SurePassID Windows Logon MFA Guide

SurePassID Authentication Server 23.1

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 Windows Logon MFA 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 Windows Logon MFA?**
  - A brief introduction to the SurePassID Windows Logon MFA.
- **Installing and Configuring SurePassID Windows Logon MFA**
  - Detailed explanations for installing the SurePassID Windows Logon MFA 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:

- System Administration Guide
- Local Agent Guide
  - High performance Radius Server
  - Windows Event Log Integration
  - Active Directory Synchronization
- SurePassID Desktop Authenticator Guide
- Google Authenticator Guide
- SurePassID Authenticator Guide

What is the SurePassID Windows Logon MFA?

The SurePassID Windows Logon MFA is a Windows Security plug-in component that adds Multi-Factor Authentication (MFA) to any Windows system. The SurePassID Windows Logon MFA protects laptops, desktops, and servers from attacks when locally logging into a Windows device or login via Windows Remote Desktop Services (RDS).

The SurePassID Windows Logon MFA works with any SurePassID server (cloud, on-premises) and supports all the SurePassID MFA supported OTP devices including key fobs, FIDO tokens, display cards, soft tokens such as SurePassID Mobile Authenticator, Google authenticator, and mobile app push technologies such Tap Auth (SurePassID Mobile App) , Tap Auth Fido (SurePassID Mobile App for FIDO).

The system supports offline authentication allowing users to work securely when they do not have any network connectivity; like in a car, train, plane, and unsecure locations.

Some offline options are:

- **Single Factor Only** - Revert to username and password only. No MFA required.
- **Require MFA** - HOTP passcodes (mobile, fob, etc.) or FIDO device.

Other features:

- **Master Passcodes** - Admins can set strong OTP passcodes to access user workstations in extreme emergencies.
- **Fast and easy deployment options** – Use the system configuration tools that you already use like SCCM to deploy the system.
- **Configuration export/import templates** - Configure a single windows system as the gold standard and then easily replicate to all other machines in the network. You can then easily burn it into your corporate Windows system images so it is automatically present on any new Windows systems.

Prerequisites

SurePassID Windows Logon MFA can be installed on the following 64-bit Windows versions:

- Windows 2012 – All 64-bit versions – not recommend
- Windows 2016 – All 64-bit versions
- Windows 2019 – All 64-bit versions
- Windows 8/8.1 – Professional & Ultimate 64-bit versions – **not recommended**
- Windows 10 – All 64-bit versions

You will also need a SurePassID MFA server. This can be the public cloud version, private cloud on Microsoft Azure, Amazon AWS or on-premises. If you are using public or private cloud options, you must have TLS 1.2 enabled for communications to the server. This is also required for on-premises installations as well.

This document assumes that you have configured users in SurePassID MFA server and have assigned them MFA tokens.

If you need an account you can sign up for one here.

How does it work?

Winlogon is the Windows component that performs interactive login for windows systems. Winlogon supports a variety of authentication methods such as passwords and PINs that windows users use today. Winlogon behavior can be enhanced to add different forms of logon authentication methods (displayed as tiles) through the Windows Credential Provider (WCP) interface. SurePassID uses the WCP interface and other system settings to add a multi-factor authentication experience to Winlogon. After you add SurePassID WCP, it will be visible as another logon tile no different than password or PIN logon tiles.

To add SurePassID Windows Logon MFA, the following items must be installed on each workstation:

- SurePassID WCP – SurePassIdCredentialProviderV2.dll
- RegisterSurePassIDWithWindows.reg – Turns on the SurePassID Windows Logon MFA as a Winlogon option tile. It does not remove/restrict other logon tiles such as password or PIN tiles.
- SurePassIDWindowsLoginMFASettings.reg – Registry settings to configure the behavior for the WCP. These registry settings are created using SurePassID Login Configuration Manager. More on that later.

These files are all installed after running the product installer.

Pre-Installation Steps

Since SurePassID Windows Logon MFA is installed on Windows servers, workstations, and laptops it is important to plan out your deployment. Typically, you follow these steps:

(1) What user groups will require MFA? System administrators, shop floor workers, IT workers, general population, etc.

(2) Why types of Windows devices will you be locking down? Workstations, servers, laptops, kiosks, etc.

(3) What type of authentication methods will users be permitted to use? For instance, will all users be required to use a hard token and some users use a soft token, and still others use push authentication? Perhaps you will permit users to choose from a list of authentication methods at login time.

(4) Machine Templates

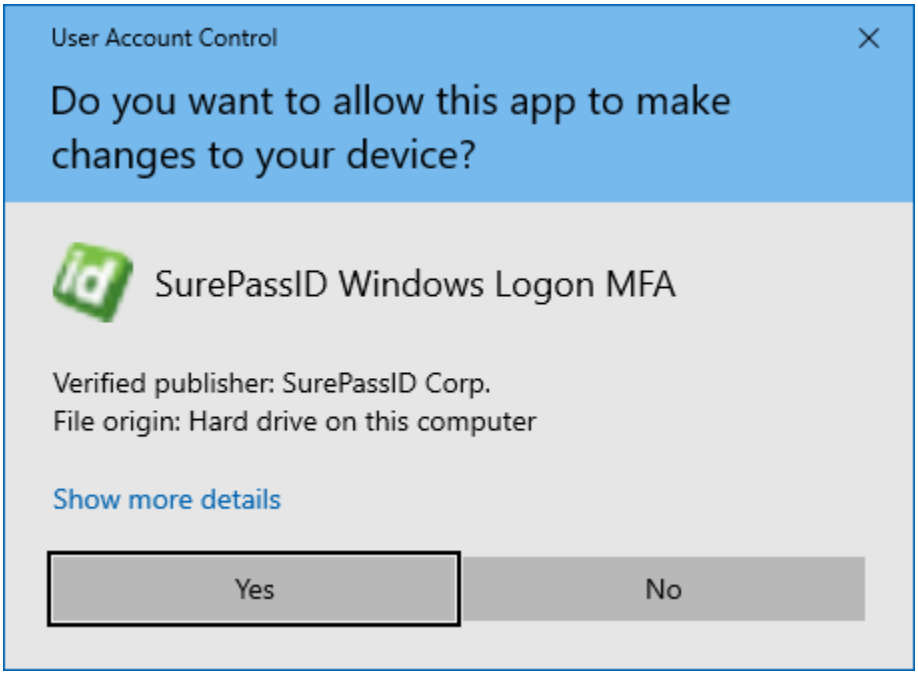
a. Create dedicated test machines that replicate the target production configuration for desktops, laptops, and server. It is recommended that these test machines are virtualized just in case you get locked out. As part of the configuration, you can fall back to the last known good save point. You can also use physical machines. **IMPORTANT: Under no circumstances should you use your personal machine or a production server at this time. It is too soon for that.**
b. Install and configure SurePassID Windows Logon MFA.
c. When configuration is complete you can create deployment packages from the machine template and deliver them to target machines. More on that later.

Installing Windows Logon MFA

The SurePassID Windows Logon MFA installer will install all of the product components and optionally display the SurePassID Logon Configuration Manager.

