

SurePass

Desktop Authenticator Guide

SurePassID Authentication Server 23.1



© 2013-2023 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

Table of Contents

Desktop Authenticator Guide	1
About the Desktop Authenticator Guide	4
Using Desktop Authenticator	5
Step 1: Manually Add Desktop Token to User Account	5
Step 2: Install the Desktop Authenticator	12
Step 3: Launch the Desktop Authenticator	13
Step 4: Activate the Desktop Token	16
Step 5: Activate the Desktop Token	17
Optional: Edit Desktop Authenticator Settings	20
Troubleshooting SurePassID Desktop Authenticator	22

About the Desktop Authenticator Guide

The Desktop Authenticator is a Windows application that acts as a container for storing SurePassID desktop security tokens. Each SurePassID desktop token is a software version of a physical two-factor authentication token.

The Desktop Authenticator offers the following advantages over traditional hardware devices:

- Desktop Authenticator tokens can be created instantaneously and electronically distributed to your users. Conversely, traditional hardware devices must be sent to individual users.
- Desktop Authenticator tokens are software and as such they are inherently less costly than traditional hardware devices. Perfect for budget constrained companies.
- Thousands of Desktop Authenticator devices can be rolled out in a matter of hours. Hardware devices can often require a set of operational procedures for the distribution of physical corporate assets.

Although the Desktop Authenticator application can be used in lieu of a physical token for production, it can really be useful in system testing of new two-factor authentication systems because you can easily create test tokens in a matter of seconds.

This guide describes how to use the Desktop Authenticator to add SurePassID tokens to generate One Time Passwords (OTPs).

Other SurePassID Guides

The SurePassID Desktop Authenticator Guide has the following companion guides that provide additional detail on specific topics for SurePassID:

- SurePassID Administrators Guide
- SurePassID Mobile OTP Guide
- SurePassID Mobile Authenticator Guide
- SurePassID Programmer API Guide
- SurePassID Local Agent Guide
- SurePassID ServicePass User Portal Guide

The latest documentation can be found on-line at:

<https://surepassid.atlassian.net/wiki/display/ProdDoc/SurePass+Authentication+Server>

Using Desktop Authenticator

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

1. Manual – Add a Desktop 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 Desktop tokens added to user accounts that are imported and setup instructions sent to users. Best for pilots and large-scale deployments.
3. SurePassID API – Using the SurePassID API, you can add Desktop Authenticator to a user's account from your existing corporate intranet or IT application.
4. ServicePass – End user self-service portal.

This document only describes the Manual method. The other methods are beyond the scope of this document. Please refer to the other respective documents for more information on other methods or contact your SurePassID representative to discuss large-scale automated deployments.

Step 1: Manually Add Desktop Token to User Account

Log in to SurePassID Authentication Server. Then select the **Tokens** tab as highlighted below:

Hello Kevin Raineri. Welcome Back

Home

Account: ▼

Open System Alerts	User Statistics	OTP Statistics
<ul style="list-style-type: none">Open Items Requiring Action: 1118Open Severe Items: 107909Items Requiring Action (This Week): 1Severe Issues (This Week): 1Items Requiring Action (Last Week): 15Severe Issues (Last Week): 0Items Requiring Action (This Month): 128Severe Issues (This Month): 4	<ul style="list-style-type: none">Total Users: 574New Users (This Week): 0New Users (Last Week): 0New Users (This Month): 1Total Disabled Users: 1Disabled Users (This Week): 0Disabled Users (Last Week): 0Disabled Users (This Month): 0	<ul style="list-style-type: none">Total Server Requests (This Week): 40Successful OTP Requests (This Week): 26Failed OTP Requests (This Week): 14Total Server Requests (Last Week): 107Successful OTP Requests (Last Week): 87Failed Server Requests (Last Week): 20Total Server Requests (This Month): 306Successful OTP Requests (This Month): 138Failed OTP Requests (This Month): 168

© 1999-2019 SurePassId Corp. All rights reserved. | [Email Support](#) | Call Support: +1 (888) 200-8144 ext 2

The **Tokens** window will open as shown below:

Tokens New Assign Tokens							
Token Group: All		Type: All		Status: All			
Serial Numbers Beginning With: <input type="text"/>			Search By User: <input type="text" value="Larry"/>				
Action	Serial Number	Status	Token Type	User	Last OTP Validation	OTP Type	
Edit Delete Check	TSFT-001291	Enabled	SurePassID Authenticator	Larry	12/27/2015 12:00:00 AM	Time (Oath)	
Edit Delete Check	TSFT-00000015	Enabled	Mobile OTP Soft Token	Larry		Time (Oath)	

1 page(s): [1]

Press the **New** button as shown below to create a new SurePassID Desktop token.

