SurePassID ADFS Multi-factor Adapter

SurePassID Authentication Server 2024

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

Table of Figures

Introduction

This guide explains how to install and configure the SurePassID Multi-factor Adapter for Windows. The purpose of this guide is to provide a reference for system administrators.

This guide provides information on the following topics:

- **What is SurePassID Multi-factor Adapter?**
    - A brief introduction to the SurePassID Multi-factor Adapter.
- **Installing and Configuring SurePassID Multi-factor Adapter**
    - Detailed explanations for installing the SurePassID Multi-factor Adapter in a Windows environment.

Other SurePassID Guides

The Server Install Guide for Windows Servers has the following companion guides that provide additional detail on specific topics for SurePassID:

- Server API Guide
- Fido U2F Mobile API Guide
- System Administration Guide
- SurePassID Desktop Authenticator Guide
- Google Authenticator Guide
- SurePassID Authenticator Guide

What is the SurePassID ADFS Multi-factor Adapter?

The SurePassID Multi-factor Adapter is an ADFS multi-factor authentication plug-in that adds Two Factor Authentication (2FA) to any application (relying party) defined to ADFS.

The SurePassID Multi-factor Adapter supports both IdP initiated logins and SP (service provider - relying party) initiated logins and with any SurePassID MFA server (cloud, on-premises) supporting all the SurePassID 2FA supported authentication methods and devices.

Send OTP Options:

- **Send SMS OTP**– Sends SMS text message containing the OTP is sent to the user's phone.
- **Send OTP by Voice Call -** Call is made to the user's phone speaking the OTP. This is an invaluable option for users that do not have SMS capabilities on their phone or users sitting at their desk or for the visually impaired.
- **Email Code** – An email containing the OTP is sent to the user's email account.

Push Authentication Options:

- **Push SMS Question** – A question is sent to the user's mobile device asking the user to confirm a request to allow access to the system. If the user responds positively, the user is allowed to login with just username and password.
- **Push Question -** A question is sent to the user's mobile device asking the user to confirm a request to allow access to the system. If the user responds positively, the user is allowed to login with just username and password. Requires SurePassID Mobile Authenticator.
- **Push OTP -** An OTP is sent to the user's mobile device. The OTP can be used as if it were an OTP from a soft token, or hard token (fob or card). Requires SurePassID Mobile Authenticator.
- **Push Voice Question -** A voice call is made to the user's phone asking the user to confirm access to the system. If the user responds positively, the user is allowed to login with just username and password. Requires SurePassID Mobile Authenticator.
- **Push Fido U2F Question -** A challenge is sent to the user's mobile device asking the user to use their Fido U2F authenticator to confirm access to the system. If the user responds positively, the user is allowed to login with just username and password. Requires SurePassID Mobile Authenticator.

Security

SurePassID ADFS Multi-factor Adapter Server requires TLS 1.2 or TLS 1.3 for transport security.

System Logging

SurePassID ADFS Multi-factor Adapter maintains it own system log files to store critical information. The system logs help you troubleshoot and repair any issues the system might encounter during daily operations.

Installing the ADFS Multi-factor Adapter

The SurePassID ADFS Multi-factor Adapter installer installs the ADFS Multi-factor Adapter components.

To install the SurePassID ADFS Adapter 2023, you must first download and unzip the installer from here:

https://downloads.surepassid.com/ADFS/ADFSA.zip
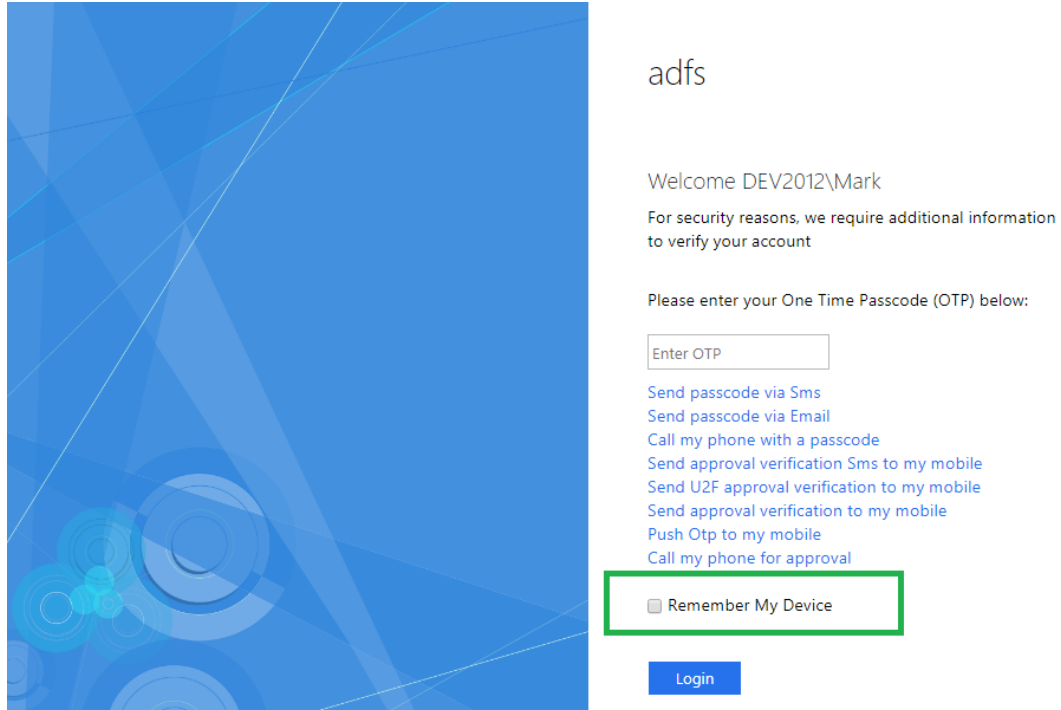
The installer and application is digitally signed by SurePassID. You must verify that as part of the installation.

After downloading the file unzip, unzip the file and run the installer file **SurePassID_ADFSAdapter2023**.

Remember My Device

You can configure the system so that users can opt in to have their device remembered for a period days in which they will not need to login with 2FA.

HINT: All messages sent to the user can be tailored to your company's needs in the SurePass portal using the Customize SMS Messages and Customize Email Messages menus.

Prerequisites

SurePassID Adfs Multi-factor Adapter can be installed on the following 64-bit Windows versions:

- Windows 2012 – All versions
- Windows 2016 – All versions
- Windows 2019 – All versions

SurePassID Adfs Multi-factor Adapter supports the following version of ADFS:

- ADFS 2.x
- ADFS 3.x
- ADFS 4.x

SurePassID Multi-factor Adapter requires a SurePassID MFA server. This can be the cloud version or on-premises version.

Post Configuration Steps

Here are a few recommended items to consider after installing the SurePassID Multi-factor Adapter.

- Configure ADFS Gateway Server Configuration

These suggestions are discussed in subsequent sections.

Installing the ADFS Multi-factor Adapter

The SurePassID Multi-factor Adapter installer will install all the Multi-factor Adapter components and prerequisites.

To install the product, you must first download the installation file https://sandbox.surepassid.com/downloads/ADFS/ADFSA.zip, unzip the file and run **SurePassID Adfs Adapter.exe** and you will see the following installation orm:
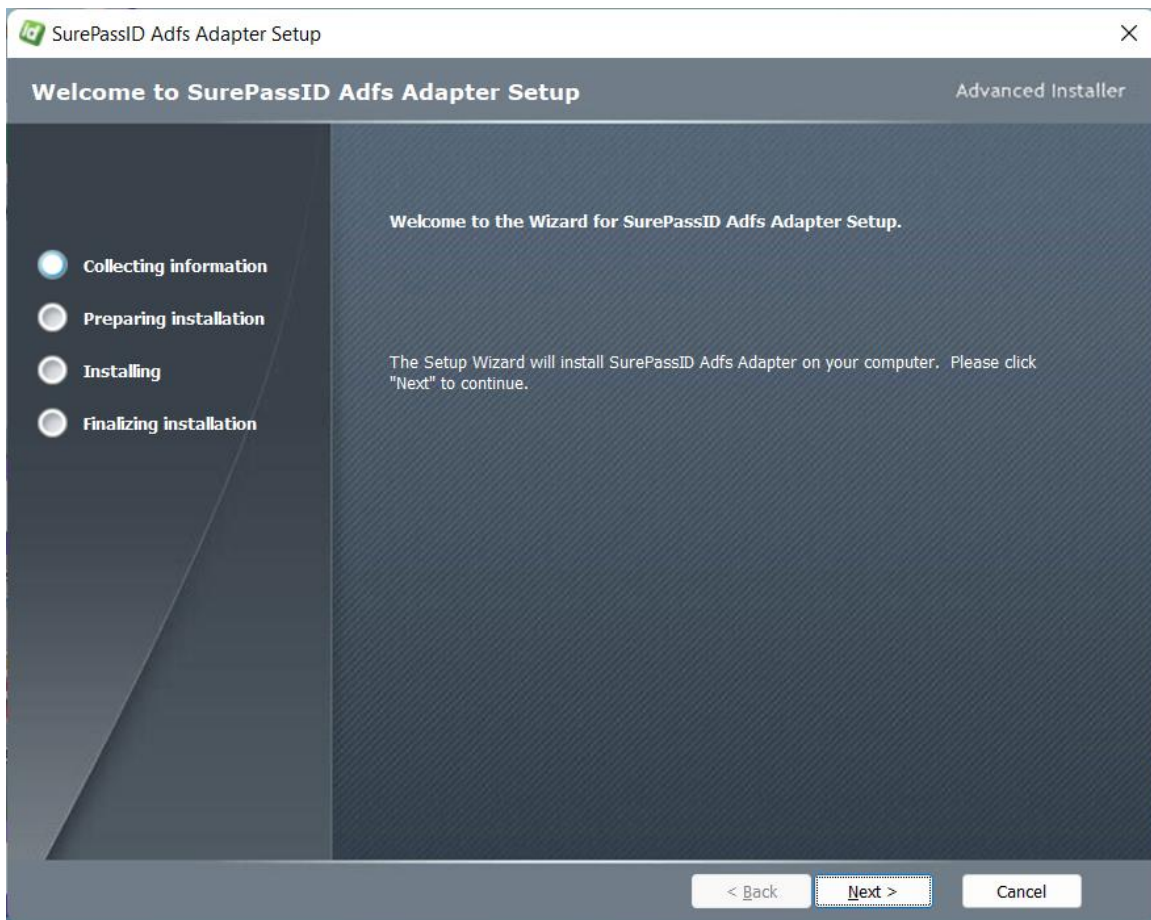
Figure 1: Installation Welcome

Click **Next** and the SurePassID Multi-factor Adapter License Agreement will be displayed.
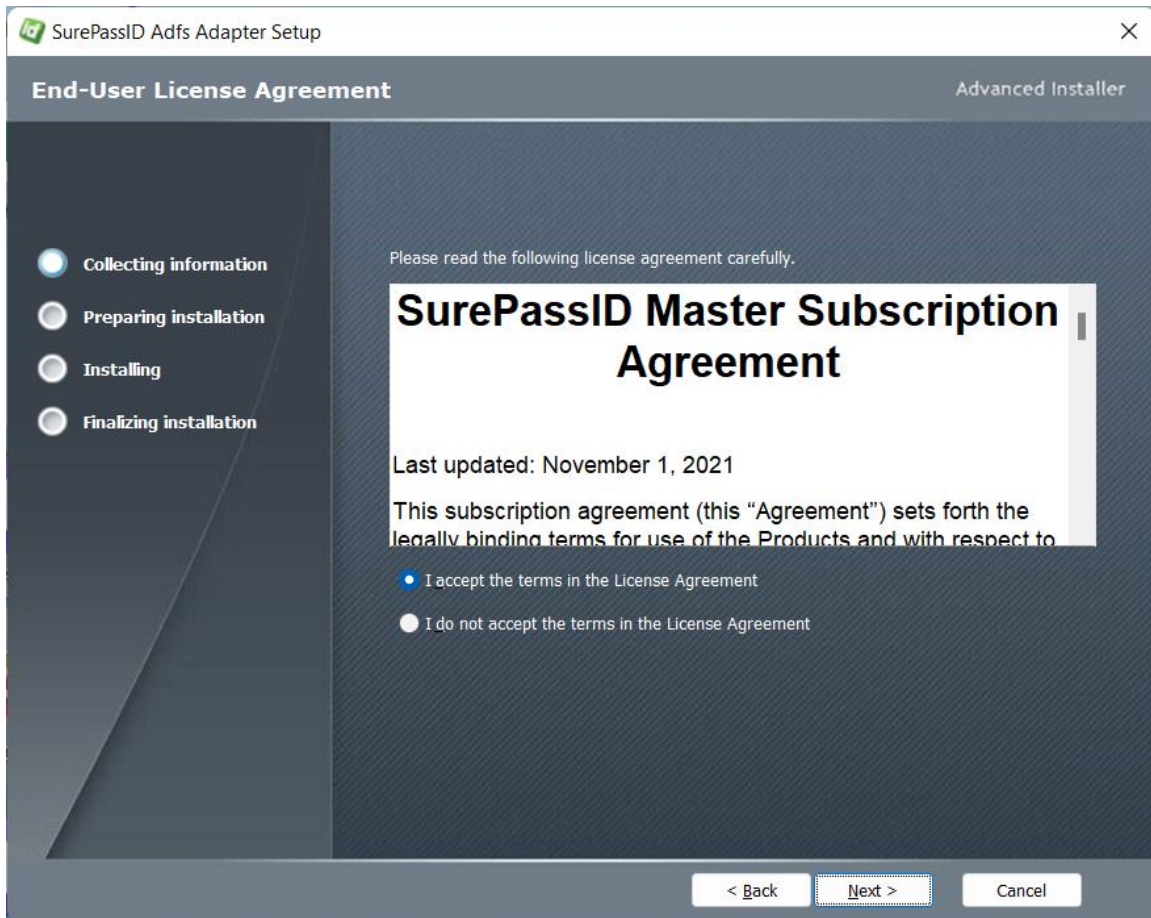
Figure 2: License Agreement