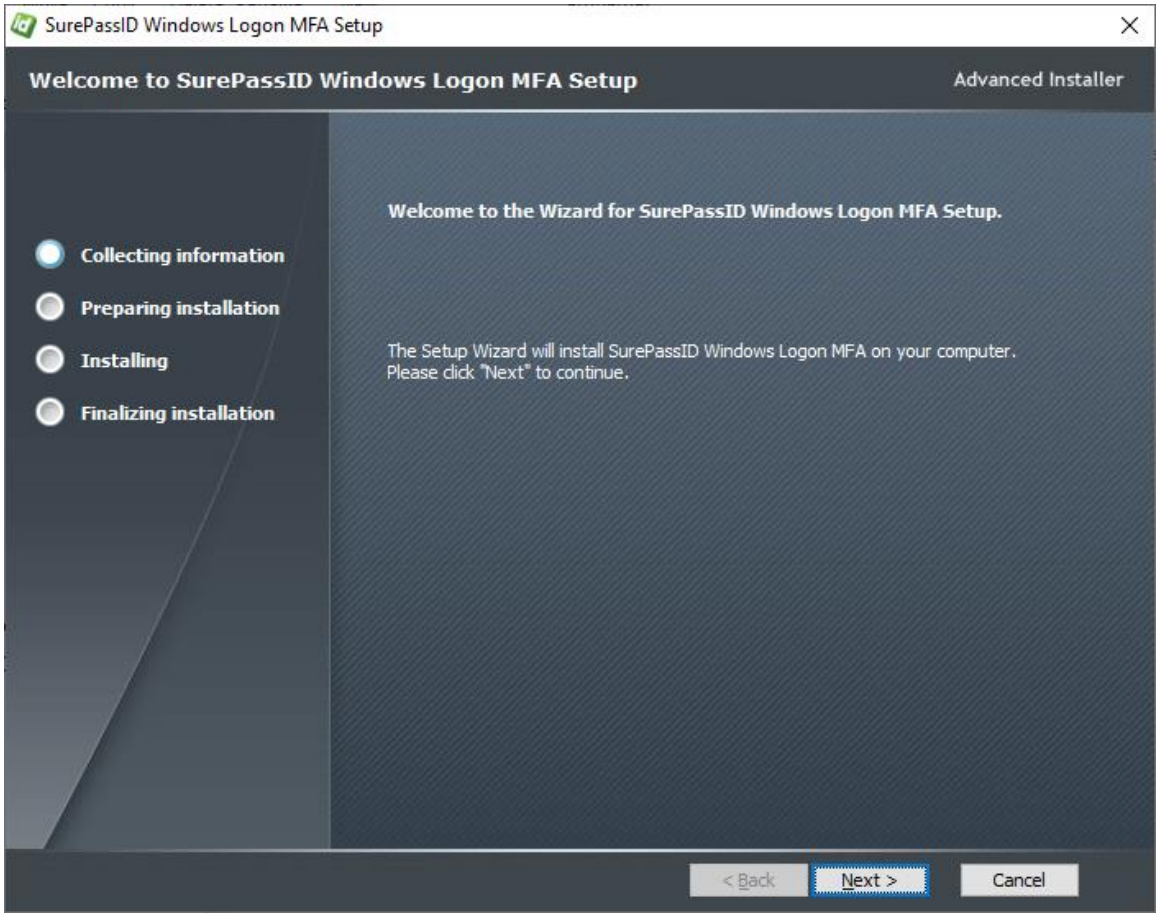
To start the installation, you must first download the installation file **SurePassIDWindowsLogonMFA_V2.exe** to one of your Windows systems.

After the file has been downloaded, execute the file and you will see a SurePassID Windows Logon MFA genuine app notice.



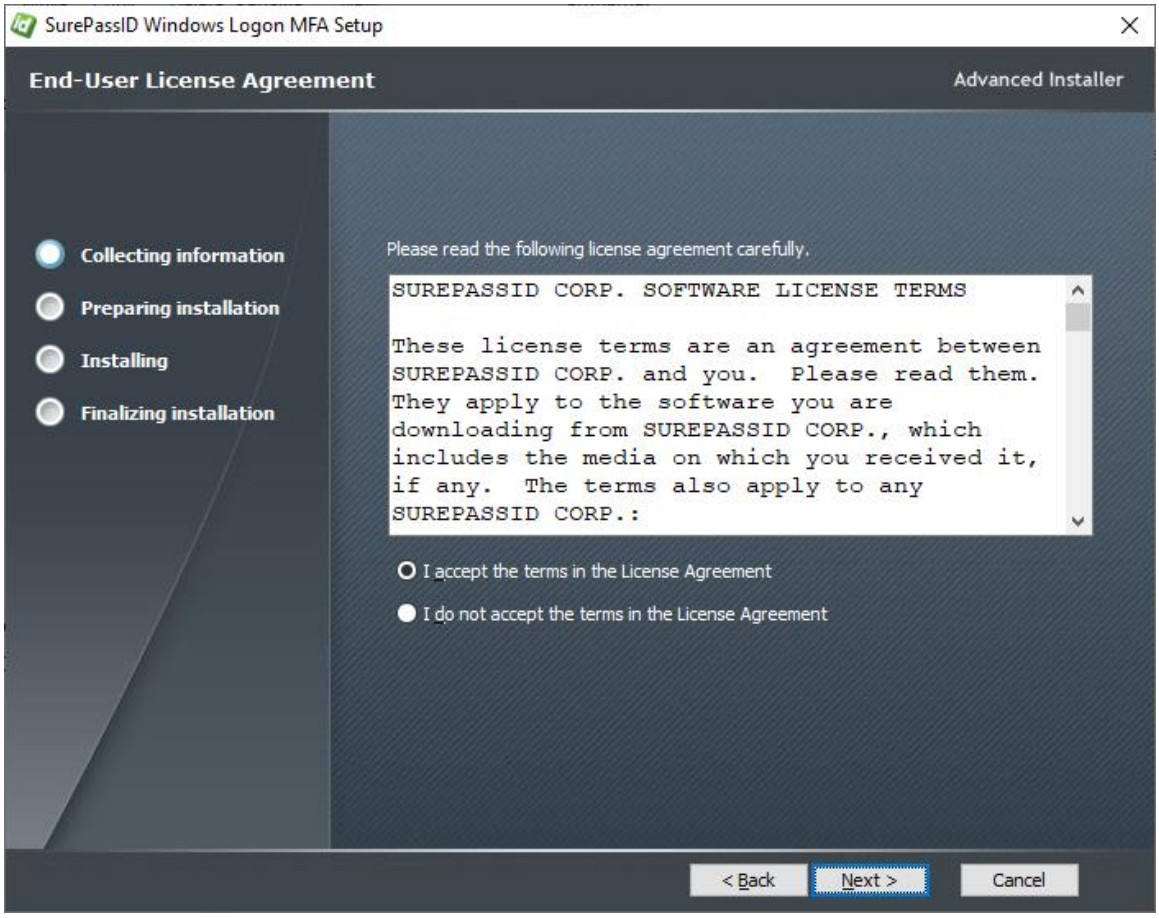
Genuine App Notification

Press the **Yes** button to proceed with the install. If you do not see this screen, cancel immediately.



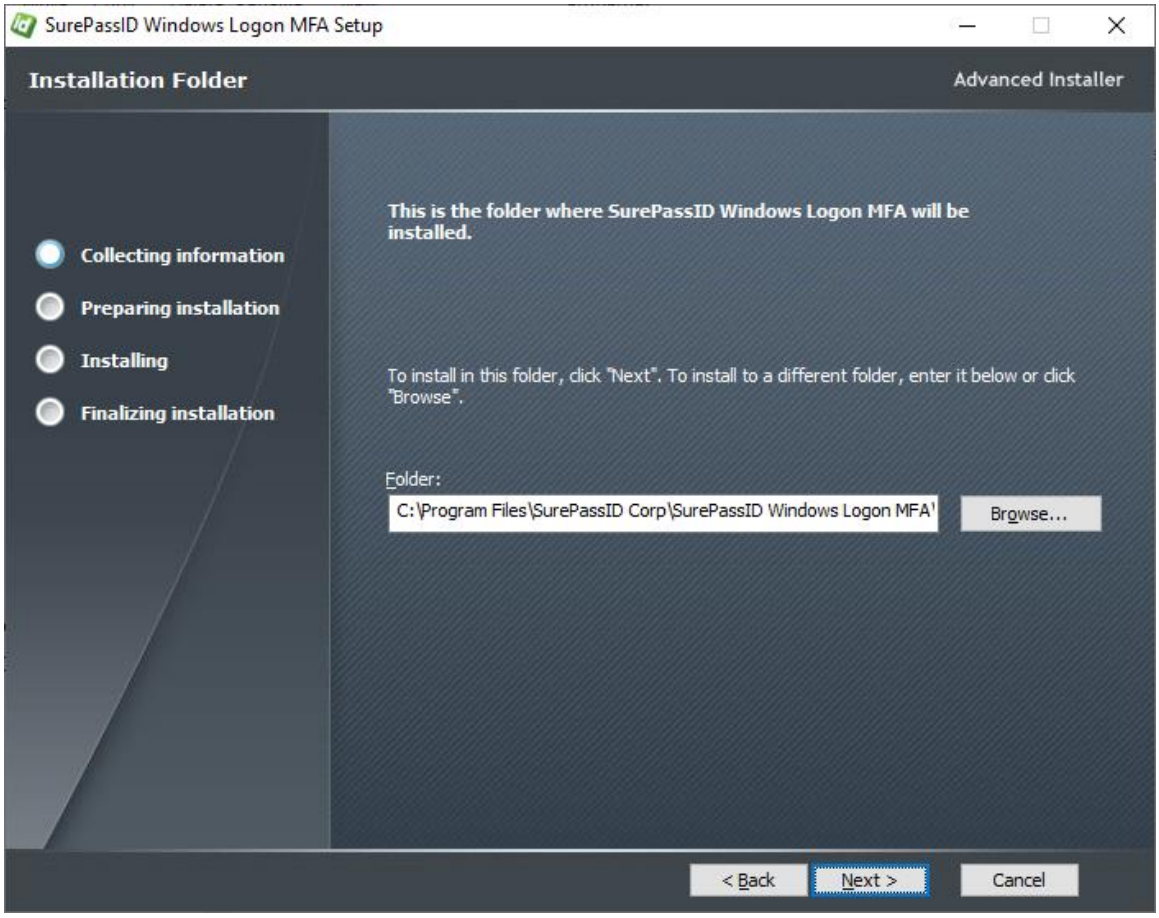
Start Installation

Press the **Next button to** proceed with the install.

