



SurePassID Authenticator Guide

SurePassID Authentication Server 2021



Introduction

This technical guide describes how to use the SurePassID Mobile 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 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.

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

- The SurePassID Authenticator can hold an almost unlimited number of SurePassID Authenticator tokens.
- 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.

The screenshot displays the SurePassID web application interface. At the top, the 'SurePassid' logo is visible. Below it, a navigation bar includes links for Home, Users, Tokens, Audit Trail, and SSO. The 'Users' tab is currently selected. The main content area is titled 'Home' and is divided into three columns: Open System Alerts, User Statistics, and OTP Statistics. The Open System Alerts column shows a list of alerts with counts. The User Statistics column shows various user counts. The OTP Statistics column shows counts for successful and failed OTP requests.

Open System Alerts	User Statistics	OTP Statistics
Open Items Requiring Action: 389	Total Users: 1211	Total Sever Requests (This Week): 10
Open Severe Items: 45	New Users (This Week): 0	Successful OTP Requests (This Week): 1
Items Requiring Action (This Week): 4	New Users (Last Week): 0	Failed OTP Requests (This Week): 9
Severe Issues (This Week): 0	New Users (This Month): 0	Total Server Requests (Last Week): 6
Items Requiring Action (Last Week): 2	Total Disabled Users: 0	Successful OTP Requests (Last Week): 3
Severe Issues (Last Week): 0	Disabled Users (This Week): 0	Failed server Requests (Last Week): 3
Items Requiring Action (This Month): 6	Disabled Users (Last Week): 0	Total Server Requests (This Month): 16
Severe Issues (This Month): 0	Disabled Users (This Month): 0	Successful OTP Requests (This Month): 4
		Failed OTP Requests (This Month): 12

© 1999-2017 SurePassID Corp. All rights reserved. | [Email Support](#) | Call Support: +1 (888) 200-8144



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 at 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 as highlighted below.


SurePass



[Home](#) [Users](#) [Tokens](#) [Audit Trail](#) [SSO](#)

tierasoft.com |  Larry |  Logout

[New](#) | [Import Users](#) | [User Groups](#)

Users [New](#)

Search:  [Delete Checked Items](#)

<input type="checkbox"/>	Action	Name	Login Name	Status	Disabled On
<input checked="" type="checkbox"/>	Edit	 Larry	Larry	Enabled	
<input type="checkbox"/>	Edit	 Joe Shmoe	jshmoe	Enabled	
<input type="checkbox"/>	Edit	No Cred	nocred	Enabled	
<input type="checkbox"/>	Edit	John Eboy	Jboy	Enabled	
<input type="checkbox"/>	Edit		725F6968613347216549	Enabled	
<input type="checkbox"/>	Edit	LastOnly	ft32	Enabled	
<input type="checkbox"/>	Edit	FirstOnly	ft33	Enabled	
<input type="checkbox"/>	Edit		ft34	Enabled	
<input type="checkbox"/>	Edit	ft35 ft35	ft35	Enabled	
<input type="checkbox"/>	Edit	ft36 ft36	ft36	Enabled	
<input type="checkbox"/>	Edit	ft37 ft37	ft37	Enabled	
<input type="checkbox"/>	Edit	ft38 ft38	ft38	Enabled	
<input type="checkbox"/>	Edit	ft39 ft39	ft39	Enabled	
<input type="checkbox"/>	Edit	ft40 ft40	ft40	Enabled	
<input type="checkbox"/>	Edit	ft41 ft41	ft41	Enabled	

81 page(s): [1] [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [Last](#) >

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

The screenshot displays the 'SurePass id' user management interface. The top navigation bar includes links for Home, Users, Tokens, Audit Trail, and SSO. The user 'Larry' is currently selected, and the page title is 'Update User [Larry]'. The form contains several sections: Login Credentials (User Name: Larry, Password: [redacted]), User Credentials (First Name: Larry, Last Name: [redacted], Email: larry@terasoft.com, Mobile Phone: +1(321)297-8051), User Time Zone (Time Zone: (UTC-05:00) Eastern Time (US & Canada)), User Privileges (Admin Privilege: [checked]), Secure SSO Settings (Mobile Activation Code: 33356F76694679434A54726253476F72566D3758, Mobile Activation Date: [redacted], Mobile 2FA Options: 2FA Not Mandatory - Only if user has 2FA token, SSO Identity: Larry), and Status (Status: Enabled, Disabled On: [redacted]). Below the form are 'Update' and 'Close' buttons. At the bottom, there is a 'Tokens' table with columns: Action, Serial Number, Status, Token Type, Last OTP Validation, OTP Type, and Digit. A 'New' button is located to the right of the table header, circled in red. The footer contains copyright information for Terasoft, Inc. and contact details.

