

SurePass

SurePassID Credential Provider Guide

SurePassID Authentication Server 2020



SurePassID Credential Provider Guide
Revision: 01012020.1

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

© 2013-2020 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.
13750 W. Colonial Drive
Winter Garden, FL 34787
www.SurePassID.com

Table of Contents

Table of Figures	4
Introduction	5
What is the SurePassID Credential Provider?	6
Prerequisites.....	7
Post Configuration Steps	8
Installing the Credential Provider	9
Post Installation & Verification Steps	14
Offline Operations	33
FIDO U2F Considerations	34

Table of Figures

Figure 1: Installation beginning	9
Figure 2: Genuine App Notice.....	9
Figure 3: Installation App: Specify Install Configuration	10
Figure 4: Installed System Component	13
Figure 5: Windows 7 Login Screen	15
Figure 6: Windows Server 2008 Login Screen.....	16
Figure 7: Windows 7 SurePassID Login Screen	17
Figure 8: Windows 7 SurePassID Login Screen Credentials	18
Figure 9: Windows Server 2008 Login Screen.....	19
Figure 10: Windows Server 2008 Login Screen SMS Verification	20
Figure 11: Windows Server 2008 Login Screen Credentials.....	21
Figure 12: Windows Desktop 8.1, Server 2012 Login Screen.....	22
Figure 13: Windows Desktop 8.1, Server 2012 SurePassID Login Screen.....	23
Figure 14: Windows Desktop 8.1, Server 2012 SurePassID Login Screen.....	24
Figure 15: Windows Desktop 8.1, Server 2012 SurePassID Login Credentials.	25
Figure 16: Windows 7 SurePassID Only Login Screen.....	26
Figure 17: Windows 2008 SurePassID Only Login Screen.....	27
Figure 18: Group Policy Editor: Disable Credential Providers.....	29
Figure 19: Group Policy Editor: Save Disabled Credential Providers.....	31

Introduction

This guide explains how to install and configure the SurePassID Credential Provider 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 Credential Provider?**
 - A brief introduction to the SurePassID Credential Provider.
- **Installing and Configuring SurePassID Credential Provider**
 - Detailed explanations for installing the SurePassID Credential Provider 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](#)
- [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 Credential Provider?

The SurePassID Credential Provider is a Windows Credential Provider plug-in component that adds Two Factor Authentication (2FA) to any Windows system. The SurePassID Credential Provider protects laptops, desktops, and servers from attacks when locally logging into a Windows device or login via Windows Remote Desktop Services (RDS).

The SurePassID Credential Provider works with any SurePassID server (cloud, on-premises) and supports all the SurePassID 2FA supported OTP devices including key fobs, FIDO U2F USB tokens, display cards, soft tokens such as SurePassID Mobile Authenticator, Google authenticator, and mobile app push technologies such as SurePass Mobile Push App, and SurePass Mobile Push App for FIDO U2F.

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 insecure locations.

Some offline options are:

- **Single Factor Only** - Revert to username and password only. No 2FA required
- **Require 2FA** - OTP passcodes (mobile, fob, etc.) or FIDO U2F device.

Other features:

- **Master Passcodes** - Admins can set strong passcodes for extreme emergencies.
- **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 Credential Provider can be installed on the following 32 and 64 bit Windows versions:

- Windows 2008 – All versions
- Windows 2012 – All versions
- Windows 2016 – All versions
- Windows 2016 – All versions

- Windows 7 – Professional & Ultimate
- Windows 8/8.1 – Professional & Ultimate
- Windows 10

The following table summarizes which installer you need for each Windows platform.

Installer Name	Windows Version
SurePassCP_V1.exe	Windows 7 Windows 2008
SurePassCP_V2.exe	Windows 2012 Windows 2016 Windows 2019 Windows 8/8.1 Windows 10/10.1
Credential Provider Configuration App (stand-alone) Email support@surepassid.com for download Url.	All Windows versions

Post Configuration Steps

Here are a few recommended items to consider after installing the SurePassID Credential Provider.

- Disable all other credential providers, forcing SurePassID 2FA for all users
- Review and configure system configuration settings to meet your requirements
- Large scale rollout to all users

These suggestions are discussed in subsequent sections.

Installing the Credential Provider

The SurePassID Credential Provider installer will install all of the Credential Provider components and prerequisites.

To start the installation you must first download the installation file **SurePassCP_V1.exe** or **SurePassCP_V2.exe** to one of your Windows systems. After the file has been downloaded, execute the file and you will see the following installation form:

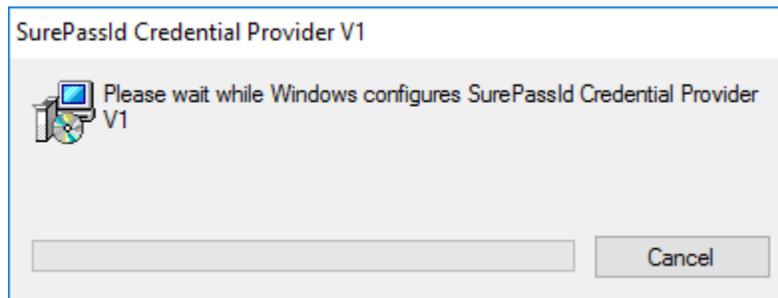


Figure 1: Installation beginning

Then you will see the SurePassID Credential Provider genuine app notice.

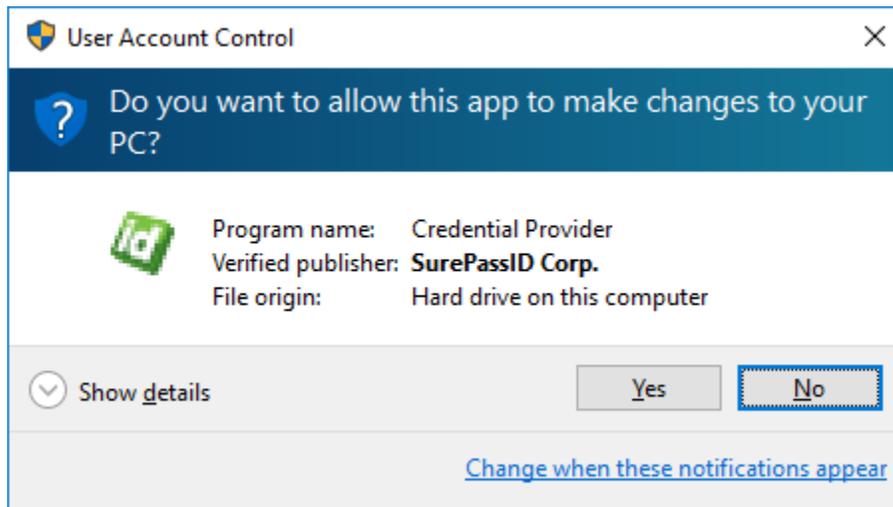


Figure 2: Genuine App Notice

Press the **Yes** button and you will see the SurePassID Credential Provider Setup form.