Read the License Agreement and if you agree then select the "**I accept the terms in the License Agreement**" radio button and then click the he **Next** button and you will see the installation folder form.
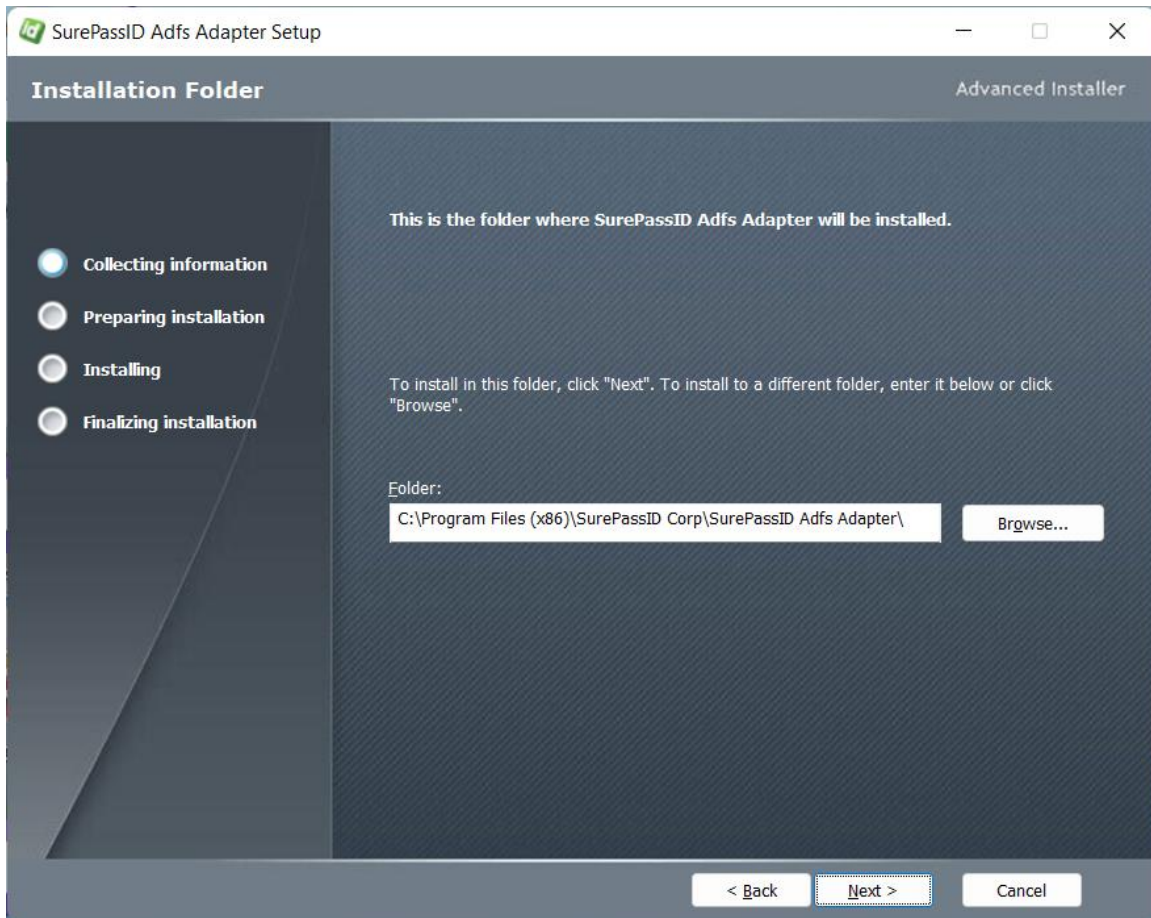
Figure 3: Installation Location: Specify Installation Folder

Browse to the product installation folder or leave the default installation folder. When done press the **Next** button and you will see the **Ready To Install** form.
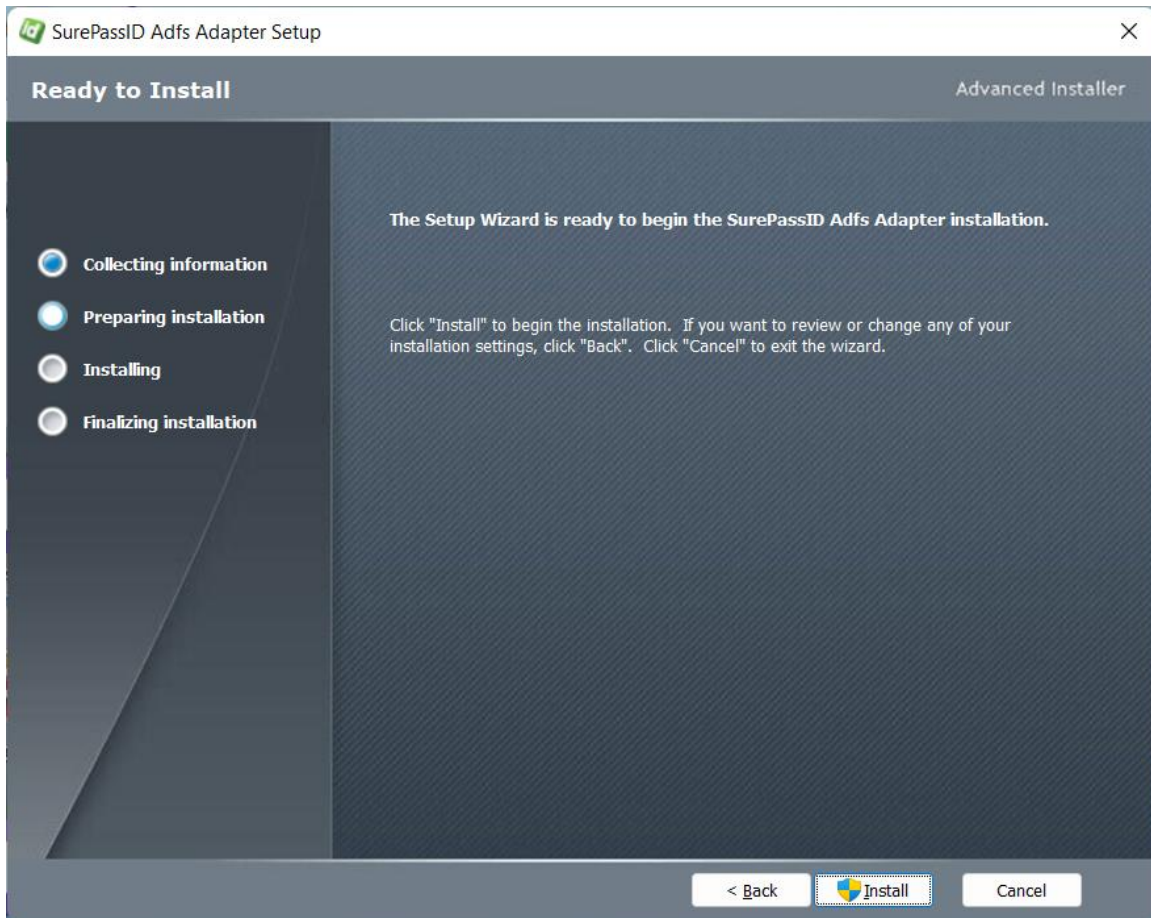
Figure 4: Ready To Install:

Click the **Install** button to start the installation process. You will first be presented with signed SurePassID verified publisher statement.
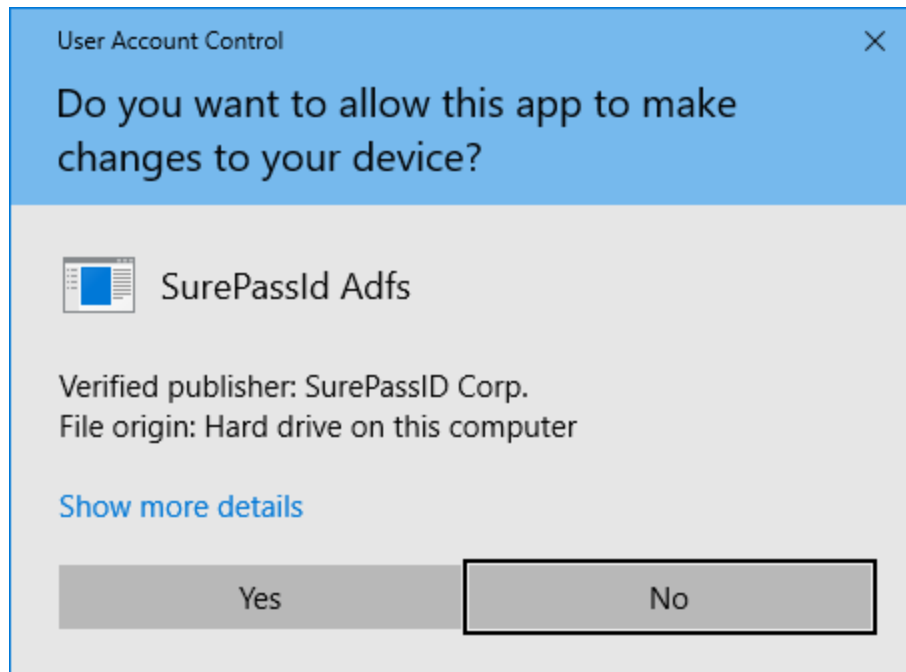
Figure 5: Installation App: Verify Publisher

If you do not see the **Verified Publisher: SurePassID Corp.** click **No** to cancel install. If you do see it, click **Yes** to install the product.
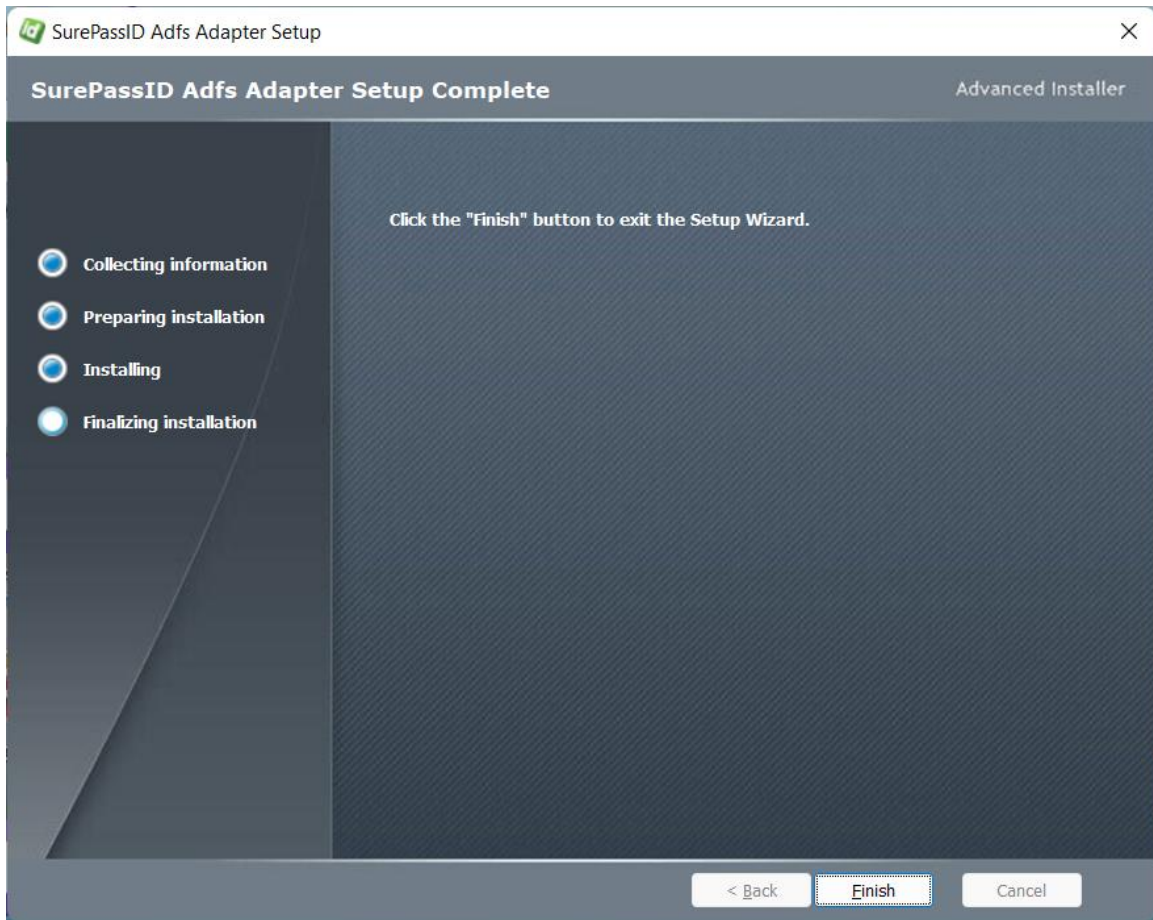
Figure 6: Complete Installation

Installation is complete. Click the **Finish** button. You are now ready to configure the system.

