

# SurePass

## SurePassID Local Agent Guide

SurePassID Authentication Server 2022



# Table of Contents

<b>Table of Figures .....</b>	<b>4</b>
<b>Introduction.....</b>	<b>5</b>
<b>What is the SurePassID Local Agent? .....</b>	<b>7</b>
Security .....	7
System Logging .....	7
<b>Installing the Local Agent .....</b>	<b>8</b>
<b>Supported RADIUS Systems.....</b>	<b>17</b>
<b>Configuring the RADIUS Server .....</b>	<b>17</b>
Timeouts and Retries .....	27
Fortinet Notes.....	28
Example 1 – Login Using Single-Factor .....	30
Example 2 – Login Using Code from Hard or Soft Token .....	30
Example 3 – Login Using Sending OTP via SMS, Email or Voice Code .....	31
Example 4 – Login Using SMS Question .....	34
Example 5 – Login Using Push Authentication .....	35
Example 6 – Login Using Push Voice Call.....	35
<b>Configuring the Directory Sync Application.....</b>	<b>37</b>
<b>Configuring the Event Log Sync Application .....</b>	<b>38</b>
Running Event Log Sync.....	39
REST API Sync to SurePassID.....	43
Event Log Sync app will sync events using the SurePassID REST API. ....	44
Direct Connect Sync to SurePassID .....	44
Command line Options for SurePassID REST API Sync .....	45
Command line Options for SurePassID Direct Connect Sync.....	45
Deployment Configurations.....	46

Security Considerations ..... 47

© 2013-2022 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

+1 (888) 200-8144

[www.surepassid.com](http://www.surepassid.com)

# Table of Figures

Start Installation .....	9
Read End User License Agreement.....	10
Specify Install Location.....	11
Ready to Install .....	12
UAC Authorization.....	13
Installation in Progress .....	14
Setup Complete .....	15
Installed RADIUS Service .....	16
Installation Directory Tree .....	16
Start Configuration Application.....	19
RADIUS Settings.....	20
Server Endpoint .....	21
SurePassID Account Settings .....	23
User Directory .....	24
Security Options.....	25
Single-Factor VPN Login.....	30
Two-Factor Authentication with Token .....	31
Two-Factor Authentication with SMS Text Code.....	32
Two-Factor Authentication with Voice Call.....	32
Two-Factor Authentication with Email .....	33
Two-Factor Authentication with SMS Question .....	34
Two-Factor Authentication with Push Notification .....	35
Two-Factor Authentication with Voice Call Notification .....	36

# Introduction

This guide explains how to install and configure the SurePassID Local Agent to meet your organization's security needs. The purpose of this guide is to provide a reference for system administrators.

This guide provides information on the following topics:

- **What is SurePassID Local Agent?**
  - A brief introduction to the SurePassID Local Agent and how it can help you get the most out of the SurePassID authentication system.
- **Installing and Configuring SurePassID Local Agent**
  - Detailed explanations for installing, configuring and maintaining the SurePassID Local Agent.

---

## Other SurePassID Guides

---

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

- [Developer API Guide](#)
- [Fido U2F Mobile API Guide](#)
- [System Administration Guide](#)
- [Local Agent Guide](#)
  - High performance RADIUS Server
  - Windows Event Log Synchronization
  - Active Directory Synchronization
- [Desktop Authenticator Guide](#)

- [Google Authenticator Guide](#)
- [SurePassID Mobile Authenticator Guide](#)
- [Mobile API Connector](#)
- [Windows Credential Provider Guide](#)
- [Self-Service Portal](#)

# What is the SurePassID Local Agent?

The SurePassID Local Agent integrates SurePassID into your existing enterprise as part of your on-premises datacenter. The SurePassID Local Agent is installed in your datacenter typically behind your firewall. The SurePassID Local Agent is comprised of the following components:

- **RADIUS Server** – A system service that allows SurePassID to authenticate users from any RADIUS-compliant system such as Microsoft Universal Access Gateway, VPN devices (Cisco, Sonic Wall, etc.), Wi-Fi Access points, etc.
- **Event Log Synchronization App** – An application that can pull SurePassID Audit Trail events and send them to external logging systems such as Windows Event Logs, Syslog, Elastic Search, synchronizing your system management tools with SurePassID.
- **User Synchronization App** – An application that can update SurePassID user information from your existing directory service. SurePassID only allows you to update information such as First Name, Last Name, Phone Number, Email, etc. SurePassID never synchronizes passwords.

## Security

SurePassID Local Agent uses transport level security (SSL) at a minimum. Optionally SurePassID Local Agent can be configured to use message level security for a higher level security. Message level security requires an X509 certificate exchange between SurePassID and your on-premises systems.