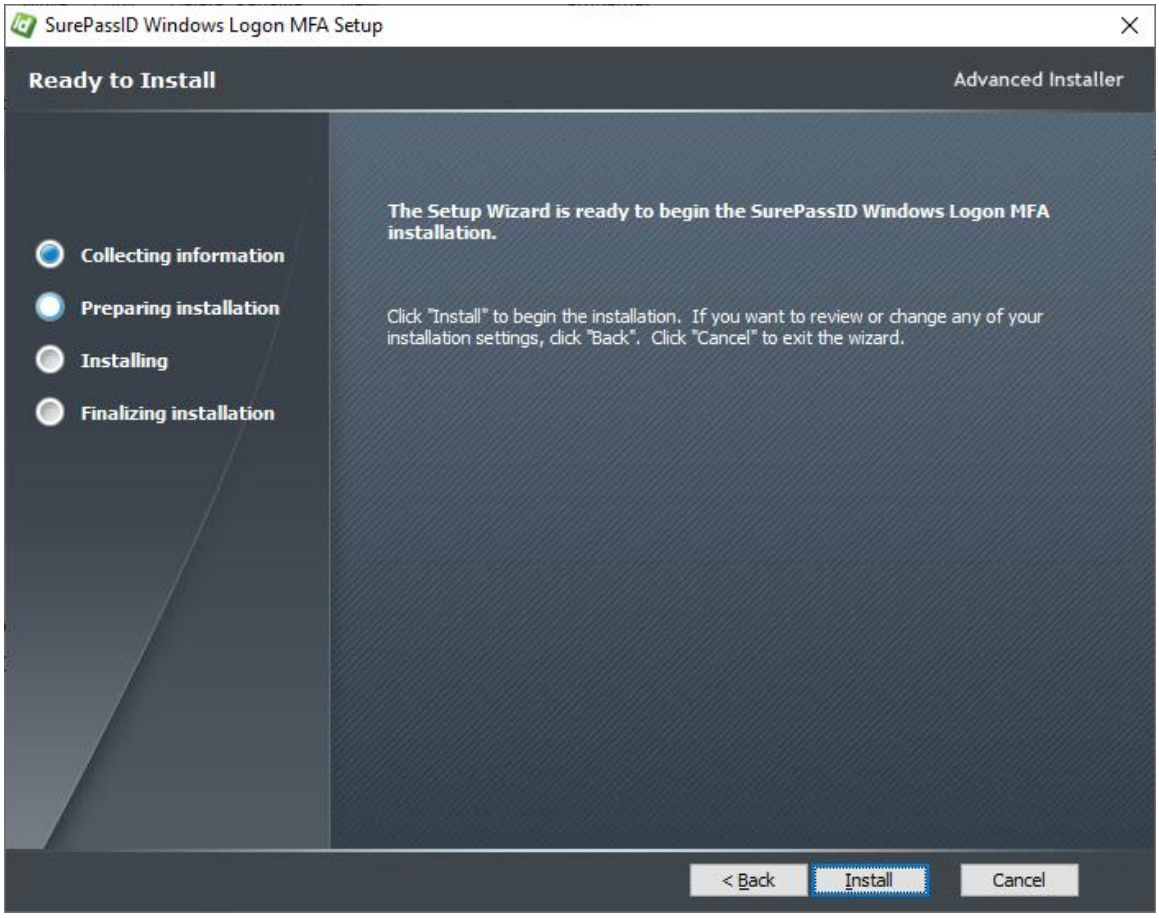


Review EULA

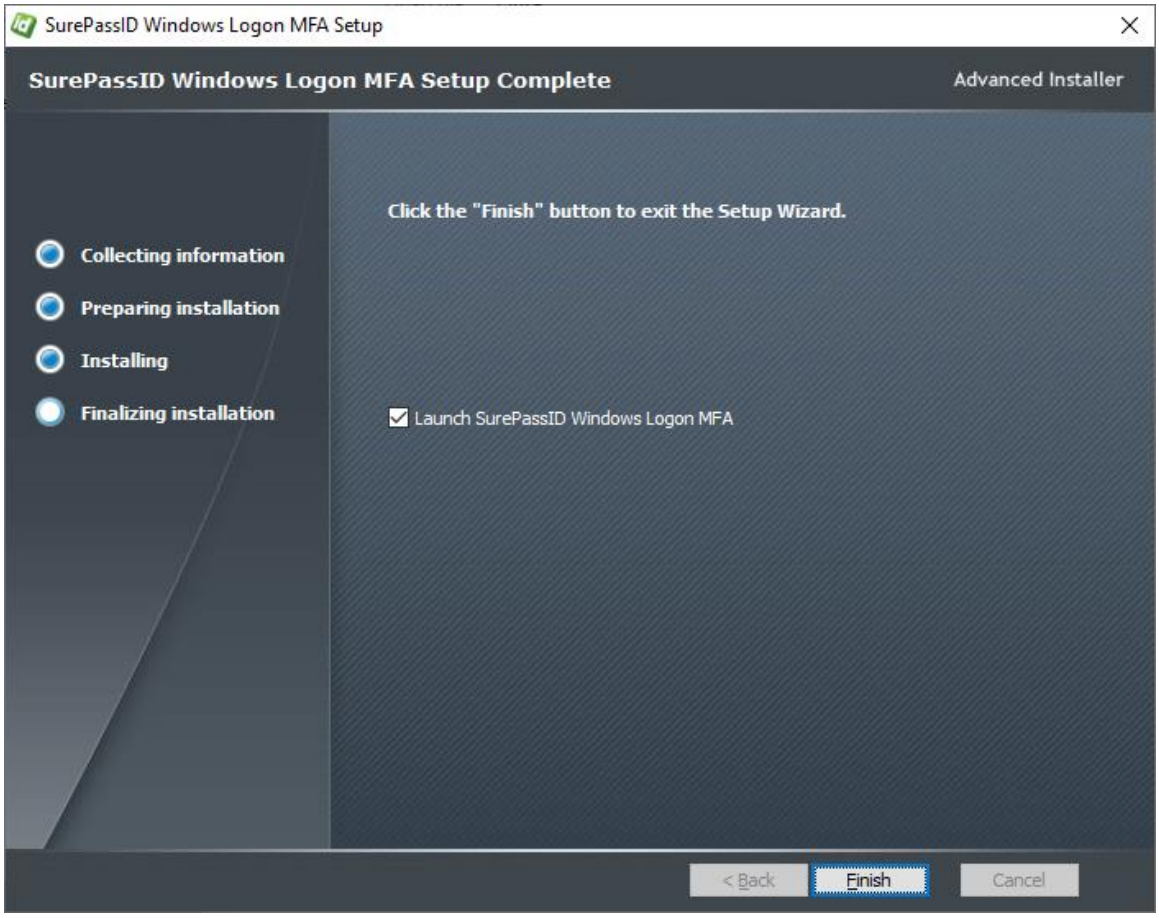
Read the End User License Agreement and click the **I accept the terms in the License Agreement** if the license Agreement is acceptable **and then** press the **Next** button to proceed with the install.



Press the **Next** button to proceed with the install.



Press the **Install** button.



Complete Installation

Check the **Launch SurePassID Windows Logon MFA** to start configuring the system now. You can always use the SurePassID Logion Configuration Manager at any time. There are short cuts on the desktop and Start menu.

