Desktop Authenticator Guide

SurePassID Authentication Server 2025

You can find the most up-to-date technical documentation at:

http://www.surepassid.com/resources

The SurePassID web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

support@surepassid.com

© 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 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 18

Optional: Edit Desktop Authenticator Settings 20

Troubleshooting SurePassID Desktop Authenticator 22

About the Desktop Authenticator Guide

The Desktop Authenticator is a Windows app that stores SurePassID desktop security tokens, which are software equivalents of physical two-factor authentication tokens.

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

- Desktop Authenticator tokens can be created instantly and distributed electronically, while traditional hardware devices must be physically shipped to users.
- Desktop Authenticator tokens, being software-based, are less expensive than hardware devices and ideal for companies with limited budgets.
- Desktop Authenticator devices can be deployed to large numbers of users within several hours. Hardware devices typically require specific operational procedures for distributing physical corporate assets.

The Desktop Authenticator app can replace a physical token in production and is especially useful for quickly creating test tokens when testing new two-factor authentication systems.
This guide explains how to use it to add SurePassID tokens and 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

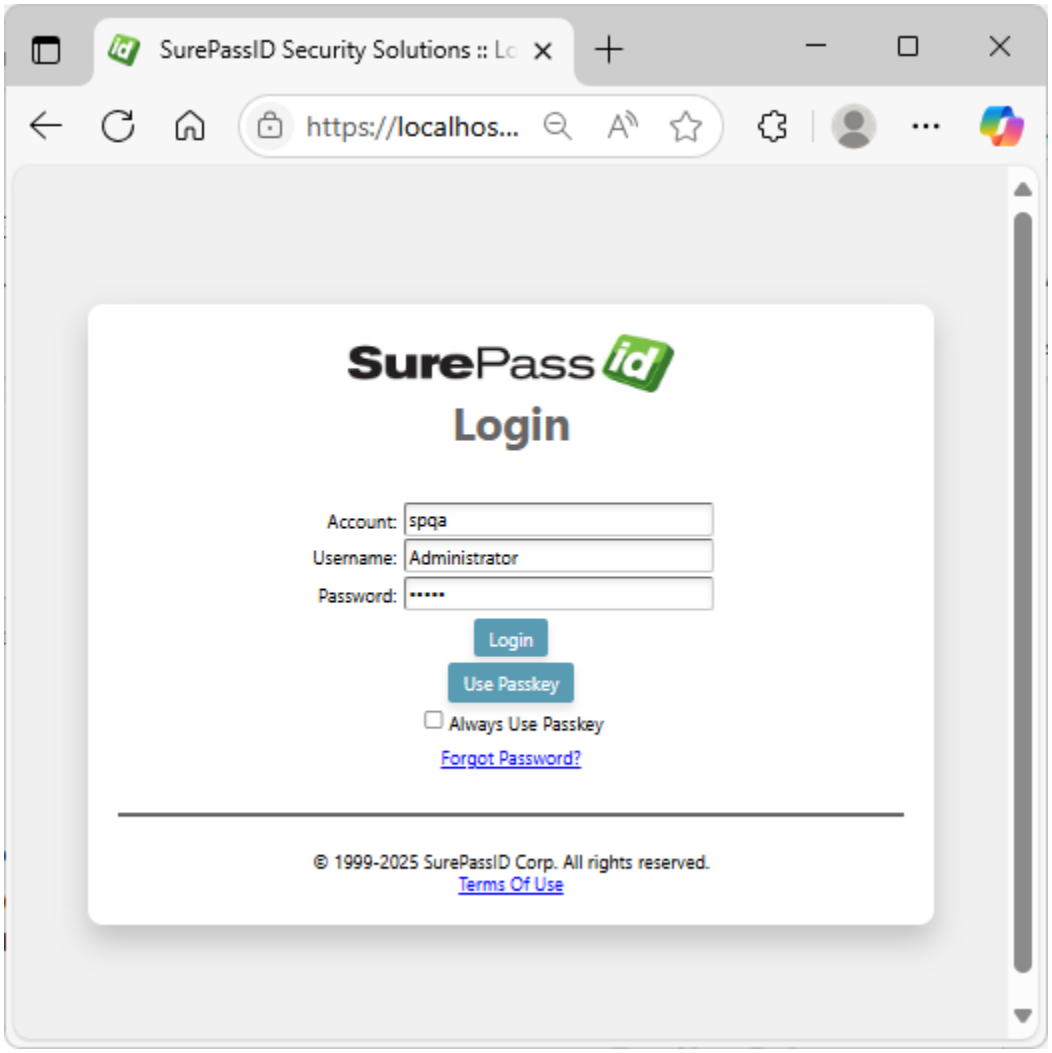
You can add a Desktop token to a SurePassID user account a few ways:

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 – During user import, Desktop tokens are added to accounts and setup instructions are sent. Ideal for pilots and large 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.

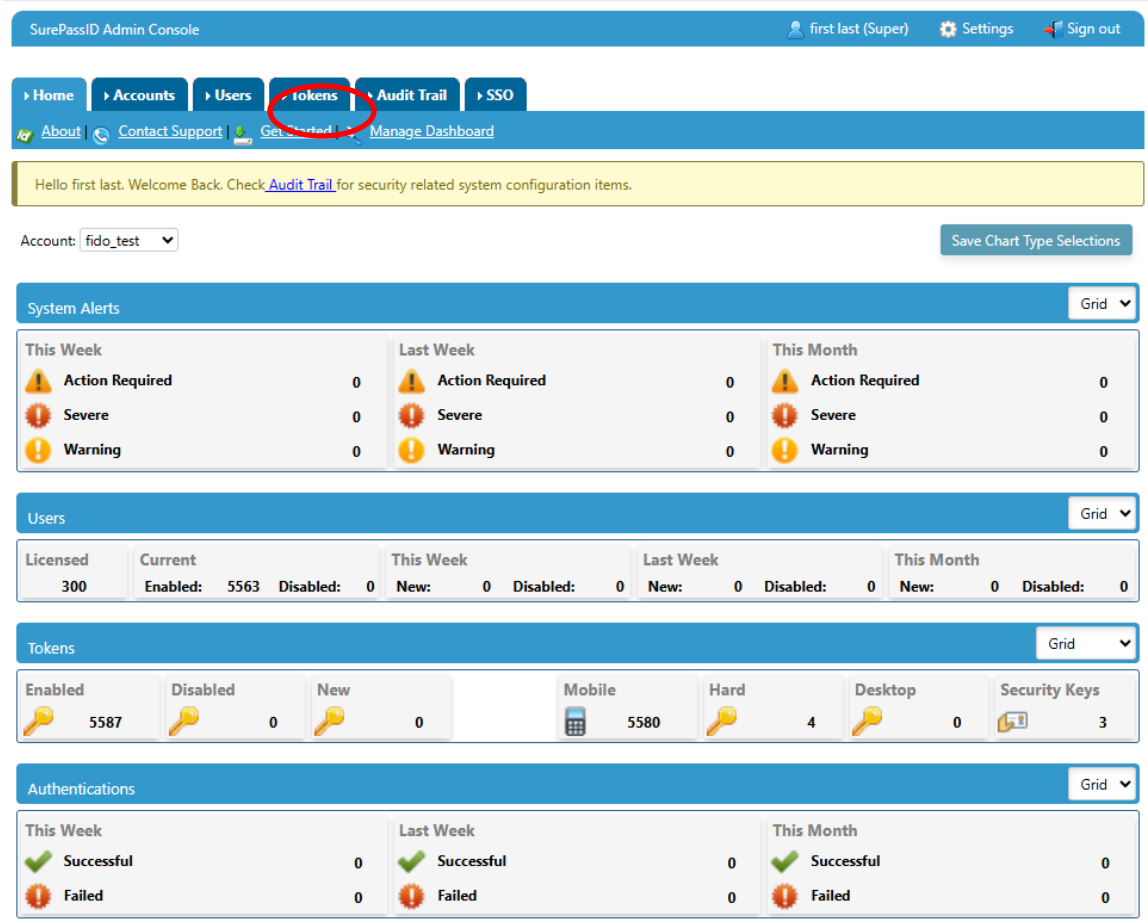
This document covers only the Manual method. For other methods, see their respective documents or contact your SurePassID representative about automated deployments.