SurePass id

Home Users Tokens Audit Trail SSO

Update Member Of Group Import Users Update

Update User [Larry] New Update Close Email Login Info

Login Credentials

User Name: Larry Password: [redacted]

User Credentials

First Name: Larry Last Name: [redacted]
Email: larry@terasoft.com Mobile Phone: +1(321)297-8051

User Time Zone

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

User Privileges

Admin Privilege: [checked]

Secure SSO Settings

Mobile Activation Code: 33356F76694679434A54726253476F72566D3758 Mobile Activation Date: [redacted]
Mobile 2FA Options: 2FA Not Mandatory - Only if user has 2FA token SSO Identity: Larry

Status

Status: Enabled Disabled On: [redacted]

Update Close

Tokens New

Action	Serial Number	Status	Token Type	Last OTP Validation	OTP Type	Digit
--------	---------------	--------	------------	---------------------	----------	-------

© 1999-2017 SurePassId, Inc. All rights reserved. | Email: Support | Call Center: +1 (888) 300-8144

The following form will be displayed:

The screenshot shows the 'Add Token' form in the SurePassID web application. The header includes the 'SurePassid' logo and navigation tabs for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as 'Larry'. The form is divided into two main sections: 'Token Information' and 'One Time Password Settings'. In the 'Token Information' section, fields include Token Group (None), Token Type (SurePassID Authenticator Token), Assigned To (Larry), Filter Assigned To (empty), Printed Serial Number (TSFT-001308), Serial Number (001308), Status (New), Expiration Date (01/11/2018), Maximum Uses (999999999), and Manufacturer (SurePassID). The 'One Time Password Settings' section includes OTP Type (Time (Oath)), OTP Length (6 Digits), Time Step (secs.) (30), Time Drift (time step units) (5), and Starting Time [T0] (secs.) (000000000). 'Add' and 'Close' buttons are at the bottom right.

SurePassid

Home Users Tokens Audit Trail SSO

New Import Tokens Token Groups

tierasoft.com | Larry | Logout

Add Token [New](#) [Add](#) [Close](#)

Token Information

Token Group: None

Token Type: SurePassID Authenticator Token

Assigned To: Larry Filter Assigned To:

Printed Serial Number: TSFT-001308

Serial Number: 001308

Status: New

Expiration Date: 01/11/2018

Maximum Uses: 999999999

Manufacturer: SurePassID

One Time Password Settings

OTP Type: Time (Oath)

OTP Length: 6 Digits

Time Step (secs.): 30

Time Drift (time step units): 5

Starting Time [T0] (secs.): 000000000

Add Close

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

- **Token Type** – SurePassID Authenticator Token
- **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, **Time** Based CSC, **Event** Based CSC.
- **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:

SurePassID

Home Users Tokens Audit Trail SSO

Record has been added.

Update Token [New](#) [Update](#) [Close](#)

Check OTP Create Temporary Passcode Synchronize

Token Information

Token Group: None
 Token Type: SurePassID Authenticator Token
 Assigned To: not assigned
 Printed Serial Number: TSFT-001312
 Serial Number: 001312
 Status: Enabled
 Expiration Date: 01/27/2018
Token Id: 669CB-C8Jg6-rDLn8
 Maximum Uses: 999999999
 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](#)

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

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 Skype.