## System Logging

All of SurePassID sub-agents maintain their own system log files and write critical information to the system log. In tandem these two different event logs help you troubleshoot and repair any issues that a sub-agent system might encounter during daily operations.

# Installing the Local Agent

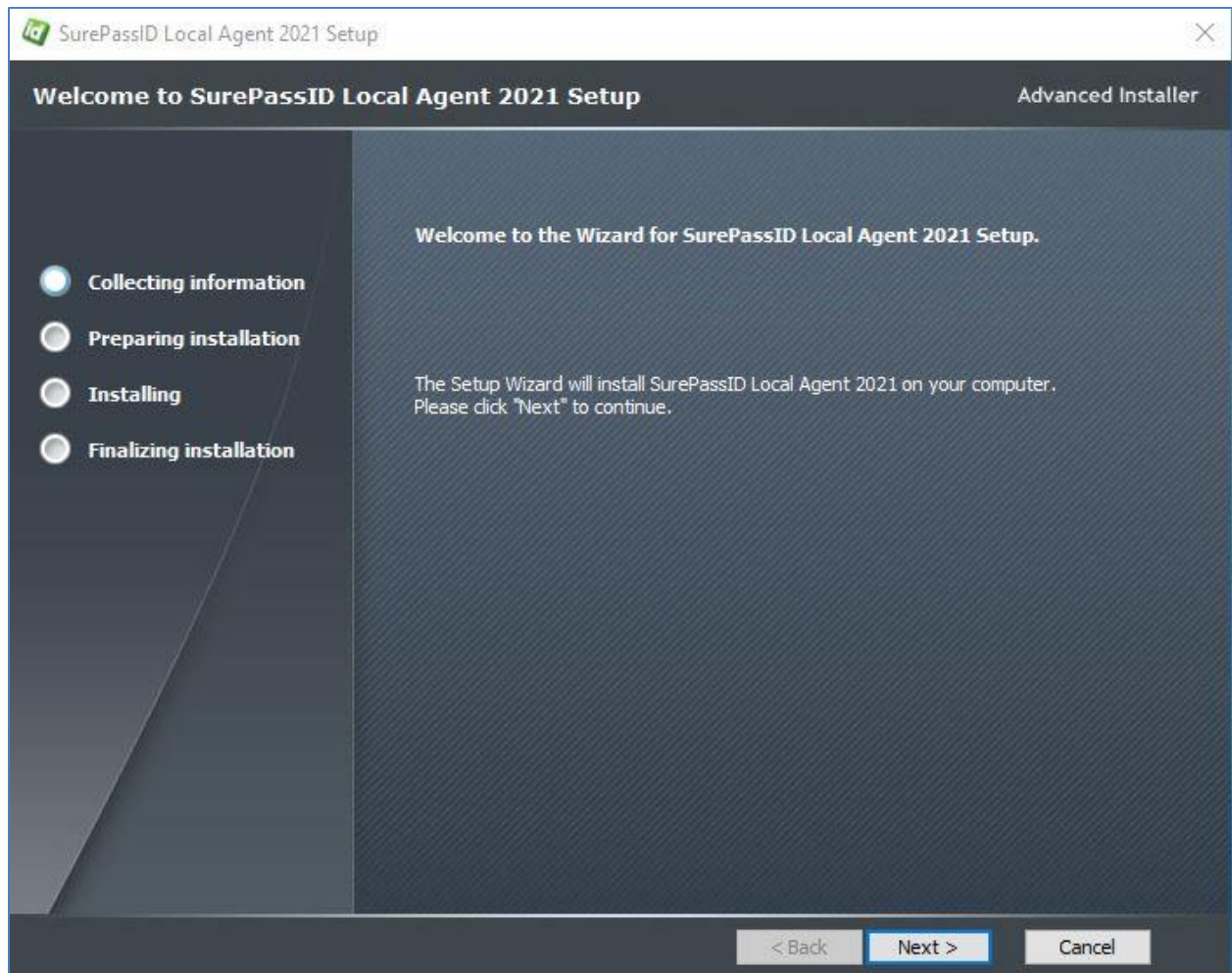
The SurePassID Local Agent installer will install all of the Local Agent components. After the SurePassID Local Agent is installed you can configure the RADIUS component using the **Configuration Manager** app that will be installed as part of the installation. The **Event Log Sync App** and **Directory Sync App** are configured by modifying parameters in their command-line arguments and configuration files.

**Note: If you require RADIUS support for linux systems you need to install and configure the SurePassID FreeRADIUS plug-in.**

To start the installation you must first download the installation file **SurePassLocalAgent.exe** to one of your Windows servers such as Windows Server 2008, Windows Server 2012 or Windows Server 2015.

