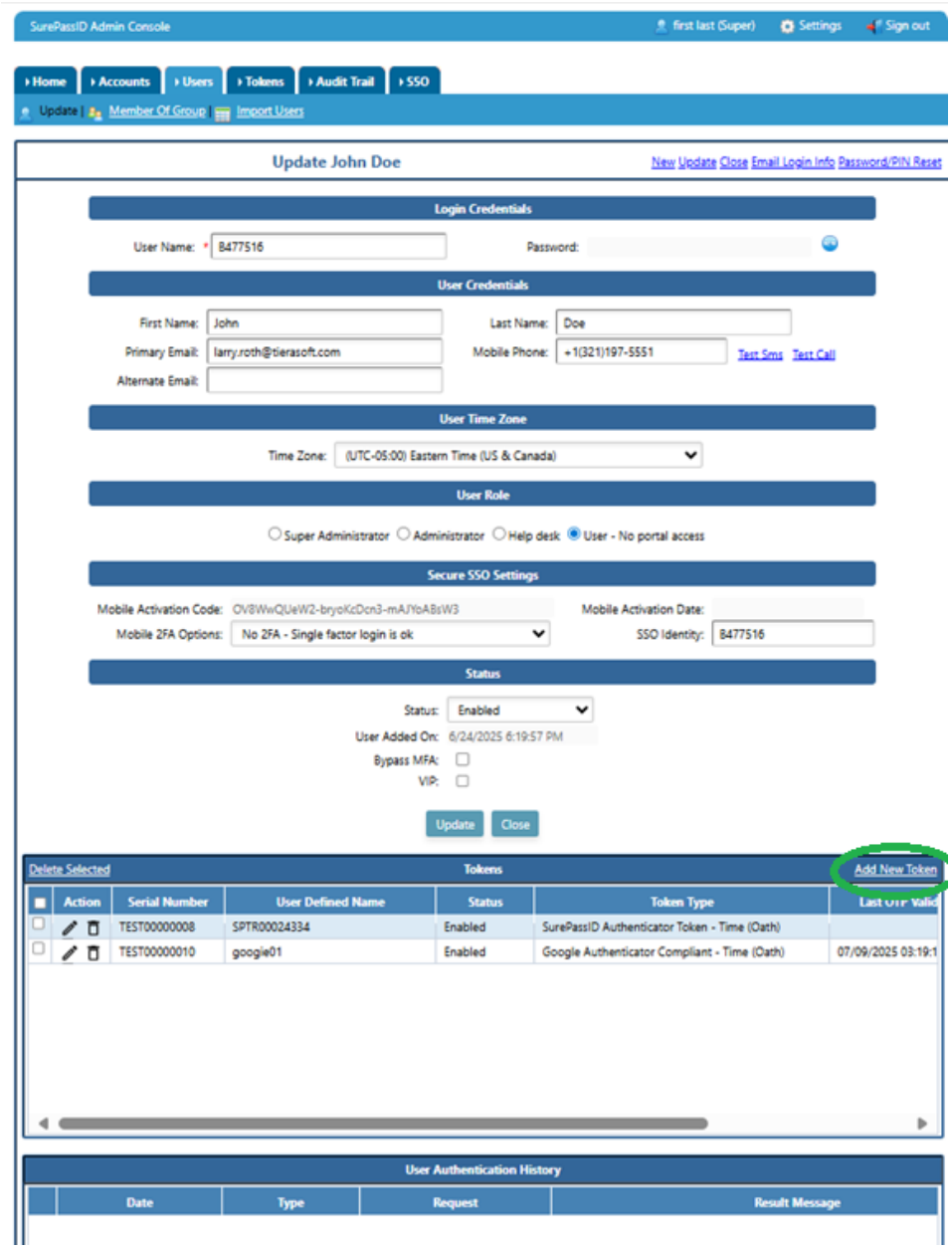
When the **Users** tab opens, select an existing user by clicking the **Edit** link highlighted below.



