Google Authenticator Guide

SurePassID Authentication Server 2021

Introduction

This technical guide describes how to use the Google Authenticator app to generate One-Time Passwords (OTP) that are compatible with SurePassID Authentication Server.

SurePassID Authentication Server increases the security of online identities and significantly improves an organization's resistance to identity theft attacks such as phishing. It addresses the real-world demand of strong authentication, making it easier to use while helping to reduce deployment and management costs.

Prerequisites

Before you start

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

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

What is Google Authenticator?

The Google Authenticator is a mobile application that acts as container for storing Google mobile security tokens. Each Google Authenticator token is a software version of a physical two-factor authentication hardware token.

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

- The Google Authenticator can hold an almost unlimited number of Google Authenticator tokens.
- No need to carry additional hardware tokens; just your phone.
- Google Authenticator tokens can be created instantaneously and electronically distributed to your users. Conversely, traditional hardware tokens must be sent to individual users.
- Google Authenticator tokens are software and as such they are inherently less costly than traditional hardware tokens. Perfect for budget constrained companies.
- Thousands of Google Authenticator tokens can be rolled out in a matter of hours. Hardware tokens can often require a set of operational procedures for the distribution of physical corporate assets.

Using Google Authenticator involves the following steps:

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

Adding a Google Authenticator token to a User Account

You can add a Google Authenticator token to a SurePassID user account a few ways:

1. Manual – Add a Google Authenticator token to each user account one at a time. Best for doing some limited testing or on an as-needed basis.
2. Automatic – When importing users, you can have Google Authenticator tokens added to all the user accounts that are imported. Best for pilots and large scale deployments.
3. SurePassID API – Using the SurePassID API, you can add a Google Authenticator token to a user's account from your existing corporate intranet or IT application.
4. ServicePass – End user self-service portal to create, activate and disable Google Authenticator tokens.

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

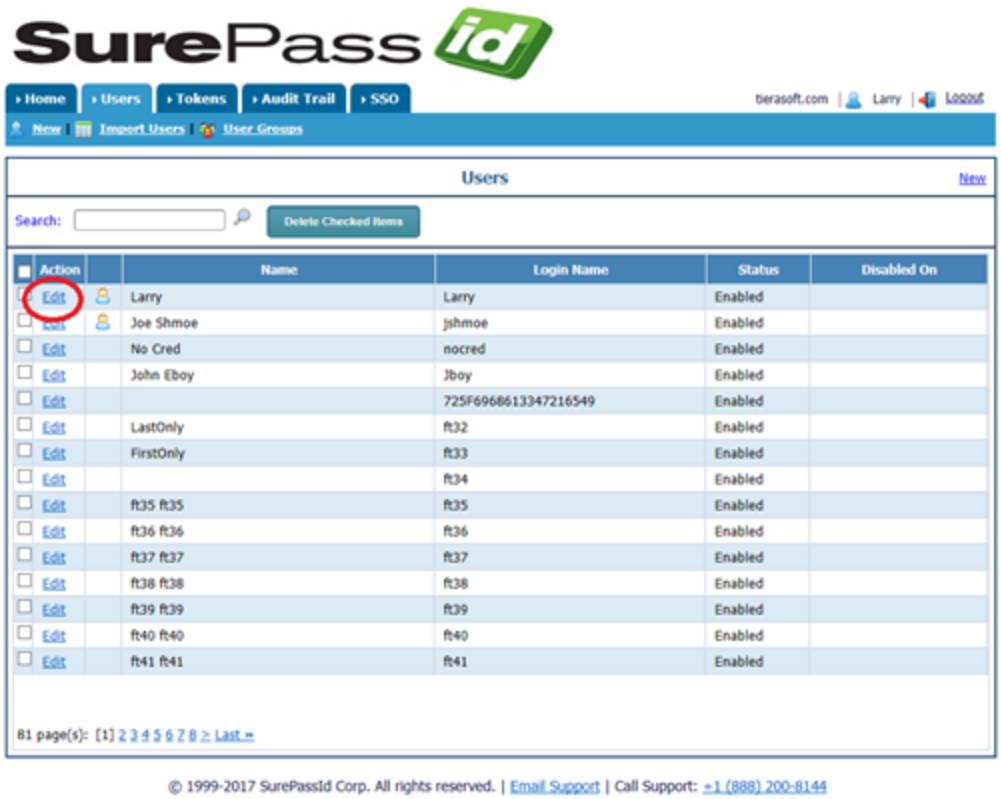
To add the Google Authenticator manually, follow these steps.