Step 1: Manually Add Desktop Token to User Account

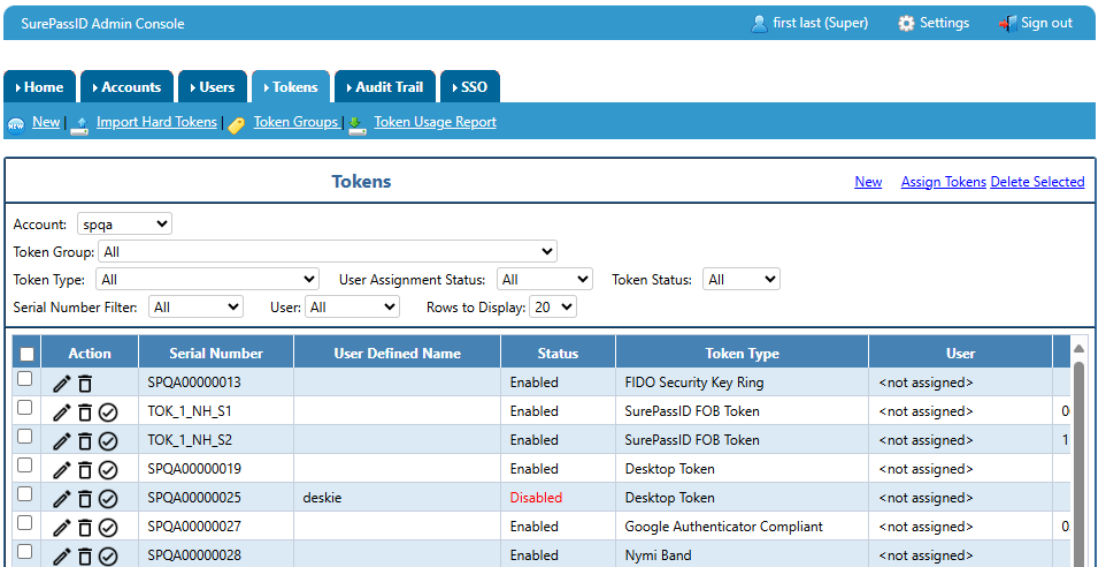
Log in to SurePassID Authentication Server.



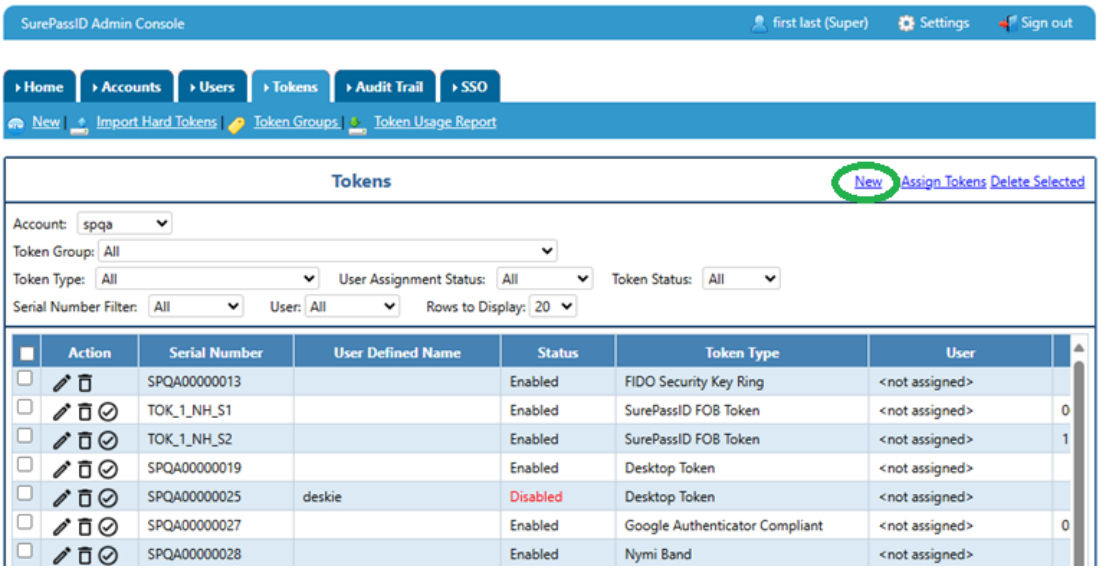
Next, from the **Home** screen navigate to the **Tokens** tab as indicated below:



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



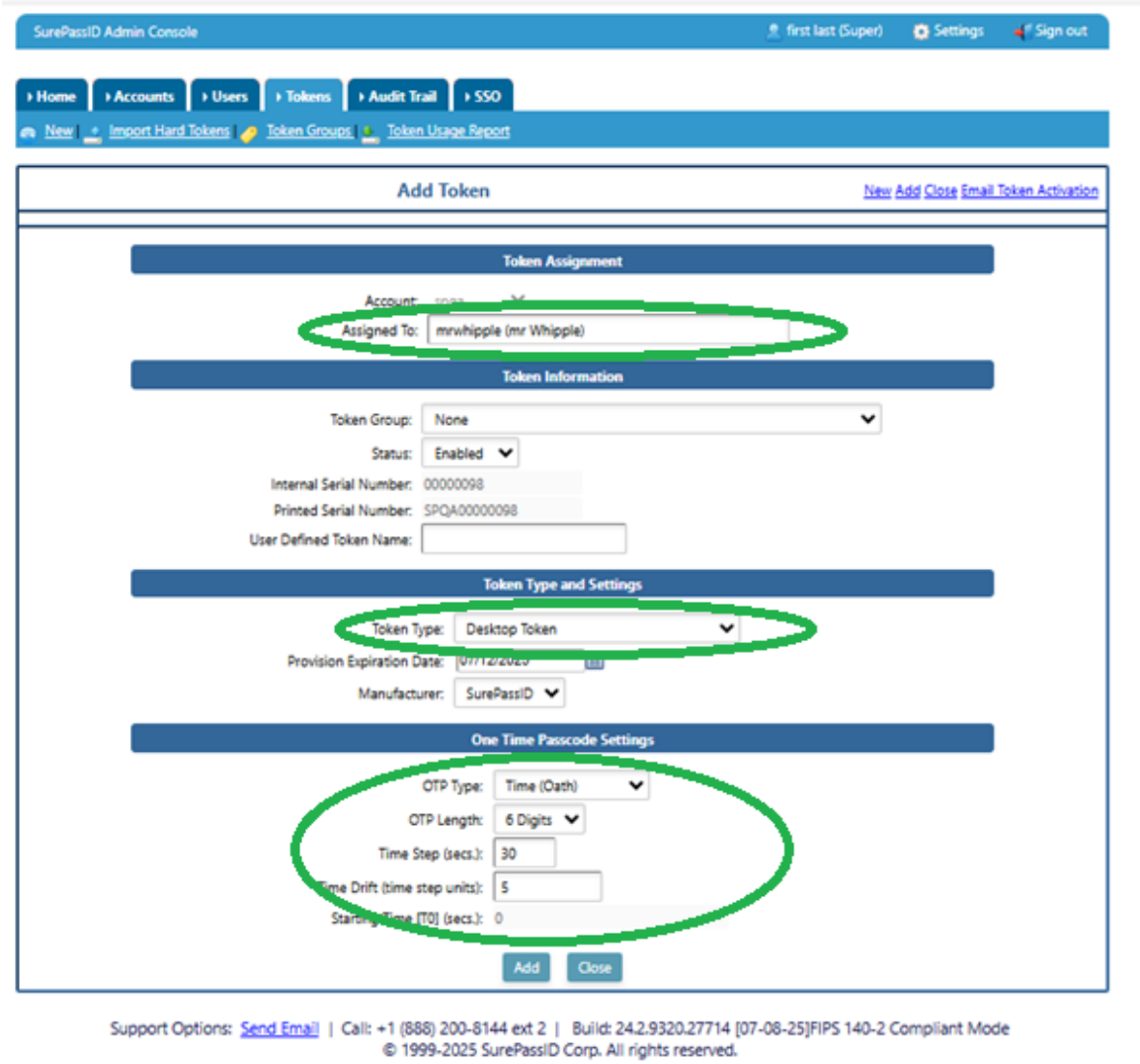
Press the **New** button as shown below to create a new SurePassID Desktop token.



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.

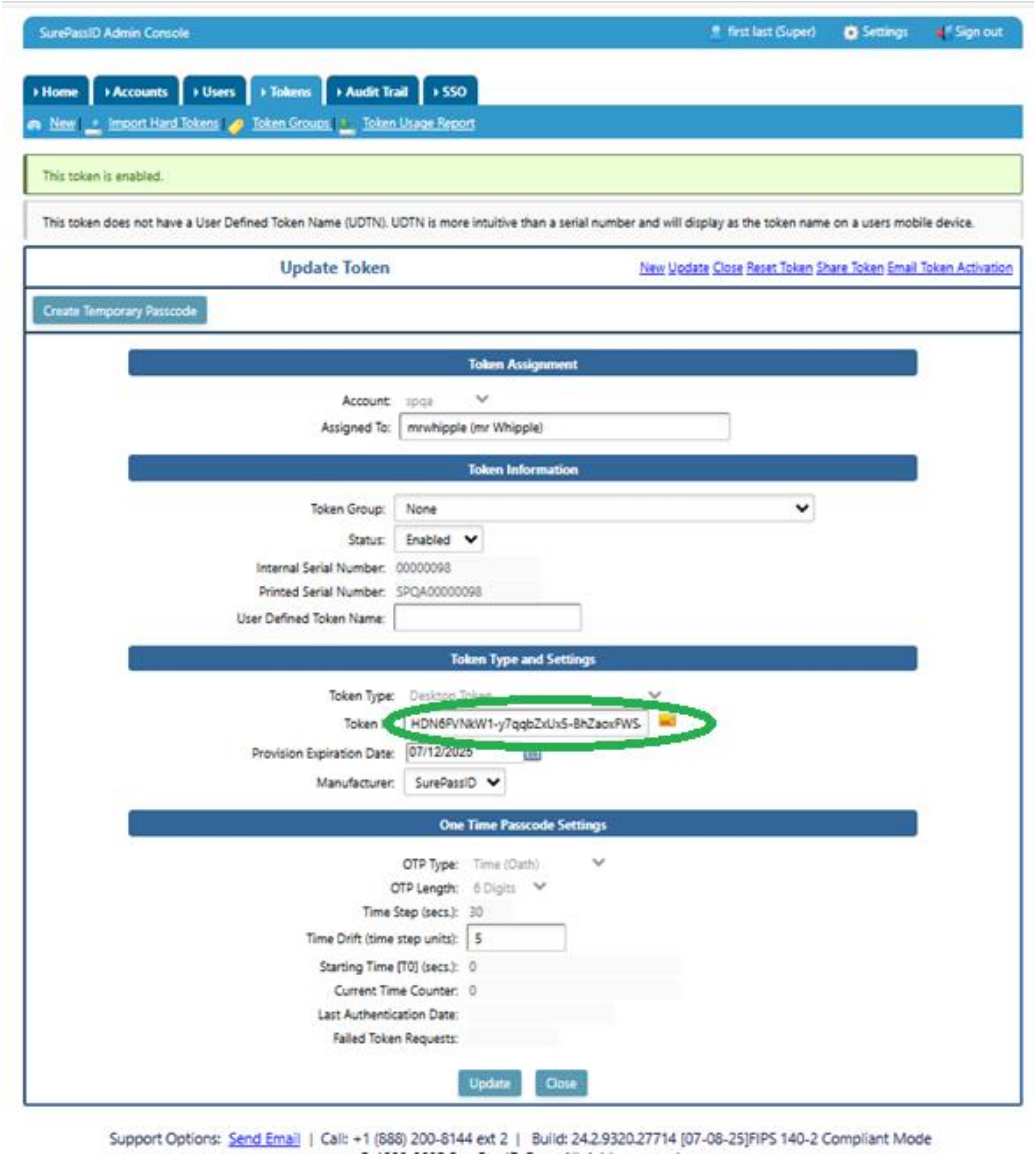
The **Add Token** window opens:



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 disabled, the user cannot 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:

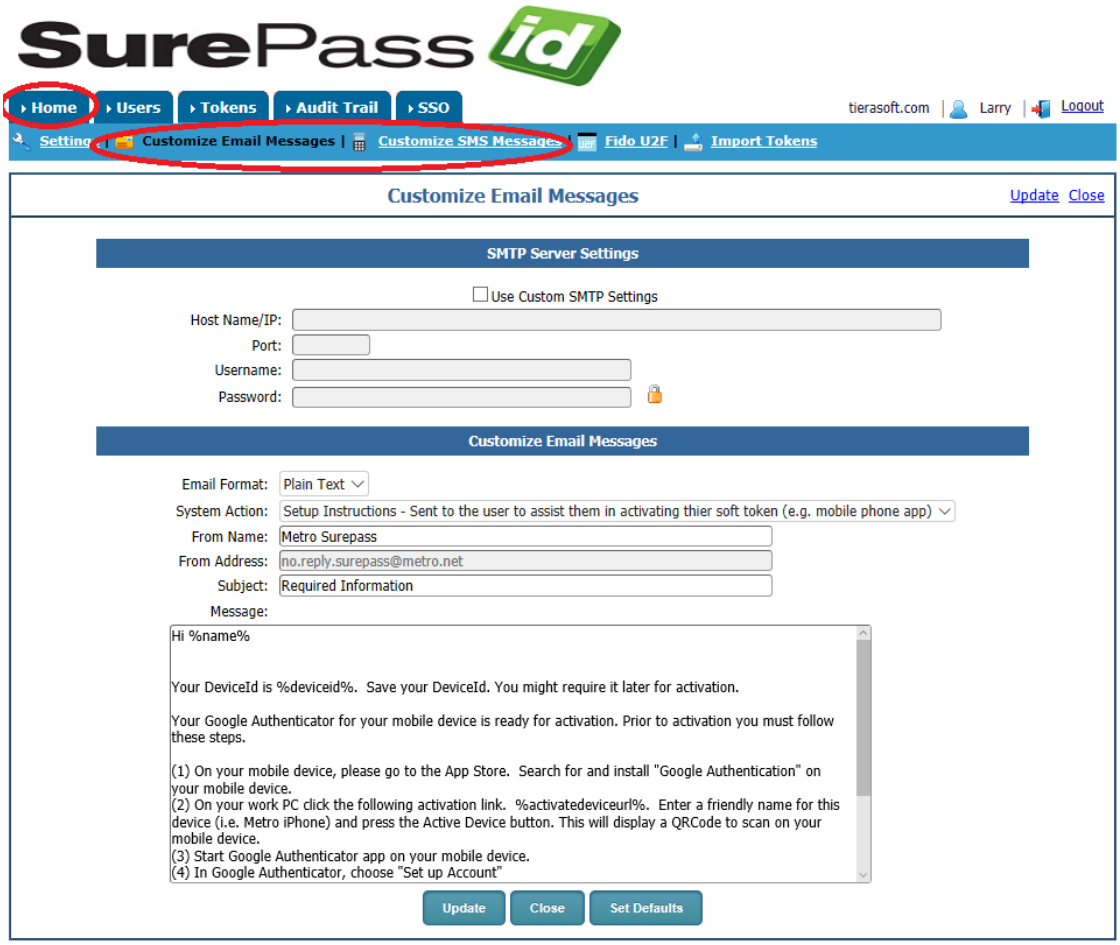


Take note of the **Token Id** field. You will need this field to configure the token in the Desktop Authenticator application after you install it onto the target PC.

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

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

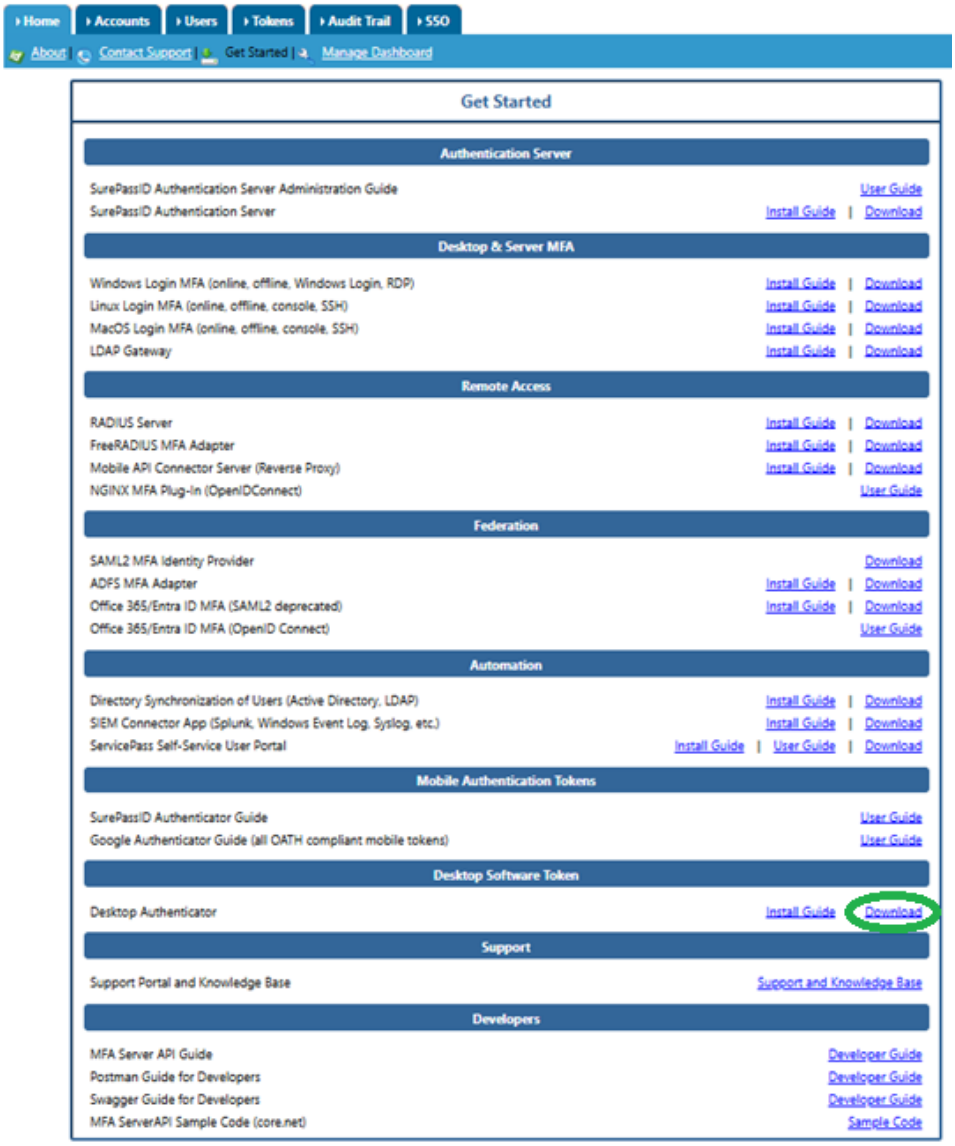
NOTE: You can customize the setup instructions by selecting the **Home > Settings > Customize Email Messages** or **Home > Settings > Customize SMS Messages** as show below:



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 **Get Started** menu item. If you already have the file downloaded, then proceed to the next step.