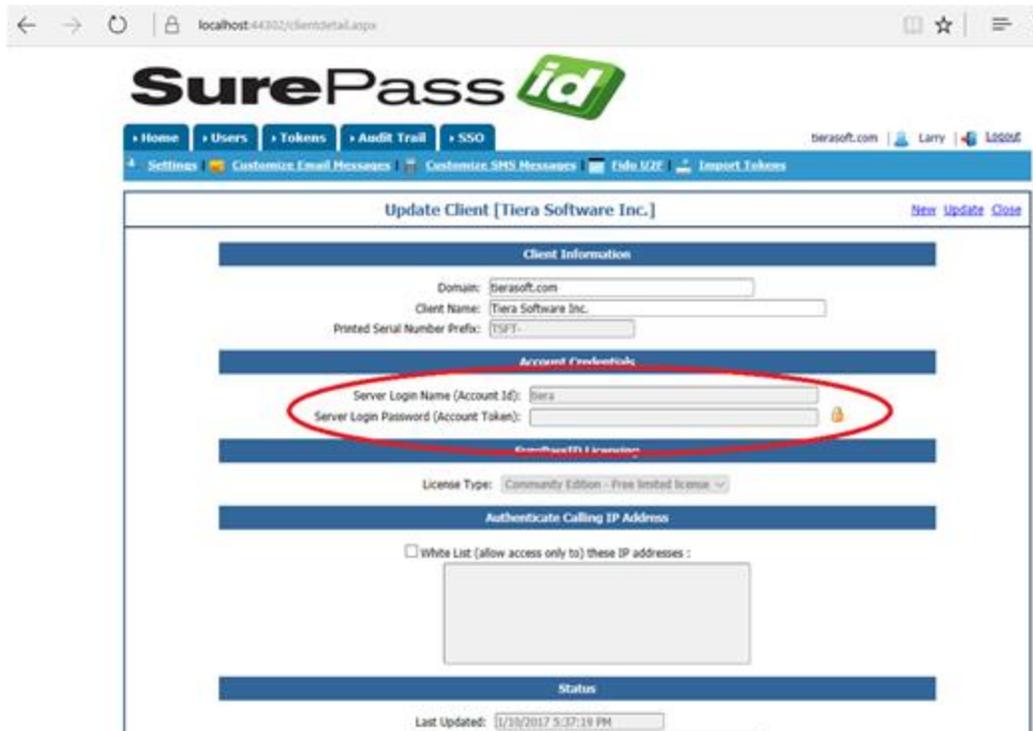
The screenshot shows the 'SurePassID Credential Provider Setup' application window. It is divided into two main sections: 'Configuration' and 'Activity Log'.
Configuration Section:
 - Server Login Name (Account Id): Tiera
 - Server Login Password (Account Token): [Redacted]
 - SurePassID Server Endpoint URL: sandbox (with a 'Test' button)
 - Server Communication Timeout (secs): 8
 - Master Passcode Override: [Redacted] FidoU2F AppId: https://fidocert.surepassid.com
 - Offline Security: Single Factory Only Auto Authentication Method: None
 - Oath Authentication Methods: Send Passcode Via Sms Send Passcode Via Email Passcode Via Voice Call
 - Push Authentication Methods: Sms Verification SurePassId Mobile App (SMS) SurePassId Mobile App
Activity Log Section:
 - Registry settings found.
Bottom Buttons: Save, Quit, Import, Export

Figure 3: Installation App: Specify Install 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.

You can get the **Server Login Name** and **Server Login Password** 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/

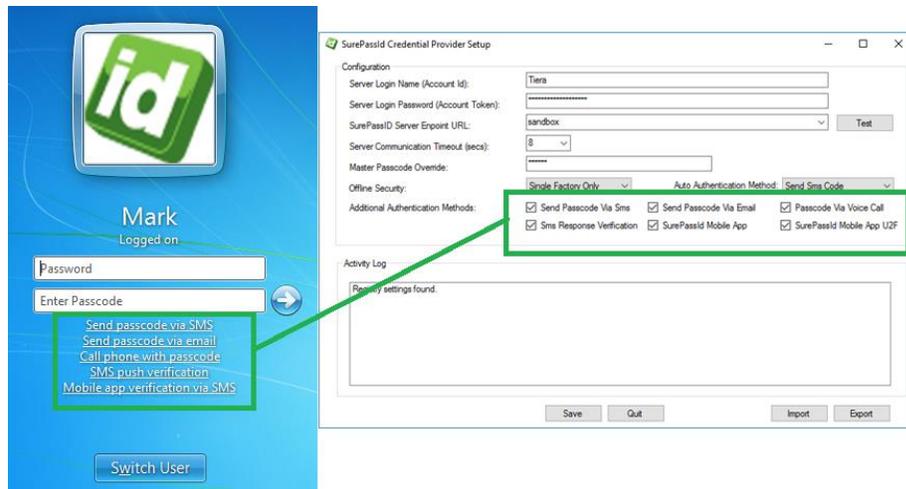
For convenience, the following abbreviations can be used as well:

- **Sandbox** – The SurePassID test cloud service
- **Production** – The SurePassID production cloud service
- **Master Passcode** – The code that can be used for the 2FA authentication One Time Passcode.
- **FIDO U2F Appld** – The FIDO Appld 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.
- **Test** button – Verify the connection and credentials (Server Login Name, Server Login Password) to the SurePassID Server installation.
- **Export** button – Export configuration to an export file. This option is only available after successful installation and you are running the app in standalone mode.
- **Import** button - Import the configuration information from a previously exported configuration file using the **Export** button.
- **Offline Security** –
 - **Single Factor Only** will allow the system to fall back to single factor (username and password only).

We strongly discourage the use of this option.

- **Require 2FA** demands that the user uses an offline 2FA method such as mobile OTP, Key Fob or FIDO U2F device.
- **Auto Authentication Method** – The selected authentication method will be triggered when the user receives the login screen. For instance, if you set this to “When user first receives the login screen”
- **Additional 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:
 - Send Passcode via SMS
 - Send Passcode via Email
 - Passcode via Voice Call
 - SMS Response Verification
 - SMS Text OTP (deprecated by NIST)
 - SurePassID Mobile App U2F

The Windows login screen is dynamically built for each user based on the parameters shown below:



- **Start** button – Start the configuration process. When completed, the screen indicates that the SurePass Credential Provider has now been installed. You can then select the **Exit** button.

NOTE: You can run the Installation App stand-alone after installing to check the user’s configuration, import a new configuration, or export the current configuration.

To verify installation of the SurePassID Credential Provider you can review the **Installed Programs** located in the **Control Panel** app as shown below:

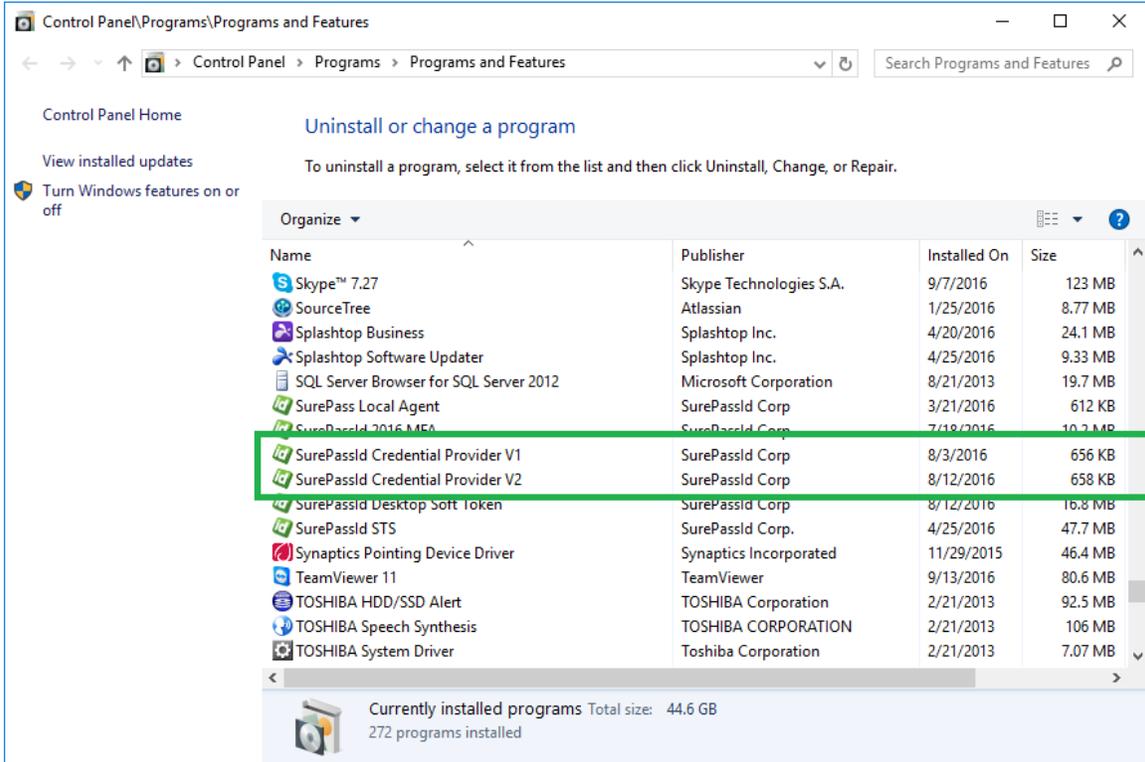


Figure 4: Installed System Component

Post Installation & Verification Steps

Before verifying the system, it is important to understand how SurePassID Credential Provider maps users Windows login credentials to SurePassID users.

IMPORTANT: The Windows login 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 2FA tokens for the user. The username is identified via the **User Name** attribute for SurePassID user account as shown below.



The screenshot shows the 'Update User [Mark]' interface. At the top, there is a navigation bar with tabs for Home, Accounts, Users, Tokens, Audit Trail, and SSO. The current user is identified as Mark Poid. Below the navigation bar, there are buttons for Update, Member Of Group, and Import Users. The main content area is titled 'Update User [Mark]' and includes links for New, Update, Close, Email, Login, and Info. The 'Login Credentials' section is highlighted with a green border and contains a 'User Name' field with the value 'Mark' and a 'Password' field.