Log in to your SurePassID account. After logging into your account you will see the **Home** folder as shown below. Select the **Users** folder.

HINT: You can use the **Tokens** folder to add an existing Google 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 Administrator's Guide.

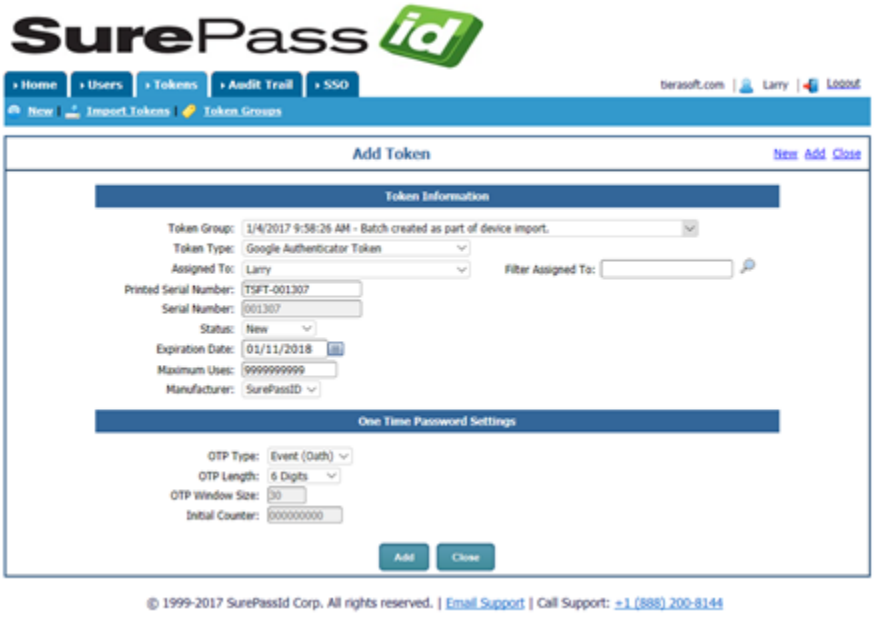
When the **Users** folder opens as shown below. Select an existing user by clicking the **Edit** link as highlighted below.



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


SurePass id
› Home
› Users
› Tokens
› Audit Trail
› SSO
tierasoft.com | Larry | Logout
Update | Member Of Group | Import Users Update
Update User [Larry]
New Update Close Email Login Info
Login Credentials
User Name: Larry
Password:
User Credentials
First Name: Larry
Last Name:
Email: larryr@tierasoft.com
Mobile Phone: +1(321)297-8051
User Time Zone
Time Zone: (UTC-05:00) Eastern Time (US & Canada)
User Priviledges
Admin Privilege:
Secure SSO Settings
Mobile Activation Code: 33356F7669467043 4A5472625347 6F72566D3758
Mobile Activation Date:
Mobile 2FA Options: 2FA Not Mandatory - Only if user has 2FA token
SSO Identity: Larry
Status
Status: Enabled
Disabled On:
Update
Close
Tokens
New
Action
Serial Number
Status
Token Type
Last OTP Validation
OTP Type
Digit

The **Add Token** form will be displayed:



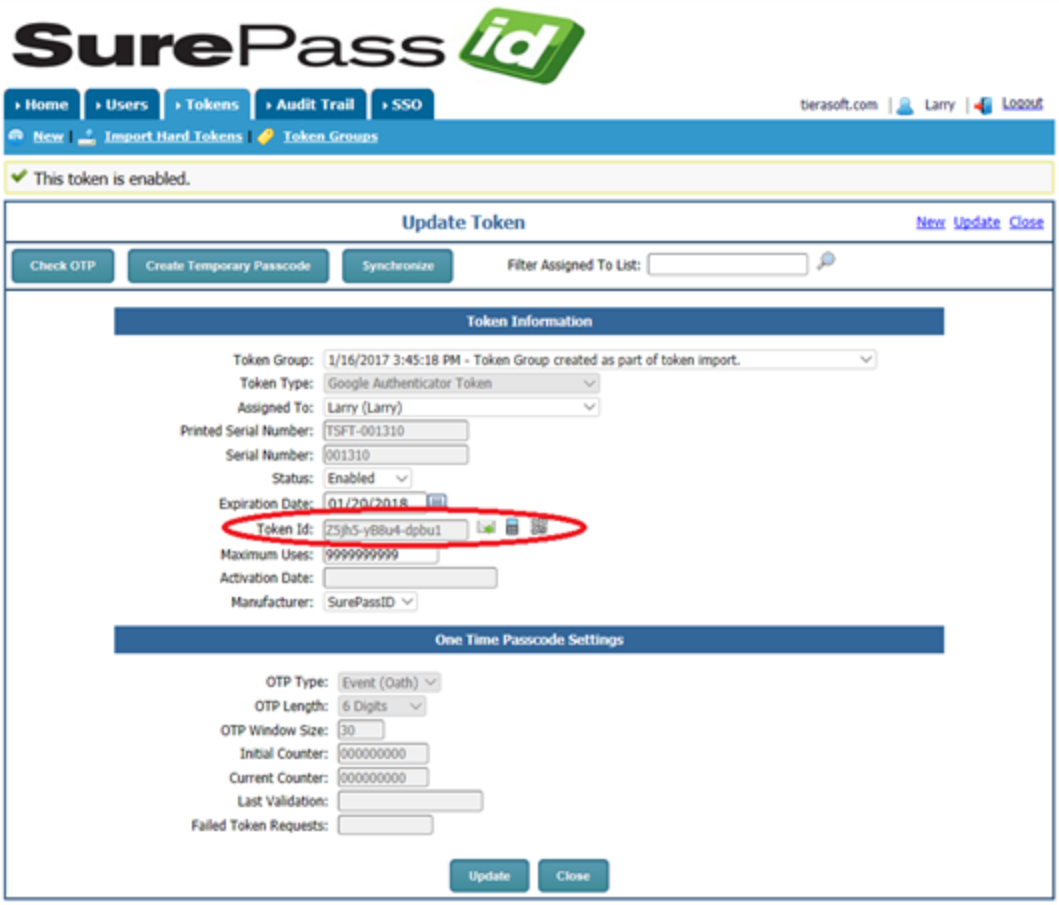
Set the applicable parameters. Specifically take notice of the following fields:

- **Token Type** – Google Authenticator Token
- **Status** – Set to **Enabled**. If the token is not enabled the user will not be able to configure the Google Authenticator token.
- **OTP Type** – Select either a **Time** Based OTP or an **Event** Based OTP.

HINT: The Google Authenticator app only supports 6 digit tokens. Time based mobile tokens are also limited to 30 second time periods. If you need a different configuration, use the SurePassID Mobile Token. It supports 3, 4, 6, 8, 10 digits and any time period.

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 configure the token in the Google Authenticator application.

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

You can click the icon to send token setup instructions to the user via email.

You can click the icon to send token setup instructions to the user via SMS text.

You can click the icon to display the QR Code and hold your mobile device to the screen or copy and paste the QR code into an email to the user.