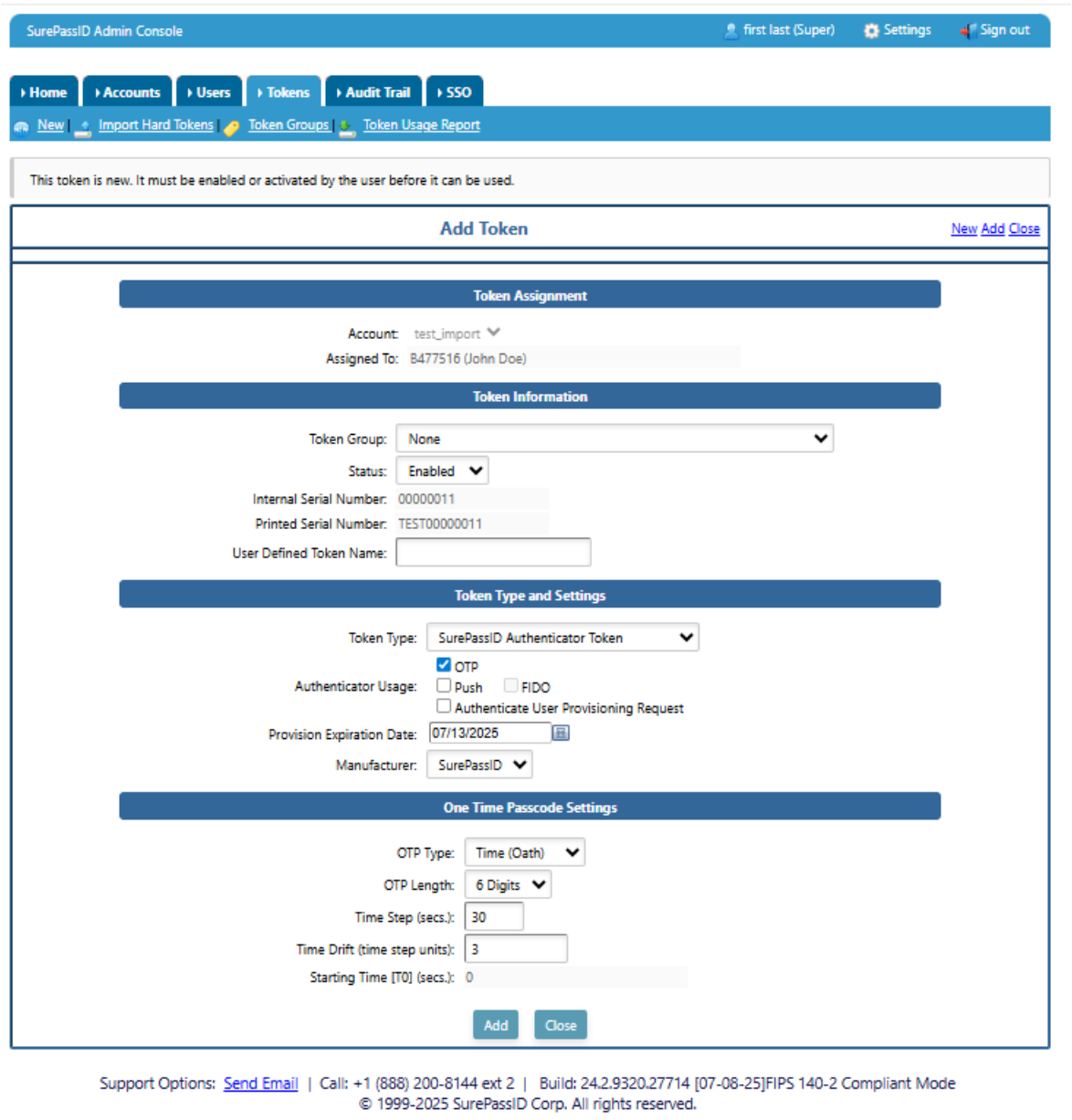
Support Options: Send Email | Call: +1 (888) 200-8144 ext 2 | Build: 24.2.9320.27714 [07-08-25]FIPS 140-2 Compliant Mode

© 1999-2025 SurePassID Corp. All rights reserved.

Add a new token to the user's account by clicking on the **Add New Token** link as shown below.



The following form will be displayed:



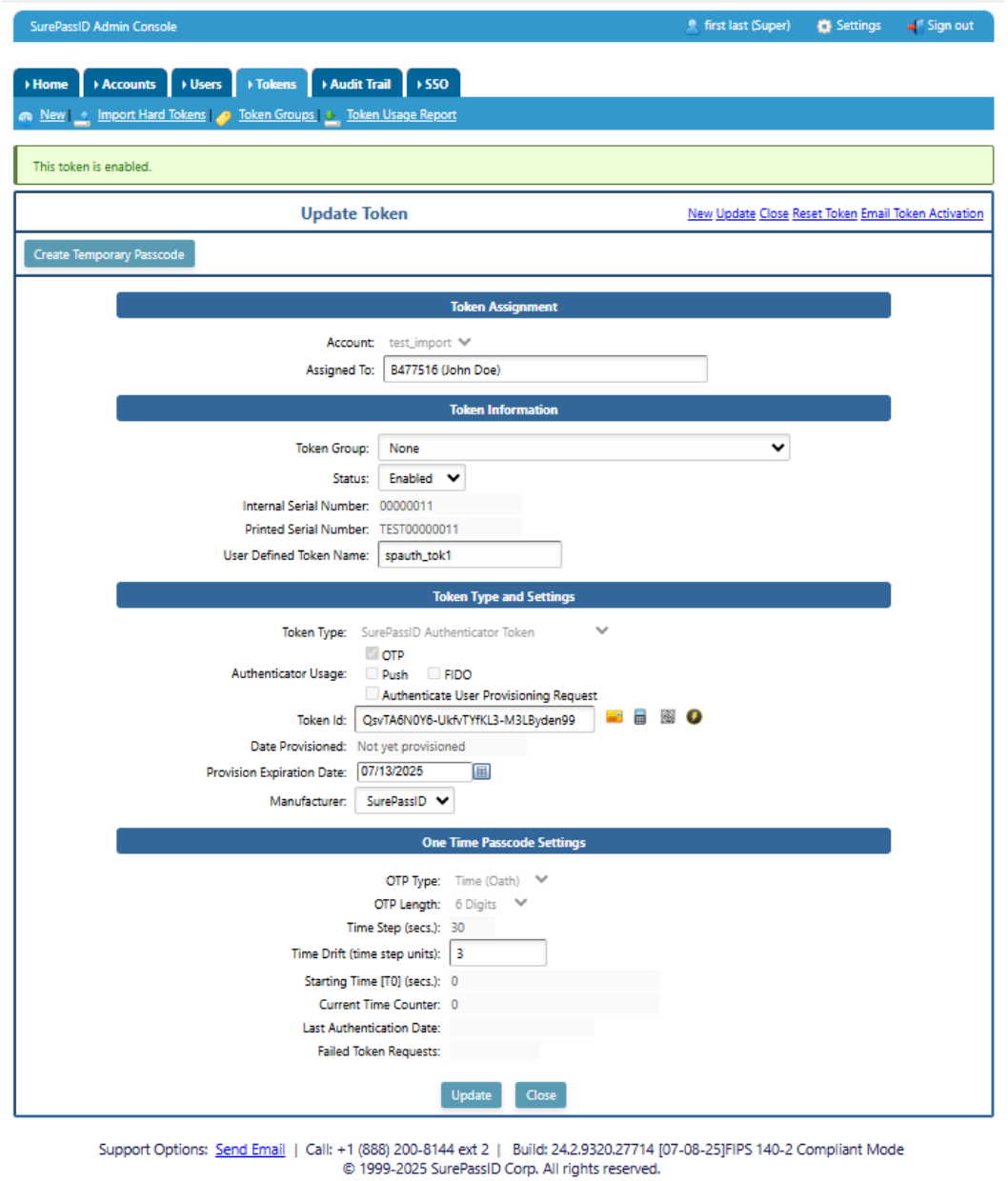
Set the applicable parameters. Specifically take notice of the following fields:

- **Token Type** – SurePassID Authenticator Token
- **Authenticator Usage** – Check any of the appropriate uses for the token
    - **OTP** – The mobile app will generate OTP codes based on the OTP Type and Length
    - **Push** – Supports push authentication

    - **FIDO** – Add phishing-resistant MFA to all push requests. The FIDO authentication on the mobile app will use the same type of token as registered, such as roaming or platform tokens.
    - **Authenticate User Provisioning Request** – To add this token, the user will need to provide username and password from their user account in SurePassID.
- **Status** – Set to Enabled. If the token is not enabled, the user will not be able to configure the SurePassID Authenticator token.
- **OTP Type** – Select either a **Time** Based OTP, **Event** Based OTP,
- **OTP Length** - 3, 4, 6, 8, 10 digits

HINT: You can find more info about all these parameters in the Administrator's Guide.

Click the **Add** button and the following form will be displayed:



Take note of the **Token Id** field. You will need this code to activate the token in the SurePassID Authenticator mobile application.

Please be aware of the **Provision Expiration Date**. After this date passes, the token cannot be activated. By default, this is set to three days after the token has been added. If the token is not provisioned before the expiration date, you may update the **Provision Expiration Date** to a future value to enable token activation.

After a token is activated, it cannot be activated again. If a user needs to reactivate their token due to a new or lost phone, use the **Reset Token** link.

There are several choices for you to send setup instructions to the user:

Click the icon to send token setup instructions to the user via email.

Click the icon to send a token activation to the user via SMS.

Click the icon to display the QR Code and hold your mobile device to the screen.

Click the icon to display the Instant Activation link

Alternatively, you can copy the **Token Id** and send it to the user via some other method such as Teams.