In addition to manually adding a user to SurePassID, there are many options to import users (and their 2FA 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.

Verifying Installation for Windows 7 and Windows 2008

After installing the product and then logging out/locking/switching users, you should see the following images:

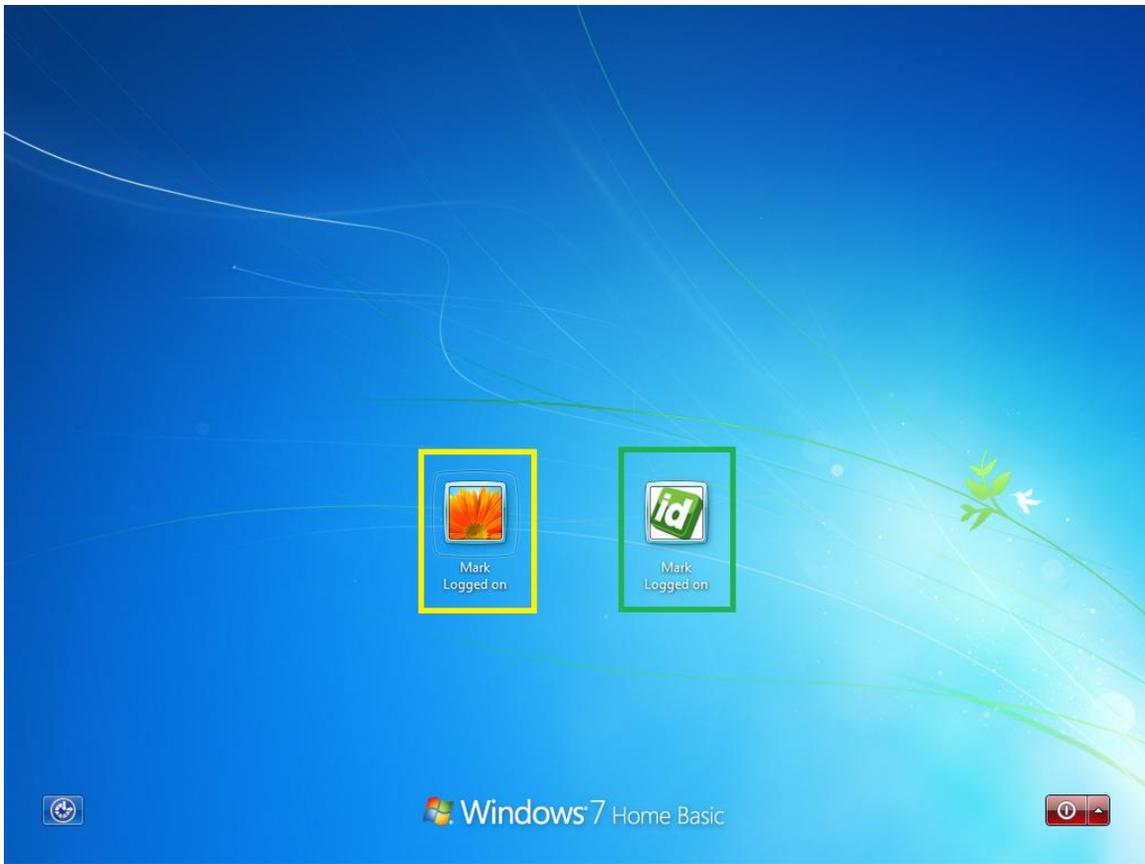


Figure 5: Windows 7 Login Screen

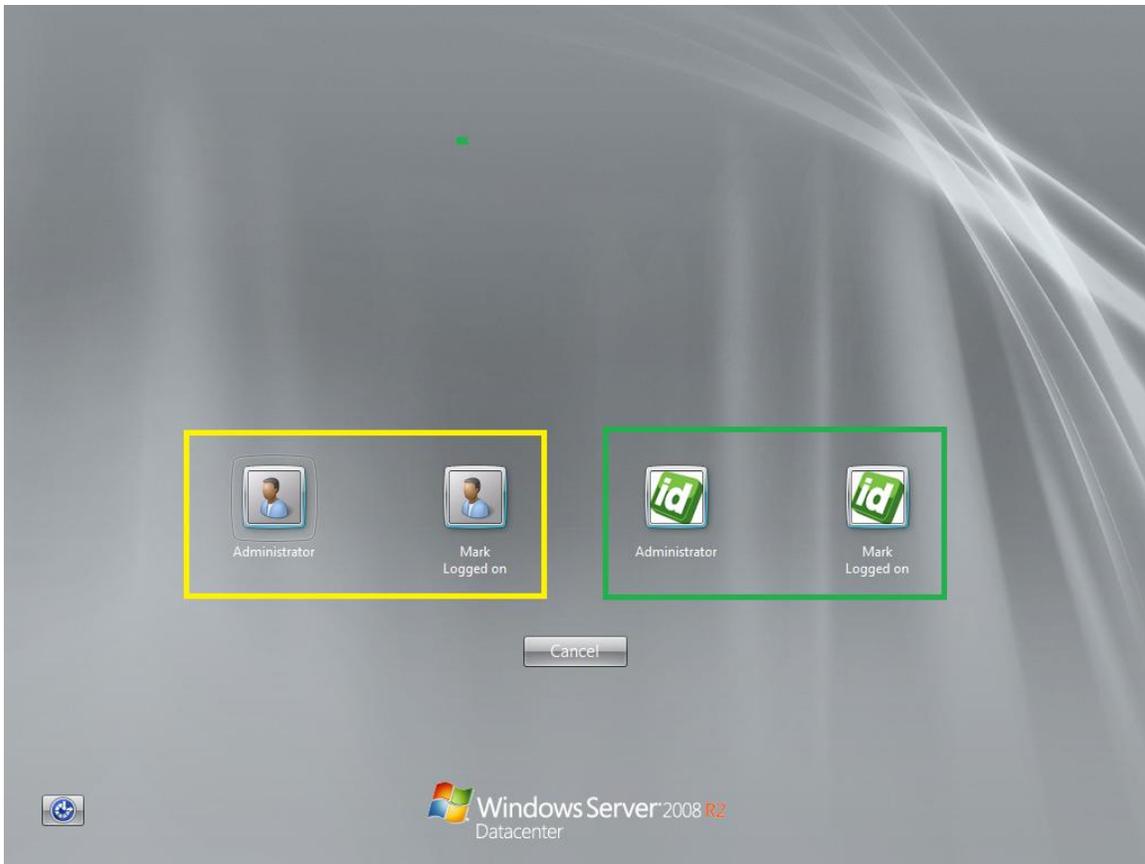


Figure 6: Windows Server 2008 Login Screen

The SurePassID login tile (green border) is added as an option in addition to the standard Windows username & password (yellow border).

NOTE: to eliminate the standard username and password option see the following section: [Enforce SurePassID Two Factor Authentication for Windows Server 2008 and Windows 7](#).

Select a SurePassID login tile to display the SurePassID login screen:



Figure 7: Windows 7 SurePassID Login Screen

To login, enter your password and two factor passcode. If you have a two factor key fob enter the number on the key fob. If you have a SurePassID Treo, position the cursor over the passcode field and tap the button on the Treo. If you have a mobile OTP app, enter the code from your mobile phone app or you can request a code via the menu items. In this case, press the button on your Treo and the passcode is filled into the Enter Passcode field as shown below:



Figure 8: Windows 7 SurePassID Login Screen Credentials

Press the login submit button (white arrow in blue circle) to complete the secure login process.