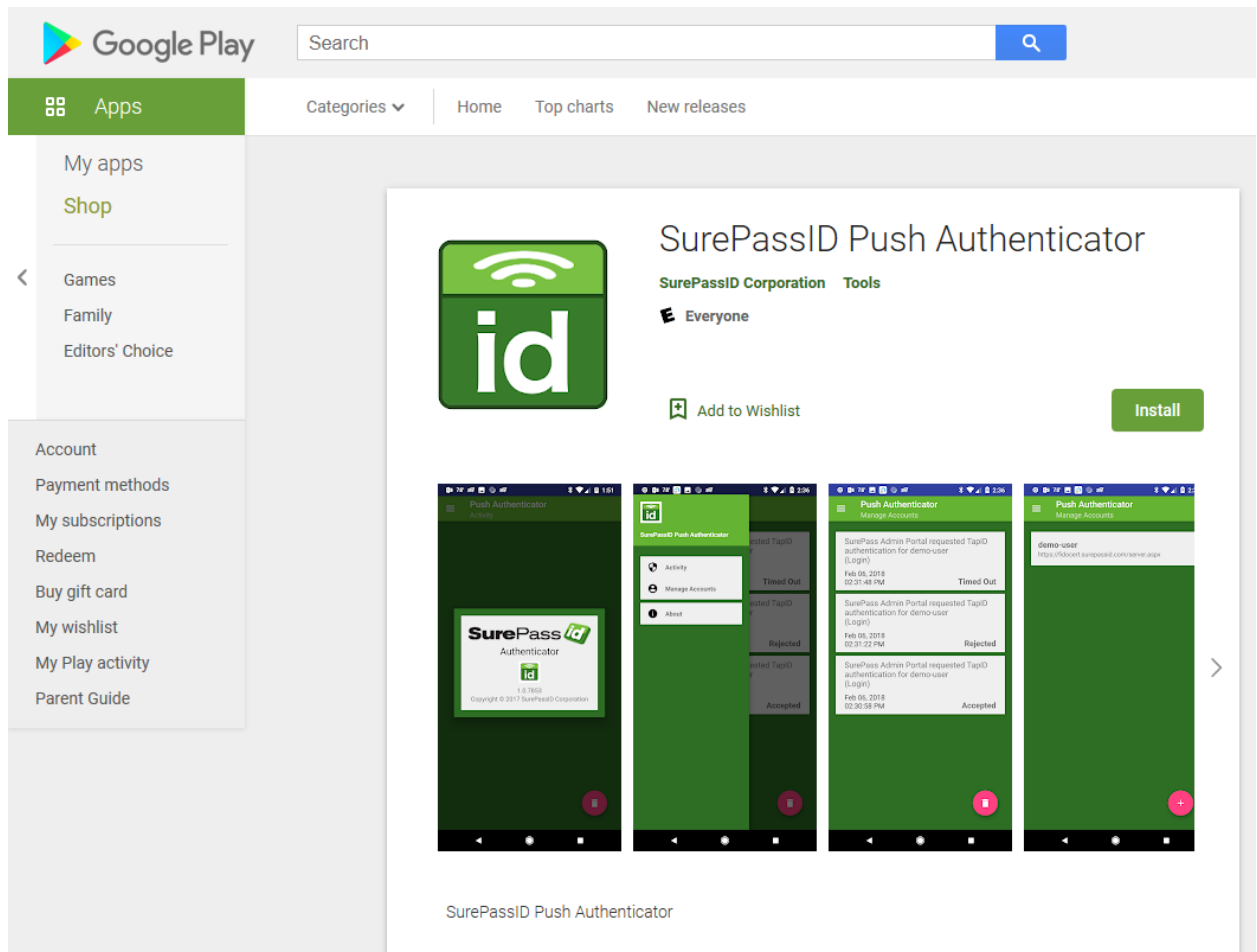
HINT: When using the Import Users method to add SurePassID Authenticators, the Unique Identifier field and the link to activate the SurePassID Authenticator will be sent to the user in an email for one-click install.

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

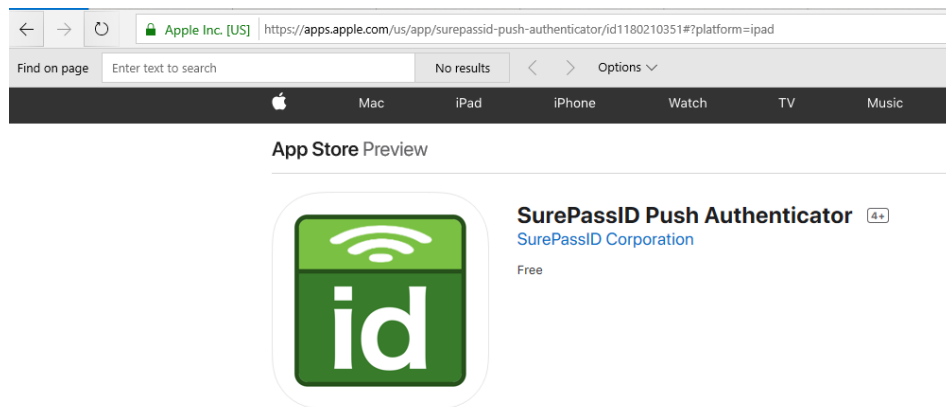
Installing the SurePassID Authenticator App