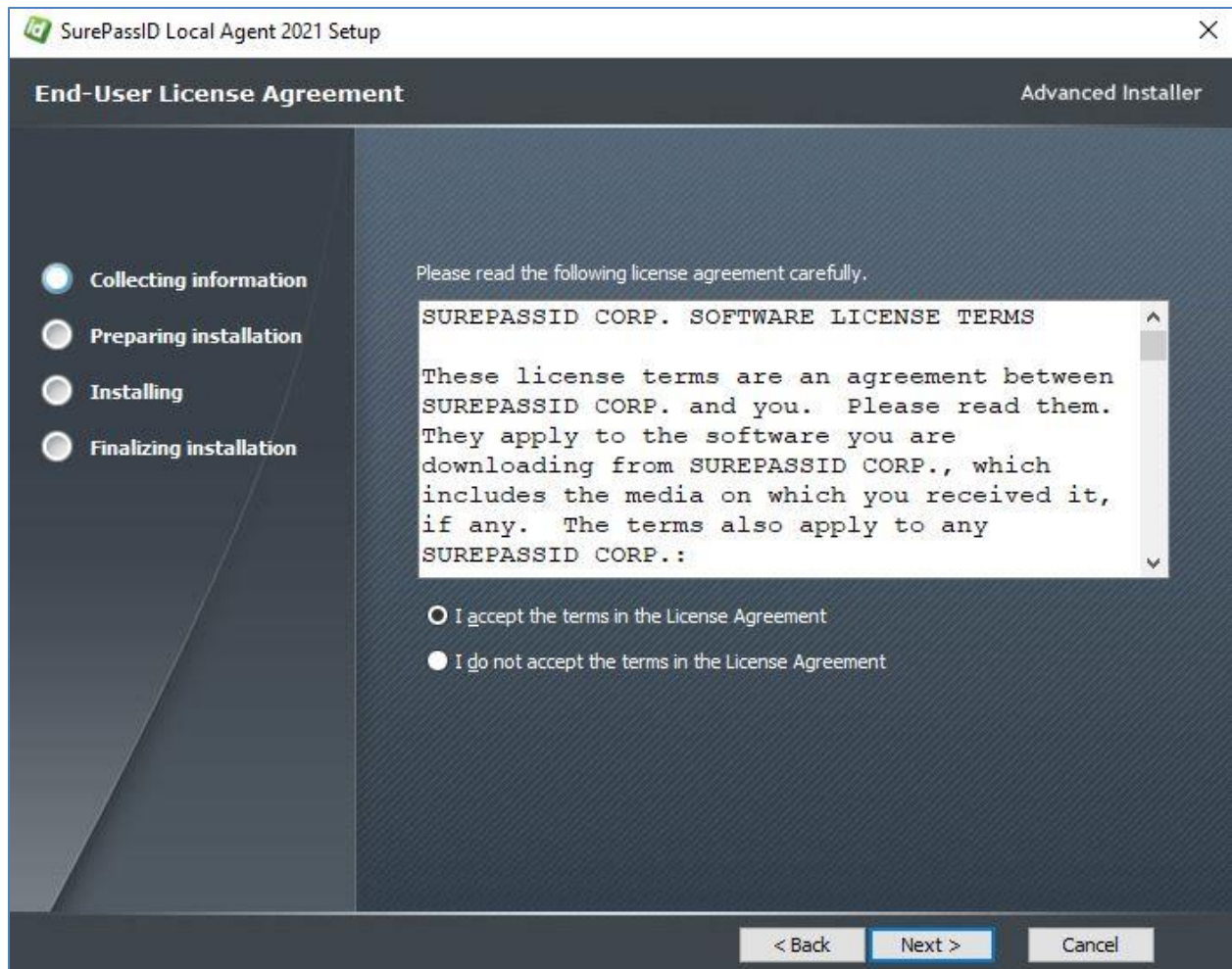
After the file has been downloaded, run **SurePassLocalAgent.exe** and you will see the following installation screen.