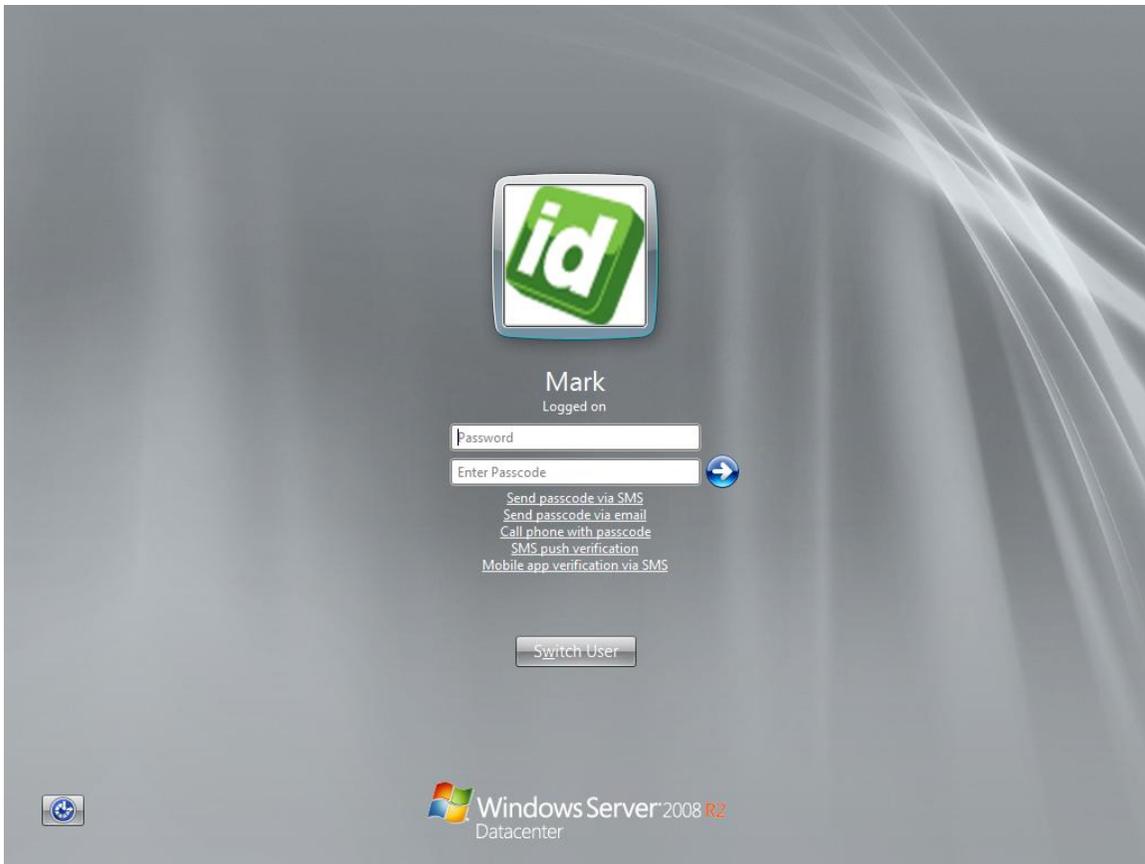


Figure 9: Windows Server 2008 Login Screen

To login, enter your password and two factor passcode. If you have a two factor key fob, enter the number on the key fob. If you have a SurePassID Treo, position the cursor over the passcode field and tap the button on the Treo. If you have a mobile OTP app, enter the code from your mobile app or you can request a code via the menu items. In this case, press the SMS push verification:

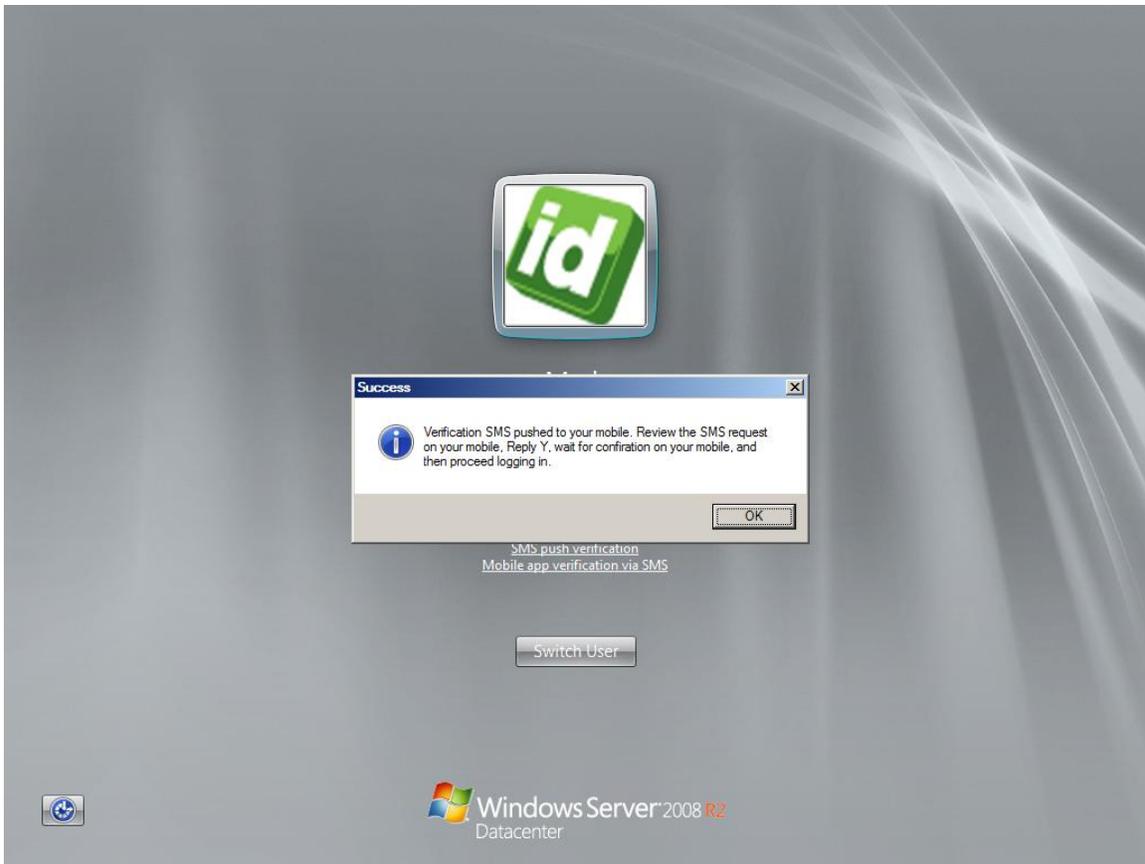


Figure 10: Windows Server 2008 Login Screen SMS Verification

You will receive the SMS verification confirmation request. Click **Ok** and wait for the verification SMS message on your mobile.

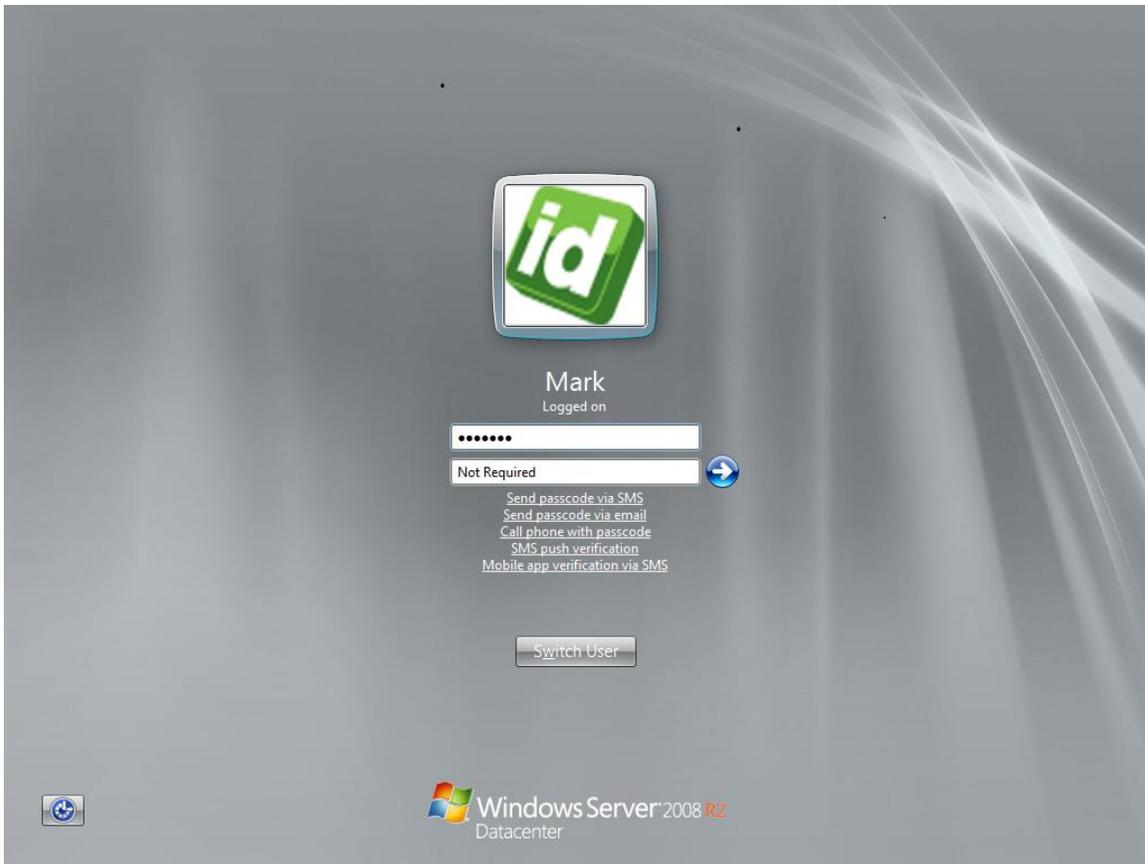


Figure 11: Windows Server 2008 Login Screen Credentials

After receiving and approving the verification SMS message on your mobile, press the login submit button (white arrow in blue circle) to complete the secure login process.