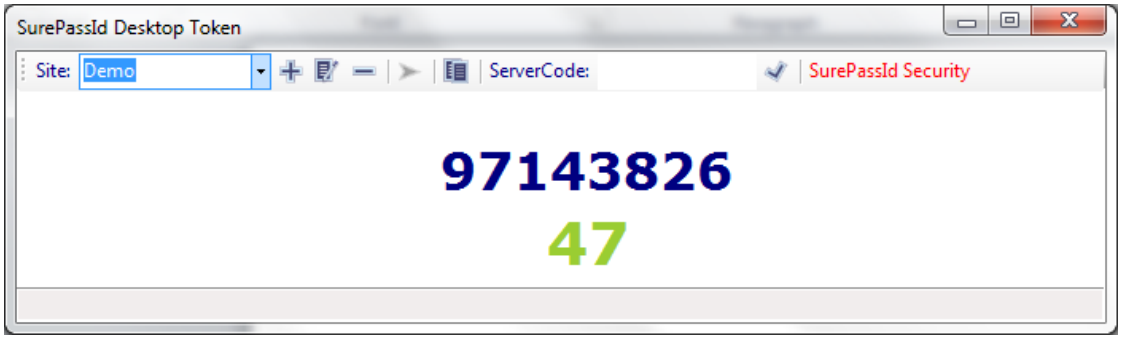


2. Save the download (SPDA.ZIP) to a temp directory such as the Downloads folder.
3. Unzip SPDA.ZIP

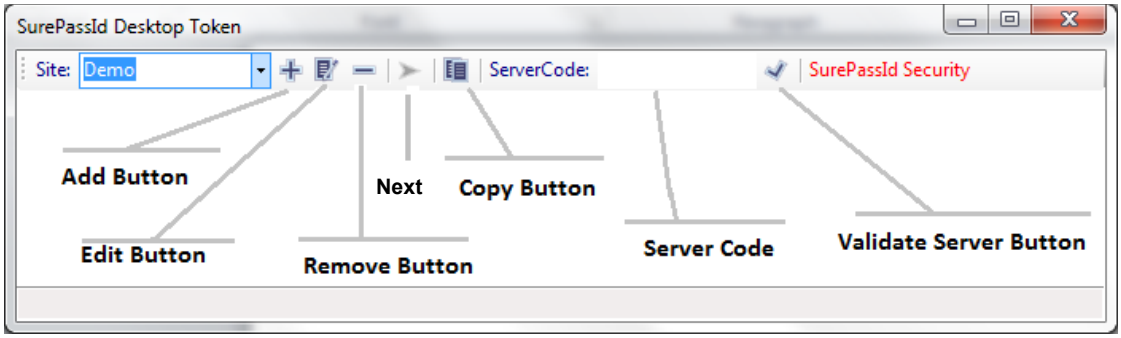
4. Run Desktop Authenticator to install.

Step 3: Launch the Desktop Authenticator

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



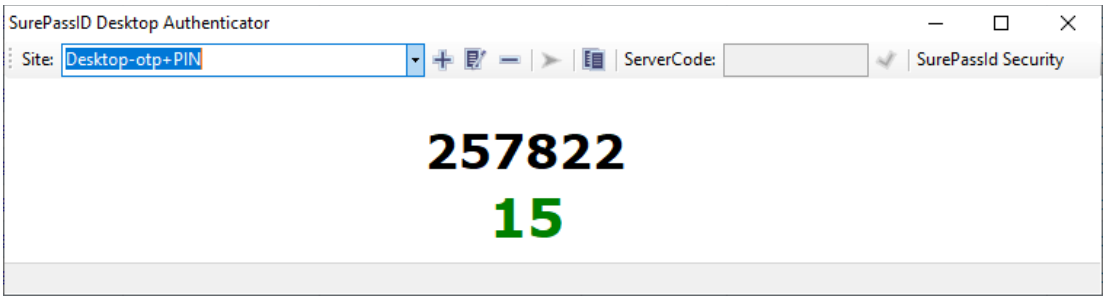
The window is divided into two sections; the toolbar section and the OTP section. The toolbar section is highlighted and described below:



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

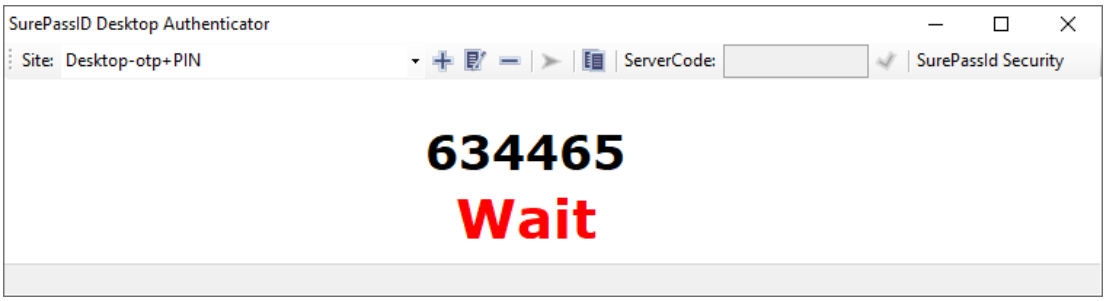
- **Server Code** – For configured Challenge Response authenticators (mutual authentication) you enter the OTP from the server and press the Server Code Validate Button.