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

Token Group: Type: Status:

Serial Numbers Beginning With: Search By User:

Action	Serial Number	Status	Token Type	User	Last OTP Validation	OTP Type
Edit Delete Check	TSFT-001291	Enabled	SurePassID Authenticator	Larry	12/27/2015 12:00:00 AM	Time (Oath)
Edit Delete Check	TSFT-00000015	Enabled	Mobile OTP Soft Token	Larry		Time (Oath)

1 page(s): [1]

HINT: To add many tokens at once, use the SurePassID User Import. For additional instructions on this, please refer to the SurePassID Administrators Guide.

HINT: You can also pick a user under the Users tab and add a token for that user.

The **Add Token** window opens:

The screenshot shows the 'Add Token' window in the SurePass ID interface. The window is titled 'Add Token' and has a navigation bar with links for 'New', 'Add', 'Close', and 'Share Token'. The form is divided into two main sections: 'Token Information' and 'One Time Passcode Settings'. In the 'Token Information' section, the 'Token Type' is set to 'Desktop Token', 'Assigned To' is 'Kevin Raineri (kevi)', 'Status' is 'Enabled', and 'Manufacturer' is 'SurePassID'. In the 'One Time Passcode Settings' section, the 'OTP Type' is 'Time + Pin (Oath)', 'OTP Length' is '6 Digits', 'Time Step (secs.)' is '30', and 'PIN' is '1234'. The 'Add' and 'Close' buttons are located at the bottom right of the form.

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

- **Token Type** – Desktop Token
- **Assigned To** – User who will use this token.
- **Status** – Set to Enabled. If the device is not enabled the user will not be able to configure the Desktop Token.
- **OTP Type** – In most cases you will select either a **Time-Based** OTP or an **Event-Based** OTP. Or you can select Time + Pin (Oath) to require a PIN code before the OTP will be displayed. Enter the desired PIN into the PIN field.

Click the **Add** button to add the token and the following window will open:



Record has been added.

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

Filter Assigned To List:

Account: Tiera Software Inc.


Token Information


Token Group: None
Token Type: Desktop Token
Assigned To: Kevin Raineri (kevr)
Printed Serial Number: TSFT-002516
User Defined Token Name:
Serial Number: 002516
Status: Enabled
Expiration Date: 07/20/2020
Token Id: 1m3u8-FhO28-HB4K5  
Maximum Uses: 999999999
OTP Activation Date:
Manufacturer: SurePassID

One Time Passcode Settings

OTP Type: Time + Pin (Oath)
OTP Length: 6 Digits
Time Step (secs.): 30
PIN: 1234
Time Drift (time step units): 3
Starting Time [T0] (secs.): 000000000
Current Time Counter: 000000000
Last Validation:
Failed Token Requests:

Take note of the **Token Id** field. You will need this field to configure the token in the Desktop Authenticator application after you install it onto the target PC.

You can click the  icon to send token setup instructions to the user via their defined Email.

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

Alternatively, you can copy the **Token Id** and send it to the user.

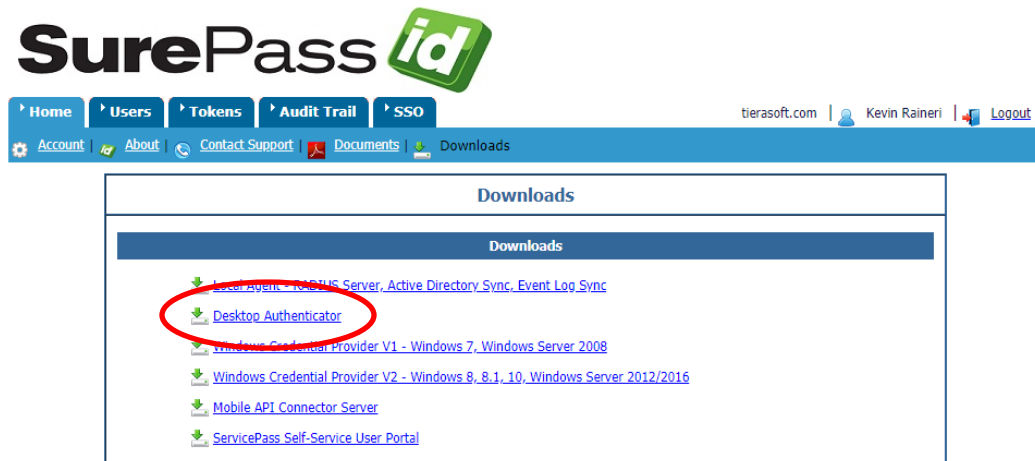
NOTE: You can customize the setup instructions by selecting the **Home > Settings > Customize Email Messages** or **Home > Settings > Customize SMS Messages** as show below:

The screenshot shows the SurePass id web interface. The navigation menu at the top includes 'Home', 'Users', 'Tokens', 'Audit Trail', and 'SSO'. The 'Home' menu item is circled in red. Below the navigation menu, there are several tabs: 'Settings', 'Customize Email Messages', 'Customize SMS Messages', 'Fido U2F', and 'Import Tokens'. The 'Customize Email Messages' tab is selected. The main content area is titled 'Customize Email Messages' and includes an 'Update' and 'Close' link. The page is divided into two main sections: 'SMTP Server Settings' and 'Customize Email Messages'. The 'SMTP Server Settings' section has a checkbox for 'Use Custom SMTP Settings' and input fields for 'Host Name/IP', 'Port', 'Username', and 'Password'. The 'Customize Email Messages' section has a dropdown for 'Email Format' (set to 'Plain Text'), a dropdown for 'System Action' (set to 'Setup Instructions - Sent to the user to assist them in activating thier soft token (e.g. mobile phone app)'), and input fields for 'From Name' (Metro Surepass), 'From Address' (no.reply.surepass@metro.net), and 'Subject' (Required Information). Below these fields is a 'Message' text area containing the following text: 'Hi %name%', 'Your DeviceId is %deviceid%. Save your DeviceId. You might require it later for activation.', 'Your Google Authenticator for your mobile device is ready for activation. Prior to activation you must follow these steps.', and a list of four steps: (1) On your mobile device, please go to the App Store. Search for and install "Google Authentication" on your mobile device. (2) On your work PC click the following activation link. %activatedeviceurl%. Enter a friendly name for this device (i.e. Metro iPhone) and press the Active Device button. This will display a QRCode to scan on your mobile device. (3) Start Google Authenticator app on your mobile device. (4) In Google Authenticator, choose "Set up Account". At the bottom of the page are three buttons: 'Update', 'Close', and 'Set Defaults'.

You are now ready to install the Desktop Authenticator and add the desktop token.

Step 2: Install the Desktop Authenticator

1. Download the Desktop Authenticator. The download URL can be found in your SurePassID account by selecting the **Home** tab followed by the **Downloads** menu item. If you already have the file downloaded then proceed to the next step.



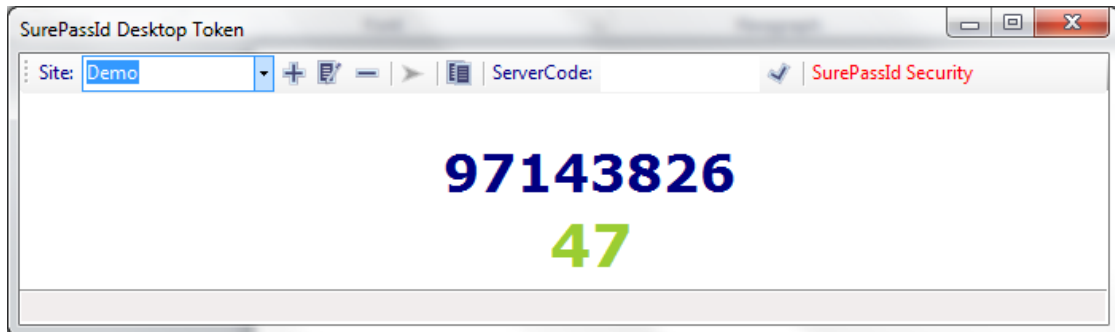
2. Save the download (SPDA.ZIP) to a temp directory such as the Downloads folder.
3. Unzip SPDA.ZIP.
4. Run SurePassVirtualToken.exe to install.