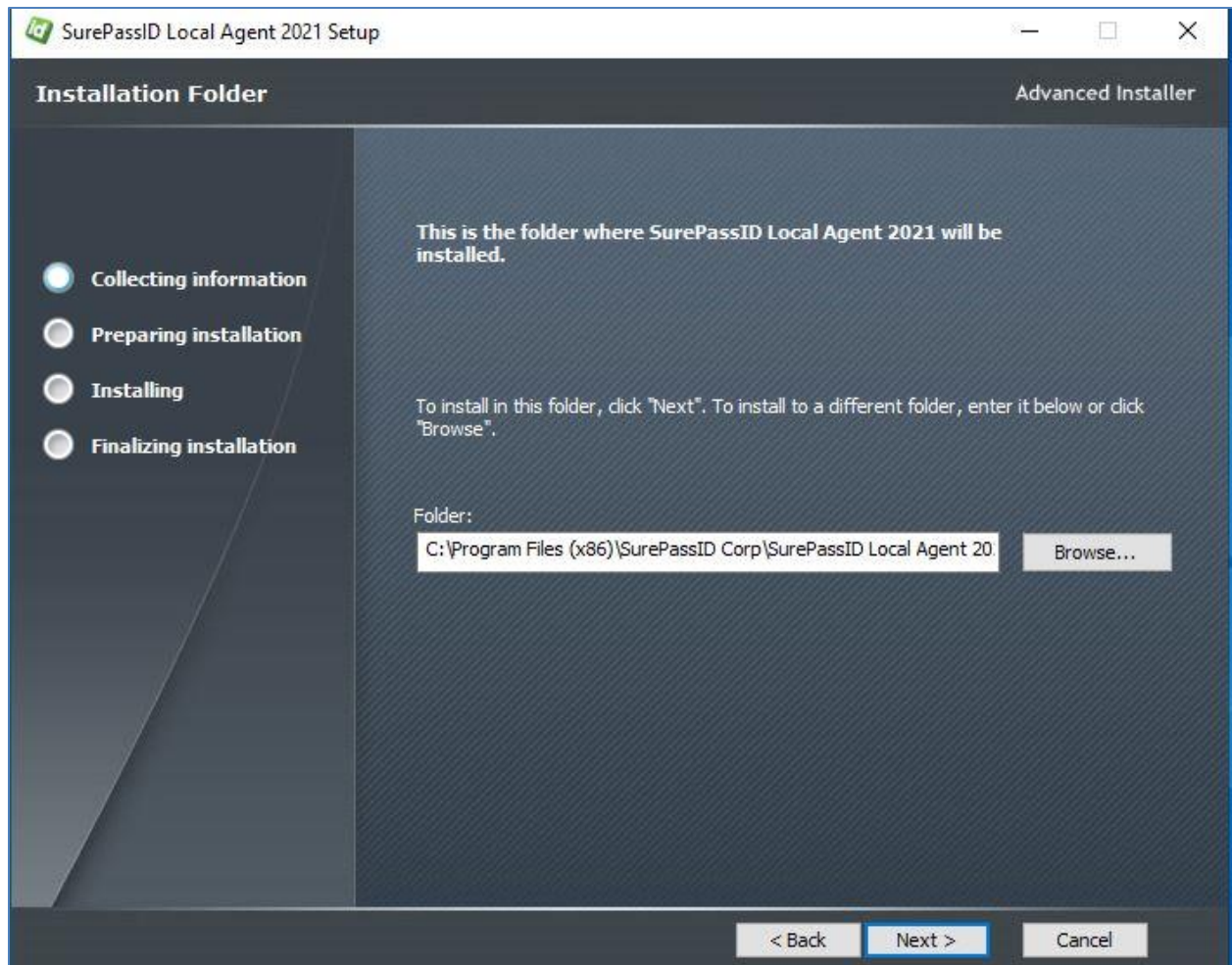
## Start Installation

Click the **Next** button.