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

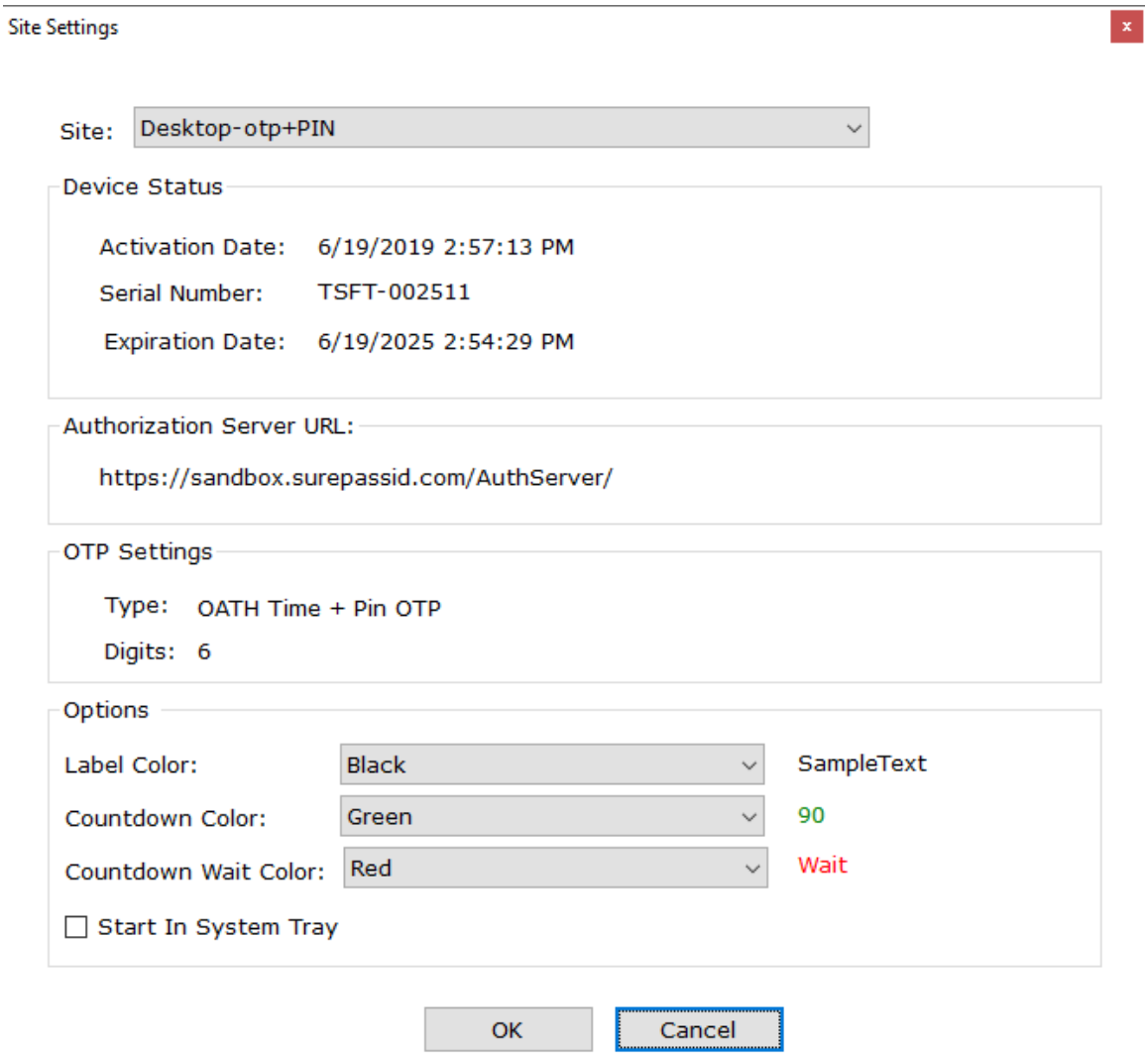
Current OTP – This is the OTP for the currently selected token.

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.**



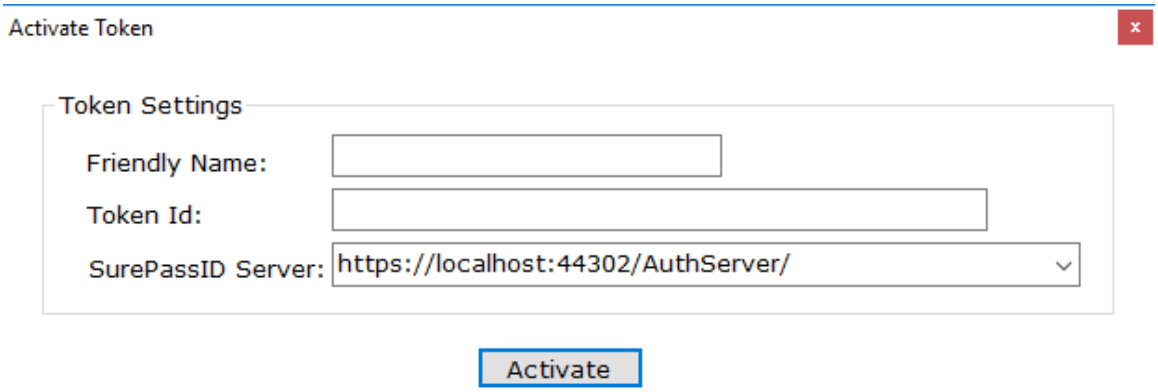
OTP Countdown Warning – For time based OTP, a "**Wait**" message will appear indicating that only a few seconds remain before the **Current OTP changes and is no longer valid. Keep in mind, once the Time-based OTP is used, it becomes invalid even though the "Wait" message may be displayed.**

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


Site Settings
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

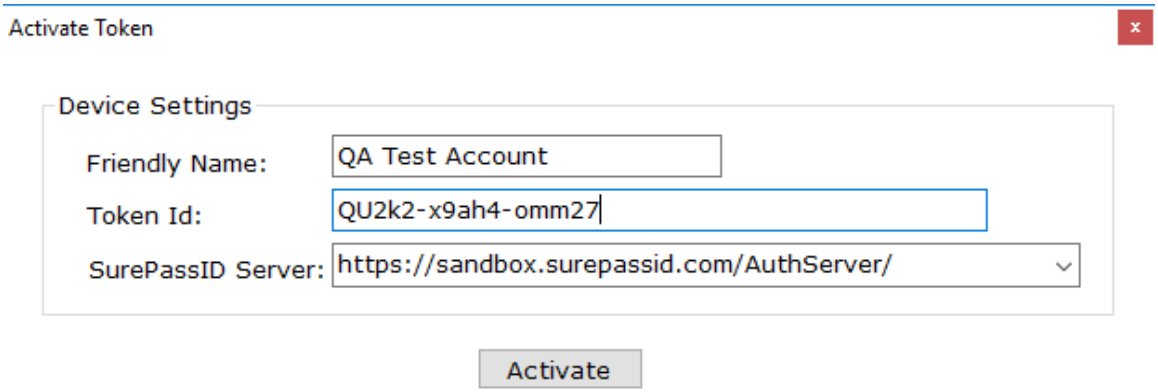
Step 4: Activate the Desktop Token

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



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.

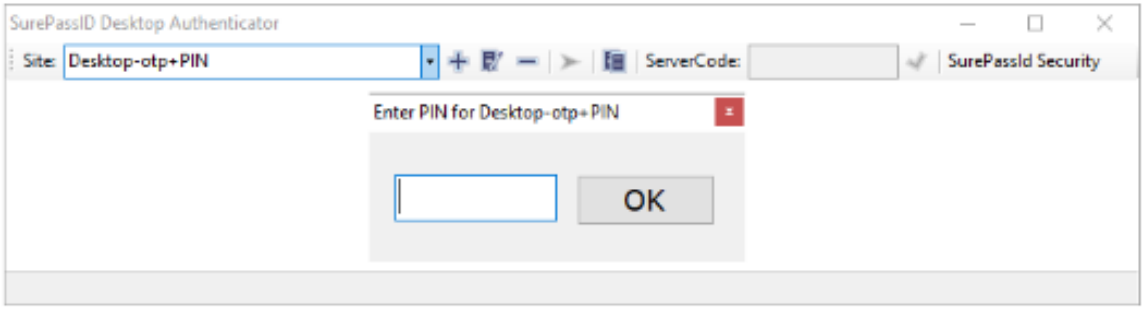


Click the **Activate** button.