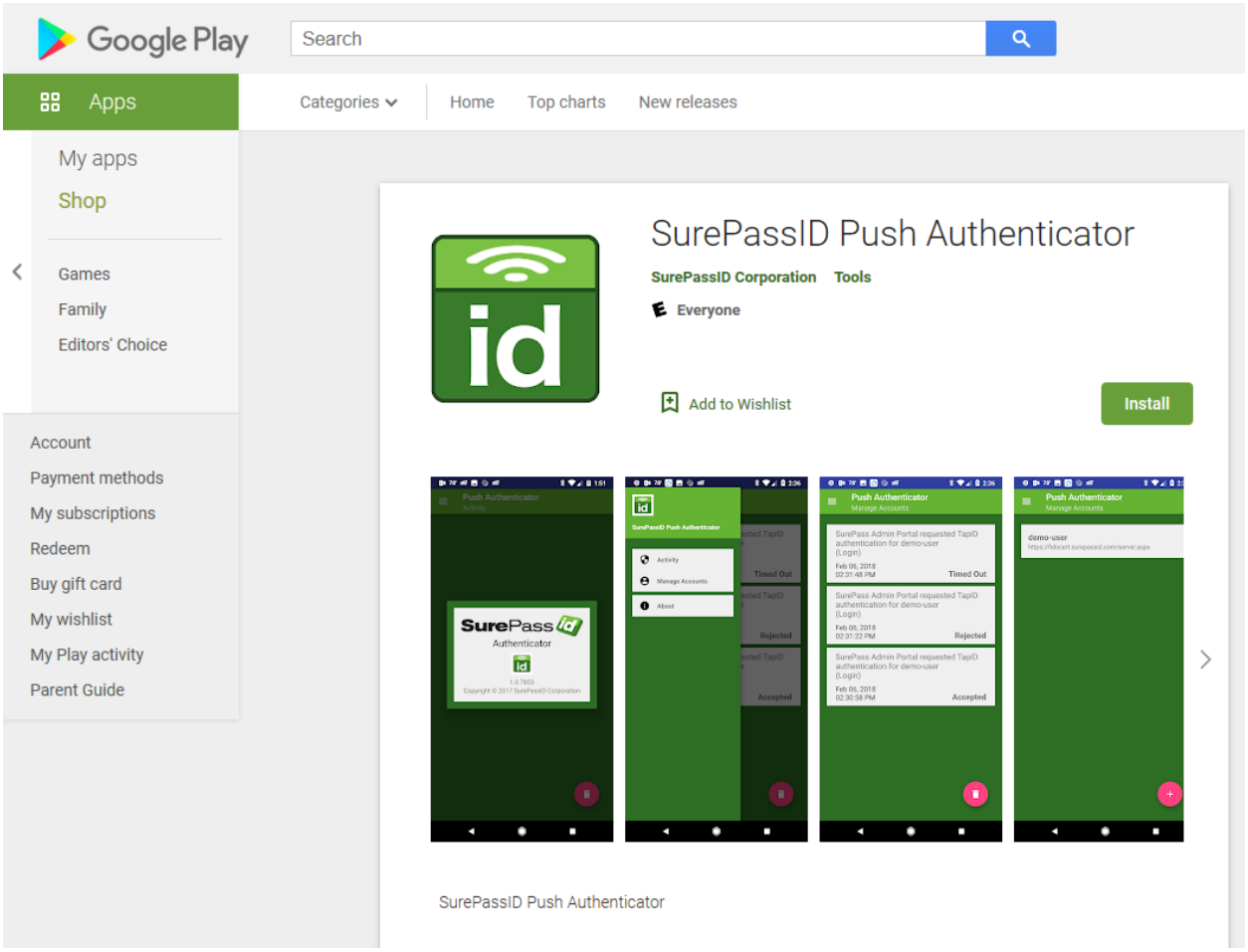
HINT: When utilising the Import Users method to add SurePassID Authenticators, the Unique Identifier field, along with the activation link for the SurePassID Authenticator, will be delivered to the user via email, enabling a streamlined one-click installation process.

NOTE: You can customize the setup instructions by selecting the **Home > Settings > Customize Email Messages** or **Home > Settings > Customize SMS Messages** as shown below:

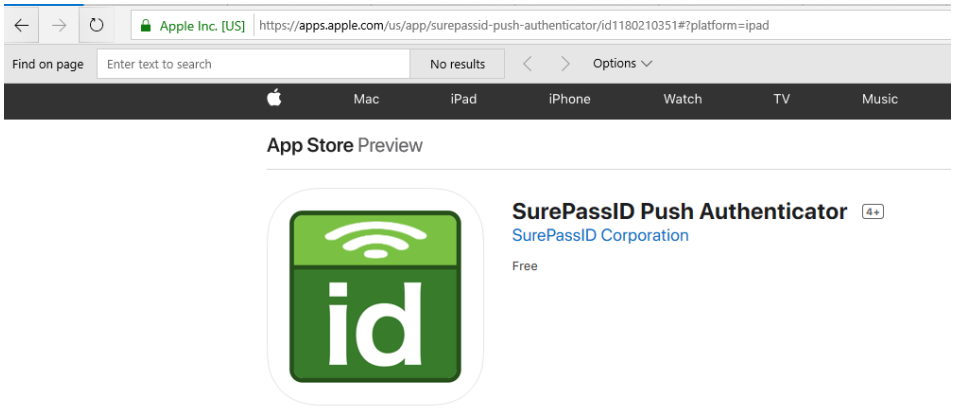
Installing the SurePassID Authenticator App

To install the SurePassID Authenticator application, follow these steps.

1. **Android** - Download the SurePassID Authenticator from the Play Store (Android) and follow the instructions to install on your mobile device. You can find the SurePassID Authenticator app by searching for **SurePassID Push Authenticator** as shown below.



iOS - Download the SurePassID Authenticator from the Apple App Store iTunes and follow the instructions to install on your mobile device. You can find the SurePassID Authenticator app by searching for **SurePassID Push Authenticator** as shown below.