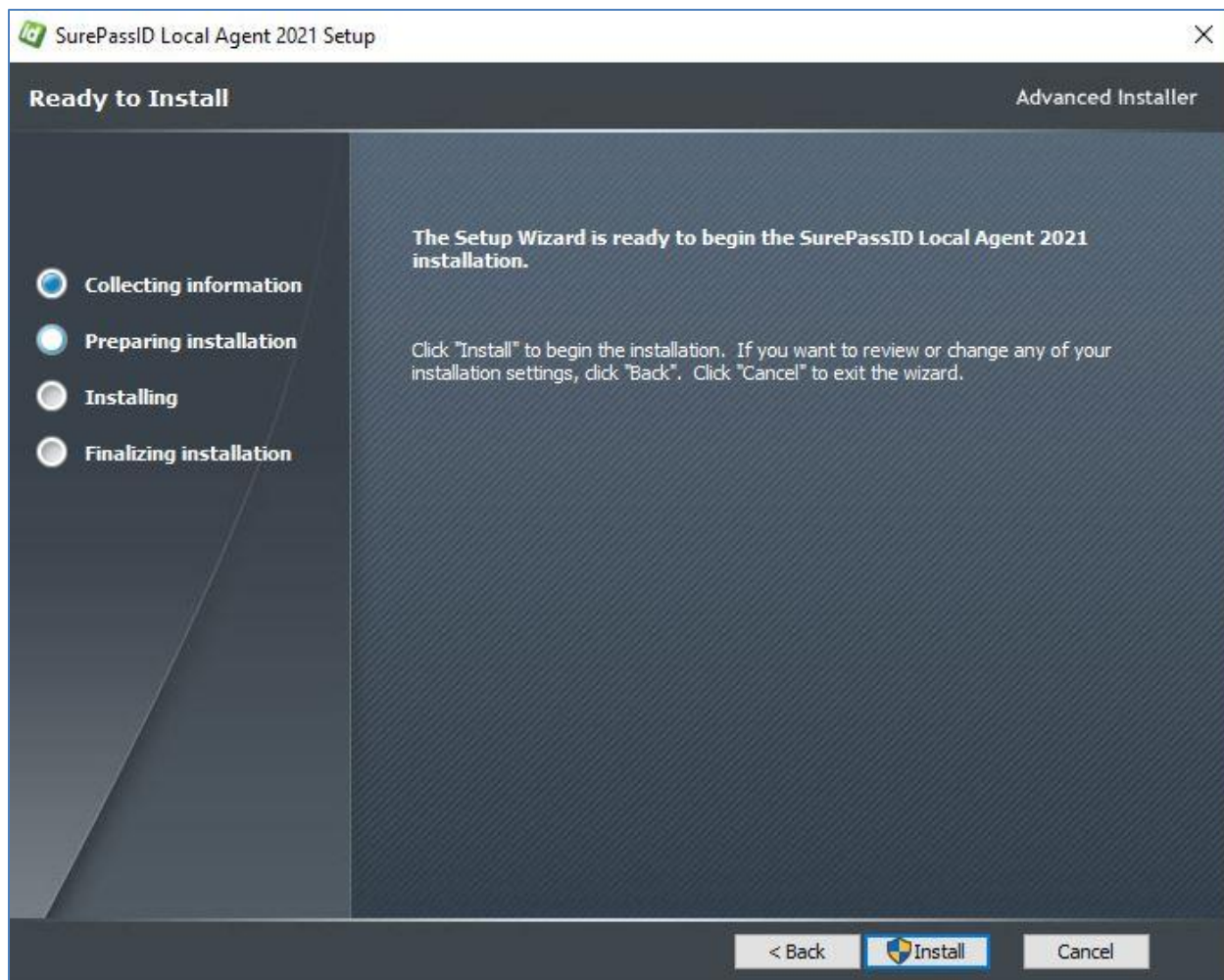
## Read End User License Agreement

Click the **Next** button.



## Specify Install Location

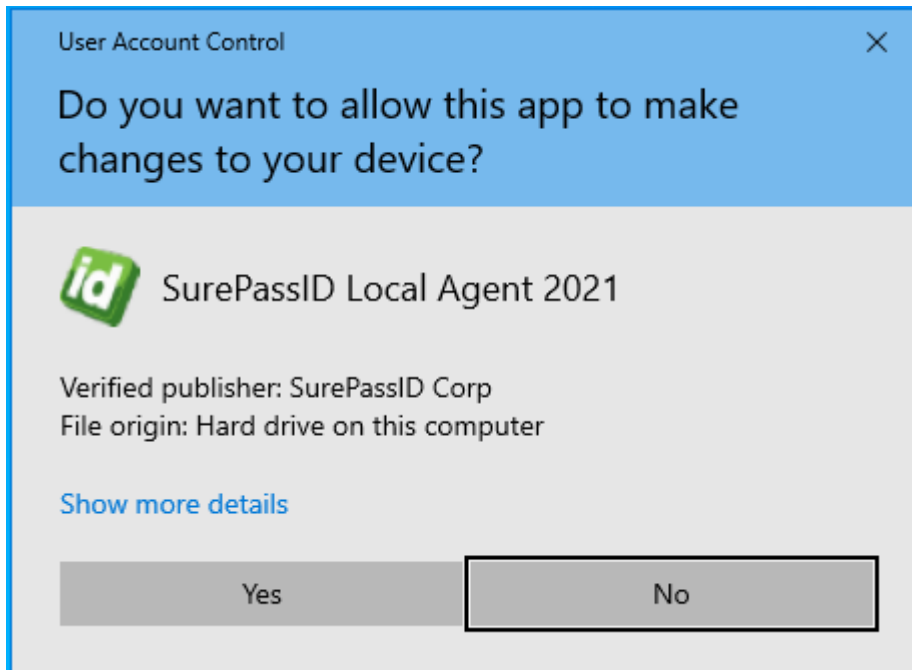
Specify the installation settings and press the **Next** button.



## Ready to Install

Press the ***Install*** button to confirm installation or select the ***Cancel*** to stop the installation. Selecting the ***Install*** button will start installing the software as shown below:

Before installing the software has been installed you will see the following screen.