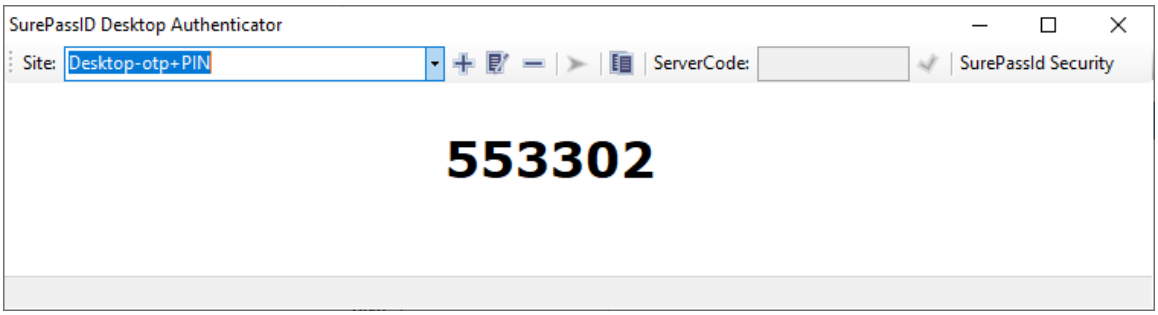
The main window will be redisplayed with your new Desktop Authenticator.

OTP + PIN

If you set up a “Time + Pin (Oath)” OTP, you'll be prompted to enter the assigned PIN when launching the Desktop Soft Token (Authenticator). If the last token used was a Time + Pin type or if you select an OTP + Pin site, you must provide the correct PIN.

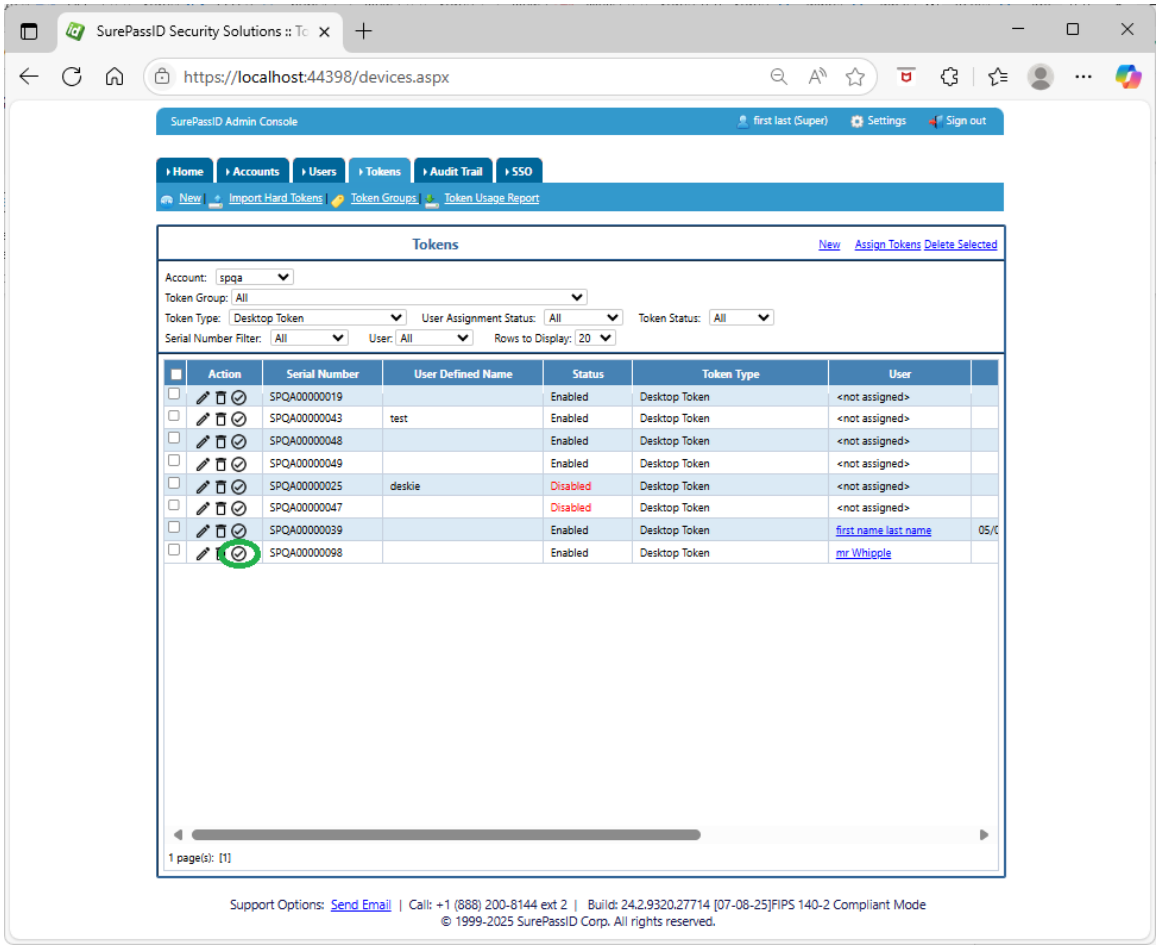


Enter the PIN that was assigned to this token in order to display the Time-based OTP.