Press the **Finish** button and you will see the SurePassID Logon Configuration Manager will be launched.

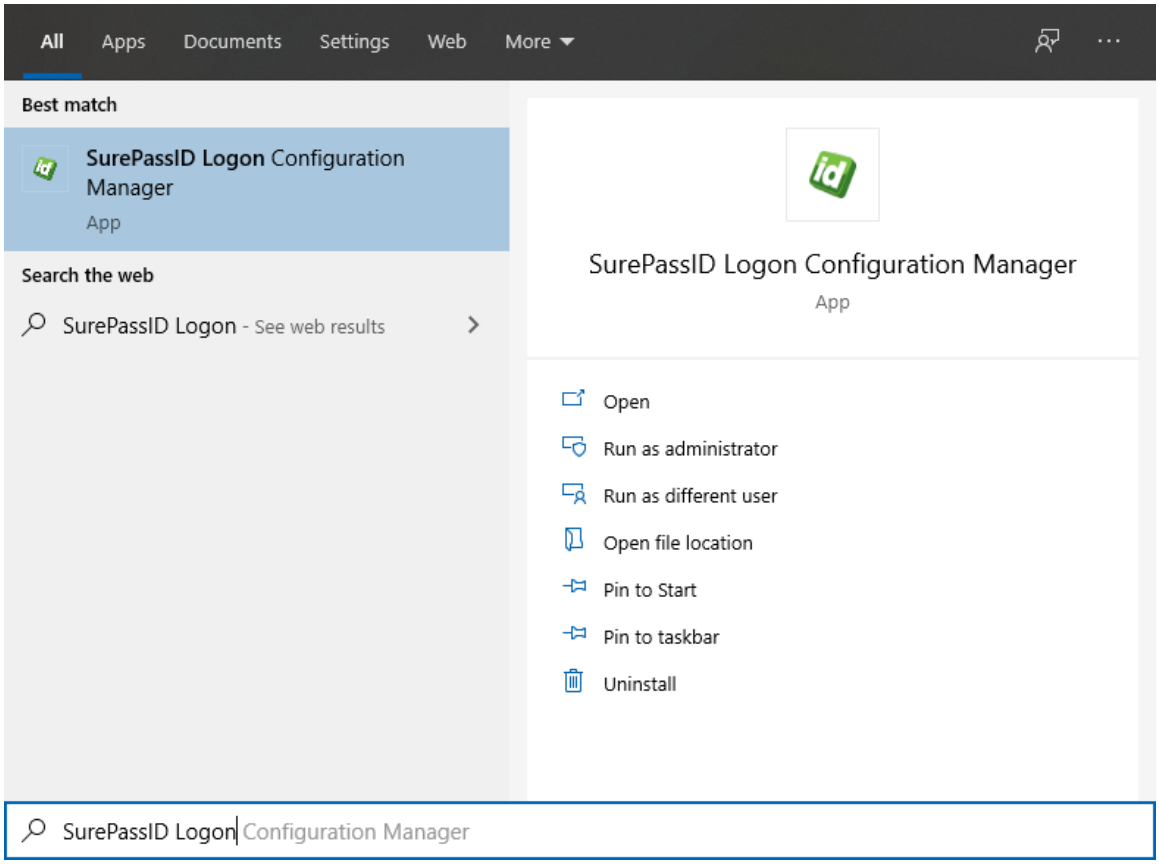
SurePassID Logon Configuration Manager

The SurePassID Logon Configuration Manager form allows you to configure SurePassID Windows Logon MFA and create a machine template for future deployment to other machines.

SurePassID Logon Configuration Manager will save all the settings in the registry so that you can test everything on the current machine. When testing is complete, you export those registry settings creating a machine template, then

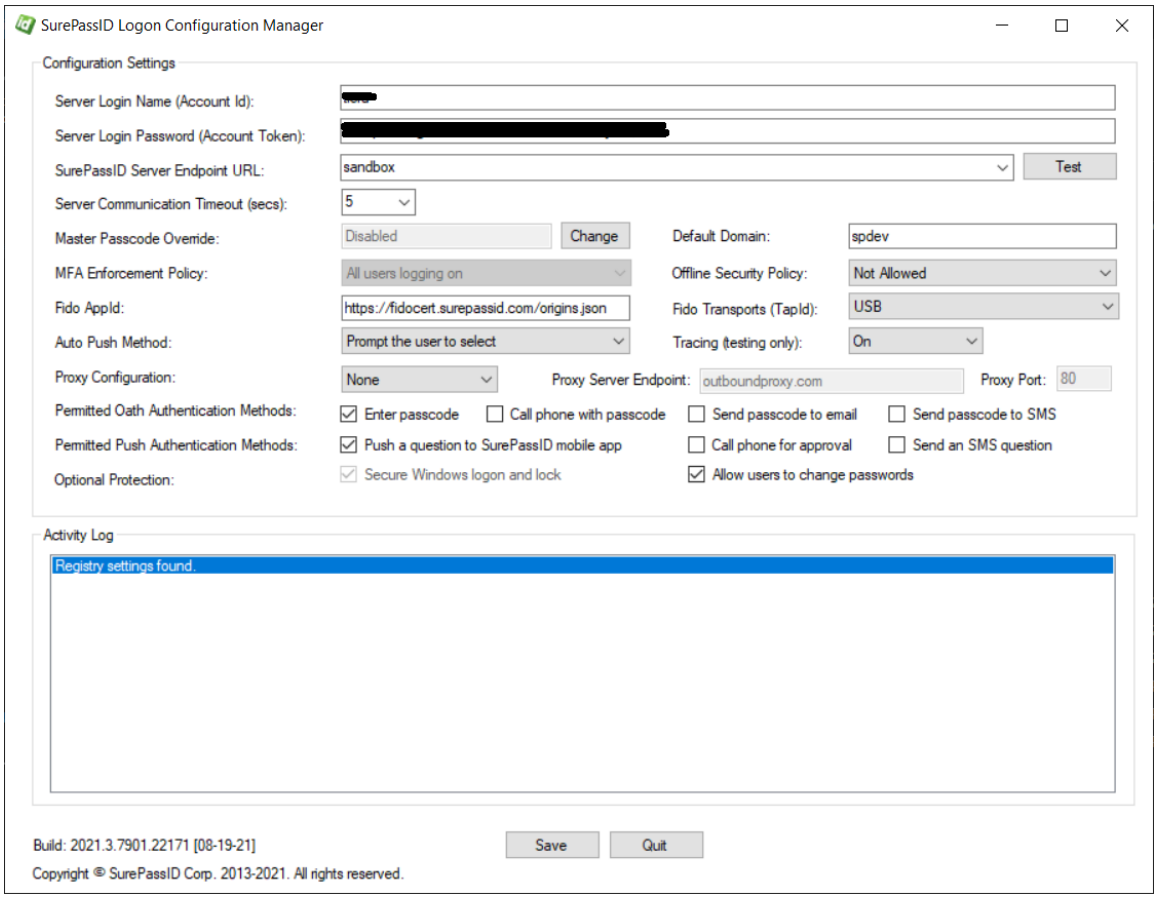
combine it with other SurePassID files to create a deployment package for other machines.

After installation, you can always start the configuration with any number of shortcuts that are created on the desktop and Start menu as shown below.



SurePassID Logon Configuration Manager Shortcut

The SurePassID Logon Configuration Manager will be displayed as shown.