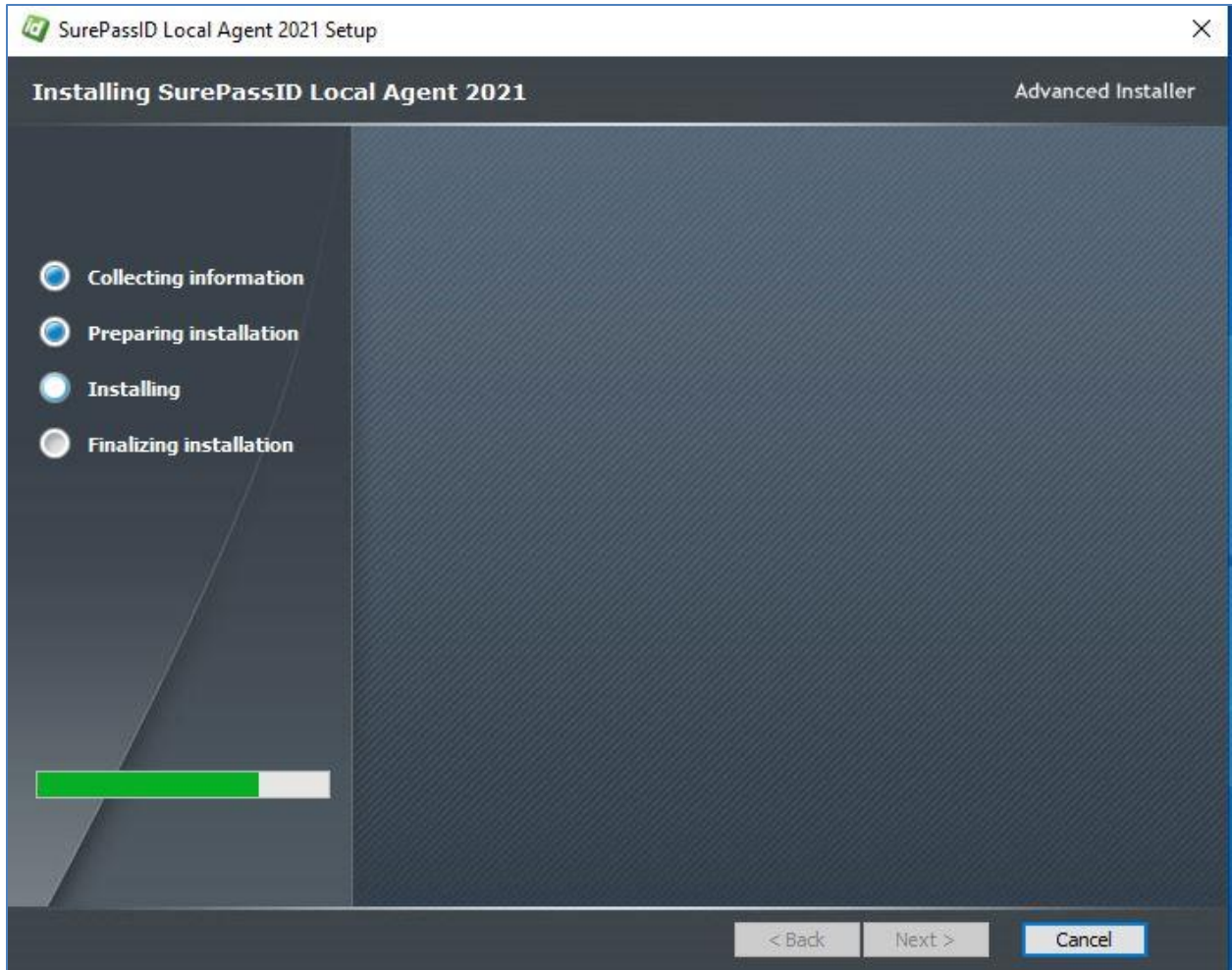


### UAC Authorization

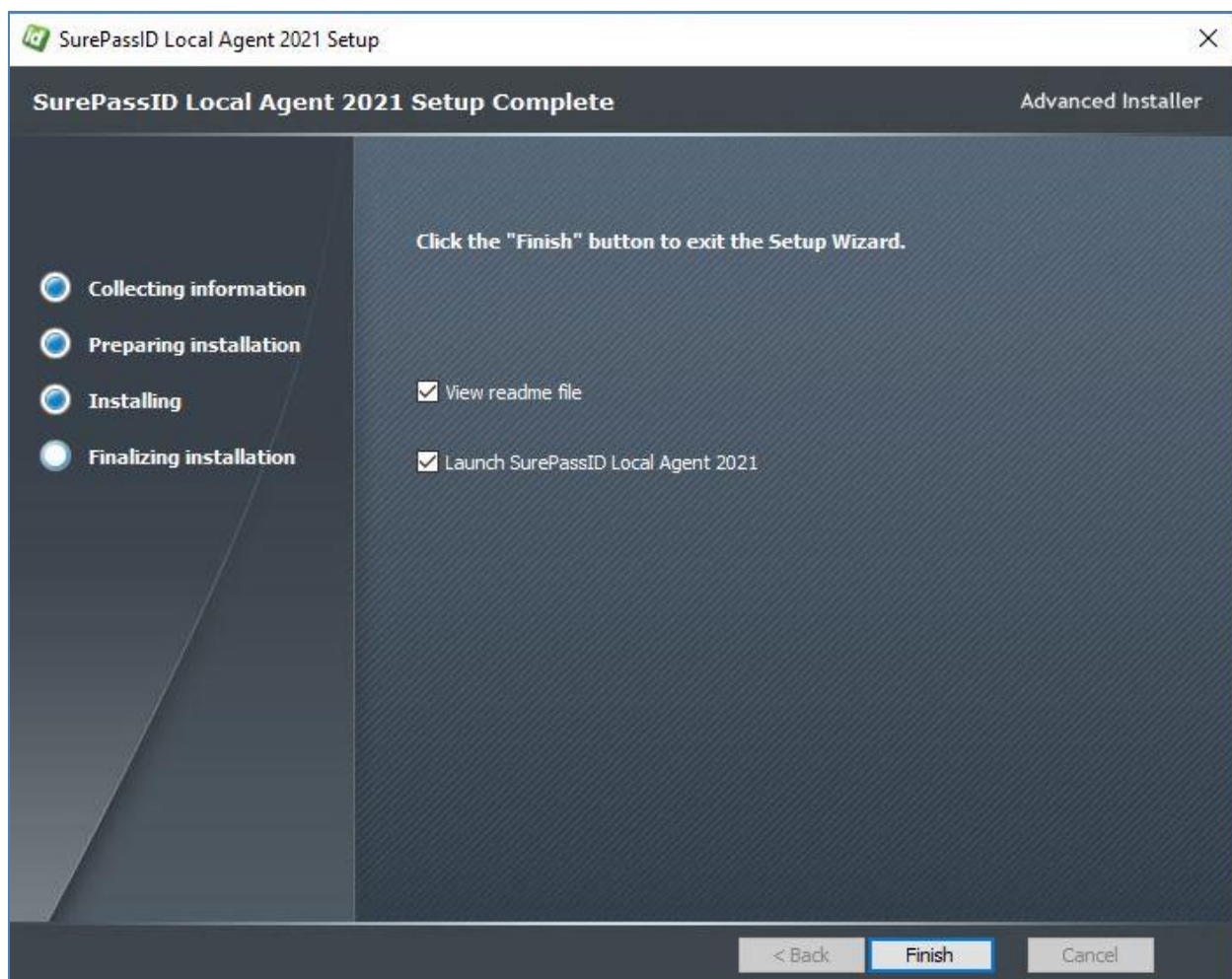
Press the **Yes** button to confirm installation or select the **No** button to stop the installation.

**If you do not see this screen then do not continue with the install.