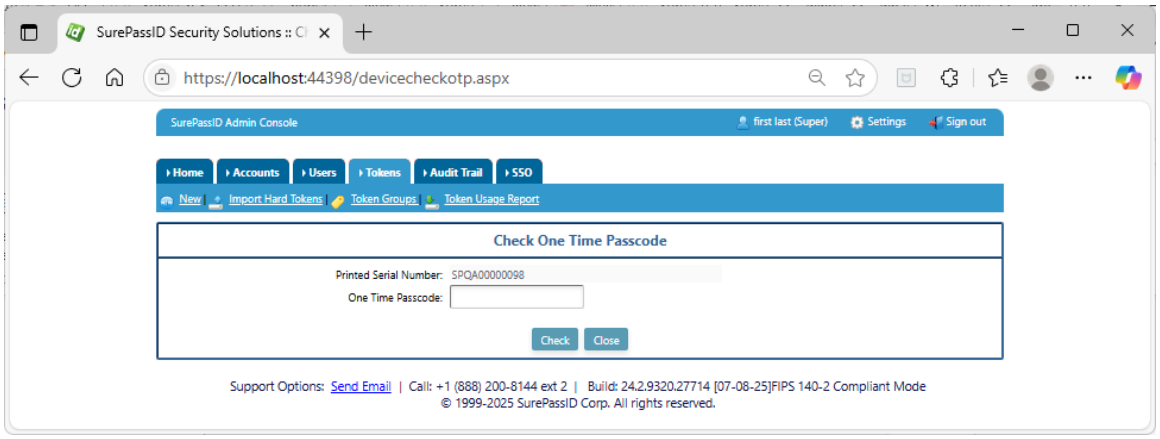


Step 5: Activate the Desktop Token

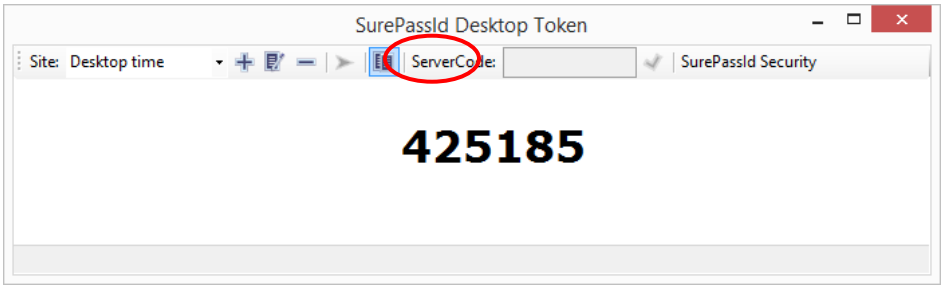
1. Log in to the SurePassID Authentication Server if you have not already logged in.
2. Select the **Tokens** tab in the SurePassID Authentication Server.
3. Find the token (by **Serial Number**) that you verify. Press the **Check** link to the left of the token as shown below.



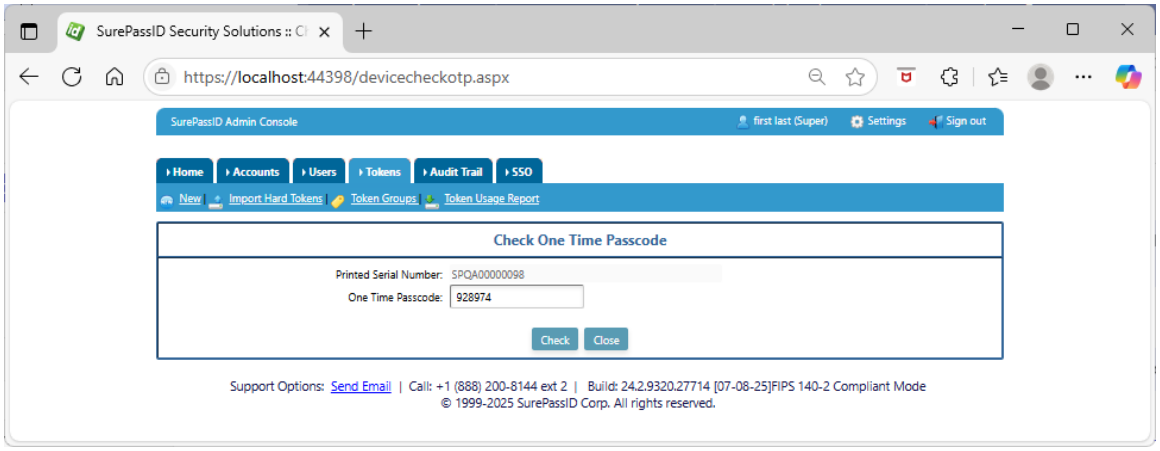
The following window will open:



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:



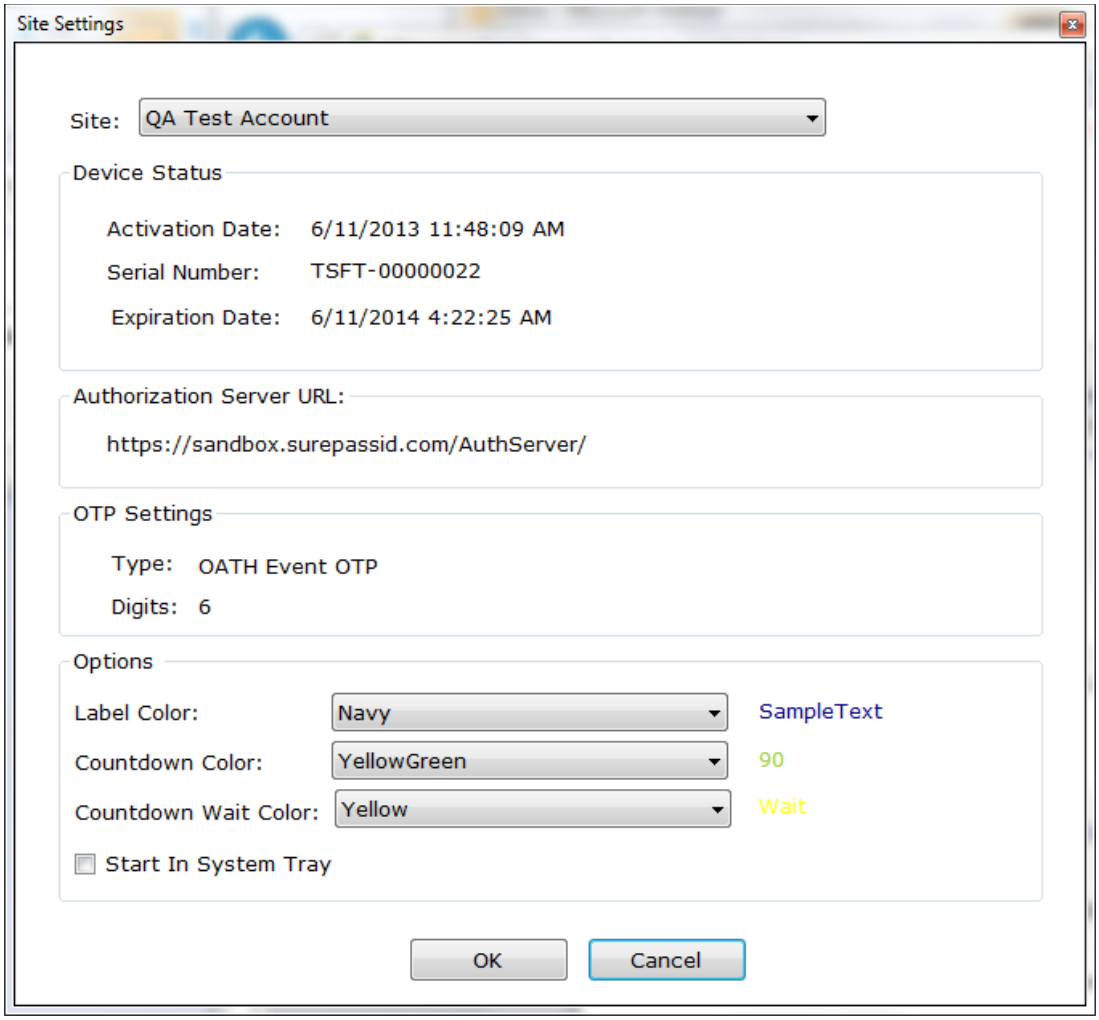
If the OTP is correct, you'll see **OTP is valid!!!** and can now use the Desktop Authenticator as a 2FA token for SurePassID. **Desktop Token is now functional!**

If the OTP is invalid, confirm that it matches the correct desktop token by checking the serial number on both the Desktop Authenticator and the SurePassID server.

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:



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.