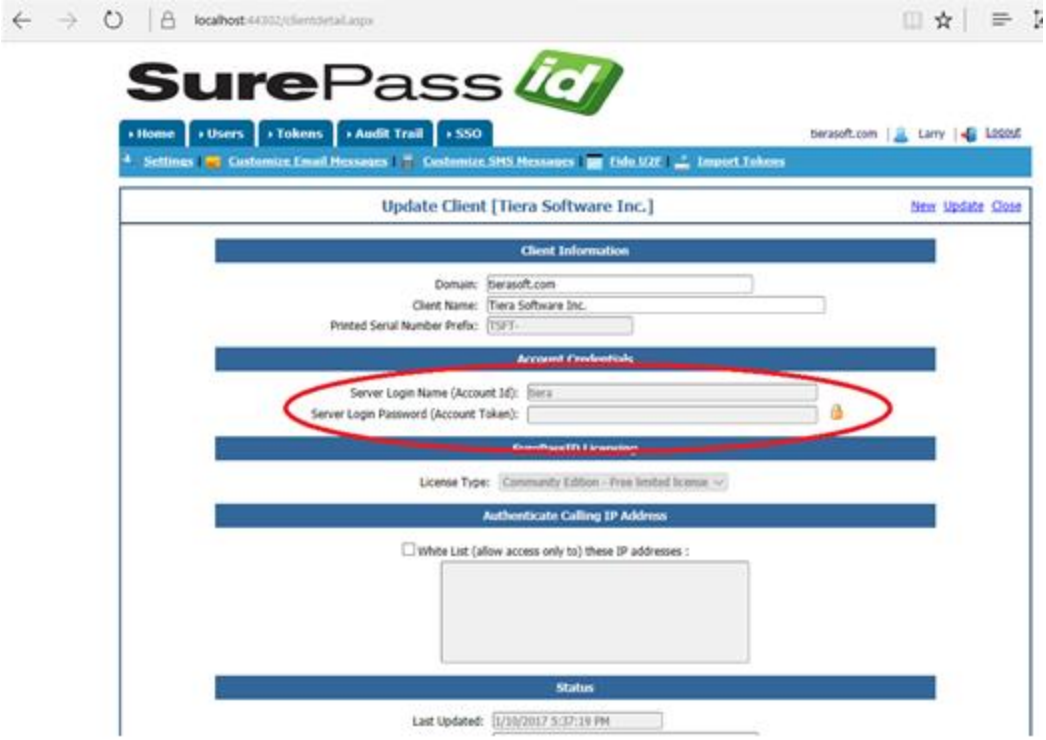


SurePassID Logon Configuration Manager App
Machine Template Configuration

The form has the following fields:

- **Server Login Name (Account Id)** – This is the identifier for your SurePassID account.
- **Server Login Password (Account Token)** – This is the password for your SurePassID account.

  The **Server Login Name** and **Server Login Password** can be retrieved from the SurePassID Administration Portal as shown below:



- **SurePassID Server Endpoint URL** – This is the listening endpoint for the SurePassID server. For example:

  https://your_SurePassID_server_url/AuthServer/

  For convenience, the following abbreviations can be used as well:
  - **sandbox** – The SurePassID test cloud service
  - **production** – The SurePassID production cloud service

- **Test Button –** Verify the connection and credentials (Server Login Name, Server Login Password) to the SurePassID Server installation.

- **Master Passcode** – The code that can be used by administrators as a substitute (bypass) for the MFA One Time Passcode. Meant to be used in emergency situations only and is an option feature.

- **Default Domain** – the default domain when logging into a workstation using the Windows login **Other** user account.

- **MFA Enforcement Policy** – Which users should have to use MFA to login.

- **Offline Security Policy** – The policy for authenticating users when they do not have connectivity to the SurePassID MFA server. The options are:
    - **Username and Password Only** - Allows the system to fall back to single factor (username and password only).
      IMPORTANT: We strongly discourage the use of this option.
    - **Require Offline MFA** demands that the user uses an offline MFA method such as mobile OTP, Key Fob or FIDO device.
    - **Not Allowed –** The user cannot login to this machine when they are not connected. This setting is applicable for machines that are stationary such as workstations and server.

- **FIDO AppId** – The FIDO AppId that was used to register the user's FIDO token. Typically, the user will register their FIDO device using a FIDO registration app as part of user enrollment in the system. The SurePassID Service Pass self-service portal is one option.

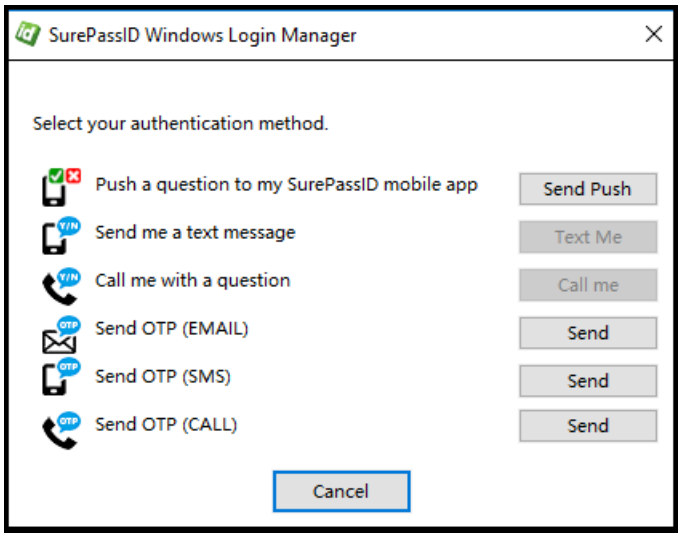
- **FIDO Transports (TapId)** – The Fido transports allowed for communications from the Fido Token to the machine. Choices are:

    - **No Fido** – Fido is not permitted.
    - **USB** – Only USB Fido devices are permitted.
    - **Smartcard** – Only Fido devices that are PCSC (including NFC) compliant tokens like SurePassID TapId.
    - **USB and smartcard** – Both USB and PCSC (including NFC) compliant Fido devices are permitted.

    IMPORTANT: For Fido Transports it is important to select the correct option. If you select an option that you are not using there will be unnecessary overhead.

Auto Authentication Method – The selected authentication method will be triggered after the user enters their password and username on the Windows login screen. The drop contains all the Oath and Push authentication methods as well as two additional options:

- **None** – Do not initiate any automatic authentication method. The user will need to enter a passcode from a hard token or mobile token.
- **Prompt the user to select**– The user will be offered a list of authentication option they can select. Users can only select options that have been permitted from the **Permitted Oath Authentication Methods** and of the **Permitted Push Authentication Methods**. When choosing this option, the user will see the following after entering thier username and correct password:



Proxy Configuration – You will need to set this if you are using SurePassID in the cloud and your organization requires all outbound traffic to go through a proxy. The options are:

- **None** – You are not using an outbound proxy or your proxy is configured to allow traffic to SurePassID endpoints.
- **Manual** – You will set the proxy server (**Proxy Server Endpoint**) and proxy port (**Proxy Port**). The **Proxy Server Endpoint** must be a valid URI such as http://proxyserver or https://192.192.192.192 .
- **Auto** – Windows Login Manager will find the proxy settings on the machine it is running on and use them.

  IMPORTANT: You will need to verify that workstation/servers that use SurePassID Windows Login Manager can send traffic to SurePassID MFA server. You might need to add a firewall access rule for traffic on port 443 to the MFA server.

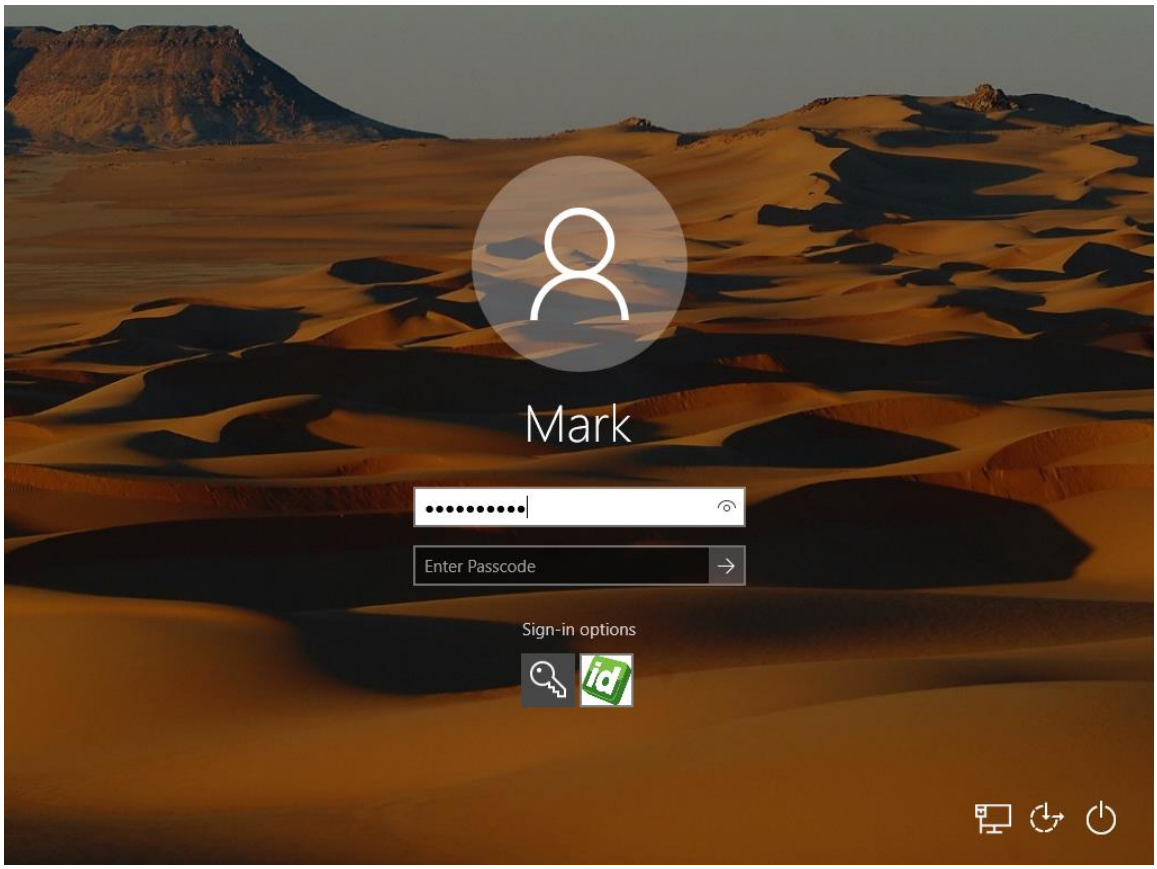
Permitted Oath Authentication Methods – Set the allowable ways a user can request or enter a passcode (OTP):