NOTE: Download the Desktop Authenticator from here:

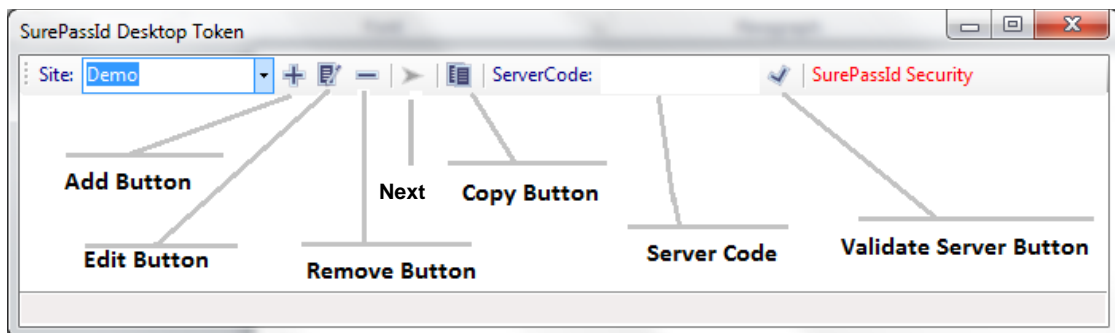
<https://sandbox.surepassid.com/downloads/SurePassVirtualToken.exe>

Step 3: Launch the Desktop Authenticator

Select the Desktop Authenticator from the start menu item to launch the application. The following window will appear:



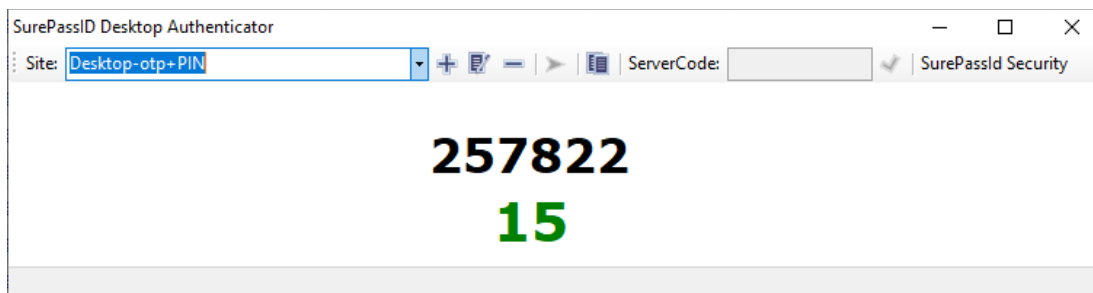
The window is divided into two sections; the toolbar section and the OTP section. The toolbar section is highlighted and described below:



Moving from left to right, the Desktop Authenticator toolbar has the following items and buttons:

- **Site List** – This is a friendly name that identifies the current Desktop Authenticator. The Desktop Authenticator can hold multiple separate “authenticators” for different sites/user accounts.
- **Add Button** – Add a new Desktop Authenticator
- **Edit Button** – Edit/View the tokens in the system plus OTP display preferences.
- **Remove Button** – Delete the current token.
- **Next Button** – Get the next OTP for Event-based authenticators.
- **Copy Button** – Copy OTP to the clipboard

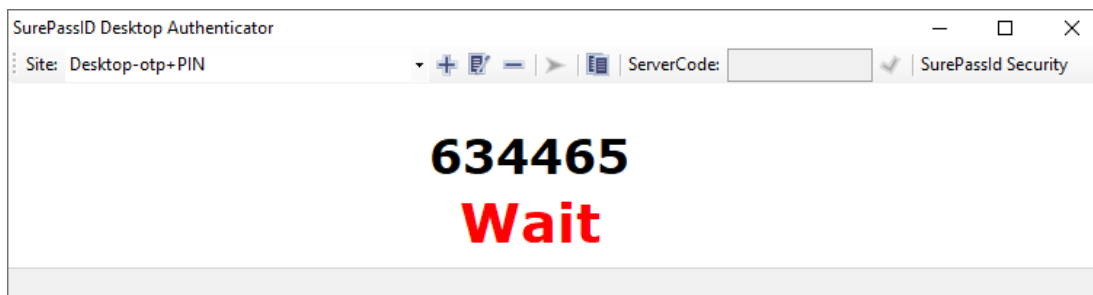
- **Server Code** – For configured Challenge Response authenticators (mutual authentication) you enter the OTP from the server and press the Server Code Validate Button.



Moving from top to bottom in the main screen area, beneath the toolbar section has the following items:

Current OTP – This is the OTP for the currently selected token.