**

When the installation is complete you will see the following screen.



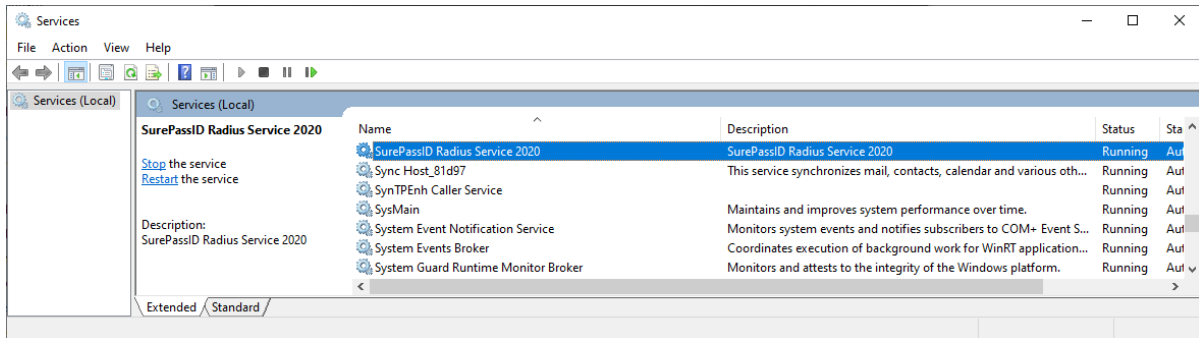
### Installation in Progress



### Setup Complete

This screen indicates that the SurePassID Local Agent has now been installed. You can select the **Finish** button.