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](https://apps.apple.com/us/app/surepassid-push-authenticator/id1180210351#?platform=ipad) 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 that the link must be clicked on the user's mobile device. The link can be displayed on a mobile browser web page, embedded in an email, or in an SMS text message. SurePassID provides you many different ways to implement for very large organizations.

The instant activation link will be in the format of:

https://<surepass_installation>/oath-ota-provision/<tokenid>

For example:

<https://sandbox.surepassid.com/oath-ota-provision/pLxP0-NOkz1-dxgo1>

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.

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

To start the process, log into your SurePassID account (if not already logged in) and locate the SurePassID Authenticator Token you want to activate. You can do this by following the same steps as Adding the SurePassID Authenticator, 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:

This token is enabled.

Update Token

[New](#)
[Update](#)
[Close](#)
[Share Token](#)

Check OTP

Create Temporary Passcode

Synchronize

Filter Assigned To List:

Account: Tiera Software Inc.

Token Information

Token Group: None

Token Type: SurePassID Authenticator Token

Assigned To: Larry Routhenstein (Larry)

Printed Serial Number: TSFT-0000473

User Defined Token Name: TSFT-0000473

Internal Serial Number: 00000473

Status: Enabled

Expiration Date: 02/26/2018

Authenticator Usage: OTP Authentication Only

Token Id: J22L7-JVQB1-dWfK7

Maximum Uses: 999999999

OTP Activation Date:

Mobile Setup Verification: Mobile user must enter username and password

Push Authentication Activation Date:

Manufacturer: SurePassID

One Time Passcode Settings

OTP Type: Time (Oath)

OTP Length: 6 Digits

Time Step (secs.): 30

Time Drift (time step units): 5

Starting Time [T0] (secs.): 0

Current Time Counter: 0


Last Validation:

Failed Token Requests:

Update

Close

Click Instant Activation Button

Click the Instant Activation  icon and the following form will be shown.

[New](#)
[Update](#)
[Close](#)
[Share Token](#)

Check OTP
Create Temporary Passcode
Synchronize
Filter Assigned To List:

Account: Tiera Software Inc.

Token Information

Token Group: None
Token Type: SurePassID Authenticator Token
Assigned To: Larry Routhenstein (Larry)
Printed Serial Number: TSFT-0000473
User Defined Token Name: TSFT-0000473
Internal Serial Number: 00000473
Status: Enabled
Expiration Date: 02/26/2018
Authenticator Usage: OTP Authentication Only
Token Id: J22L7-JVQB1-dWfK7
Instant Activation Link: https://sandbox.surepassid.com/oath-ota-provision/auth/J22L7-JVQB1-dWfK7
Maximum Uses: 999999999
OTP Activation Date:
Mobile Setup Verification: Mobile user must enter username and password
Push Authentication Activation Date:
Manufacturer: SurePassID

One Time Passcode Settings

OTP Type: Time (Oath)
OTP Length: 6 Digits
Time Step (secs.): 30
Time Drift (time step units): 5
Starting Time [T0] (secs.): 0
Current Time Counter: 0
Last Validation:
Failed Token Requests:

Update
Close

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.

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 with Token ID

1. Start the SurePassID Authenticator app on the target mobile device.
2. The SurePassID Authentic
3. Select **Download From Cloud** and enter the Token ID.
4. Log into your SurePassID account (if not already logged in) and locate the SurePassID Authenticator Token you want to activate. You can do this by following the same steps as Adding the SurePassID Authenticator, 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:

The screenshot displays the SurePassID web application interface. At the top, the logo 'SurePassid' is visible. Below it is a navigation bar with tabs: Home, Accounts, Users, Tokens, Audit Trail, and SSO. A secondary bar contains links: New, Import Hard Tokens, Token Groups, and Token Usage Report. The top right shows the user 'Mark Poid(sa)' and a Logout button.