- **Enter passcode** – User can enter a passcode from a token or a mobile app. If you do not have this checked then the following three options cannot apply
- **Send passcode to SMS** – Passcode is sent via SMS to the users phone.
- **Send passcode to email** – Passcode is sent to the users email.
- **Call phone with passcode** – User will be called and a passcode will be spoken to them.

Permitted Push Authentication Methods – By default, every user will need to enter a One-Time Passcode in addition to their username and password. You can allow the user to use other authentication methods:

- **Push a question to SurePassID mobile app*** - The user receives a login approval request notification**.** The user them accepts the SurePassID Authenticator mobile app.
- **Call phone for approval** – User receives a call on their phone and accepts or denies login access.
- **Send an SMS question** - User receives an SMS and accepts or denies login access with a Y or N.
- **Save Button –** Start the configuration process. When completed, the screen indicates that the SurePassID Windows Logon MFA has now been configured. You can then select the ***Quit*** button.

  The Windows Logon screen is dynamically built for each user based on these parameters.

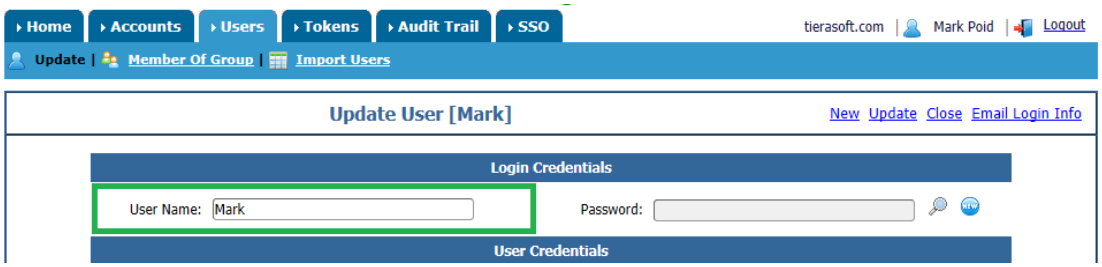


Testing the Template

Before verifying the system, it is important to understand how SurePassID Windows Logon MFA maps users' Windows Logon credentials to SurePassID users.

IMPORTANT: The Windows Logon username must match the username defined to SurePassID.

For example, if the user Mark logs into Windows with Mark, mydomain\Mark or Mark@mydomain.com, there must be a SurePassID user named Mark. This SurePassID account holds the MFA tokens for the user. The username is identified via the **User Name** attribute for the SurePassID user account as shown below.



In addition to manually adding a user to SurePassID, there are many options to import users (and their MFA tokens) into SurePassID such as csv files, Active Directory repositories, etc. Check the Import Users section of the System Administration Guide for additional information about these options.

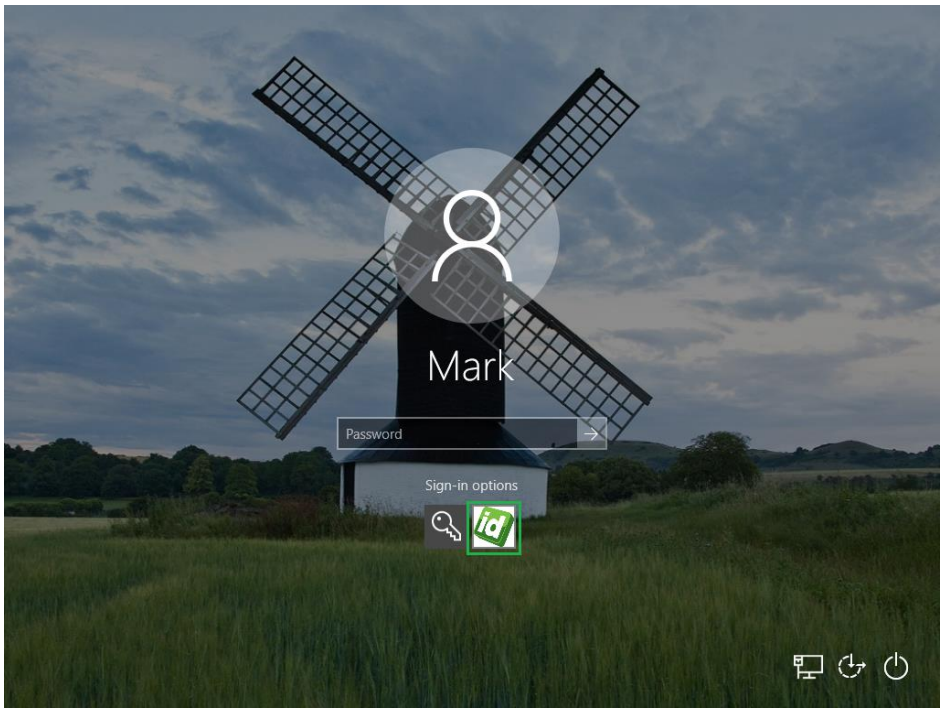
At this point you are ready to login and test the system.

Testing Installation on Windows Server 2012, Windows Server 2016, Windows Server 2016, Windows 10.1

After installing the product, Sign out or Lock the desktop and switch users, you should see the following images for Windows 8.1. The screen will look nearly identical for Windows Server 2012, Server 2016, and Windows 10.

When the Windows Logon Manager screen is displayed press the *Sign-in options* link. The screen will be updated to include all available sign-in options. The SurePassID login option is now available and highlighted below.

SurePassID WLM Login - Passcode (OTP) Option

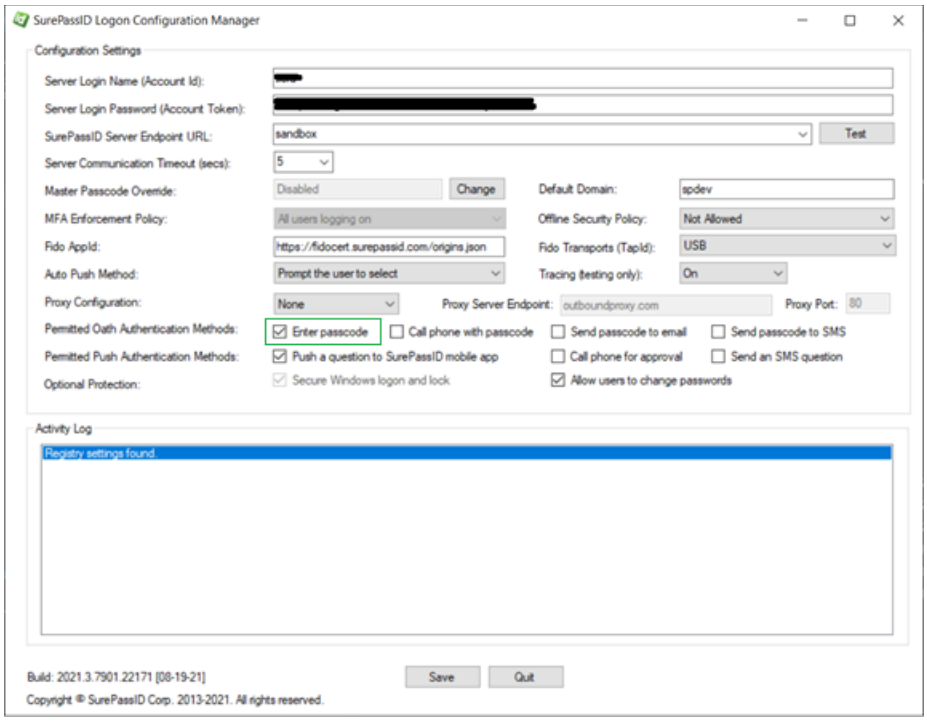


SurePassID WLM Login – Without Passcode (OTP) Option

There are several ways your users can login to the system based on the way you have configured the system in the prior section.