OTP Countdown Seconds – For time based OTP, the number of seconds remaining before the **Current OTP changes and is no longer valid. Keep in mind, once the Time-based OTP is used, it becomes invalid even though the OTP and timer may still show time remaining.**



OTP Countdown Warning – For time based OTP, a **“Wait”** message will appear indicating that only a few seconds remain before the **Current OTP changes and is no longer valid. Keep in mind, once the Time-based OTP is used, it becomes invalid even though the “Wait” message may be displayed.**

Note: You can change the colors of the OTP, Countdown seconds, and **“Wait”** message by using the Edit button in the toolbar:



Site: Desktop-otp+PIN

Device Status

Activation Date: 6/19/2019 2:57:13 PM
Serial Number: TSFT-002511
Expiration Date: 6/19/2025 2:54:29 PM

Authorization Server URL:
<https://sandbox.surepassid.com/AuthServer/>

OTP Settings

Type: OATH Time + Pin OTP
Digits: 6

Options

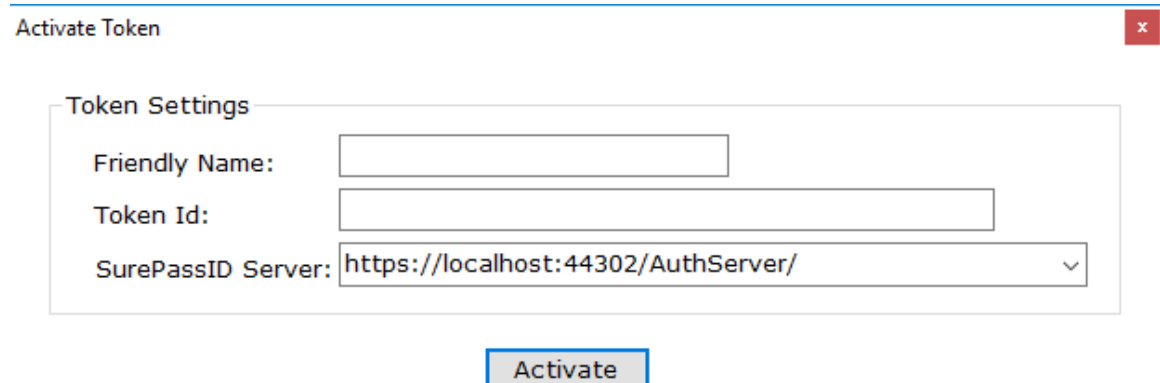
Label Color: Black SampleText
Countdown Color: Green 90
Countdown Wait Color: Red Wait

Start In System Tray

OK Cancel

Step 4: Activate the Desktop Token

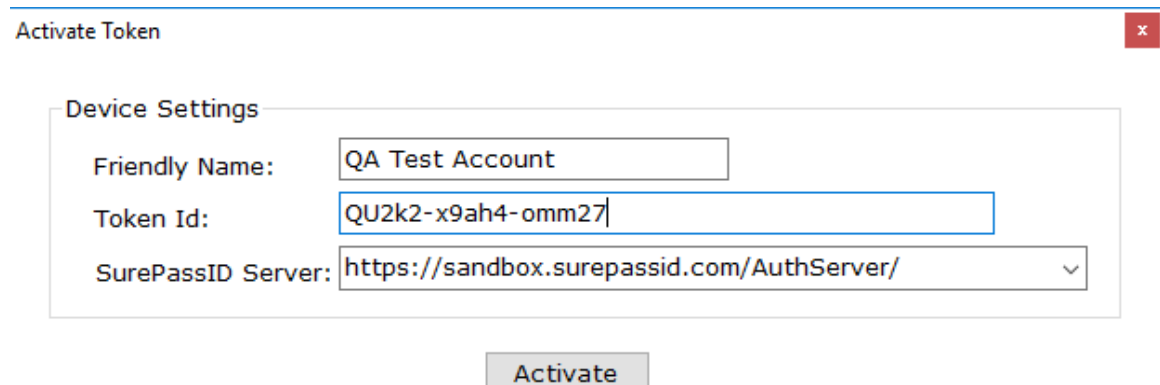
In Desktop Authenticator, click the toolbar **+** button. The following window will appear:



The screenshot shows a window titled "Activate Token" with a close button in the top right corner. Inside the window is a section titled "Token Settings" containing three input fields: "Friendly Name:" (empty), "Token Id:" (empty), and "SurePassID Server:" (containing the URL "https://localhost:44302/AuthServer/"). Below these fields is a blue "Activate" button.

Enter the following fields:

- **Friendly Name** – A descriptive name for the Desktop Authenticator.
- **Token Id** – The **Token Id** for the Desktop Token when it was created in Step 1.
- **SurePassID Server** - SurePassID Authentication Server location. If you are using your own installation of the SurePassID Authentication Server, enter your URL.



The screenshot shows a window titled "Activate Token" with a close button in the top right corner. Inside the window is a section titled "Device Settings" containing three input fields: "Friendly Name:" (containing "QA Test Account"), "Token Id:" (containing "QU2k2-x9ah4-omm27"), and "SurePassID Server:" (containing the URL "https://sandbox.surepassid.com/AuthServer/"). Below these fields is a grey "Activate" button.