The main content area is titled 'Update Token' with links for 'New', 'Update', 'Close', and 'Share Token'. Below this is a toolbar with buttons: 'Check OTP', 'Create Temporary Passcode', 'Synchronize', and a 'Filter Assigned To List' dropdown.

The 'Account' dropdown is set to 'Tiera Software Inc.'. The 'Token Information' section contains the following fields:

- Token Group: None
- Token Type: SurePassID Authenticator Token
- Assigned To: Larry Routhenstein (Larry)
- Printed Serial Number: TSFT-0000473
- User Defined Token Name: TSFT-0000473
- Internal Serial Number: 00000473
- Status: Enabled
- Expiration Date: 02/26/2018
- Authenticator Usage: OTP Authentication Only
- Token Id: J22L7-JVQB1-dWfk7** (highlighted with a green box)
- Maximum Uses: 999999999
- OTP Activation Date: (empty)
- Mobile Setup Verification: Mobile user must enter username and password
- Push Authentication Activation Date: (empty)
- Manufacturer: SurePassID

The 'One Time Passcode Settings' section contains the following fields:

- OTP Type: Time (Oath)
- OTP Length: 6 Digits
- Time Step (secs.): 30
- Time Drift (time step units): 5
- Starting Time [T0] (secs.): 0
- Current Time Counter: 0
- Last Validation: (empty)
- Failed Token Requests: (empty)

At the bottom of the form are 'Update' and 'Close' buttons.

5. Copy the **Token Id** and send it to the user.
6. The user will then enter the Token id into the Token ID field in the SurePassID Authenticator app.

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

To activate token with QR Code

1. Start the SurePassID Authenticator app on the target mobile device.
2. Select **Scan QR Code for Account** from the menu. The SurePassID Authenticator is now waiting for a bar code to scan.
3. Log into your SurePassID account (if not already logged in) and locate the SurePassID Authenticator Token you want to activate. You can do this by following the same steps as Adding the SurePassID Authenticator, 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:

This token is enabled.

Update Token

[New](#) [Update](#) [Close](#) [Share Token](#)[Check OTP](#)[Create Temporary Passcode](#)[Synchronize](#)

Filter Assigned To List:


Account: Tiera Software Inc.

Token Information

Token Group: None Token Type: SurePassID Authenticator Token Assigned To: Larry Routhenstein (Larry) Printed Serial Number: TSFT-0000473 User Defined Token Name: TSFT-0000473 Internal Serial Number: 00000473 Status: Enabled Expiration Date: 02/26/2018 Authenticator Usage: OTP Authentication Only Token Id: J22L7-JVQB1-dWfK7 Maximum Uses: 999999999 OTP Activation Date: Mobile Setup Verification: Mobile user must enter username and password Push Authentication Activation Date: Manufacturer: SurePassID

One Time Passcode Settings


OTP Type: Time (Oath) OTP Length: 6 Digits Time Step (secs.): 30 Time Drift (time step units): 5 Starting Time [T0] (secs.): 0 Current Time Counter: 0 Last Validation: Failed Token Requests: [Update](#)[Close](#)

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

SurePass

[Home](#) [Accounts](#) [Users](#) [Tokens](#) [Audit Trail](#) [SSO](#)

[New](#) [Import Hard Tokens](#) [Token Groups](#) [Token Usage Report](#)

tierasoft.com  Mark Poid(sa) [Logout](#)

[New](#) [Update](#) [Close](#) [Share Token](#)

[Check OTP](#) [Create Temporary Passcode](#) [Synchronize](#) [Filter Assigned To List:](#)

Account: Tiera Software Inc.