Configuration Settings

The SurePassID Multi-factor Adapter configuration settings are stored in the **SurePassIdAdfsAdapterconfig.txt** file located in the SurePassID Multi-factor Adapter installation folder. By default, this:

 C:\Program Files (x86)\SurePassId Corp\ SurePassID ADFS Adapter 2023/

The format of this file is the same format as the settings file for the Windows Credential Provider and other SurePassID plug-ins. The default settings file SurePassIdAdfsAdapterconfig.txt is discussed below:

Step1: Configure SurePassID ADFS Adapter Settings

All the configuration settings for the system are in ADFS.conf file located in the folder where the product is installed. The default product installation folder is: C:\Program Files (x86)\SurePassID Corp\SurePassID ADFS Gateway 2019.

Note: When you make changes to the SurePassIdAdfsAdapterconfig.txt file, the settings will not take effect until the remove and install powershell scripts have been rerun. See Step2 below.

The format of the file is one option per line, each option is a combination of an option name and value separated by an equal (=) sign. Option names are described in the following sections.

Operations and Setup

- **AuthenticationMode –** The multi-factor adapter can operate in Primary Authentication mode (PA) or Secondary Factor Only mode (SFO).
   - In PA mode the multi-factor adapter will perform both first factor authentication (using SurePassID directory) and second factor.
    - SFO mode only performs the second factor authentication after Active Directory perform the users first factor (username, password) authentication.

    AD FS Configuration Manager allows you to set ADFS to allow external authentication (e.g. multi-factor adapter) as primary or second factor.

    - If you configure ADFS to use SurePassID as the primary authentication then set this value to **p**.
    - If you configure ADFS to use SurePassID as second factor authentication then set this value to **s.**

The default is s (second factor).
NOTE: Only ADFS 4.0 and later support primary authentication.

- **AuthServerURL** – The SurePassID authentication endpoint URL. In most cases, you will not need to change this unless you are using a custom SurePassID installation. The values are:
    - **sandbox** - The SurePassID sandbox system.
    - **prod** – The SurePassID production cloud system.
    - **SurePassID MFA System** (Full Name)- On-premises or custom install of the SurePassID MFA server. The format of this parameter is usually:

https://<surepassid_server>/AuthServer/REST/OATH/OATHServer.aspx

    - **SurePassID MFA System** (Short Name)- On-premises or custom install of the SurePassID MFA server. The format of this parameter is usually:

https://<surepassid_server>/

- **AuthServerToken** - The login name (**Server Login Name**) for your SurePassID account.

- **AuthServerKey** - The login password (**Server Login Password**) for your SurePassID account.

    The **AuthServerToken** (**Server Login Name**) and **AuthServerKey** (**Server Login Password**) can be retrieved from your SurePassID account as shown below. To view the password, click the 'lock' icon to toggle the display of the password:

Figure 7: SurePassID Account Settings

- **LogLevel** - Turn on local logging for the system. This setting is used to debug issues with the system. Unless required, logging should be turned off. By the default log files are created in the c:\windows\temp folder. The default log path can be changed by setting the **LogFilePath** to the desired location. Values for **LogLevel** are:
    - o 0=no logging
    - o 1=logging is on
    - o 2=advanced (REST API logging – trouble shooting only)

- **LogFilePath** – The path where log files will be written to. This path must exist. If not specified, the default path is c:\windows\temp. By default the system does not log events to the Windows Event Log. If you want the logs sent to the Windows Even Log run the following Powershell command:
    New EventLog -LogName SurePass – SourceName ADFSAdapter

- **SecureCookieName** – The name of the cookie that will be used to store state information about the Remember My Device session. The default value is SP_CookieMonster_.

- mailto:**DoNotShowCookieName** – The name of the cookie that will be used to store information about the Remember My Device session state information.The default value is SP_DNSCookie.
- **SurePassUseUpn** – By default SurePassID sends the user account name without domain information to the SurePassID MFA server when performing user authentication.   Setting this parameter changes the default behavior and SurePassID multi-factor Adapter sends the entire user User-Principal-Name (UPN) to the MFA Server server. A UPN consists of a UPN prefix (the user account name) and a UPN suffix (a DNS domain name). This means the user name in SurePassID MFA server will need to be the UPN and not just the username.
- **SessionDays** – This parameter turns on and configures the Remember My Device option. If you set this parameter to 0 or do not provide it then the Remember My Device option is not available to the user. A non-zero value represents the number of days a user's access will not require multi-factor authentication for login. The user turns on this feature by checking the Remember My Device option when in the option is presented. For example, if you set SessionDays=10 and the user checks the Remember My Device the user will not need to use multi-factor authentication for the following 10 days after they login with multi-factor authentication. This feature if for convenience in low risk situations only.
- **DoNotShowDays** – The number of days that the Remember My Device option will not be shown. This value cannot be less than Session days. The default value is SessionDays.
- **WaitForPushResponse** – All push requests will wait for the user to authenticate on their mobile or until the request times out. 0=no 1=yes. Default is 1.
- **GenericErrorText** – The html text that will be displayed to the user when an error is received from the SurePassID MFA server. If this setting is not specified the message displayed to the user is the message received from the SurePassID MFA server. The original error from the server is always written to the trace log if tracing is turned on (**LogLevel= 1 | 2**).

Security Settings

- **AllowSMS** - Allow the user to request an OTP be sent by SMS to their mobile device. 0=no 1=yes.
- **AllowEmail** - Allow the user to request an OTP be sent to their email. 0=no 1=yes.
- **AllowCall** - Allow the user to request an OTP be sent by voice call. 0=no 1=yes.
- **AllowPushApp** - Allow the user to request that a push authentication be sent (pushed) to their mobile device to confirm their identity. Requires the

user to have SurePassID Mobile Authenticator installed on their mobile device. 0=no 1=yes.

- **AllowPushSMS** - Allow the user to request that an SMS push question can be sent to their mobile device to confirm their identity. 0=no 1=yes
- **AllowPushVoice** - Allow users to request a voice call that will allow them to confirm their identity. 0=no 1=yes.
- **SurePassUseVerifyMethod**– By default the SurePassID admins sets user allowable authentication methods in the config file as defined by the Allow settings (e.g. AllowSMS) in the config file. This setting can dynamically adjust the user's allowable authentication methods. This is an advanced function and requires additional server side set-up and may not be available on your platform. 0=no 1=yes.
- **PushAppName** - For push authentications, the name of the application requesting access. The PushAppName is displayed to the user when they receive a push notification. The default is ADFS. Users should not accept push requests from unknown app names or requests that were not initiated by them.
- **PushAuthnReason** – For push authentications, the reason why the application is requesting access that is displayed to the user on their mobile. The default is Login. Users should not accept push requests for known reasons.
- **RelyingPartyUrl** - For push authentications, the url of the application requesting access. This is the endpoint that will accept push responses from the user's mobile device. This can be complex depending on your configuration. You should not specify this parameter unless instructed by SurePassID technical support.

User Interface Settings

- **PasswordText** – The textbox helper text for the user to enter their password
- **PasscodeText** - – The textbox helper text for the user to enter their passcode (OTP).
- **RMD_DNSText** – The html text that will be present at the bottom the multi-factor authentication form. The default value is
  Please select an option and press the Done button
- **RMD_DNSButtonText** – The html text that will be present at the bottom the multi-factor authentication form. The default value is Done.
- **RemeberMyDeviceText** – The html text that will be present at the bottom the multi-factor authentication form. The default value is Remember My Device
- **DoNotShowAgainText** – The html text for the Do Not Show This Again checkbox that relates to the RememberMyDevice option.
  The default value is Do Not Show This Again.
- **SupportText** – The html text that will be present at the bottom the multi-factor authentication form. The default is
  Support Email: helpdesk@surepassid.com

- **NoValidAuthenticationMethods** – The html text that will be displayed to the user if they have no multi-factor authentication methods assigned to them. Default is:
  No authentication methods available for your account. Contact your administrator.

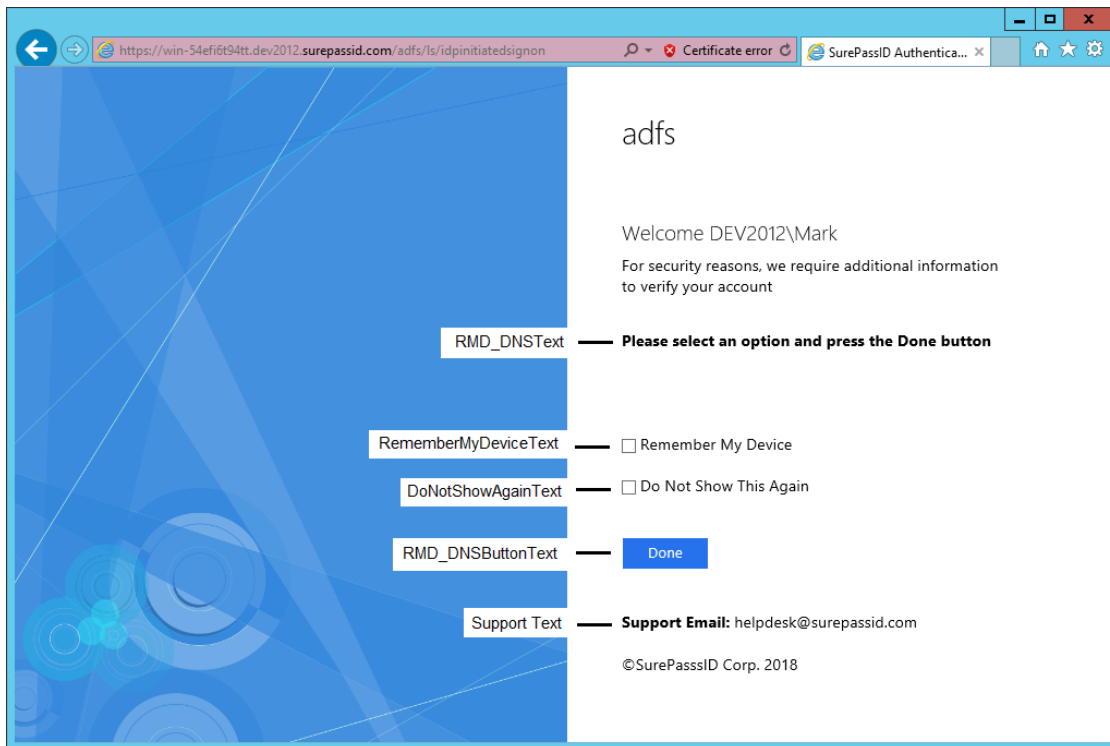The following figure shows the locations of each of these user interface settings on the form.

Figure 8: Remember My Device Form

Configure ADFS For Second Factor Only

Follow these steps to add SurePassID MFA as a strong authentication provider for ADFS.

Open the ADFS Management Console select **Authentication Policies** in the left pane to see settings in the right pane.
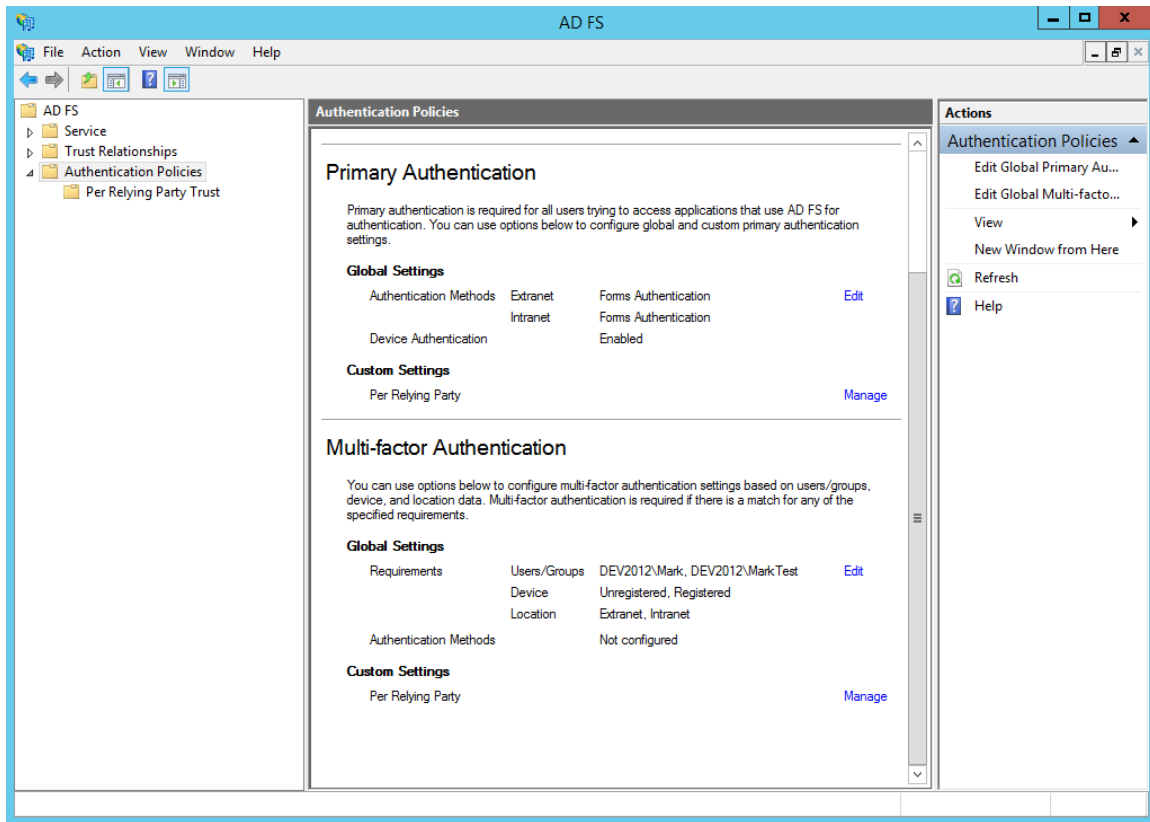
Figure 9: ADFS Authentication Policies

The **Authentication Policies** setting defines how ADFS will handle primary authentication (first factor) which is usually user name and password as well as multi-factor authentication configured in each of their respective sections.