2. Click Install.

Activating SurePassID Authenticator Tokens

SurePassID Authenticator can activate SurePassID Authenticator tokens the following ways:

- Instant Activation – Click an instant activation link on your mobile device (SMS or mobile email) and the token will be instantly activated without user interaction.
- Scan QR Code –Scan a QR code for a specific SurePassID Authenticator token.

To activate with Instant Activation

How does it work?

Instant Activation is a method of installing SurePassID Authentication tokens using over-the-air provisioning. This means the user can just click on a token activation link and the following things will happen:

1. The SurePassID Authenticator will automatically launch on the mobile device
2. The token will be pulled from the server, installed into the SurePassID Authenticator, and locked from further activations.

Instant Activation requires users to click the link on their mobile device. The link can appear in a mobile browser, email, or SMS message sent by the system. SurePassID offers multiple implementation options for large organizations.

The instant activation link will be in the format of:
https://<surepass_installation>/oath-ota-provision/<tokenid>

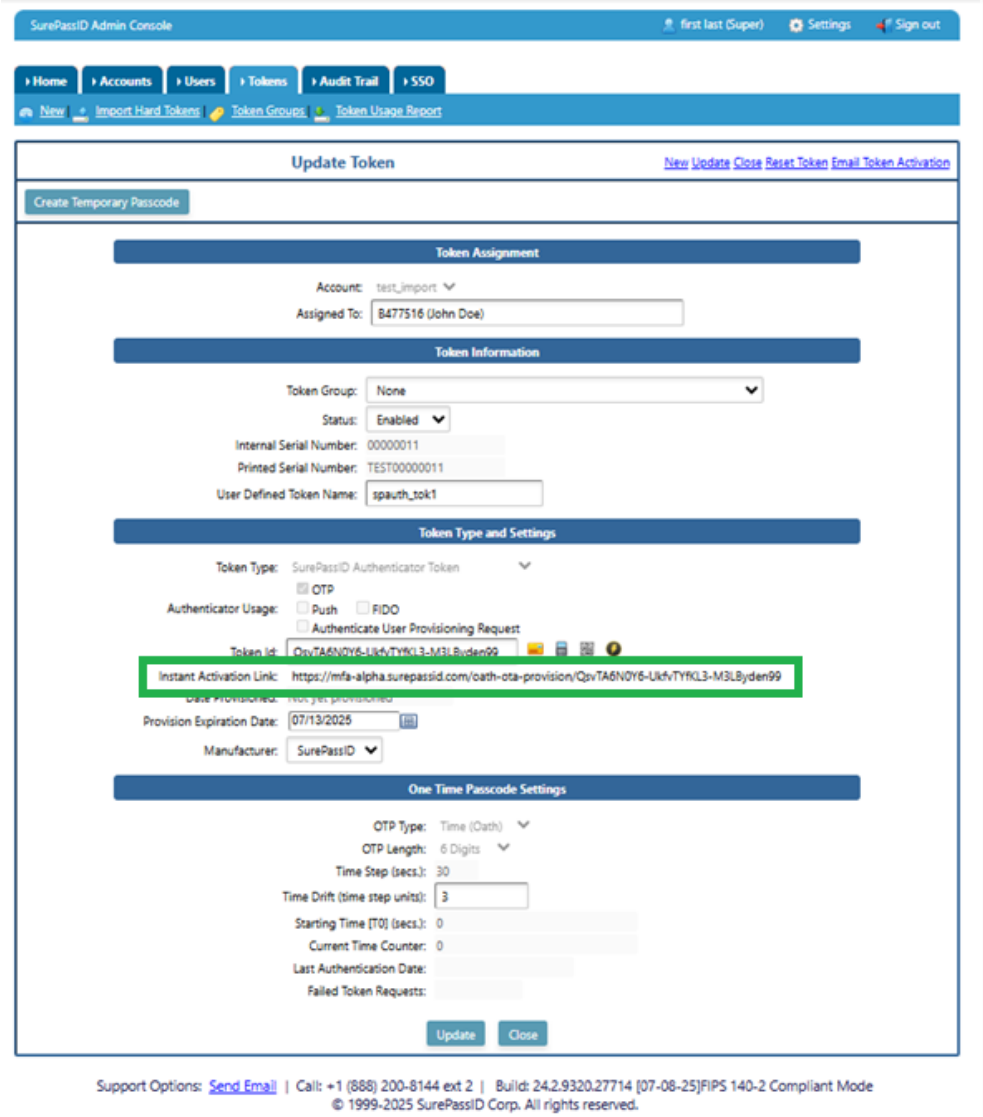
For example:

https://mfa-alpha.surepassid.com/oath-ota-provision/QsvTA6N0Y6-UkfvTYfKL3-M3LByden99

HINT: This is the most secure way to add a SurePassID Authenticator token but sometimes not the most convenient. When importing users into the system, they can automatically receive this link.

NOTE: If you are using SurePassID Server installed in your datacenter; (not in the cloud) then you will need to use a reverse proxy, or ServicePass to allow users to activate their tokens.