Login via passcode (OTP)

To enable this option you must set Enter Password option as show below. If you do not have this option the user will not be allowed to enter a passcode and the user must use a push notification (more on that later) or Fido token to log into the system.



SurePassID Logon Configuration Manager App

To logon to windows enter your AD password and two-factor passcode into the **Enter Passcode** field and press the press/click the arrow (->) key of hit enter.

You can find your two-factor passcode using one of these methods:

- If you have a two-factor hard token, enter the number displayed on the token into the two-factor passcode field.

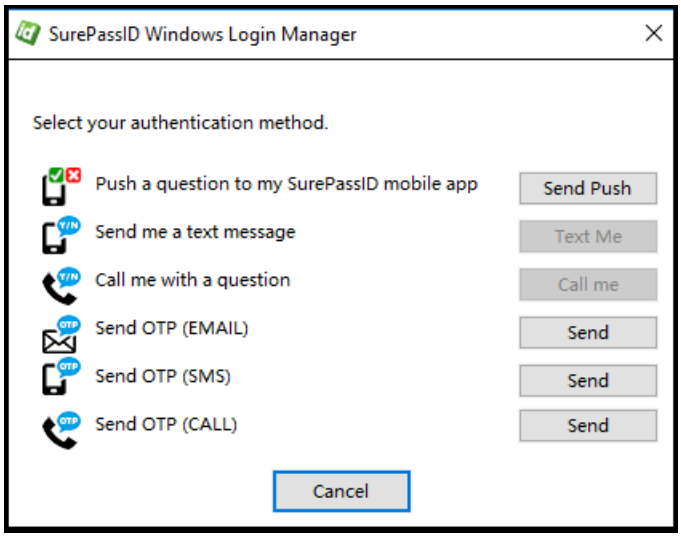
- If you have a SurePassID Treo, position the cursor over the passcode field and tap the button on the Treo which will auto fill the passcode.

- If you have The SurePassID Authenticator mobile app (or compatible mobile app such as Google Authenticator, enter the code displayed in the app.

Login via Push Notification

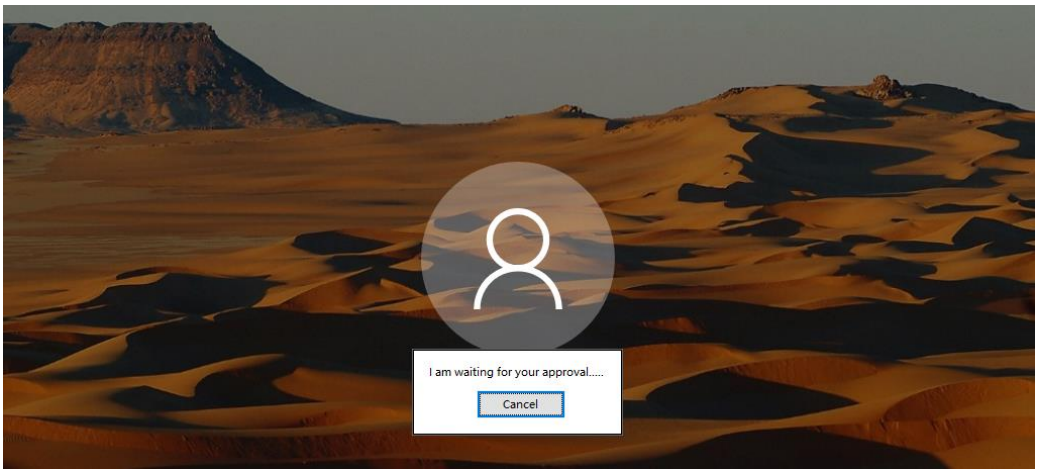
The system can be configured to use push authentication in two ways. Either method is set via the **Auth Push Method** dropdown list. The options in the dop down list are:

Prompt the user to select - With this option the users enter thier AD password and presses/click the arrow (->). The user will be prompted to select the push method the push options you have enabled as show below:



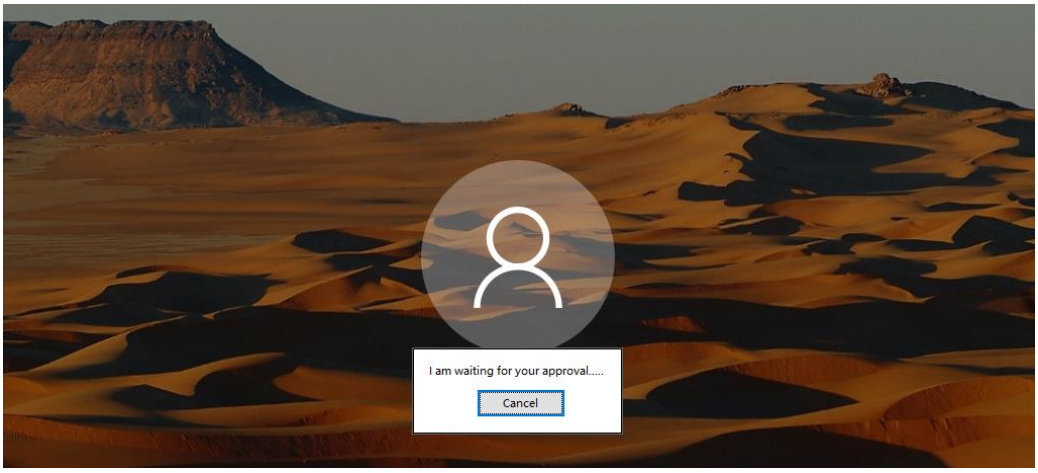
SurePassID WLM - Login Prompt

After the user selects desired push method (e.g. pressing the **Send Push** button for push authentication) the Windows logon screen waits for the user to approve the push message on the their mobile phone (or the user can press **Cancel**) as shown below:



SurePassID WLM Login – Waiting on Push After Prompt

Send Push, Call Me Text, Me – With this option the users enter thier AD password and presses/click the arrow (->). The user will be sent the chosen push message and the logon screen waits for the user to approve the push message on the their mobile phone (or press **Cancel**) as shown below:



SurePassID WLM Login – Waiting on Push

Login via Fido (TapId, Treo, and Yubikey)

Users can use your Fido tokens such as SurePassID TapId, SurePassID Treo, or Yubikeys as their second factor of authentication. The system supports both USB and NFC Fido tokens.

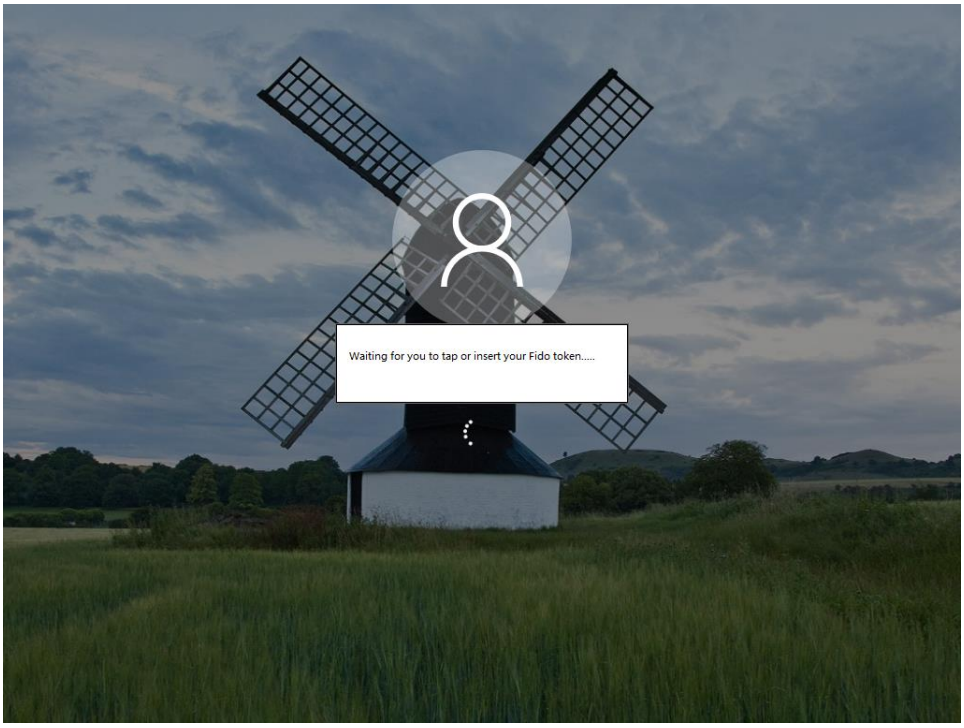
To enable Fido key usage the users Fido key must be registered using a standard Fido2/U2F registration app (web or window32) provided by SurePassID and other vendors.