Clicking the **Edit** button to the right of **Global Settings** in the Multi-factor Authentication section allows you to set any number of multi-factor authentication providers at the global level for all relying party apps such as Outlook Web Access, Office 365, SharePoint, etc. that will use these authentication settings.

Clicking **Manage** to the right **Custom Settings** can let you set the multi-factor authentication options on a relying party by relying party basis.   When clicking the **Edit** button, you will see the following form.
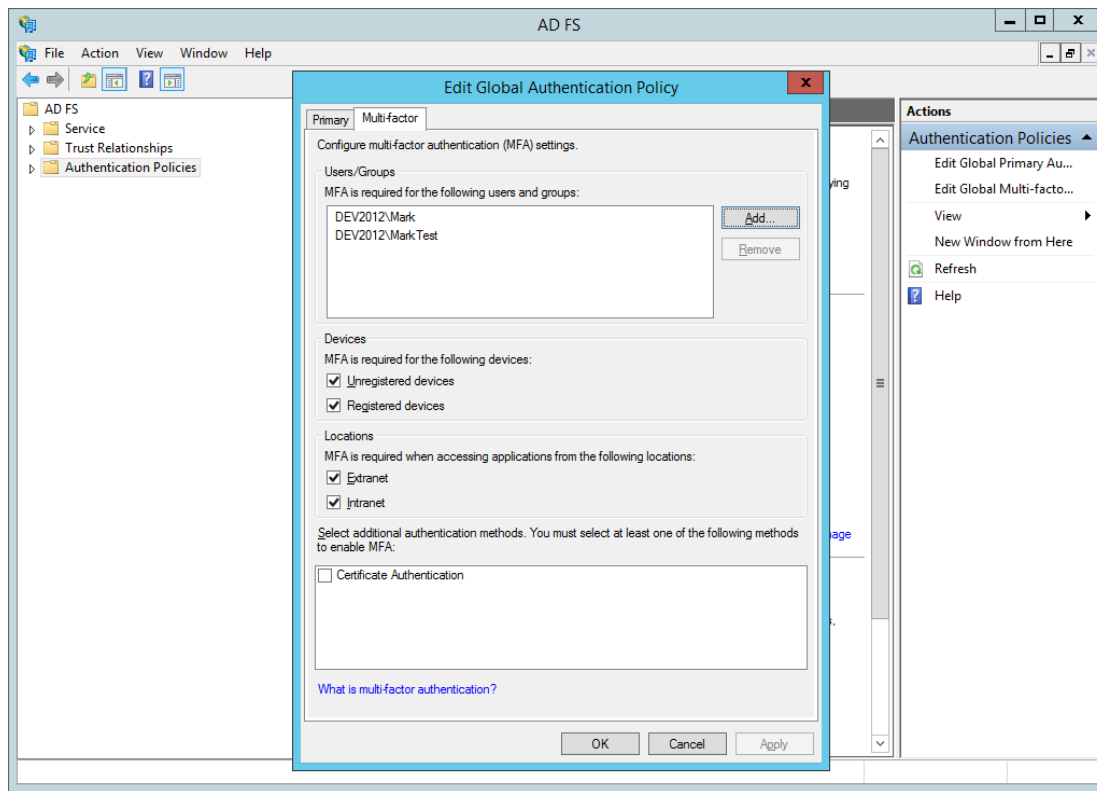
Figure 10: ADFS Multi-factor Adapters

As you can see the only multi-factor authentication option is Certificate Authentication.

To add SurePassID as the multi-factor authentication option, follow these steps:

Start your favorite version of PowerShell as an Admin and open the **install.ps1** located in the *scripts* folder of the SurePassID ADFS installation folder.

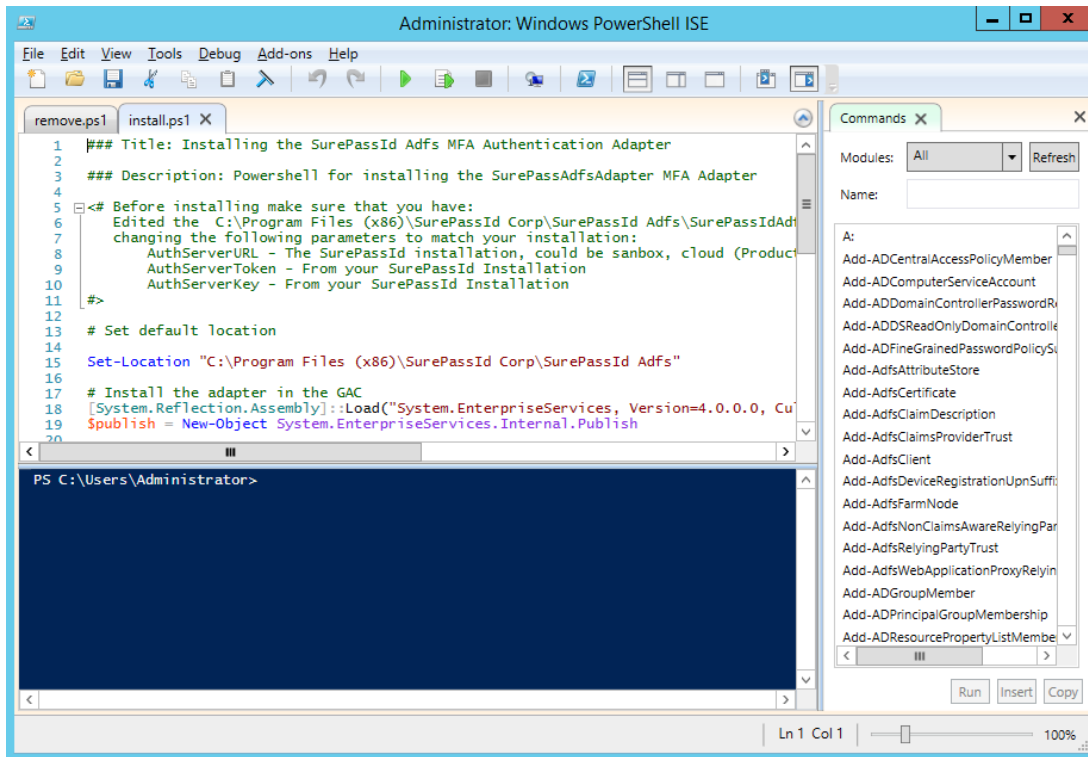**C:\Program Files (x86)\SurePassId Corp\SurePassId Adfs\scripts**

As shown below.

Figure 11: PowerShell Installation Script

Click the green run button on the top of the toolbar and you will see the following screen showing that the adapter is configured as is highlighted in a green box.
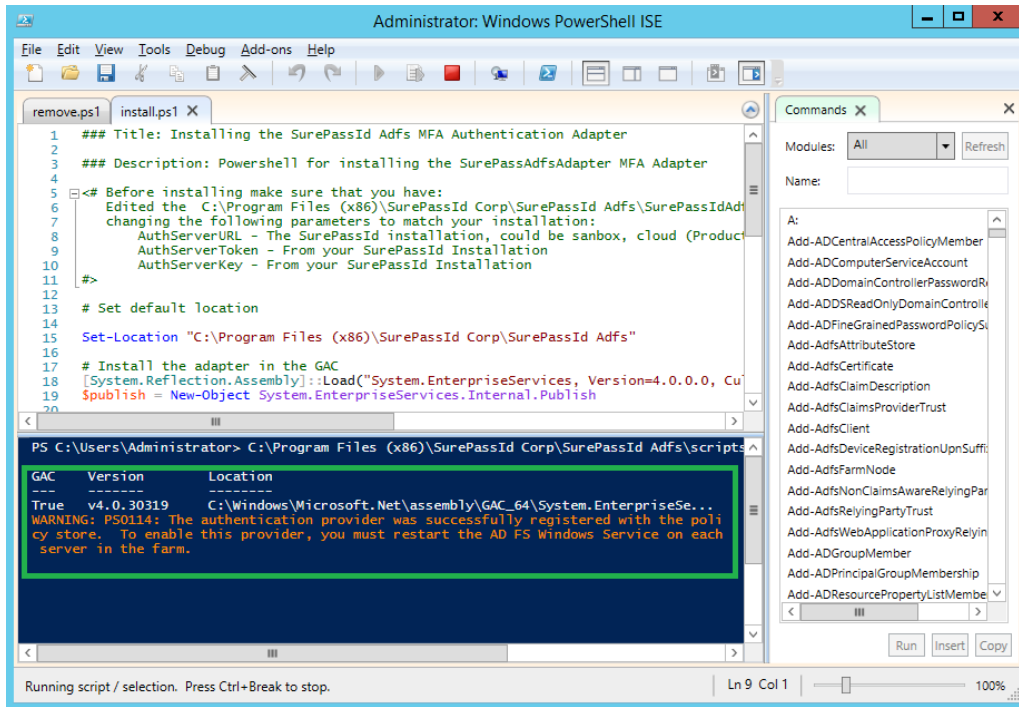
Figure 12: PowerShell Installation Script Success

After running the script, selecting **Authentication Policies** and clicking on the **Edit** button to the right of **Global Settings,** the SurePassID MFA Adapter is installed and ready to be turned on by clicking the checkbox as shown below.
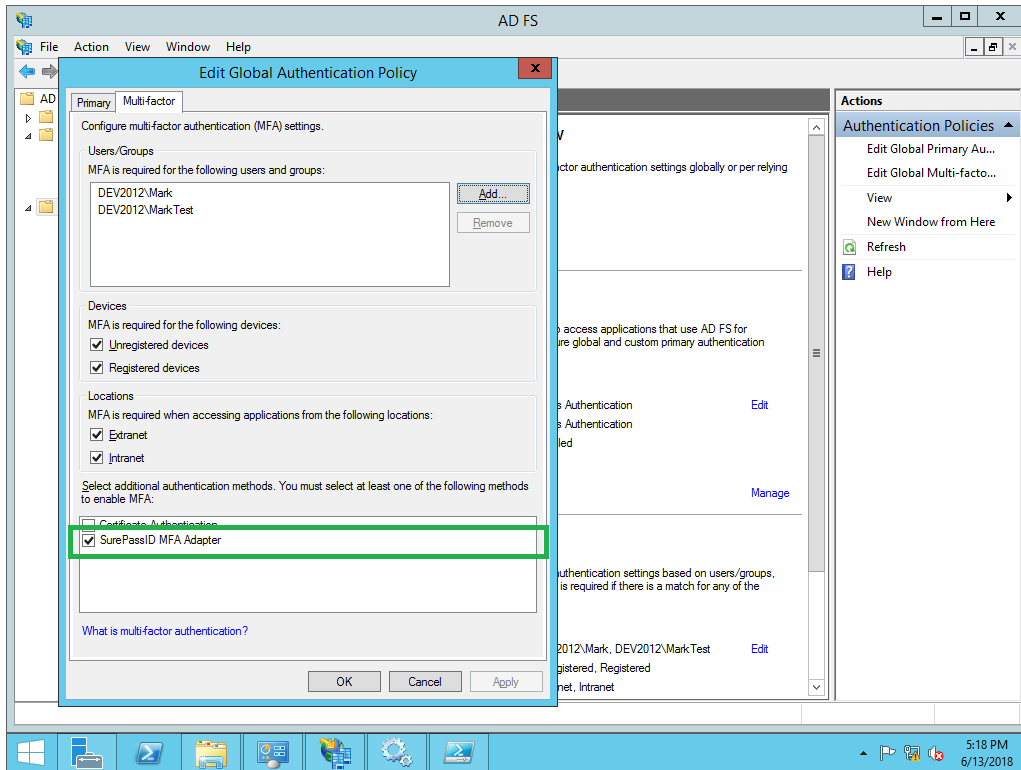
Figure 13: SurePassID Multi-factor Adapter Confirmation

NOTE: When you install the SurePassID MFA Adapter, the configuration settings in SurePassIdAdfsAdapterconfig.txt are read by ADFS and stored in the ADFS repository.   If you modify them, they will not take effect until the SurePassID MFA Adapter is removed (run the remove.ps1 script) and then re-installed (run the install1.ps script).

Configure ADFS For Primary Authentication

Configure ADFS Applications (Relying Parties)

This document does not delve into the setting up of relying party apps as there are too many option settings and they change frequently. You will need to consult the Microsoft ADFS documentation. We will gladly assist if you contact our support team.

Step 4: Using MFA Adapter For Multi-factor Authentication

After you have turned on SurePassID Multi-factor Adapter for an app (relying party) or globally for all relying parties, you can login to the system using multi-factor authentication.

This example will show you how to use the IdP initiated method however, the SP (Service Provider) initiated method will be nearly identical.