Verifying Installation on Windows Server 2012, Windows Server 2016, Windows Desktop 8.1, and Windows Desktop 10.1

After installing the product, log out, 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, Windows 10.

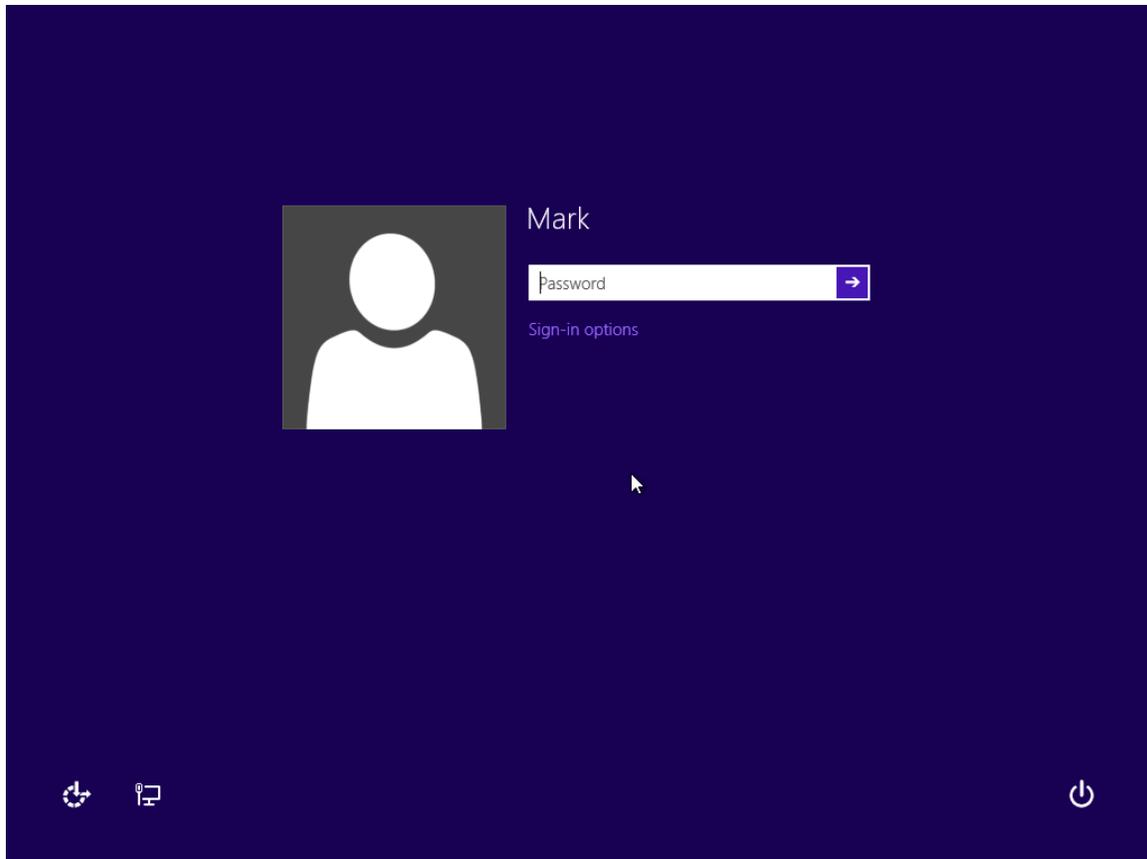


Figure 12: Windows Desktop 8.1, Server 2012 Login Screen

Press the *Sign-in options* link. The screen will be updated to include all available sign-in options. The SurePassID login option is highlighted below.

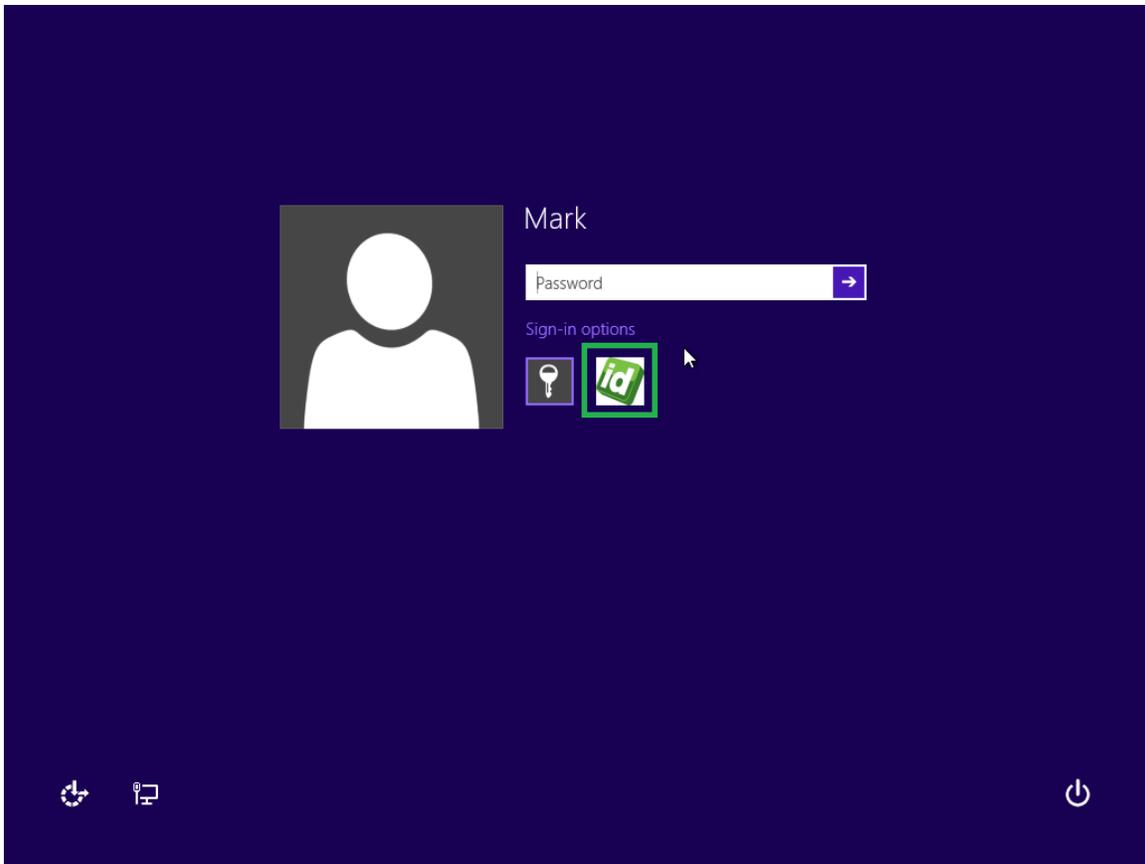


Figure 13: Windows Desktop 8.1, Server 2012 SurePassID Login Screen

Press or click on the SurePassID tile. The SurePassID login screen will be shown below.