It is important that you set the **Fido AppId** and **Fido Transports** settings to match the type of Fido tokens your users will have.

When using NFC Fido tokens the user enters thier AD password and presses/click the arrow (->). The user will be prompted to tap their NFC device to the NFC reader.

When using USB Fido the user enter thier AD password and presses/click the arrow (->). The user will be prompted to press the button on their Fido key when the device blinks.

Regardless of what Fido token you choose to use the user will see the following screen:



SurePassID WLM Login – Waiting on Fido

If authentication fails they can just presses/click the arrow (->) and try again with the same token or insert the correct key.

Preparing Deployment Packages

Deployment packages are used to add SurePassID Windows Logon to any Windows workstations, servers and laptops. SurePassID Windows Logon is a system component and needs to be installed on each machine that you want to add MFA. This is a Windows operating system requirement based on the Windows Credential Provider interface specifications.

The first deployment package that you must create is a staged deployment package. The staged deployment would be used to add SurePassID MFA as an additional logon option to existing login methods that users are familiar with. This deployment package allows users to be trained and get familiar with MFA for some period time before they are required to use it exclusively.

Once users are comfortable with MFA, you can create a production lockdown deployment package that enforces SurePassID MFA and other approved Windows MFA logon methods such as smart cards and biometric logins.

After you have become familiar with the system you can combine the staged and production lockdown packages into one and do a single deployment to enforce MFA in one step.

A staged deployment package configuration is comprised of three components:

- SurePassID Windows Logon component (SurePassIdCredentialProviderV2.dll) – The component provides all the support for the SurePassID Windows Logon tile. This file must be placed in the windows\system32 folder.
- SurePassID Windows Logon Activation (RegisterSurePassIDWithWindows.reg) – This set of registry entries turns on the SurePassID Windows Logon.
- SurePassID Windows Logon Configuration ([HKEY_LOCAL_MACHINE\SOFTWARE\SurePassId\CredProv]) – This set of registry entries are managed on the template machine by the SurePassID Logon Configuration Manager app. When you are ready to create a deployment package, you will export these settings from the registry into your deployment package.

NOTE: You can have multiple staged configurations for different users. For instance, some groups of users can be forced to use key fobs but other users can use mobile OTP apps. Each staged deployment would have a different SurePassID Windows Logon Configuration set of registry entries.

Once all users have been trained and a deadline is communicated to your users when two-factor authentication will be mandatory, the following registry entries will be activated to force MFA for Windows Logon.

- SurePassID Windows Logon Lockdown (EnforceSurePassIDMFA.reg) – This set of registry entries is used to turn off all methods of login except for SurePassID MFA and other login methods you have added to the inclusion list.

A complete production deployment package contains both the stage and production deployment packages.

You can create other deployment packages such as master passcode deployment packages for password rotation. This deployed package updates the master passcode on existing Windows systems.

Deploying Windows Logon MFA

The following list is in the least to most desirable option to deliver deployment packages:

- **Manual** - Install the deployment package on each user's computer individually. The deployment package could be placed on a network share for easy installation.
- **System Image Burn** - Install and configure the system in the same manner as the **Manual** method except that you install the Windows Logon MFA onto your user system image; the one that is used to stage all new Windows machines. In this way, the Windows Logon MFA will be set-up by default on each new user's machine.
- **Microsoft SCCM –** Create an SCCM package that includes the deployment package you created earlier.
- **PowerShell scripts and Group Policy –** If you are unfamiliar with how to do this, we can provide some sample scripts that you can tailor to your company's needs. Just contact support.
- **Other package managers –** You can use any package manager to install the SurePassID deployment package provided that the package manager can copy a file to the windows\system32 folder and run .reg files.

Note: It is important that you do this in a controlled manner as it could affect your user's ability to log into their Windows systems. If you have any questions or concerns please contact SurePassID technical support at helpdesk@surepassid.com where assistance and guidance will be provided.

Master Passcodes

Master Passcodes can be used by administrators as a substitute (bypass) for the MFA One Time Passcode. This is an optional feature and if you choose to use it, you should know the following:

- The Master Passcode is a password and should be treated as any system password (do not leave it in plain text on a server, only provide to a small number of administrators, etc.) and it should be rotated periodically as you would other passwords.
- The Master Passcode is stored in the machine template (registry) using the SurePassID Logon Configuration Manager (LCM) app.
- To change (rotate) the new Master Passcode change the Master Passcode using the LCM app and then create a master passcode deployment package and deliver to the appropriate Windows machines.
- The Master Passcode is stored as a SHA256 hash. If you forget the Master Passcode there is no way to recover it. Your only option is to create a new Master Passcode using the SurePassID Logon Configuration Manager app, create a new deployment package and deliver to the appropriate Windows machines.

Offline Operations

SurePassID Windows Logon MFA offline operations are situations when the user does not have network connectivity such as when the user is on a plane or the WIFI in a public area is not available, etc.

This situation supports offline authentication using OATH Event based (HOTP tokens).

To use offline, the user's account must be enabled for offline operations.

OATH event-based offline authentication requires that the user has an OATH event-based HOTP device assigned to their account. The device can be any mobile HOTP app, key fob, display card, etc. This does not have to be the normal device the user logs in with. For instance, the user could use an OATH time-based device (mobile, OTP, key fob) for normal login and use the event-based device only when offline. The system maintains the local cache for offline operations securely and transparently to the user. When the user logs in and the system is offline, the system will automatically detect this and try to authenticate the passcode using the local cache.

FIDO Considerations

How do I login using a FIDO key?

To login using a FIDO key, enter your username and password and click the login submit button (usually an arrow). If your username and password are correct, and with your FIDO device plugged in, the FIDO device will flash/blink, prompting you to press the button. If the device is registered to your account, you will be logged in to the system.

What is the process for using a FIDO key?

FIDO authentication was designed to provide a secure login to a specific web relying party origin such as https://sandbox.surepassid.com/login. The origin is referred to in FIDO terminology as the appId. The process to use a FIDO key is a two-step process for the user:

(1) Register their FIDO device with the relying party origin after the user is authenticated with another MFA method such as SMS code, Mobile OTP, etc.
(2) Subsequently, login to that relying party origin authenticating the user with the same registered U2F key.

The SurePassID Windows Logon MFA provides the second part of the process allowing the user to login into Windows using their key. This raises the following question:

How can the user register their FIDO key and what appId should I use since this is not a web-based login?

The answer to these two questions is related. First, there are many ways to register a FIDO device with SurePassID. We offer APIs that allow you to build many different ways to register a FIDO device such as a native Windows app, intranet/extranet web sites, etc. We recommend that you set up an intranet/extranet location where users can register their devices such as **https://fidoreg.yourcompany.com/register** or you can install the SurePassID ServicePass self-service portal where users can manage all their account, tokens and password recovery.

When configuring the SurePassID Windows Logon MFA, you would set the **FIDO AppId** to the website origin (URL) that the user registers their FIDO U2F token such as **https://fidoreg.yourcompany.com/register.**This must match the origin that is used for the device registration.

SurePassID also supports FIDO facets. In large companies with many FIDO apps, it might be advantageous to use an appId that is a facet. If you are not certain about the best path for your company, contact us for assistance.