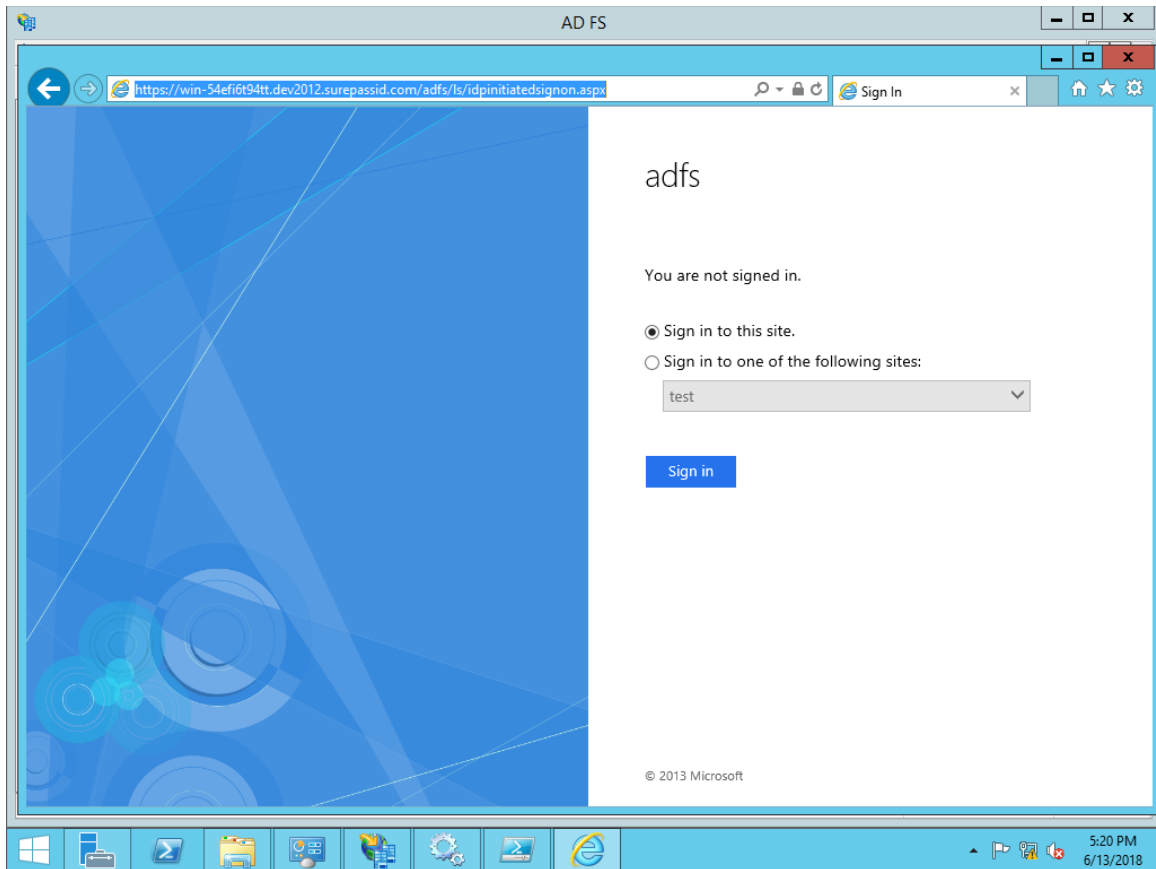Open the IdP initiated ADFS login page as show below.

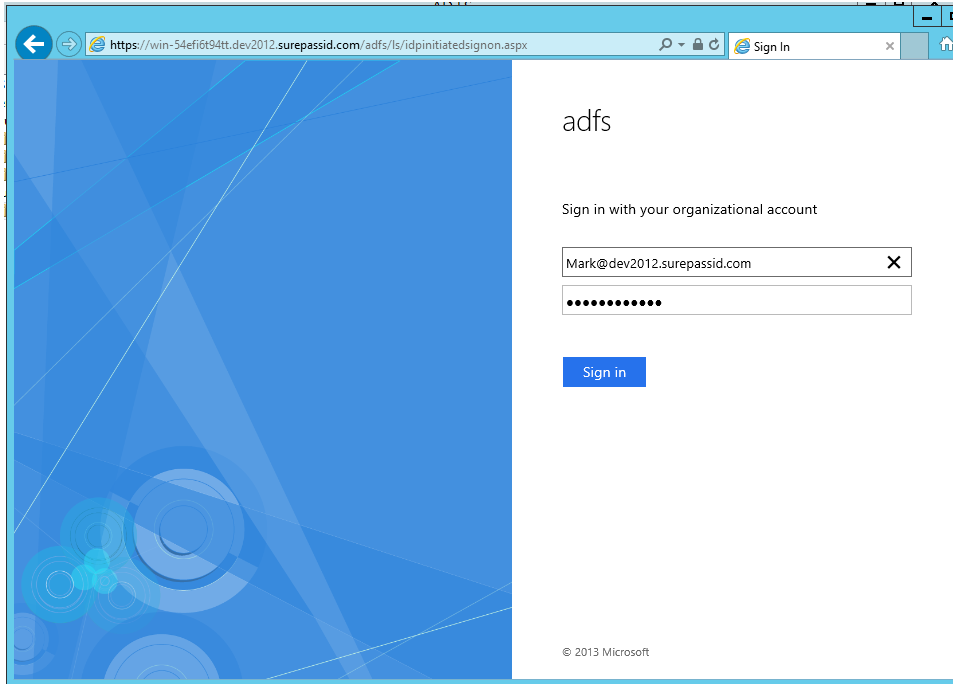**Figure 14: IdP Initiated Login**

Click the **Sign in** button.

Figure 15: IdP Initiated Login – AD Credentials

Enter your Active Directory credentials and click the **Sign in** button. If they are correct you will see the following:
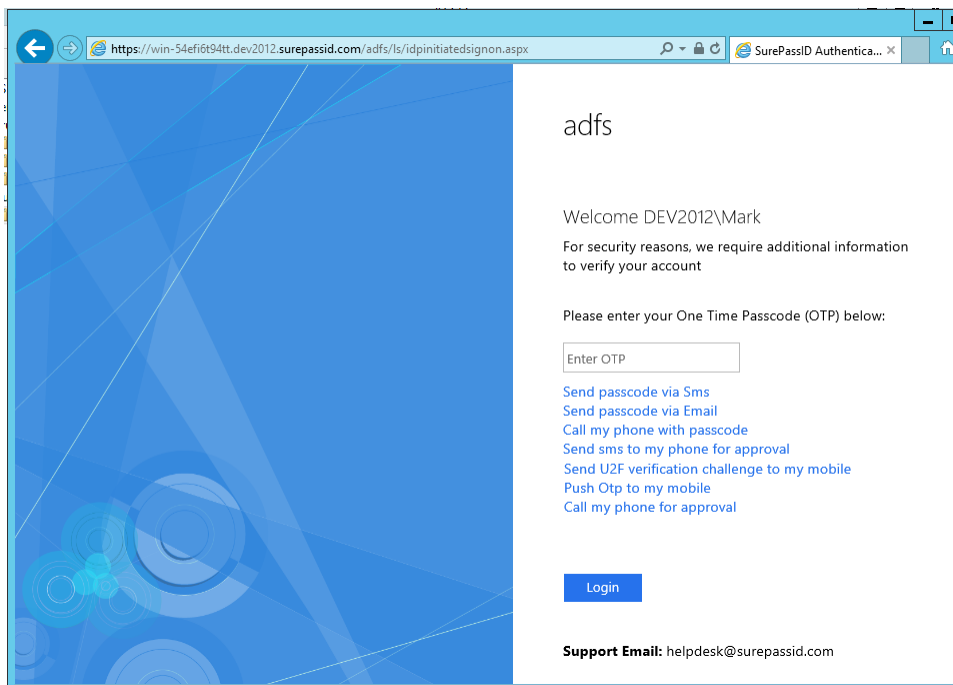
Figure 16: IdP Initiated Login – SurePassID Authentication Options

If the system administrator as reset the users Password/PIN account the user will see the following options to reset their Password/PIN:

You can enter your OTP from a hard or soft token or select an alternative method from the links below. For example, if **Send passcode via Sms was selected,** the following will be displayed.
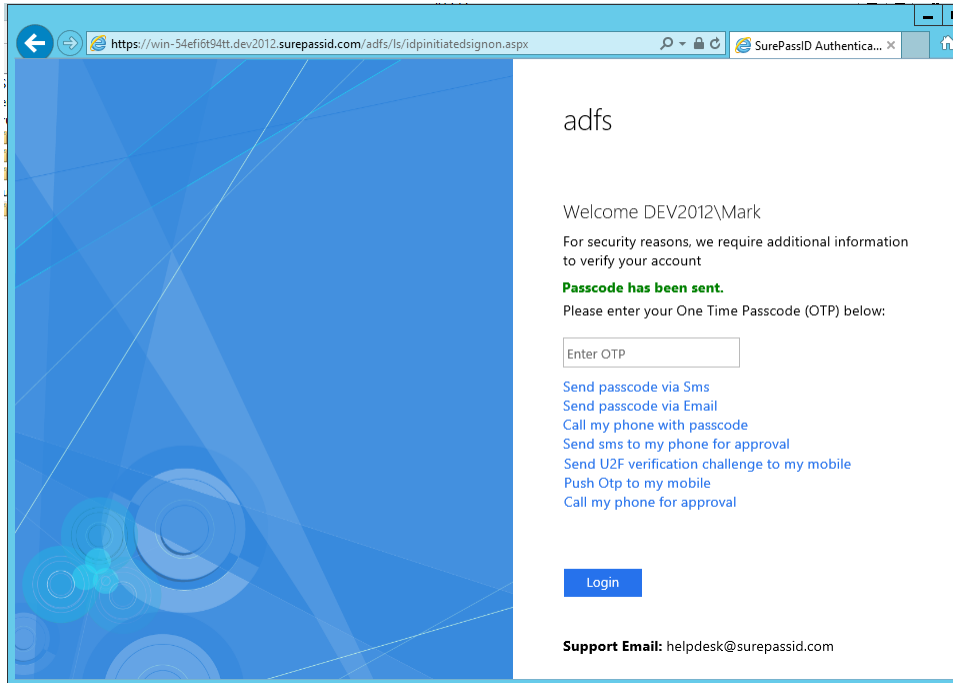
Figure 17: IdP Initiated Login – SurePassID Passcode Sent

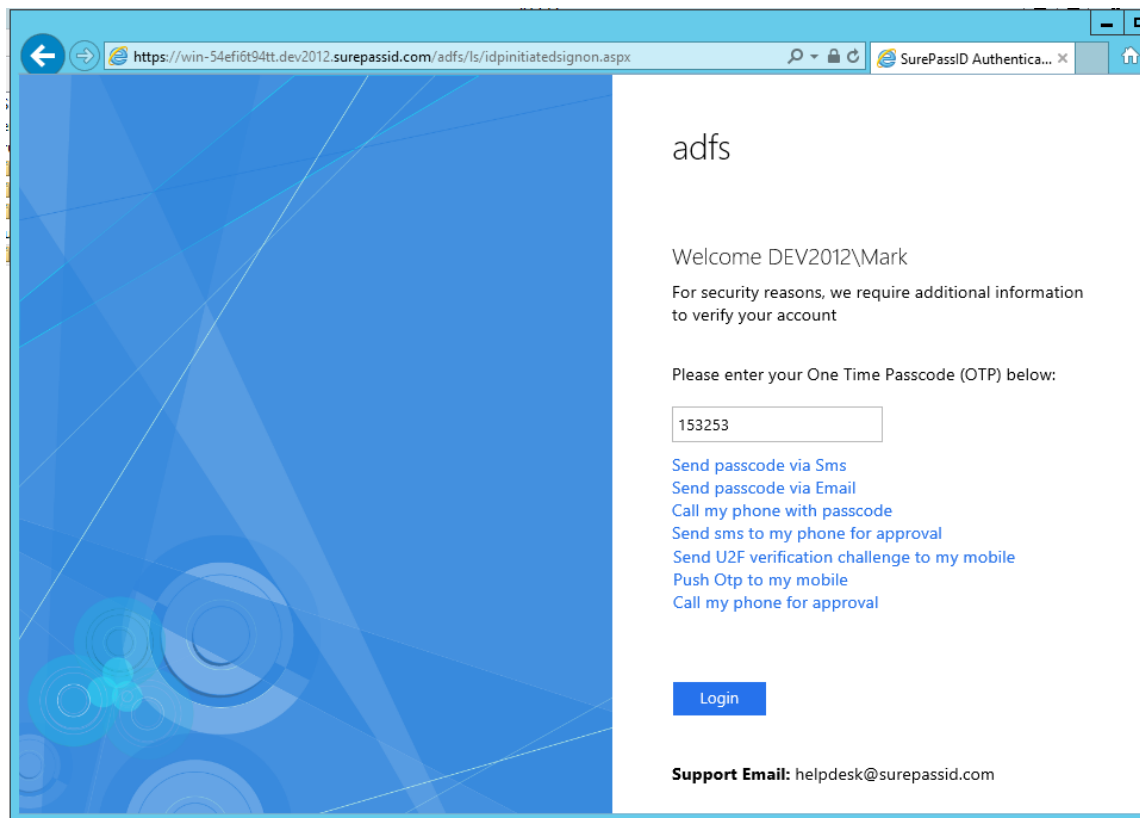The page is updated to show the Passcode has been sent.