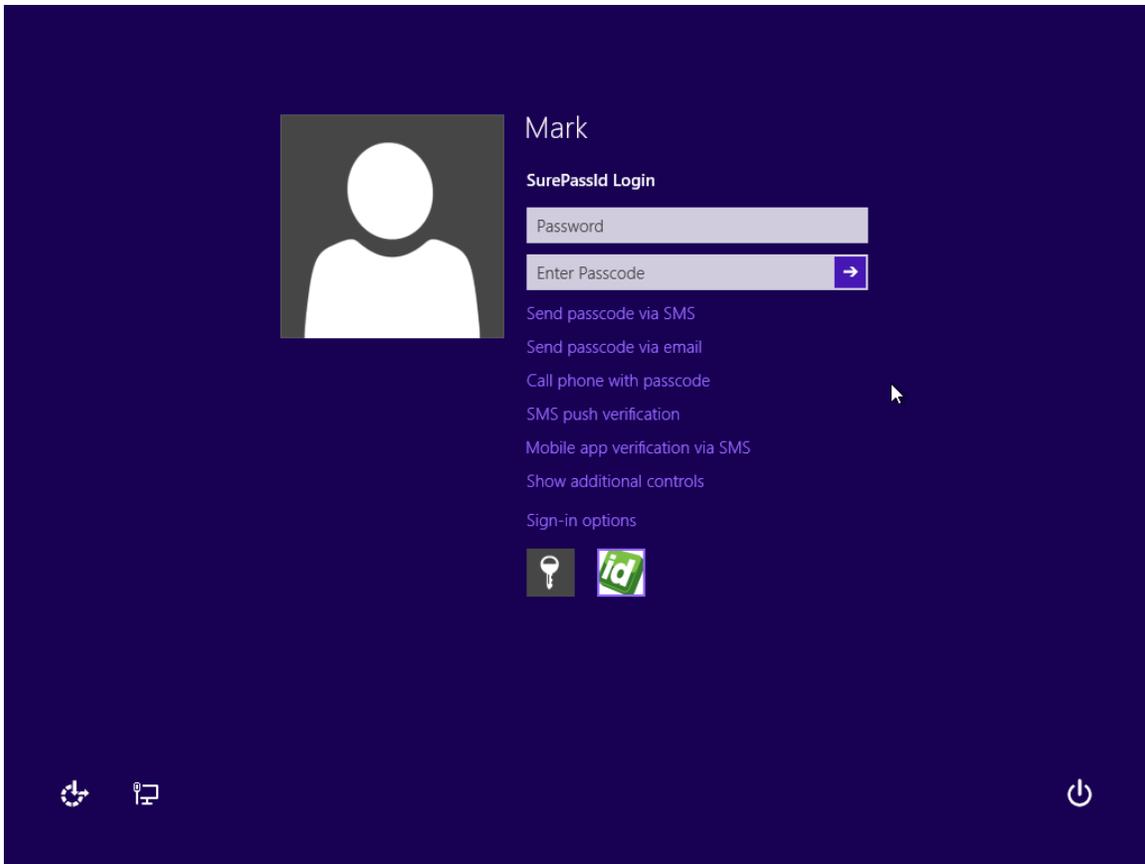


Figure 14: Windows Desktop 8.1, Server 2012 SurePassID Login Screen

To login, enter your password and two factor passcode. If you have a two factor key fob, enter the number on the key fob. If you have a SurePassID Treo, position the cursor over the passcode field and tap the button on the Treo. If you have a mobile OTP app, enter the code from your mobile or you can request a code via the menu items. In this case, press the button on your Treo and the passcode is filled into the Enter Passcode field as shown below:

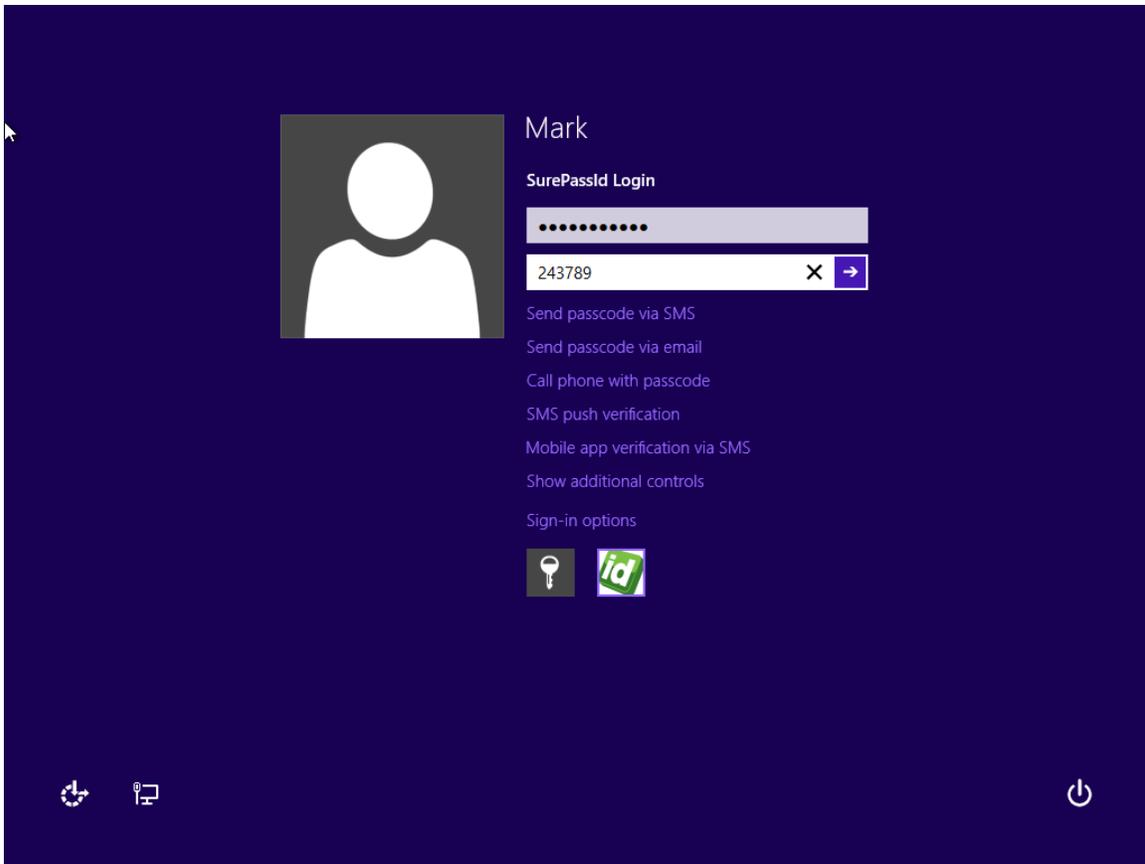


Figure 15: Windows Desktop 8.1, Server 2012 SurePassID Login Credentials

Press the login submit button (arrow) to complete the secure login process.

Enforce SurePassID Two Factor Authentication for Windows Server 2008, Windows Desktop 7

Disabling other logon methods to enforce SurePassID 2-Factor Authentication: Registry

Download, unzip and run the following registry script:

https://sandbox.surepassid.com/downloads/CP_V1/SurePassCP_V1_RegisterFilter.zip

When you log into the system next time, the login screen will only show the SurePassID tile as shown below:

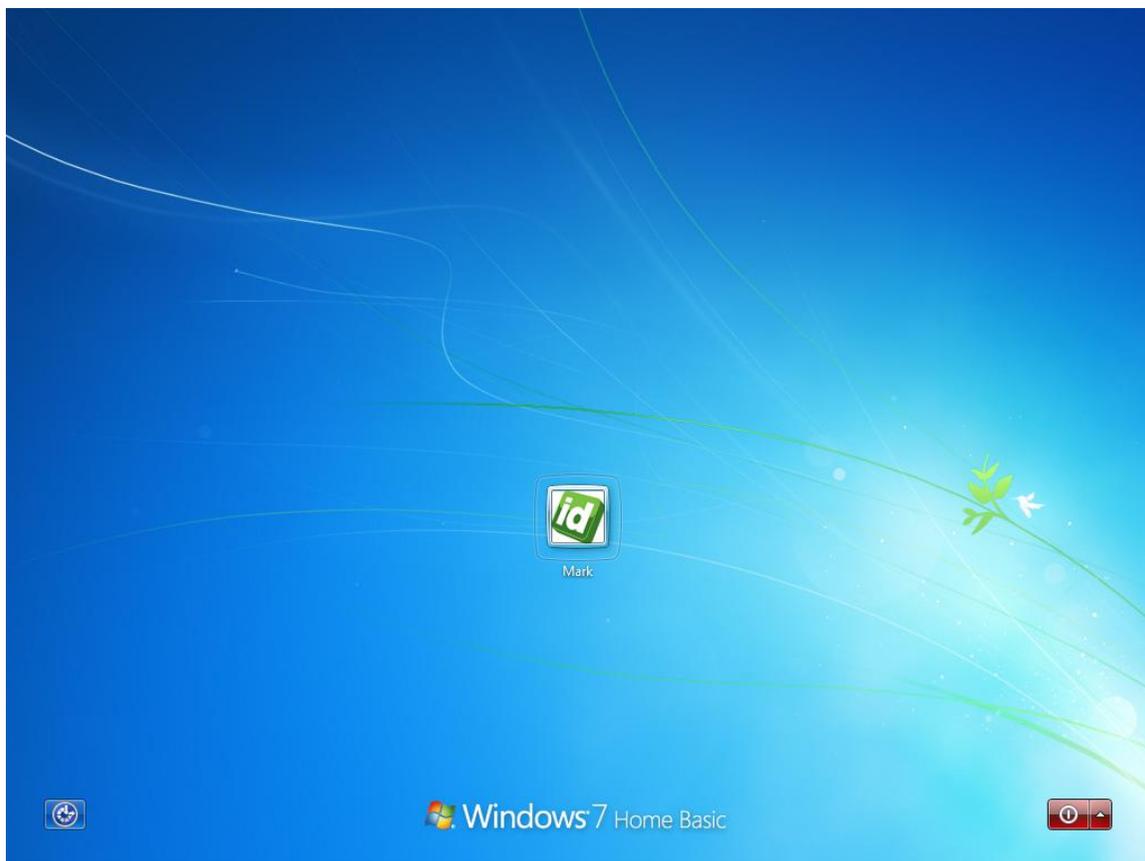


Figure 16: Windows 7 SurePassID Only Login Screen

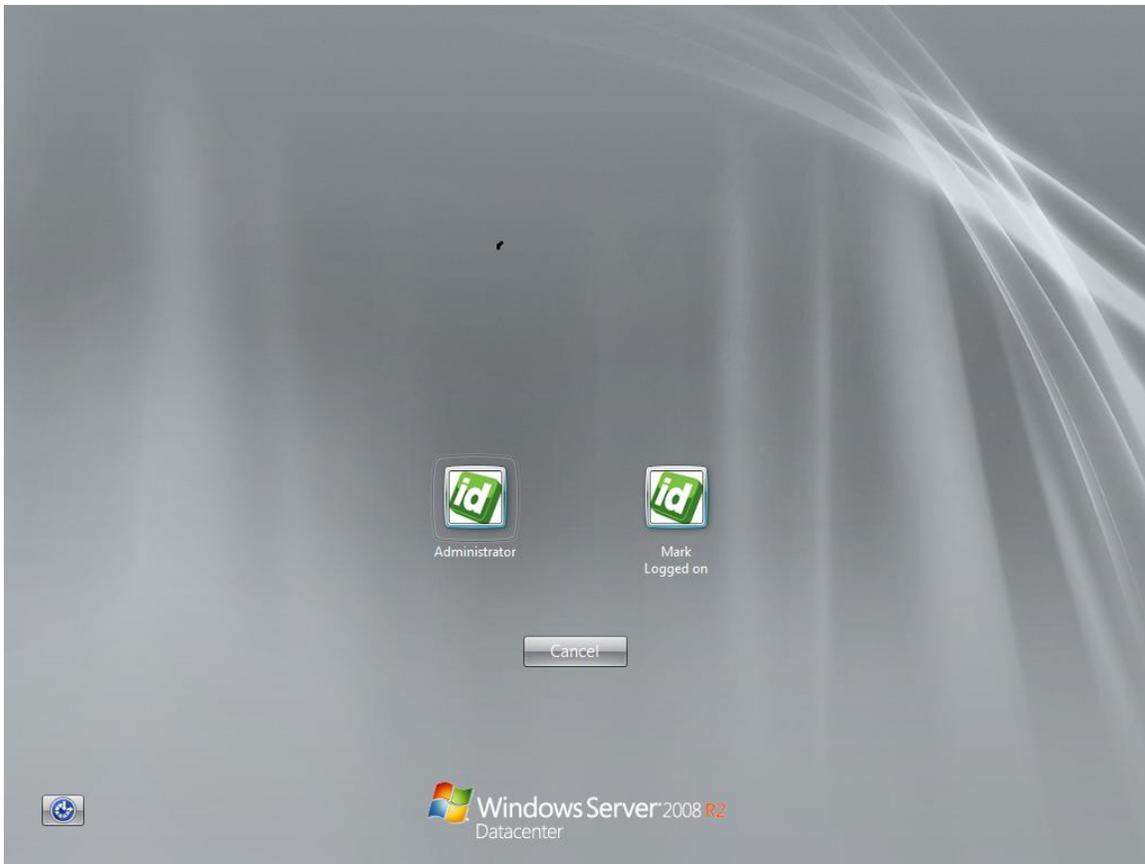


Figure 17: Windows 2008 SurePassID Only Login Screen

Enforce SurePassID Two Factor Authentication For Windows Server 2012, Desktop 8.1, and Desktop 10.1

Disabling other logon methods to enforce SurePassID 2-Factor Authentication: Method 1 Registry

https://sandbox.surepassid.com/downloads/CP_V2/SurePassCP_V2_RegisterFilter.reg

Disabling other logon methods to enforce SurePassID 2-Factor Authentication: Method 2 Group Policy Edit

1. Open **gpedit.msc**
2. Navigate to **Local Group Policy Editor > Computer Configuration > Administrative Templates > System > Logon > Exclude credential providers**

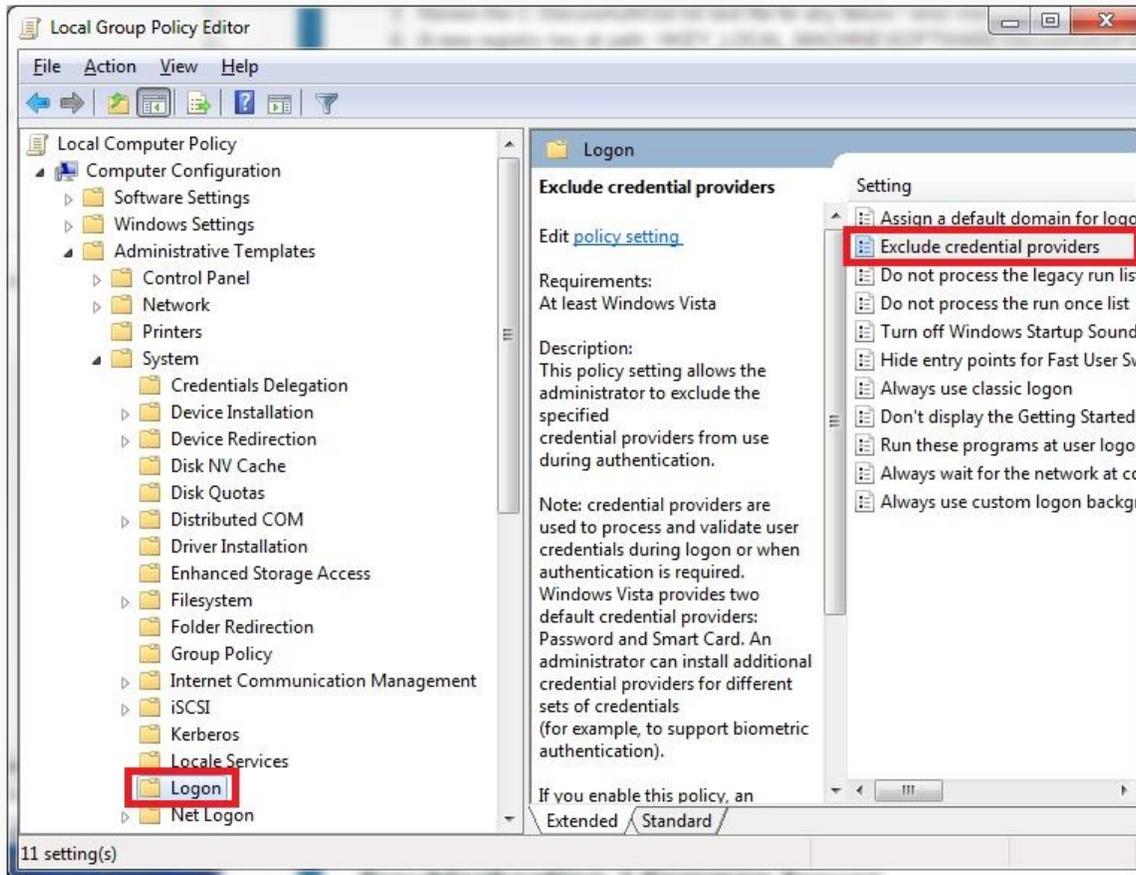


Figure 18: Group Policy Editor: Disable Credential Providers

3. Select **Enable** and then add the following string to exclude the following standard single factor (username and password) login:

{60b78e88-ead8-445c-9cfd-0b87f74ea6cd}

You can also add the following strings to disable all credential providers such as Smartcards, biometrics, etc. if they are currently active.