Click the icon to display the Instant Activation link.



The **Instant Activation Link** is shown in red. Emailing or sending the link to a user will allow them to click on the link to activate the token on their mobile.

Click icon to email the token setup instructions with the Instant Activation link to the user.

Click icon to send the Instant Activation link to the user via SMS.

When the user clicks the Instant Activation link while they are on their mobile device, the token will be installed without any user interaction.

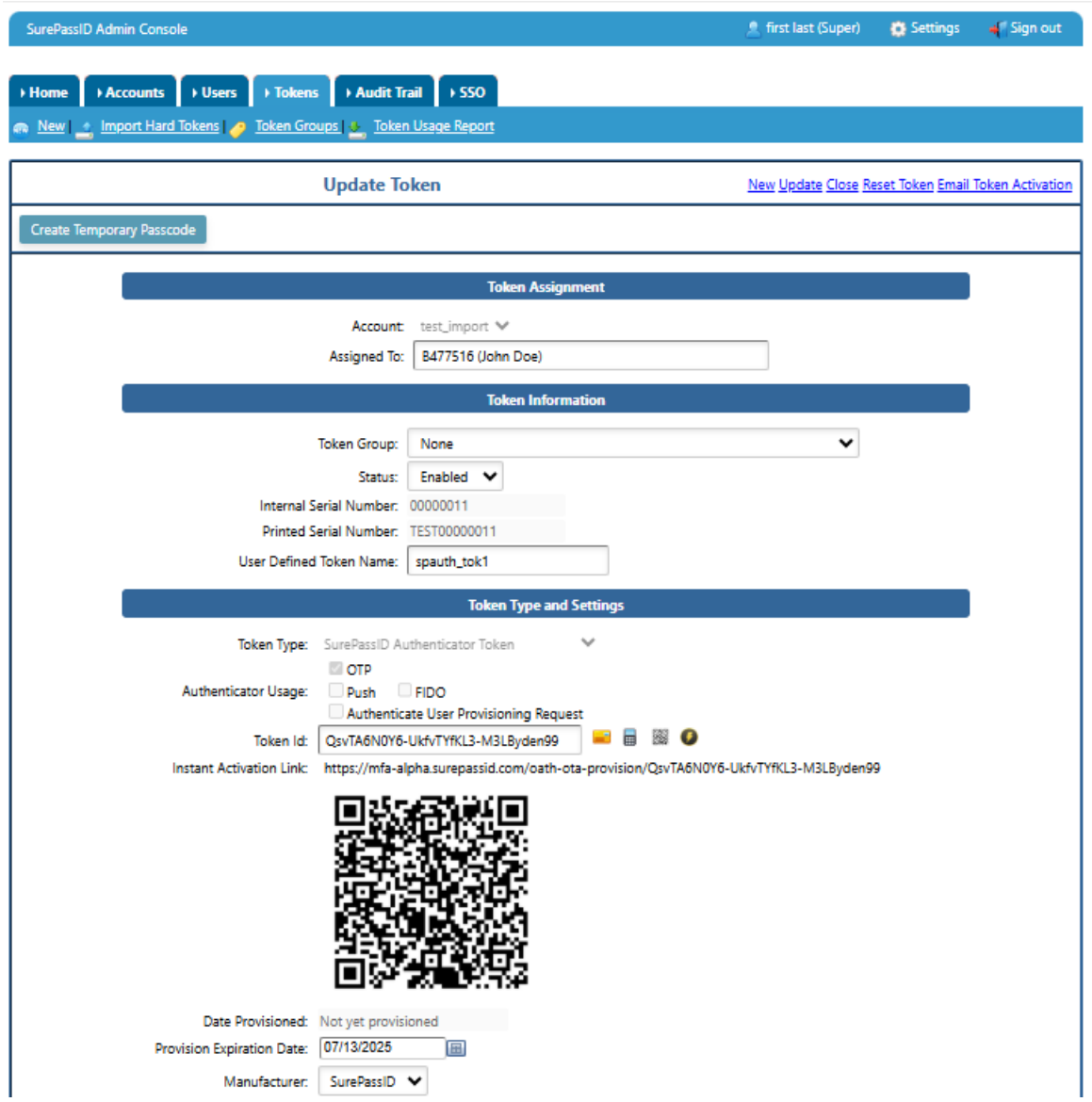
HINT: This is the easiest and most secure way to add a SurePassID Authenticator token. When importing users into the system, they can automatically receive this link.

To activate token with QR Code

Start the SurePassID Authenticator app on the target mobile device.

Select the camera to open the bar code scanner.