Figure 18: IdP Initiated Login – SurePassID OTP Verification

Enter the passcode and click the **Login** button. If the passcode entered is correct, you will see the following:
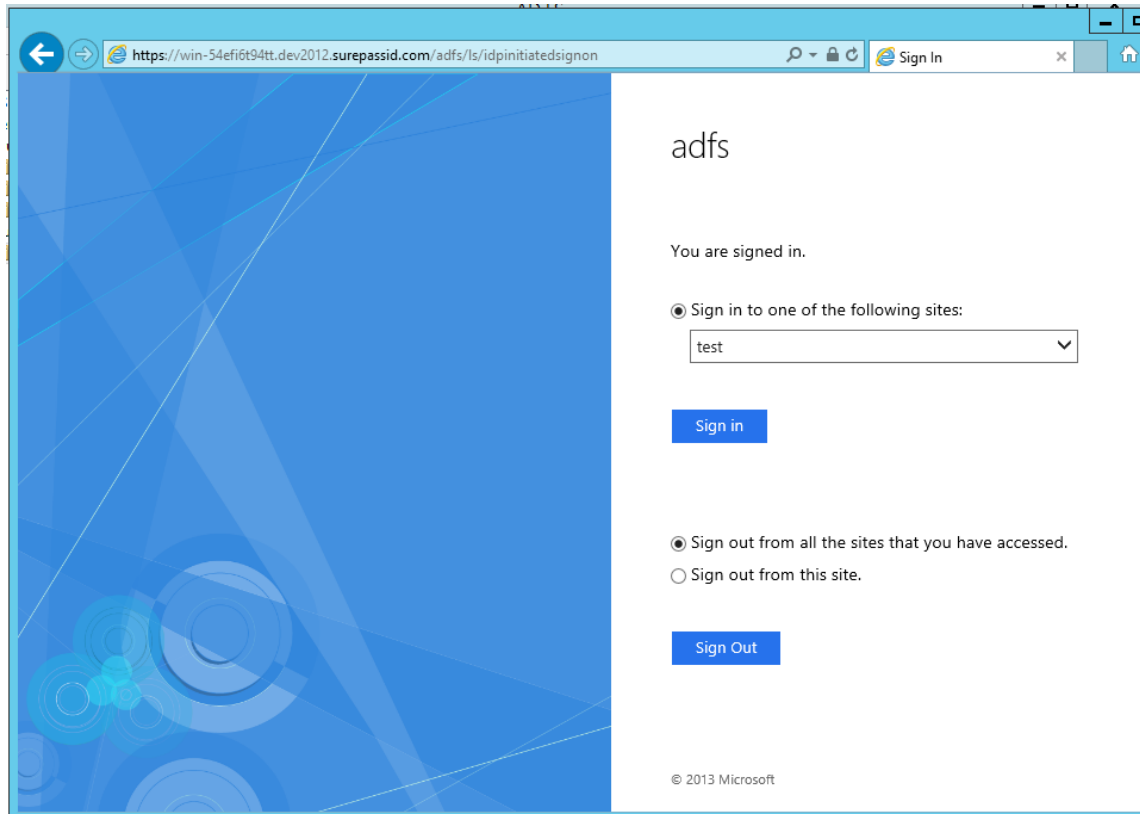
Figure 19: IdP Initiated Login – AFDS Login Success

You are signed in. You can now access any ADFS apps without re-entering any credentials.

Step5: Using MFA Adapter For Primary Multi-factor Authentication

After you have turned on SurePassID Multi-factor Adapter for an app (relying party) or globally for all relying parties, you can login to the system using primary multi-factor authentication. Primary multi0fator authentication allows SurePassID to authenticate both first factor (usename, password) and second factor.

This example will show you how to use the IdP initiated method however, the ADFS Service Provider (SP) initiated method will be nearly identical.

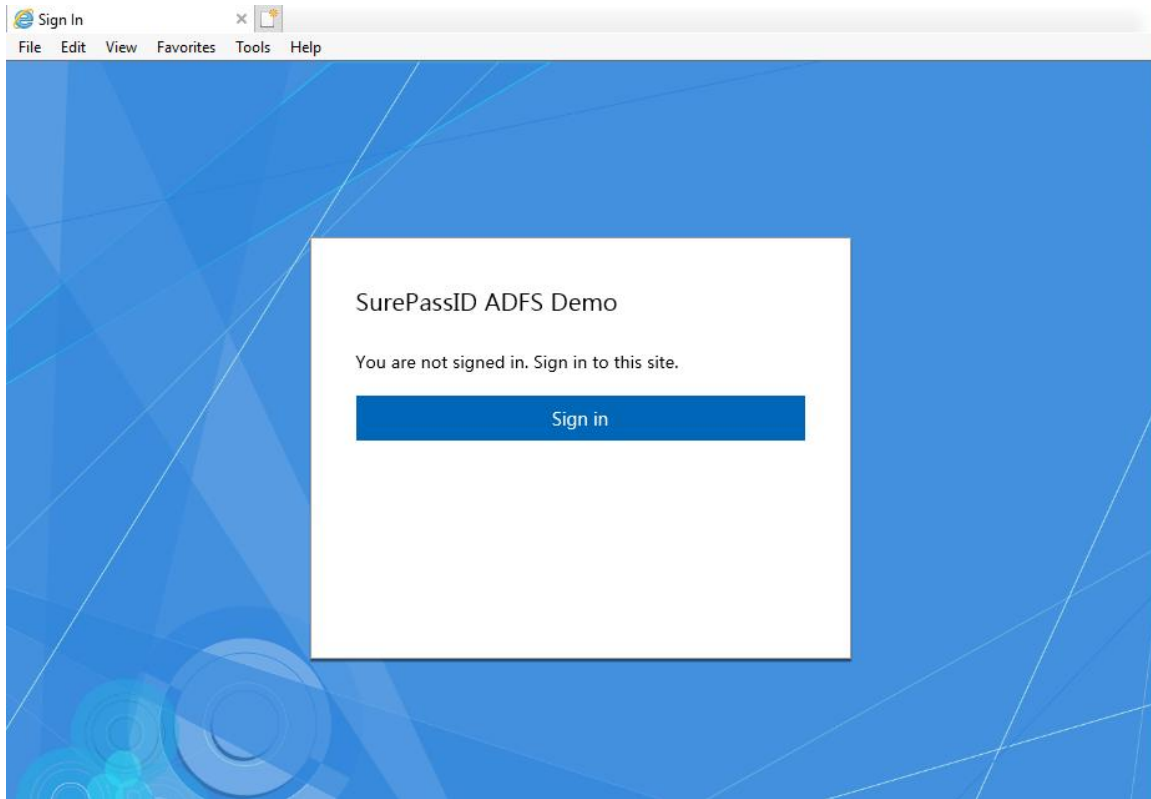Open the IdP initiated ADFS login page as show below.

Figure 20: IdP Initiated Login - Primary Authentication
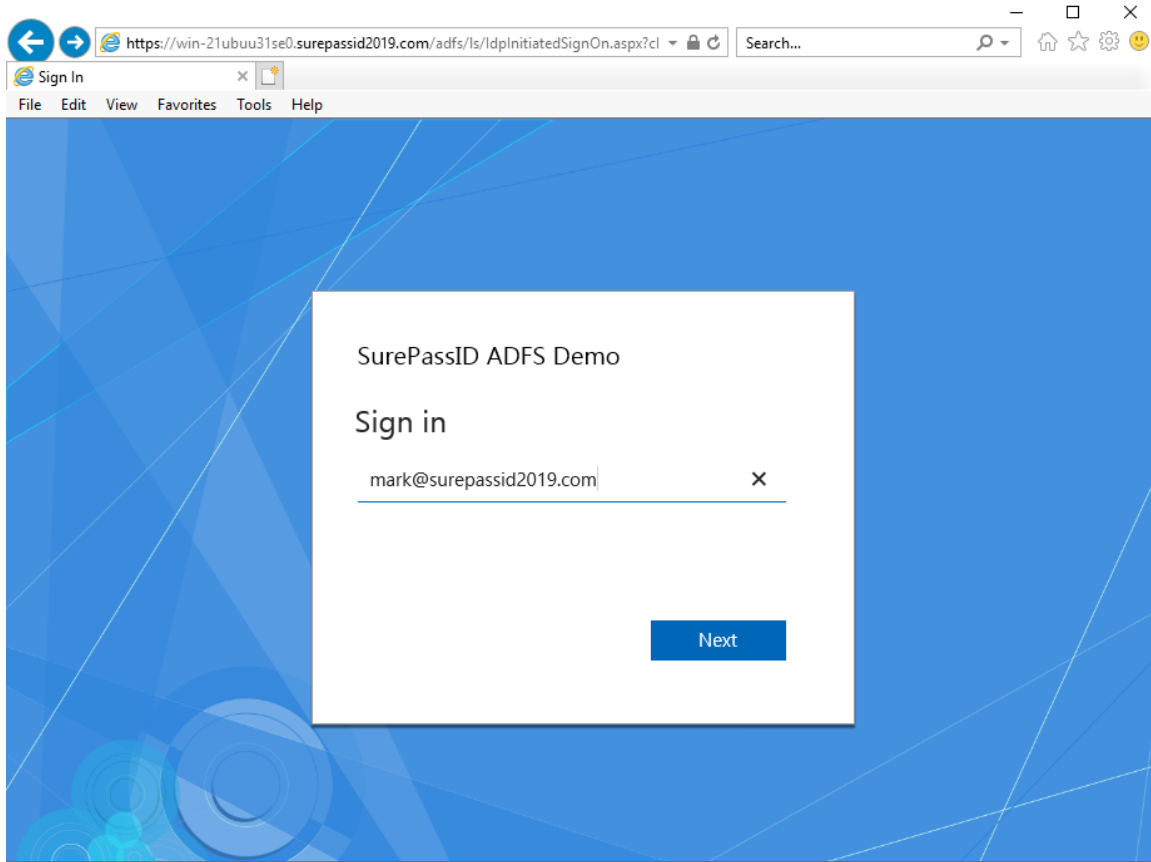
Click the **Sign in** button.

Figure 21: IdP Initiated Login – Primary Authentication – Enter AD Username

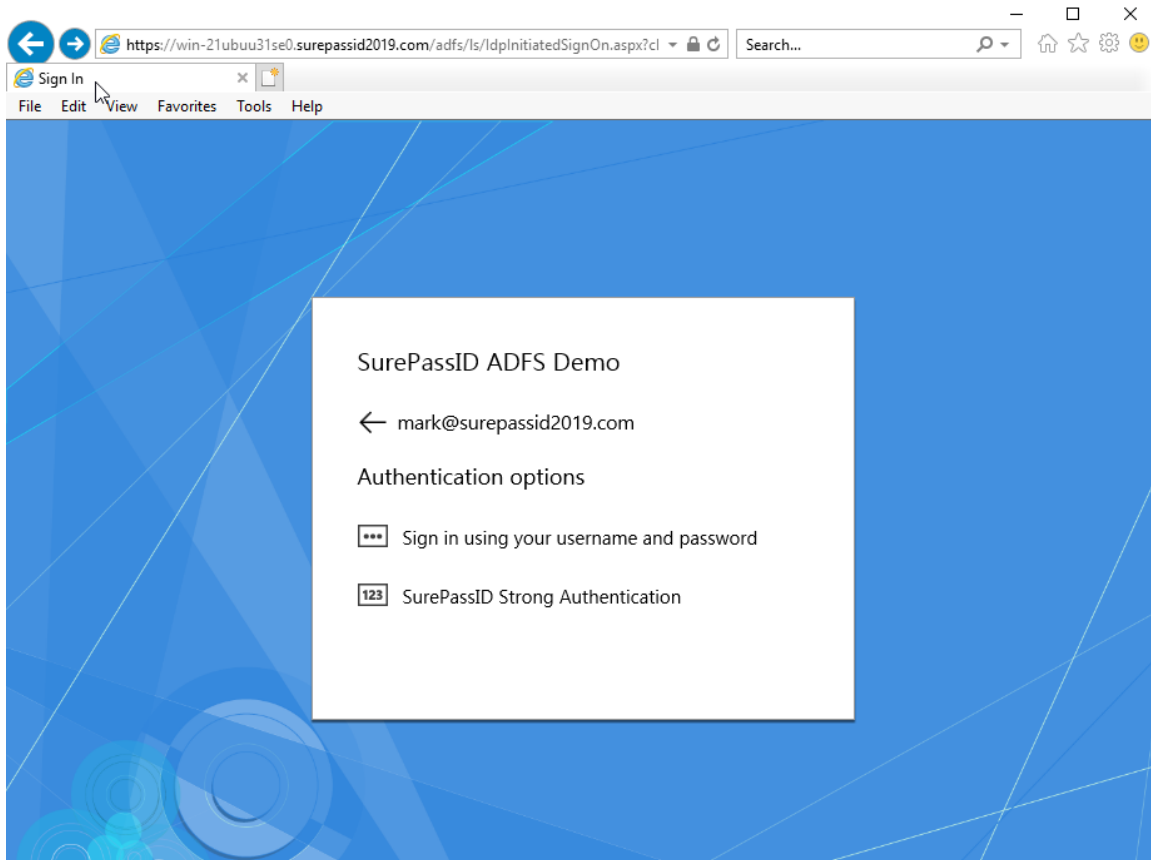Enter your Active Directory username and press the **Next** Button.