Token Information

Token Group: None

Token Type: SurePassID Authenticator Token

Assigned To: Larry Routhenstein (Larry)

Printed Serial Number: TSFT-0000473

User Defined Token Name: TSFT-0000473


Internal Serial Number: 00000473

Status: Enabled

Expiration Date: 02/26/2018

Authenticator Usage: OTP Authentication Only

Token Id: J22L7-JVQB1-dWfk7



Maximum Uses: 999999999

OTP Activation Date:

Mobile Setup Verification: Mobile user must enter username and password

Push Authentication Activation Date:

Manufacturer: SurePassID

One Time Passcode Settings

OTP Type: Time (Oath)

OTP Length: 6 Digits

Time Step (secs.): 30

Time Drift (time step units): 5

Starting Time [T0] (secs.): 0

Current Time Counter: 0

Last Validation:

Failed Token Requests:

[Update](#) [Close](#)

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



Activate Mobile Token

TokenId:

Name for this token:

[Install mobile authenticator app \(SurePassID, Google, or Google compliant\) on your mobile device first.](#)

© 1999-2017 SurePassID Corp. All rights reserved.

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

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



Activate Mobile Token

✓ Scan the QRCode into the authenticator app on your mobile device.

TokenId:

Name for this token:

[Install mobile authenticator app \(SurePassID, Google, or Google compliant\) on your mobile device first.](#)



Code From Mobile App To Verify:

© 1999-2017 SurePassId Corp. All rights reserved.

Press the **Select QR Code for Account** menu item, 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 **Code From Mobile App To Verify** field and press the **Verify Code** button as shown below. If your token is configured correctly, you will see the following form:



Activate Mobile Token

✓ The code you entered has been verified.

tokenid: wQrO8-EzwP6-nwGr2

Name for this token: QA token

[Install mobile authenticator app \(SurePassID, Google, or Google compliant\) on your mobile device first.](#)



Code From Mobile App To Verify: 843222 **Verify Code**

© 1999-2017 SurePassID Corp. All rights reserved.

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

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

Verifying SurePassID Authenticator Token on the Server

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

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

SurePassid

Home Accounts Users Tokens Audit Trail SSO

tierasoft.com | Mark Poid(sa) | Logout

New Import Hard Tokens Token Groups Token Usage Report

Tokens [New](#) [Assign Tokens](#)

Account: Tiera Software Inc.

Token Group: All

Token Type: All User Assignment Status: All Device Status: All

Serial Number Filter: Is TSFT-0000473 User: Begins with Larry Rows to Display: 20

Action	Serial Number	User Defined Name	Status	Token Type	User
Edit Delete Check	TSFT-0000473		Enabled	SurePassID Authenticator Token	Larry Routhenstein

1 page(s): [1]

The following form will be displayed:



SurePass **id**

Home Users Tokens Audit Trail SSO

New Import Tokens Token Groups

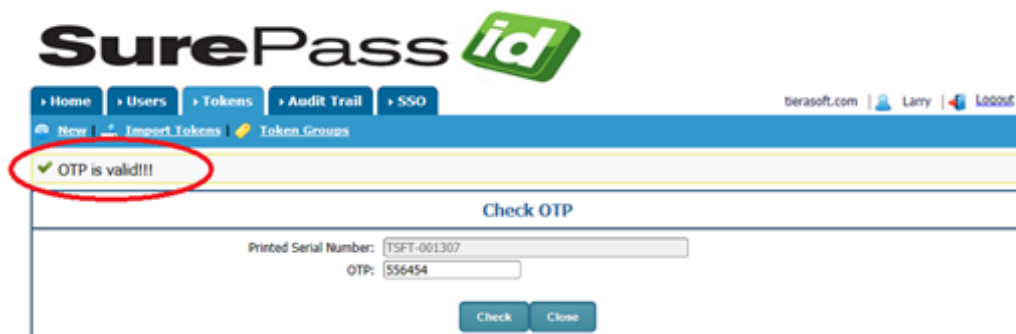
Check OTP

Printed Serial Number: TSFT-001307

OTP:

Check Close

5. Ask the user to start the SurePassID Authenticator app on their mobile device.
6. Have the user select the token in the SurePassID Authenticator App and provide you with the code displayed by SurePassID Authenticator. Enter that code into the **OTP** field. Press the **Check** button and the following form is displayed.



SurePass **id**

Home Users Tokens Audit Trail SSO

New Import Tokens Token Groups

✓ OTP is valid!!!

Check OTP

Printed Serial Number: TSFT-001307

OTP: 556454

Check Close

If the OTP is correct, you will see the **OTP is valid!!!** The user can use the SurePassID 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.