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

HINT: When using the Import Users method to add Google Authenticators, the **Token Id field** and the link to activate Google Authenticator will be sent to the user in an email for one-click install.

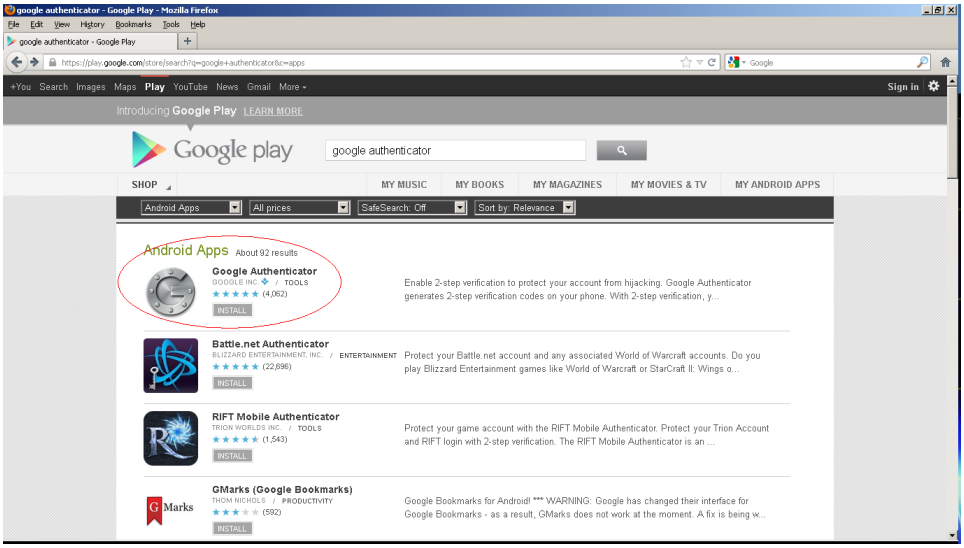
HINT: The Google Authenticator app only supports 6 digit tokens. Time-based mobile tokens are also limited to 30 second time periods. If you need a different configuration use the SurePassID Mobile Authenticator. It supports 3, 4, 6, 8, 10 digits and any time period.

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 Google Authenticator App

To install the Google Authenticator application, follow these steps.

1. Download the Google Authenticator from the Play Store (Android), iTunes (iOS), App World (Blackberry) and follow the instructions to install on your mobile device. You can find the Google Authenticator app by searching for **Google Authenticator**.



Activating Google Authenticator Tokens

Activate Google Authenticator tokens by scanning a QR code for a specific token. The QR code can be sent to the user via email or an activation link that will display the QR code to the user.