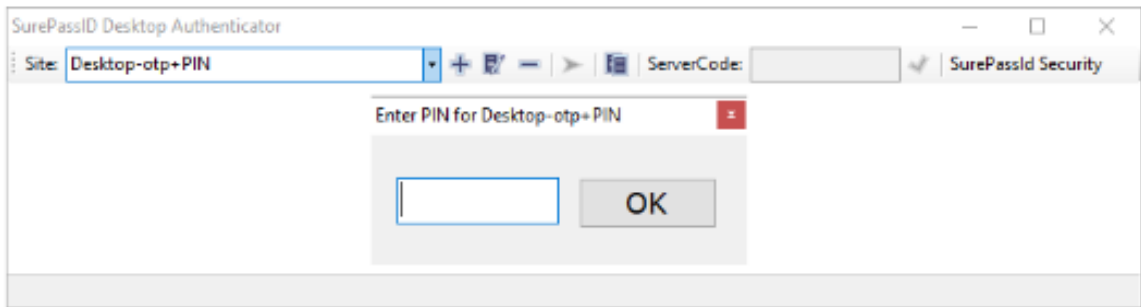
Click the **Activate** button.

The main window will be redisplayed with your new Desktop Authenticator.

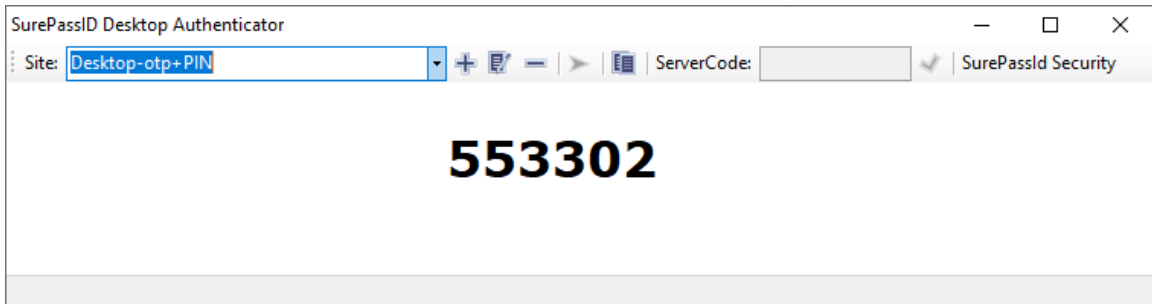


OTP + PIN

If you created an OTP Type of “Time + Pin (Oath)” in Step 1 above, you will be prompted for the PIN that was assigned to the token when it was created. When you launch the Desktop Soft Token (Authenticator) application, if the last token type that was used was a Time + Pin token, you will be required to enter the appropriate PIN. Or if you change the Site name to select an OTP + Pin type, you will be prompted for the appropriate PIN:



Enter the PIN that was assigned to this token in order to display the Time-based OTP.



Step 5: Activate the Desktop Token

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

SurePass id

Home Users Batches Devices Audit Trail SSO

tierasoft.com Larry Routhenstein Logout

New

Devices [New](#)

Batch: All Type: All Status: All

Serial Numbers Beginning With: Search By User:

Action	Serial Number	Status	Device Type	User	Last OTP Validation	
New Edit Delete Check Sync	TSFT-00000020	Enabled	Desktop Soft Token	Larry Routhenstein	6/11/2013 10:15:32 AM	Tim
New Edit Delete Check Sync		New	Android	Odin Soli		Eve
New Edit Delete Check Sync	TSFT-00000022	Enabled	Desktop Soft Token	Joe Schmo		Eve

2 page(s): [1](#) [2](#)

The following window will open:

SurePass id

Home Users Batches Devices Audit Trail SSO

tierasoft.com Larry Routhenstein Logout

New

Check OTP

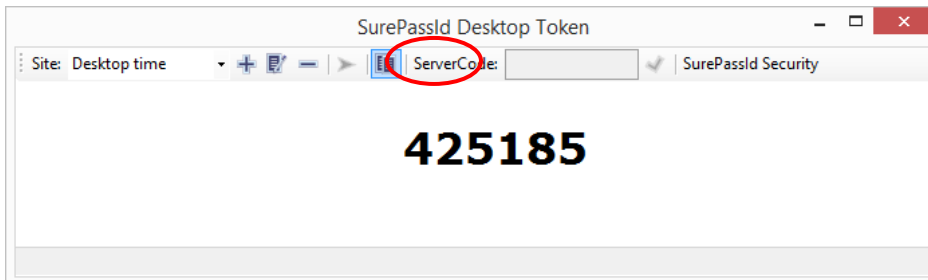
Printed Serial Number: TSFT-00000022

OTP: 571608 x

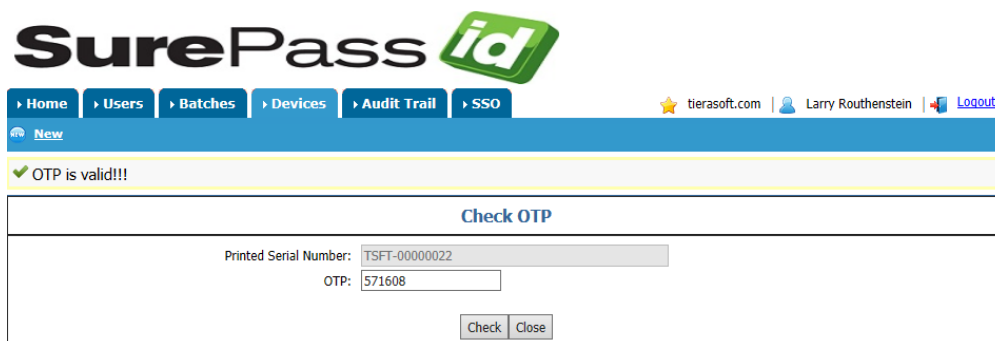
Check Close

© 1999-2013 SurePassId Corp. All rights reserved. | [Email Support](#) | Call Support: 1 (888) 200-8144

1. Start the Desktop Authenticator if it is not already running. You can start it by clicking on it in the system tray.
2. Find the Desktop Token in the Desktop Authenticator, select it in the drop down (if not already selected) and press the **Copy** button to copy the OTP that is displayed.



3. Paste the OTP copied from the Desktop Authenticator into the **OTP** field in the server as shown below and press the **Check** button. The following window is displayed:




© 1999-2013 SurePassId Corp. All rights reserved. | [Email Support](#) | Call Support: 1 (888) 200-8144

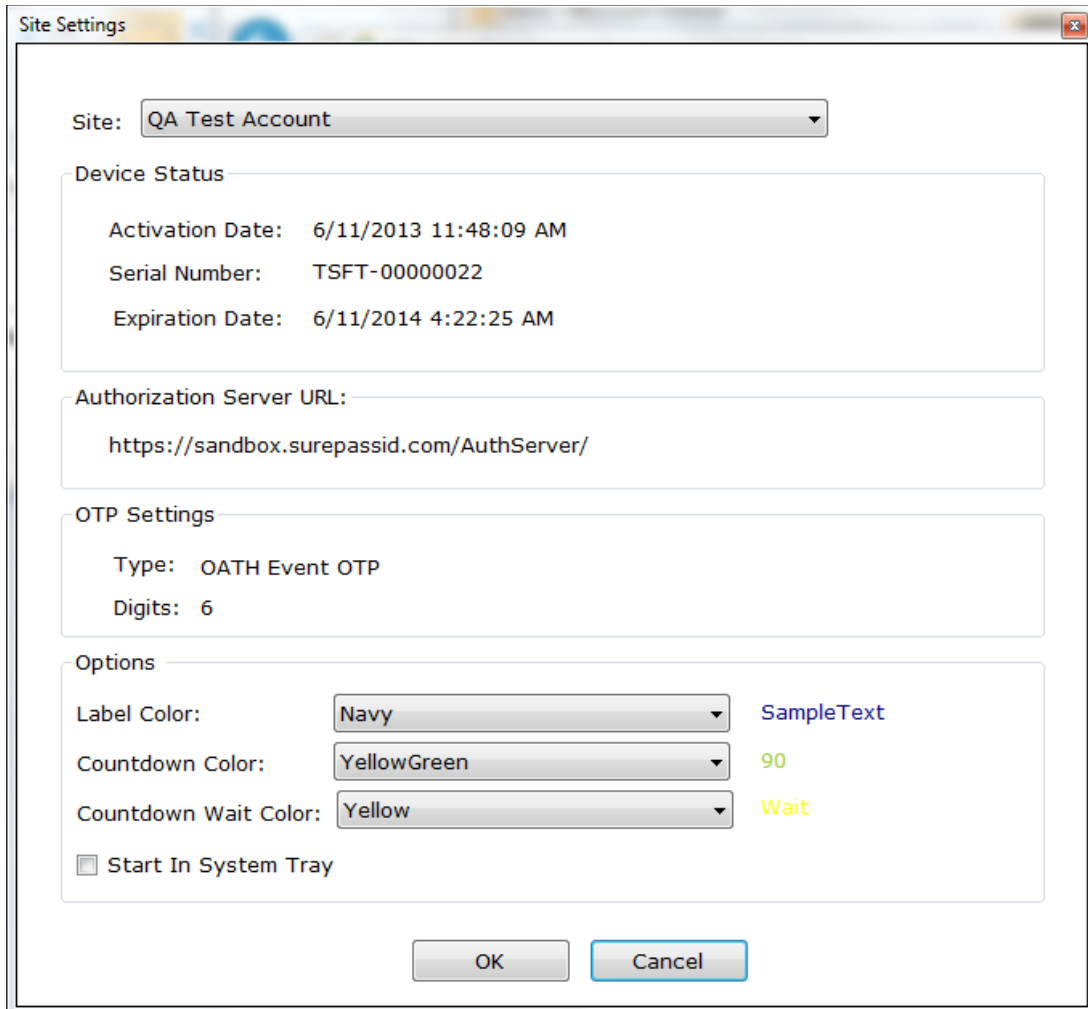
If the OTP is correct, then you will see the message **OTP is valid!!!** You can now use the Desktop Authenticator as a Two-Factor Authentication (2FA) token to generate OTP codes for SurePassID Authentication Server. **Desktop Token is now functional!**