Clicking the icon will toggle the showing of the QR code as shown below:

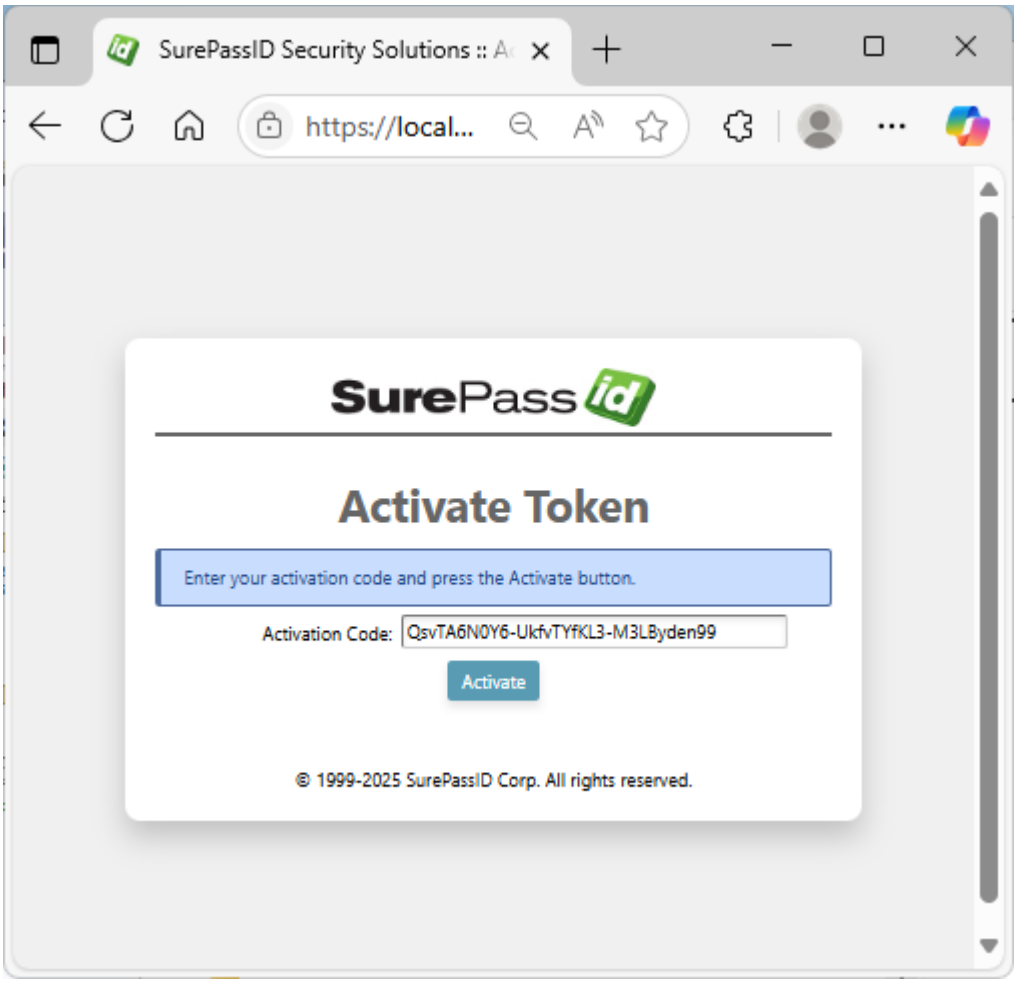


Hold the mobile device up to the QR code until the code is read and the SurePassID Authenticator adds the account.

Activate the SurePassID Authenticator token using activation portal

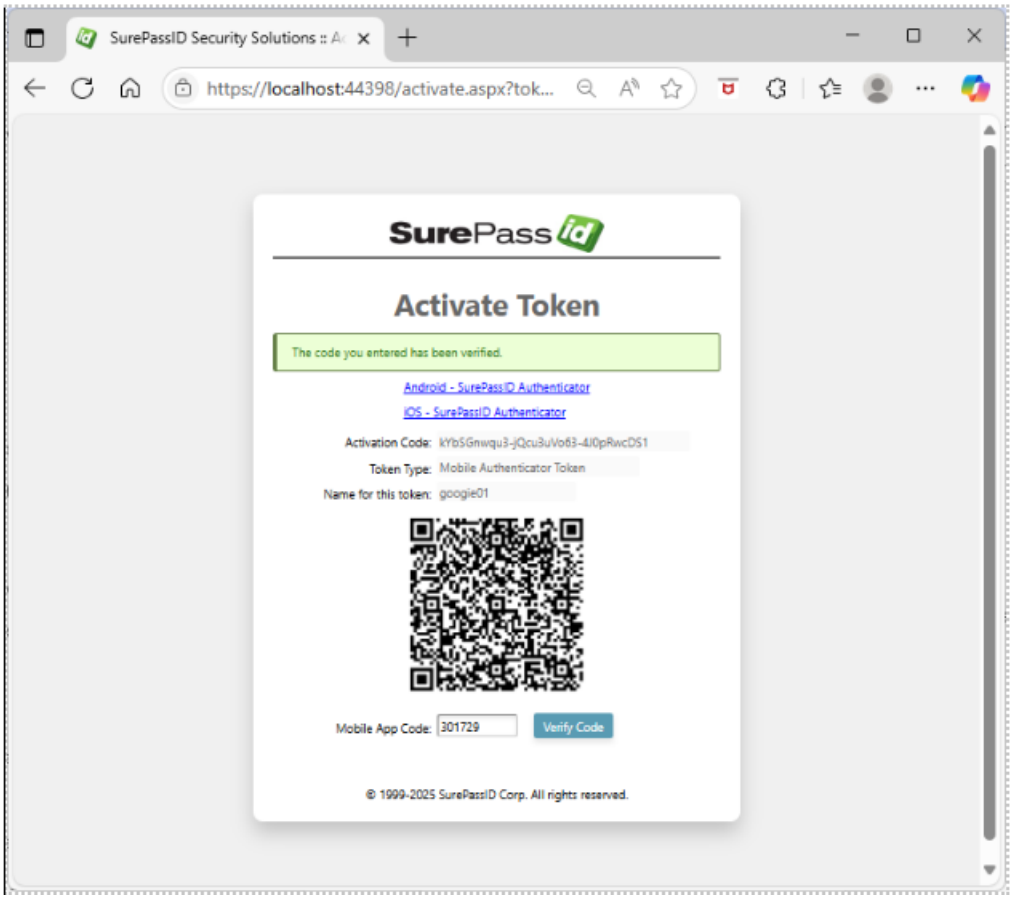
Users can activate a SurePassID Authenticator token by QR Code using the activation URL. This can process can be automated in the following ways:

The user will go to https://<surepassid_installation/activate.aspx?tokenid=<tokenid> and the following form is displayed.



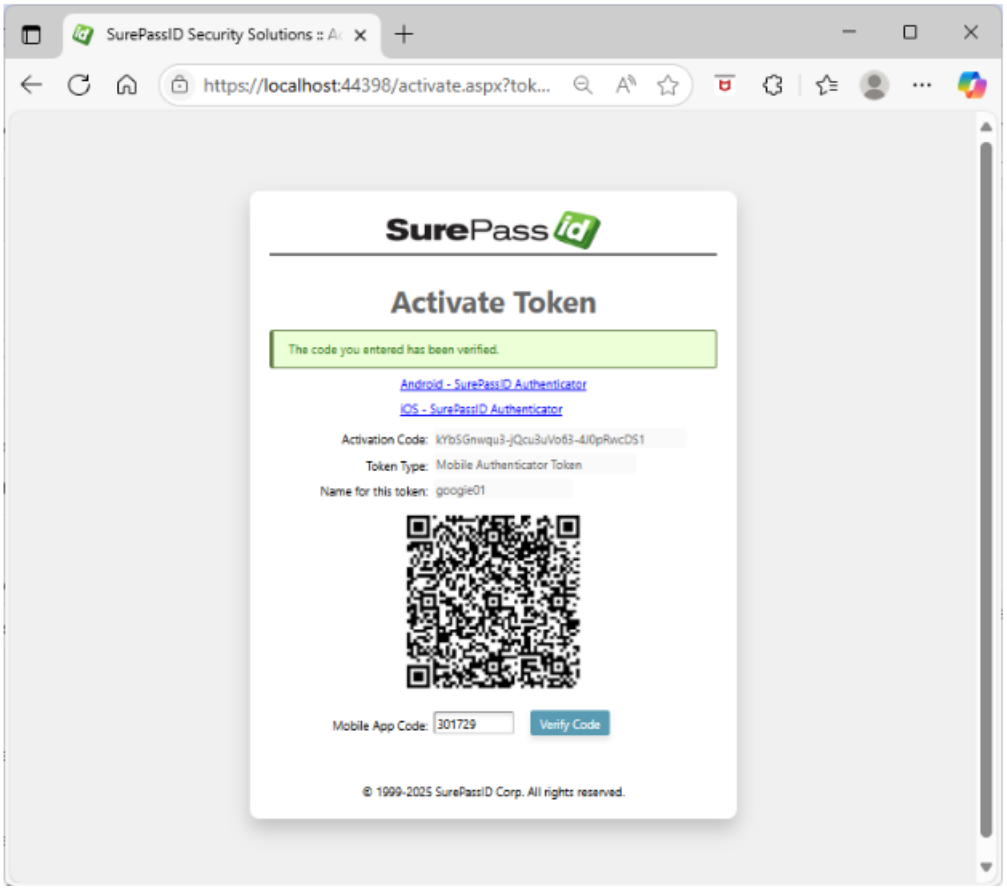
HINT: You can configure the system to require a CAPCHA for additional security.

Pressing the **Activate** button will show the following form:



Hold the mobile device up to the QR Code until the QR code is read, and the SurePassID Authenticator app adds the token.

To verify and activate your token, select the token in the SurePassID Authenticator App, then enter the displayed code into the **Mobile App Code** field and press **the Verify Code** button as shown below. If your token is configured correctly, you will see the following form:



Your token is ready to log into any SurePassID enabled system.

Alternatively, your users can use the SurePassID ServicePass Self-Service portal.