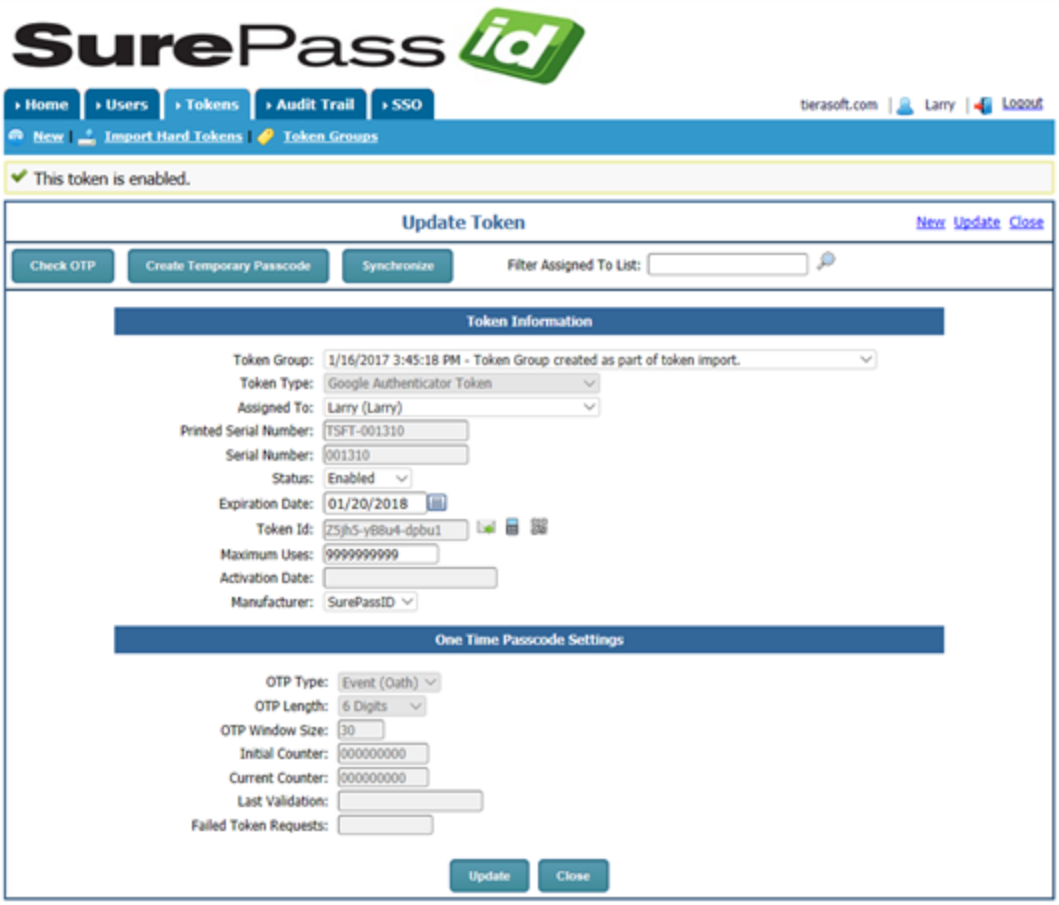
Google Authenticator tokens can be distributed to users the following ways:

1. Manual – Add a Google Authenticator to an admin account one at a time. Best for doing some limited testing or on an ad-hoc basis.
2. Email Self-Service– You direct users to the SurePassID Activate Token web app and they can install the Google Authenticator on their mobile device and activate their Google Authenticator token.
3. SurePassID API – Use the SurePassID API to create Google Authenticator tokens from your existing corporate intranet or IT application and assign them to users.
4. SurePassID ServicePass – End-user self-service portal to create, activate and disable Google Authenticator tokens.

This document only describes the Manual and Email Self-Service method. The other methods are beyond the scope of this document.