Figure 22: IdP Initiated Login – Primary Authentication – Select Primary Method

You will see this option if ADFS is configured to allow more than one primary authentication method. If SurePassID authentication is the only primary authentication option configured then you will not see the form.
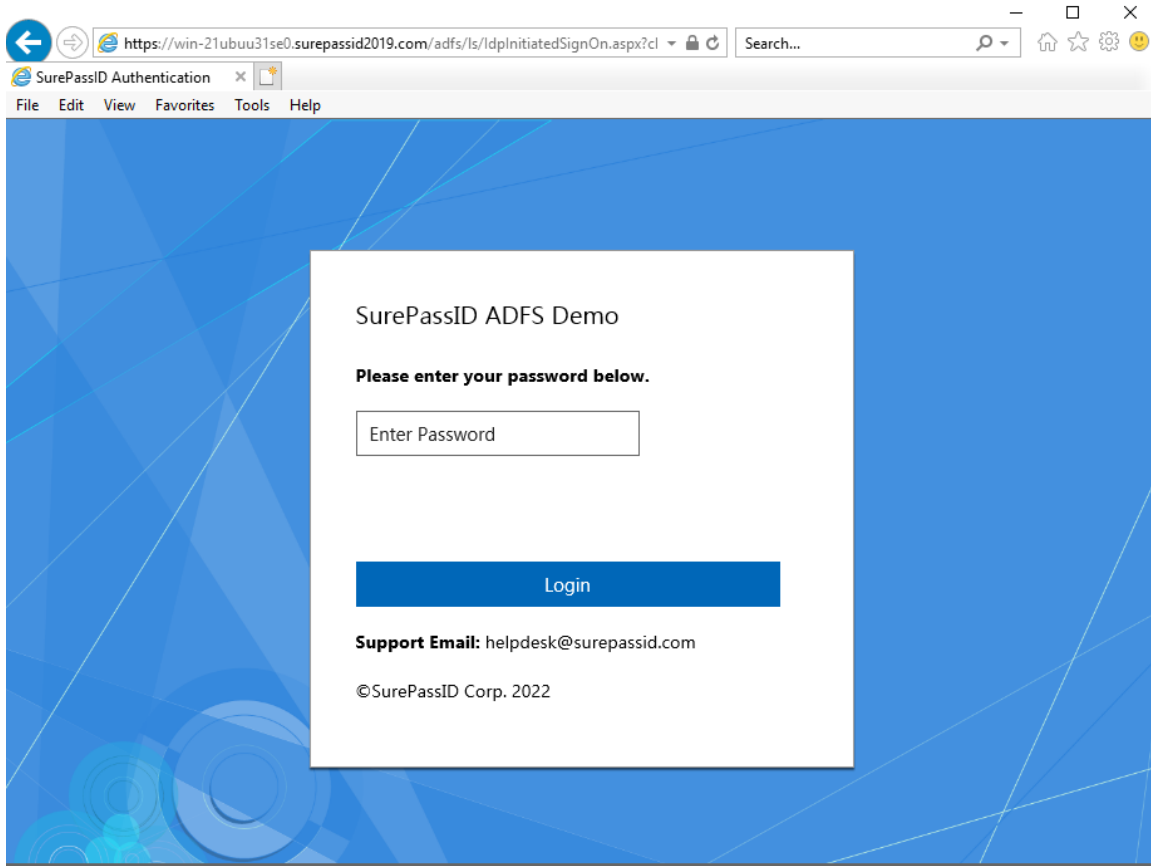
Select SurePassID Strong Authentication.

Figure 23: IdP Initiated Login – Primary Authentication – Enter SurePassID Password/PIN

Enter the SurePassID Password/PIN for this user and press **Login**.

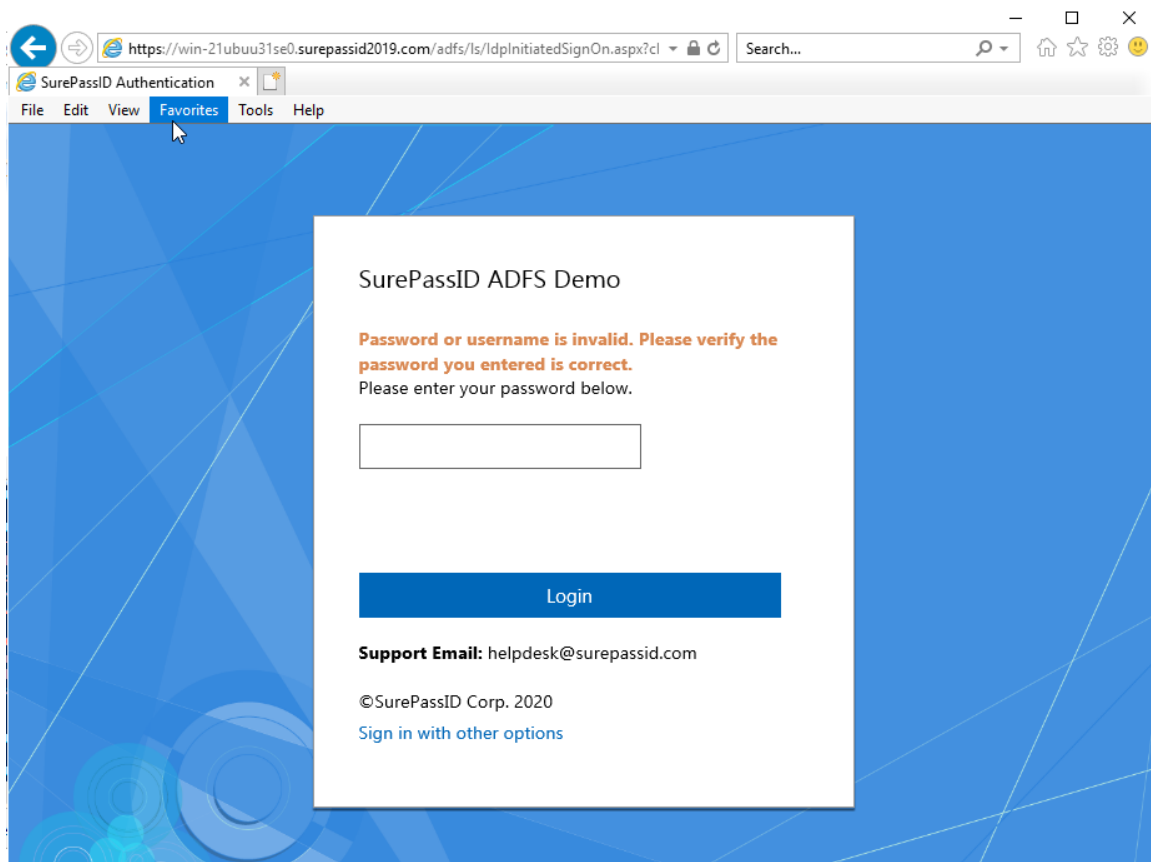The password/PIN is incorrect the form will be updated.

Figure 24: IdP Initiated Login – Primary Authentication – Invalid SurePassID Password/PIN

Re-enter you password/PIN and press the Login button. When the password is correct you will see the following form.
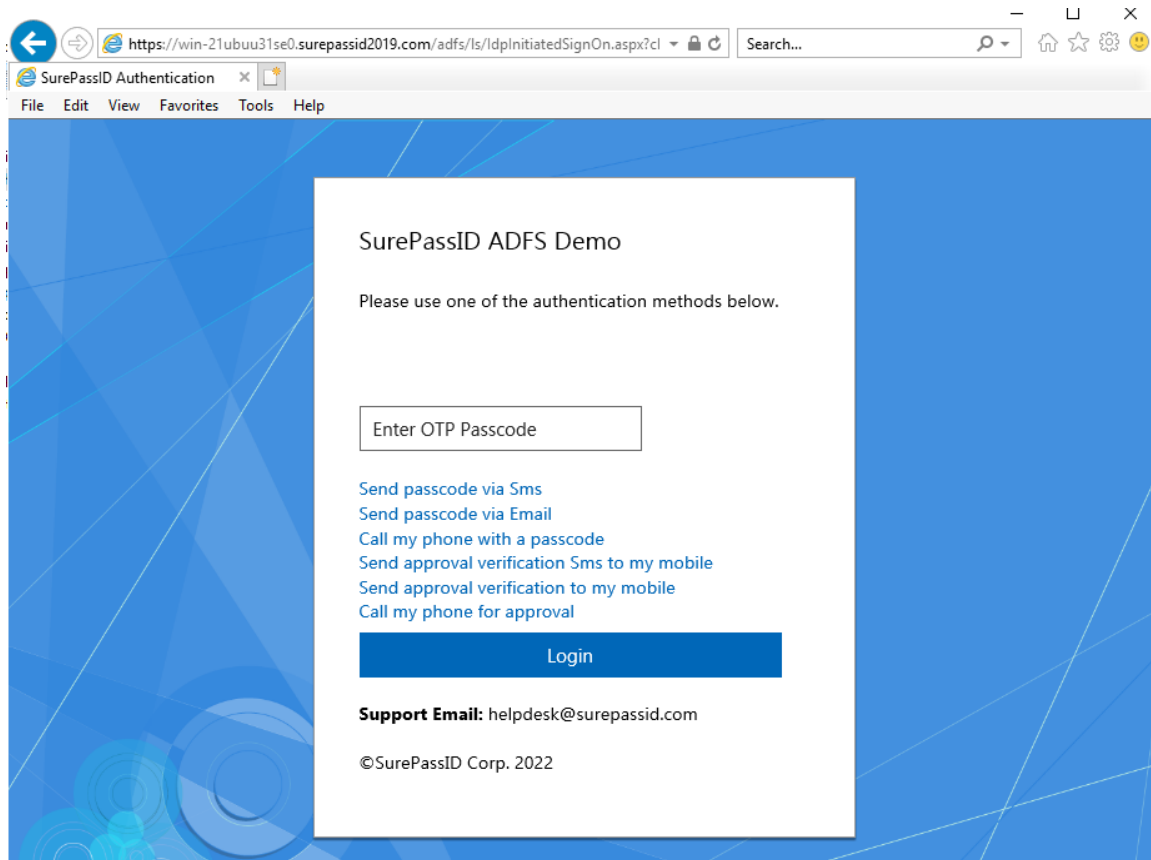
**Figure 25: IdP Initiated Login – Primary Authentication – Second
Factor Authentication**

Enter your passcode (OTP) and press **Login** or select another authentication
method.

If your administrator has reset the users SurePassID password/PIN you will not
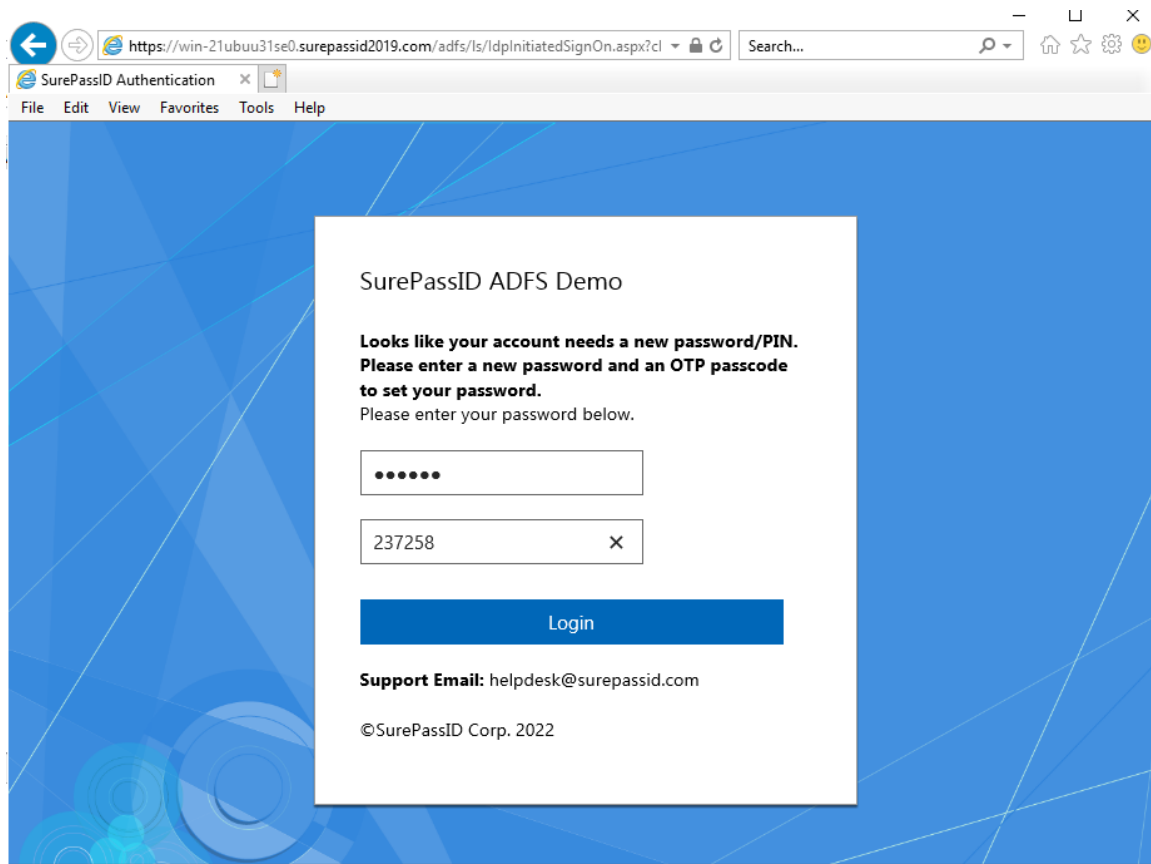see the previous form you will see the following form:

Figure 26: IdP Initiated Login – Primary Authentication – Password Reset

To reset the password/PIN enter your new password/PIN followed by a valid passcode (OTP) and press **Login**.