**{1b283861-754f-4022-ad47-a5eaaa618894},
 {1ee7337f-85ac-45e2-a23c-37c753209769},
 {2135f72a-90b5-4ed3-a7f1-8bb705ac276a},
 {25CBB996-92ED-457e-B28C-4774084BD562},
 {3dd6bec0-8193-4ffe-ae25-e08e39ea4063},
 {600e7adb-da3e-41a4-9225-3c0399e88c0c},
 {8FD7E19C-3BF7-489B-A72C-846AB3678C96},
 {94596c7e-3744-41ce-893e-bbf09122f76a},
 {BEC09223-B018-416D-A0AC-523971B639F5},
 {cb82ea12-9f71-446d-89e1-8d0924e1256e},**

{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435},
{F8A0B131-5F68-486c-8040-7E8FC3C85BB6},
{503739d0-4c5e-4cfd-b3ba-d881334f0df2},
{6f45dc1e-5384-457a-bc13-2cd81b0d28ed},
{8bf9a910-a8ff-457f-999f-a5ca10b4a885},
{AC3AC249-E820-4343-A65B-377AC634DC09}

IMPORTANT NOTE: If you have any questions, contact SurePassID support. It is very important that you get this registry change correct. If you do not, you could lock yourself out of the system. It is recommended that your first test be on a virtual machine and that you first do a system snapshot of the virtual machine before installing so you can always restart in the previous state.

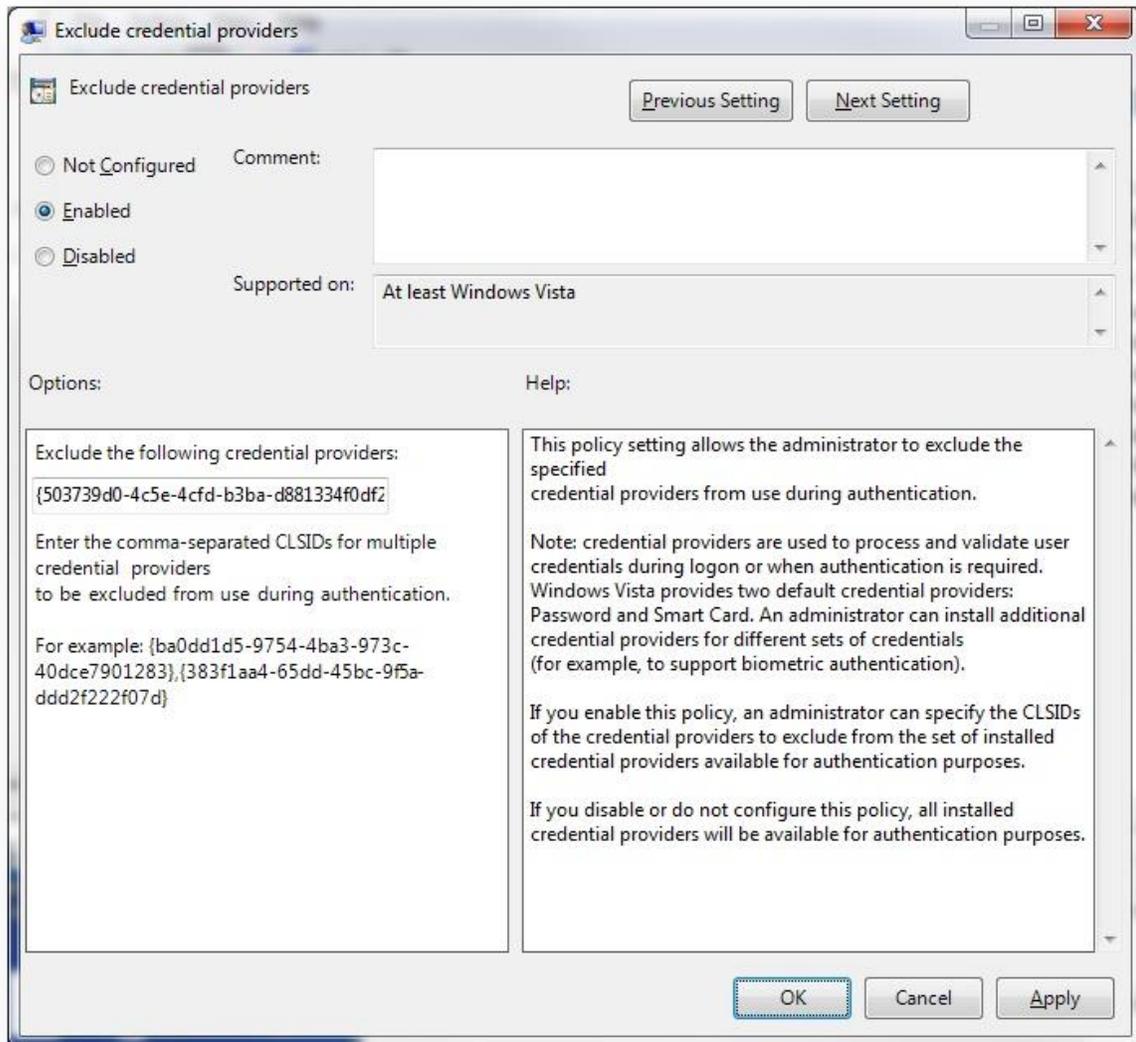


Figure 19: Group Policy Editor: Save Disabled Credential Providers

4. Click **Apply**
5. Click **OK**

Deploying Credential Provider

You have several options in deploying Credential Provider. The first thing you should do is install the credential provider on a test machine, get everything configured to your requirements and verify it is working properly.

Preferably, the first install will be on a virtual machine with the target operating system. If using a virtual machine, take a snapshot of the operating system prior to installing. If something goes wrong, you can revert back to the clean operating system and start again.

The following list is in the least to most desirable deployment options:

- **Manual** - Install the system on each user's computer and manually set the configuration settings.
- **Export/Import** - Configure a single Windows system (on a VM) as the gold standard and then easily replicate to all other machines in the network by exporting the settings to a file that is on a shared drive. When you install the credential provider on a Windows machine, you then import the gold standard settings from the export file located on a shared drive.
- **System Image Burn** - Install and configure the system in the same manner as the **Export/Import** method except that you install the credential provider onto your user system image; the one that is used to stage all new Windows machines. In this way, the credential provider will be set-up by default on each new user's machine.
- **System Image Burn Copy** – Copy the required executable files, install registry entries onto your user system image - the one that is used to stage all new Windows machines. In this way, the credential provider will be set-up by default on each user's machine.
- **Silent Install & Microsoft SCCM** – Use the same technique as **Export/Import** method describe previously to create you gold standard settings file and place that file on a shared network path that is accessible to all of your users, run the SP installer silently using the settings file. The command line syntax to do this is as follows (the command is case sensitive):

```
<sp_installer_exe> /quiet IMPORT_PATH=<import settings path>  
PASSCODE=<file_passcode>
```

<sp_installer_exe> is the installer file. Specify SurePassCP64_V1.exe for the Windows 7/2008 and SurePassCP64_V2.exe for Windows 8,10,2012, 2016.

IMPORT_PATH is required and **<import_settings_path>** is the full path to the export file including file extension.

For example:

\\sysadmin\Installers\Approved_Index\SurePass\CP64\user_conf\file.txt

PASSCODE is optional and only required if the configuration file was encrypted when it was exported. **<file_passcode>** is the encryption passcode for the file.

Once you have verified that the command line runs as expected and installs the system correctly, you can use Microsoft SCCM to push this app out as you would any other application.

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 and assistance and guidance will be provided.

Offline Operations

SurePassID credential provider offline operations. 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 two types of offline authentication:

- OATH Event based
- FIDO U2F

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 device assigned to their account. The device can be any mobile OTP 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 U2F Considerations

How do I log in using a FIDO U2F key?

To login using a FIDO U2F key, enter your username and password and click the login submit button (usually an arrow). If your username and password is correct, and with your FIDO U2F device plugged in, the FIDO U2F device will flash, 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 U2F key?

FIDO U2F 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 U2F terminology as the Appld. The process to use a FIDO U2F key is a two-step process for the user:

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

The SurePassID credential provider provides the second part of the process allowing the user to login into Windows using their FIDO U2F key. This raises the following question:

How can the user register their FIDO U2F key and what appld should I use since this is not a web-based login?

The answer to these two questions are related. First, there are many ways to register a FIDO U2F device with SurePassID. We offer APIs that allow you to build many different ways to register a FIDO U2F 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 Credential provider, you would set the **FIDO U2F Appld** to the website origin (uri) that the user registers there 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 U2F facets. In large companies with many FIDO U2F apps, it might be advantageous to use an appld that is a facet. If you are not certain about the best path for your company, contact us for assistance.