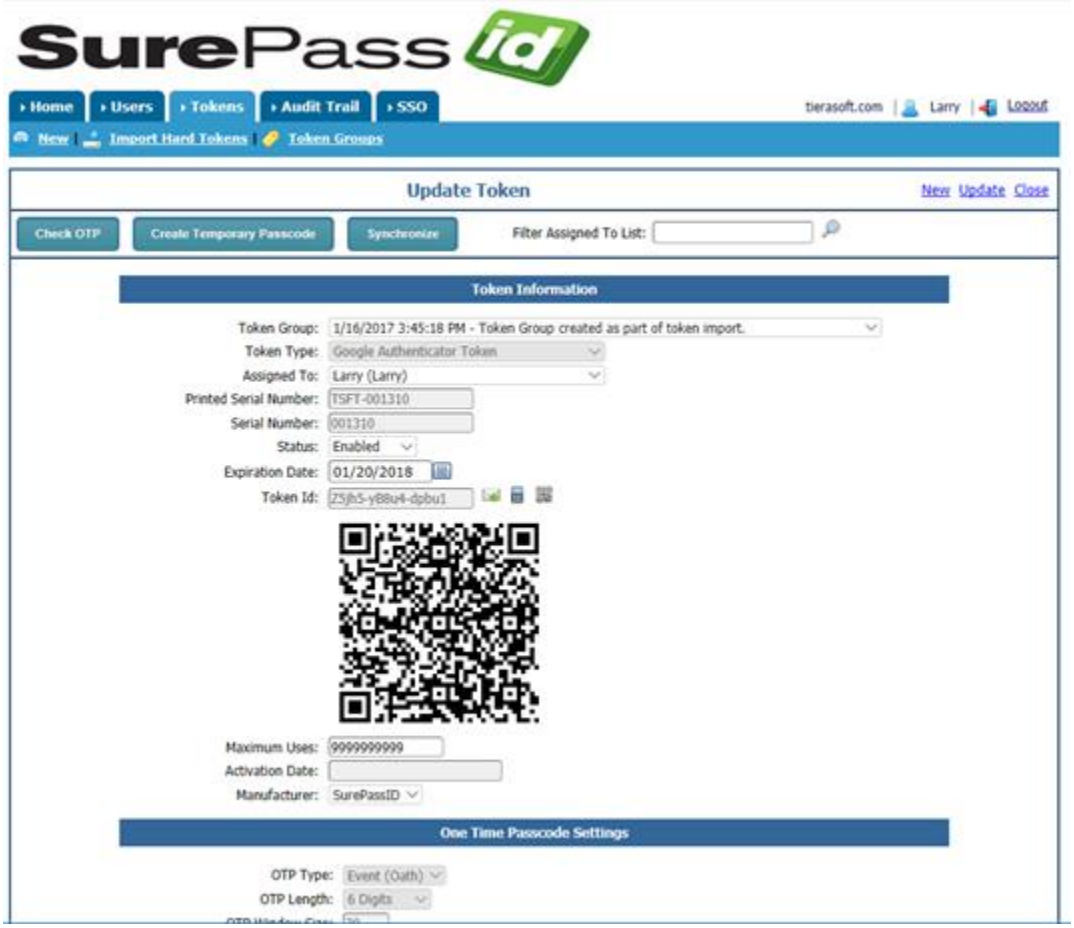
Regardless of which method you choose, the user must first follow these steps:.

1. Start the Google Authenticator app on the target mobile device. In this example, we will use the Android version
2. The current Google Authenticator has a (+) button in the lower right to add a new token. Press the (+) button and a menu is displayed.
3. Select **Scan a barcode** from the menu. The Google Authenticator is now waiting for a bar code to scan.
4. Log into your SurePassID account (if not already logged in) and locate the Google Authenticator Token you want to activate. You can do this by following the same steps as Adding the Google Authenticator explained above, or by selecting the **Tokens** folder (filtering/sorting the tokens for a user and selecting that token). In either case, you will see the form below:


SurePass id
Home
Users
Tokens
Audit Trail
SSO
tierasoft.com | Larry | Logout
New | Import Hard Tokens | Token Groups
This token is enabled.
Update Token
New Update Close
Check OTP
Create Temporary Passcode
Synchronize
Filter Assigned To List:
Token Information
Token Group: 1/16/2017 3:45:18 PM - Token Group created as part of token import.
Token Type: Google Authenticator Token
Assigned To: Larry (Larry)
Printed Serial Number: TSFT-001310
Serial Number: 001310
Status: Enabled
Expiration Date: 01/20/2018
Token Id: Z5jh5-yB8u4-dpbu1
Maximum Uses: 9999999999
Activation Date:
Manufacturer: SurePassID
One Time Passcode Settings
OTP Type: Event (Oath)
OTP Length: 6 Digits
OTP Window Size: 30
Initial Counter: 000000000
Current Counter: 000000000
Last Validation:
Failed Token Requests:
Update
Close

To activate the Google Authenticator token manually, follow these steps.