If you are successful in authentication with your second factor or changing your Password/PIN you will see the following form.
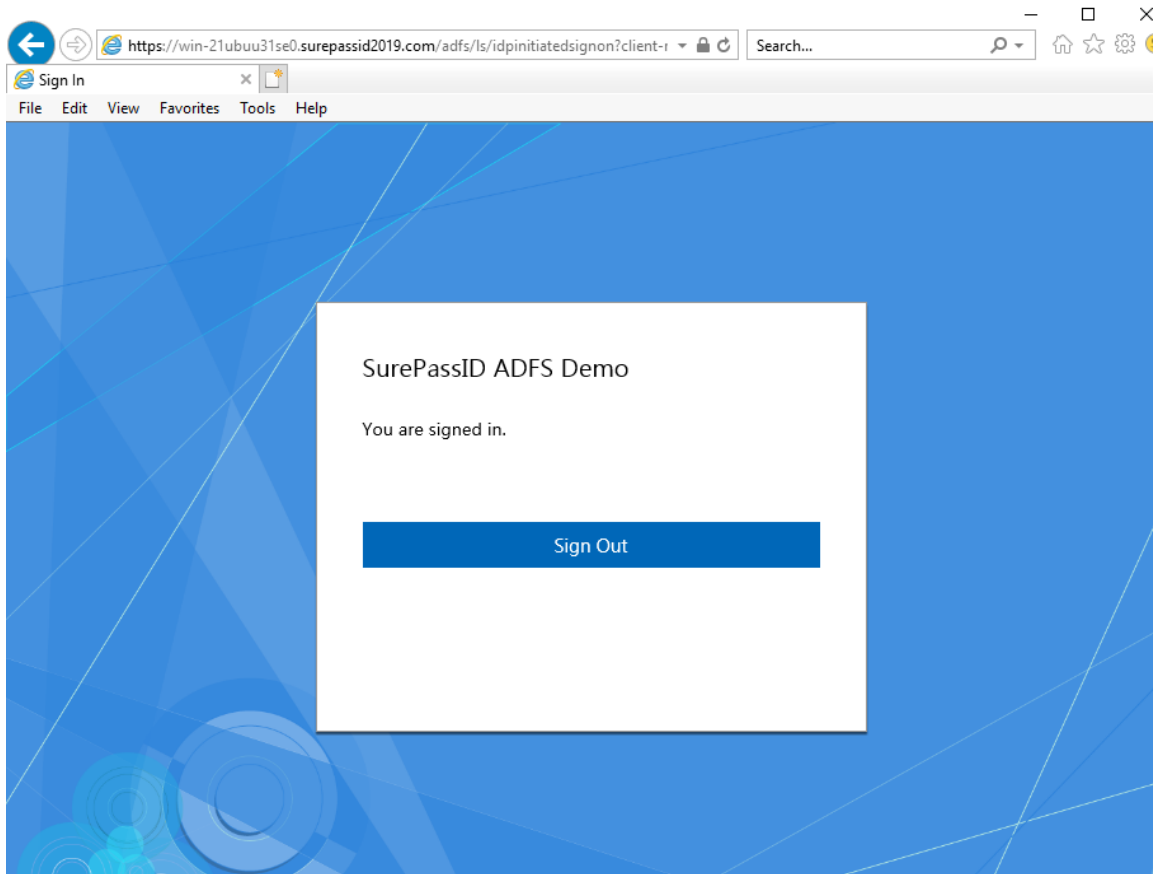
Figure 27: IdP Initiated Login – Primary Authentication – Successful Authentication

You are now signed in and can use all of your ADFS applications.
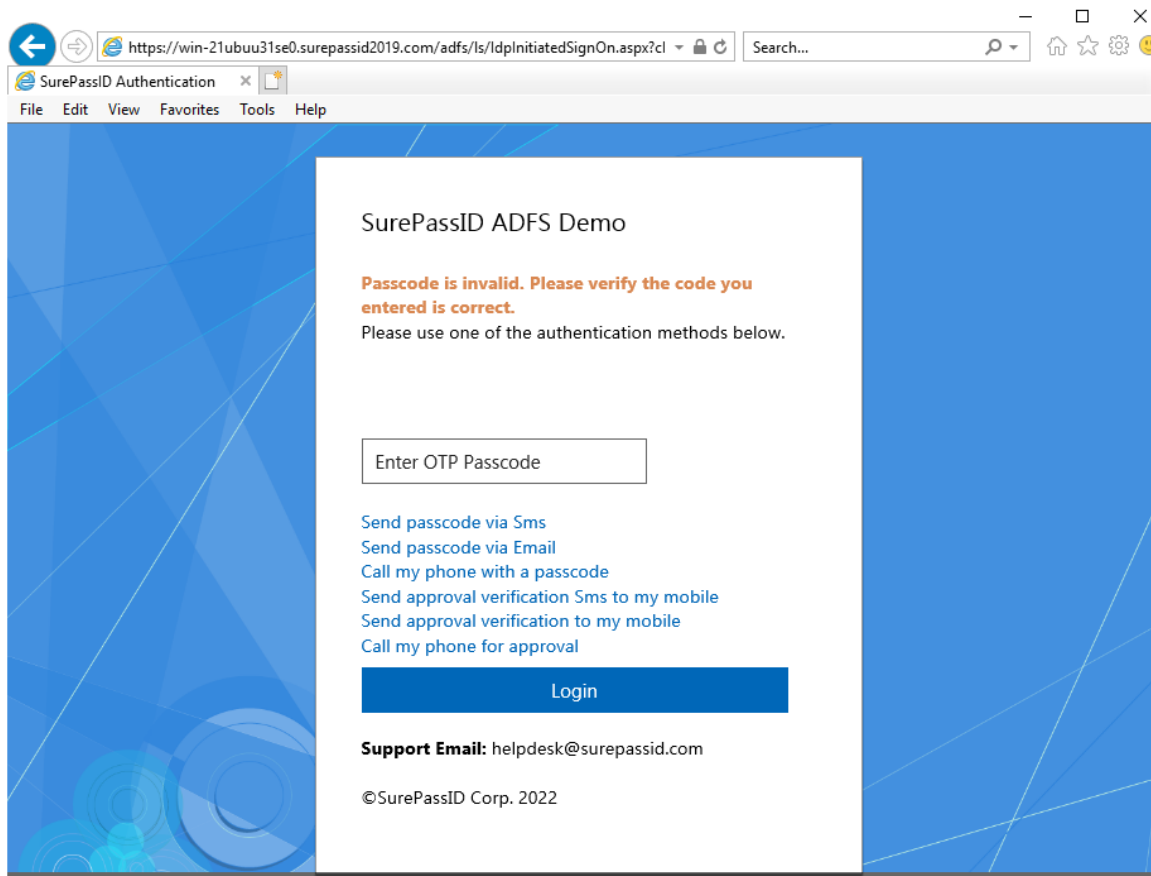
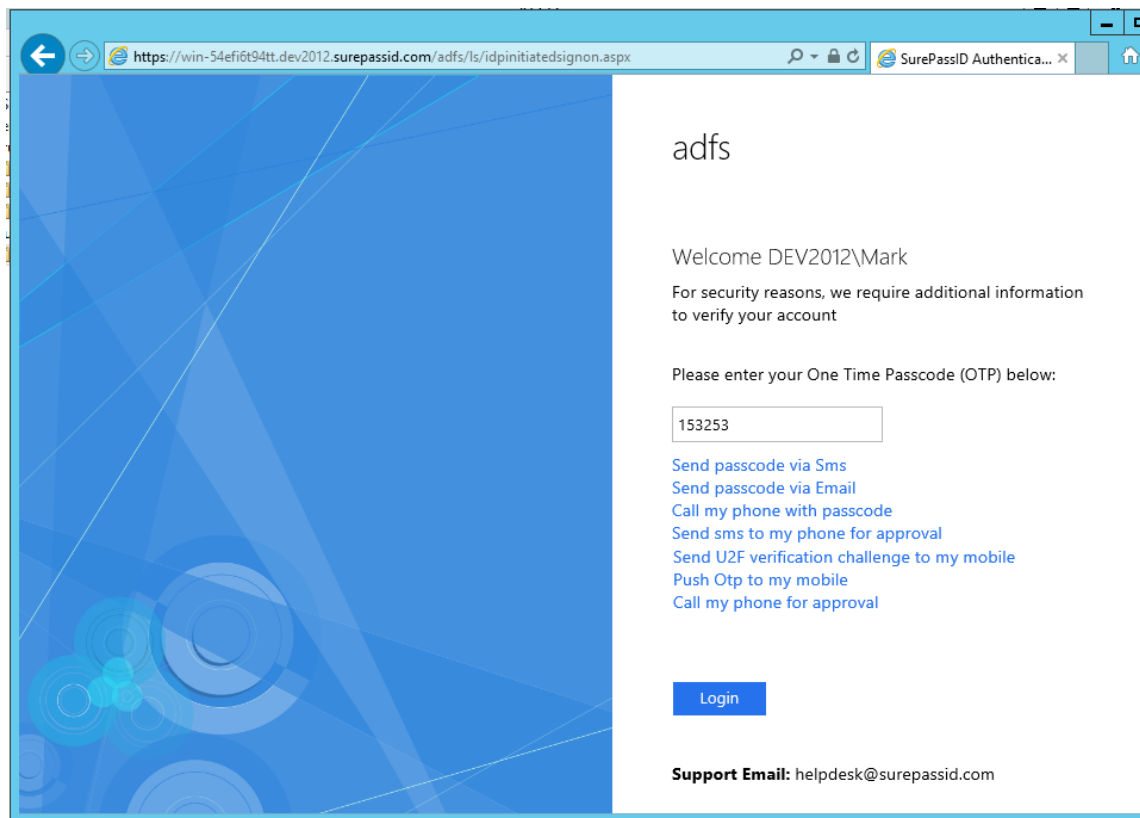**Figure 26: IdP Initiated Login – Primary Authentication – Second Factor Authentication Failed.**

Figure 18: IdP Initiated Login – SurePassID OTP Verification

Enter the passcode and click the **Login** button. If the passcode entered is correct, you will see the following:
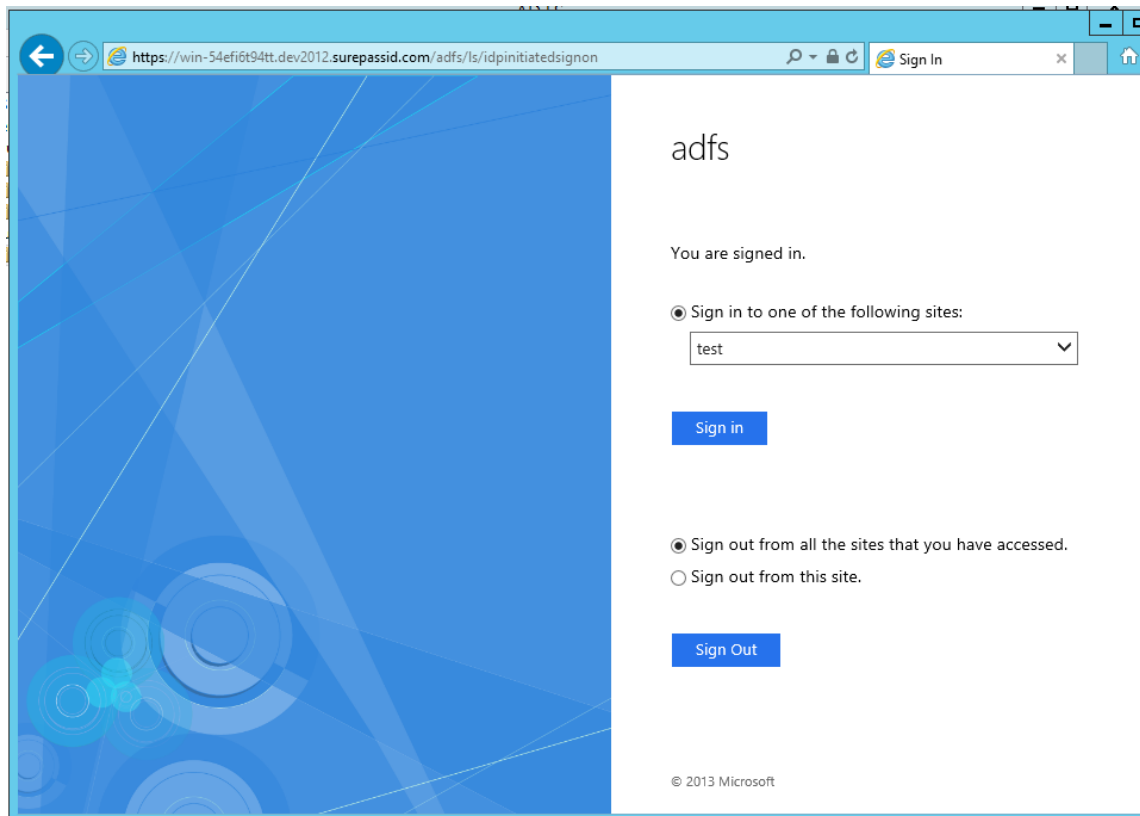
Figure 19: IdP Initiated Login – AFDS Login Success

You are signed in. You can now access any ADFS apps without re-entering any credentials.