If the OTP is NOT valid verify that the OTP entered is for the correct desktop token. The easiest way to do this is to check token serial number on the Desktop Authenticator with the serial number on the SurePassID server as defined in the Tokens form.

Optional: Edit Desktop Authenticator Settings

To edit Desktop Authenticator or its system settings, follow these steps:

Press the toolbar **Edit**  button. The following window will appear:



Site Settings

Site: QA Test Account

Device Status

Activation Date: 6/11/2013 11:48:09 AM
Serial Number: TSFT-00000022
Expiration Date: 6/11/2014 4:22:25 AM

Authorization Server URL:
https://sandbox.surepassid.com/AuthServer/

OTP Settings

Type: OATH Event OTP
Digits: 6

Options

Label Color: Navy SampleText
Countdown Color: YellowGreen 90
Countdown Wait Color: Yellow Wait

Start In System Tray

OK Cancel

You can view the status of individual tokens by selecting them in the **Site** drop down.

You can change the system display options by changing the various choices in the **Options**. The choices are:

- **Label Color** – The color to be used for non-enterable fields.
- **Countdown Color** – For Time based authenticators, this is the color of the countdown clock in seconds.

- **Countdown Wait Color** – For Time based authenticators this is the color of the Wait message when the clock is about to expire.
- **Start In System Tray** – Check this box if you want the Desktop Authenticator to start in the system tray.

Click the **OK** button to save changes.

Troubleshooting SurePassID Desktop Authenticator

Cannot connect to the SurePassID server – This is often caused by a corporate firewall that blocks all outbound traffic. You will need to talk to your system admin staff. The Desktop Authenticator requires port 443 to be open.

HTTP 407 Error connecting to the SurePassID server – This is often caused by a corporate proxy server that blocks all direct outbound traffic. To fix this you will need to instruct the Desktop Authenticator to use your corporate proxy server. To do this you will need to take the following steps:

1. Get proxy server info from your corporate system admin person.
2. Locate the Desktop Authenticator **OTPSoftToken.config** file which is usually located in “**C:\Program Files (x86)\SurePassId\Desktop Authenticator**”. This is also where the OTPSoftToken.exe file is located.
3. Open the **OTPSoftToken.config** file with a text editor.
4. The file should look like this:

```
<?xml version="1.0"?>
<configuration>

  <startup>
    <supportedRuntime version="v4.0"
sku=".NETFramework,Version=v4.0"/>
  </startup>
</configuration>
```

5. You need to modify this file by adding the highlighted lines and changing **myproxy:9000** to your corporate proxy server name and port:

```
<configuration>
<system.net>
  <defaultProxy enabled="true"
useDefaultCredentials="true">
    <proxy proxyaddress="myproxy:9000"
      usesystemdefault="true"
      bypassonlocal="true"
      autoDetect="true" />
  </defaultProxy>
</system.net>
<startup>
  <supportedRuntime version="v4.0"
sku=".NETFramework,Version=v4.0"/>
```

```
</startup>  
</configuration>
```

6. Restart the Desktop Authenticator.