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



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

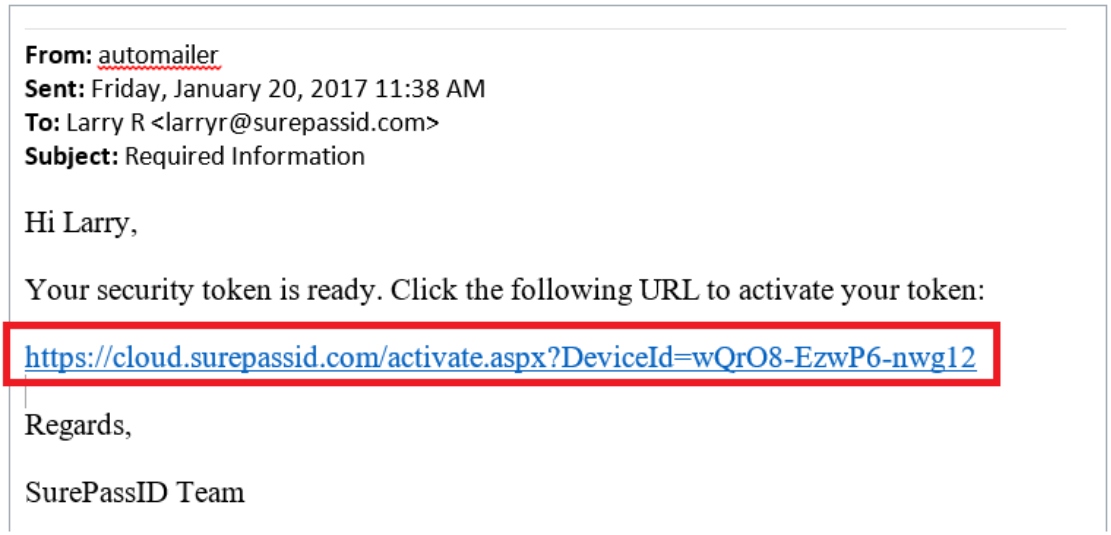
Press the email icon for self-service.

Pressing the email icon will result in the user being sent a token activation email. This email will contain the token activation URL for the Google Authenticator token assigned to their account.

HINT: You can configure the system to customize the email sent to the user. More information is available in the Administrator's Guide.

HINT: When you import users you can have an email sent to them automatically with these instructions.

1. Open the token activation email. The email will look similar to this:



From: automailer
Sent: Friday, January 20, 2017 11:38 AM
To: Larry R <larryr@surepassid.com>
Subject: Required Information

Hi Larry,

Your security token is ready. Click the following URL to activate your token:

https://cloud.surepassid.com/activate.aspx?DeviceId=wQrO8-EzwP6-nwg12

Regards,

SurePassID Team

2. In the email body click the link to activate the token and the following form will be displayed.

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

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

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

5. Select the token just added to Google Authenticator, then enter the code displayed into the **Code From Mobile App To Verify** field and press the **Verify Code** button. If your token is configured correctly you will see the following form:

6. Your token is ready to login into other apps.

Verifying Google Authenticator Token on the Server

To verify a user's Google Authenticator is properly working, follow these steps.

1. Start the Google Authenticator app.
2. Log in to the SurePassID Authentication Server if you are not already logged in.
3. Select the **Tokens** tab.
4. Find the token (by **Serial Number or Assigned User**) that you will verify. Click the **Check** link to the left of the token as shown below.

The following form will be displayed.

5. User starts the Google Authenticator app on their mobile device.
6. Select the token to test in the Google Authenticator App. Enter the code displayed for the selected token into the **OTP** field. Press the **Check** button and the following form is displayed.

If the OTP is correct, you will see the message **OTP is valid!!!** The user can use the Google Authenticator token as a security token in any SurePassID enabled app.

If the OTP is invalid, check the following:

1) Make sure the token is Enabled in the Admin portal.
2) For event-based tokens, go into the Admin portal, locate the token in the Tokens tab and then click Edit. Click the Synchronize button and follow the instructions. Try Check OTP again.
3) For time-based tokens, make sure the user's phone is set to Automatic Date & Time so that it uses the mobile network to synchronize its clock. Then go into the portal for that token and Check OTP again.