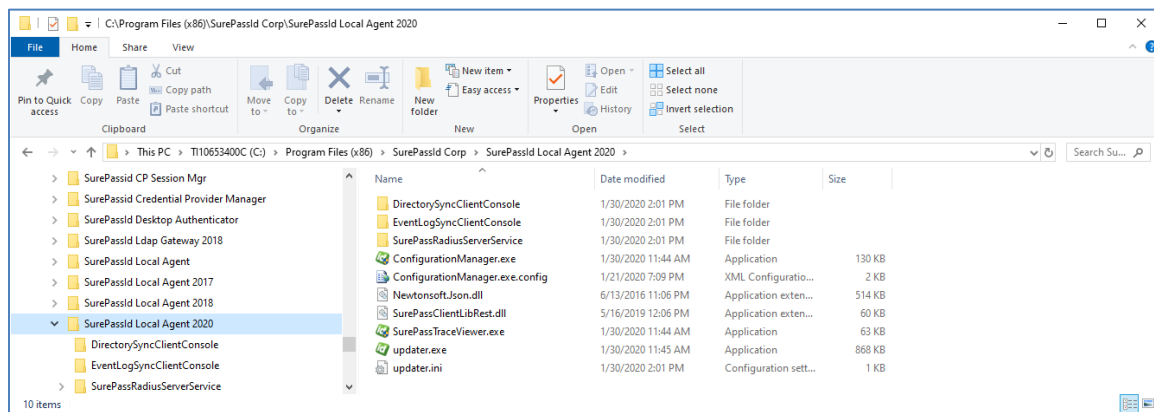
As part of the installation the SurePassID RADIUS server is installed as a Windows service as shown below:



## Installed RADIUS Service

By default, this service is installed in a non-running state as shown below. This allows you to configure the service and then start it **only** when you plan to use it. When you plan to use the SurePassID RADIUS Service, you should set the service to start automatically.

The installation process also creates the following directory tree structure shown below.



## Installation Directory Tree

It is important to note that:

- Each component has its own folder; and
- Each component has its own Trace sub-folder for storing the sub-agent traces and log files.



## Supported RADIUS Systems

The **RADIUS Server** can be integrated with most appliances (virtual and physical) and software systems that support RADIUS standards for authentication. We've verified compatibility with a wide variety of vendors and devices. Here is just a short list:

- Barracuda SSL VPN
- Cisco ACS / ISE / ISR / Catalyst / SSH Network Device Access / IPsec VPN / ASA
- Citrix ACS NetScaler Gateway including XenDesktop & XenApp
- F5 Networks BIG-IP VPN
- Juniper and Pulse Secure SSL VPN
- Microsoft NPS
- Palo Alto Global Protect, IPSEC and SSL VPN
- SonicWALL TZ, NSA, SMA, SRA, etc.
- VMware View
- VPN Routers and NAS (LinkSys, ASUS, etc.)
- Web Application Firewalls (WAF)

**The SurePassID RADIUS Server only requires that the RADIUS compliant system (VPN, Firewall, etc.) use the PAP protocol for communication.**

## Configuring the RADIUS Server

The **RADIUS Server** allows you to add two-factor authentication (two-step authentication) to any system that supports RADIUS.

The server supports the following RADIUS features:

- **Challenge Response** – The user can be challenged for many different credentials. Most of the time, the challenge will be to provide a One-Time Password after successfully entering a valid username and password. Some RADIUS devices (such as VPNs) only support single-factor authentication. Two-

factor authentication can still be used by appending the One-Time Password to the user's password.

- **Proxy Server Chaining** – In RADIUS authentication, there can often be multiple RADIUS servers as part of the authentication process.

The **RADIUS Server** supports the following directories for single-factor (username and password) authentication:

- **Active Directory** – For tight integration with existing enterprise Identity Management Systems
- **SurePassID Directory** – For use with other cloud systems or external users that are not part of the existing enterprise Active Directory forest.
- **LDAP Directory** – For companies that use an LDAP directory such as Unix and Linux systems.

The **RADIUS Server** only the authentication of pass codes and allow the VPN client to perform the first factor of authentication (LDAP, AD, local, etc.) or participate in more sophisticated authentication strategies such as Citrix [nFactor](#).

The **RADIUS Server** supports the sending One Time Passcode (OTP) to the user. The user will concatenate the OTP code after the password unless the user chooses challenge response. The choices are:

- **SMS Code** – An OTP code is sent via SMS text to the user.
- **Voice Code** – A call is made to the user providing them an OTP code with a human voice.
- **Email Code** – An email is sent to the user which contains an OTP. This code is concatenated after the user's password.

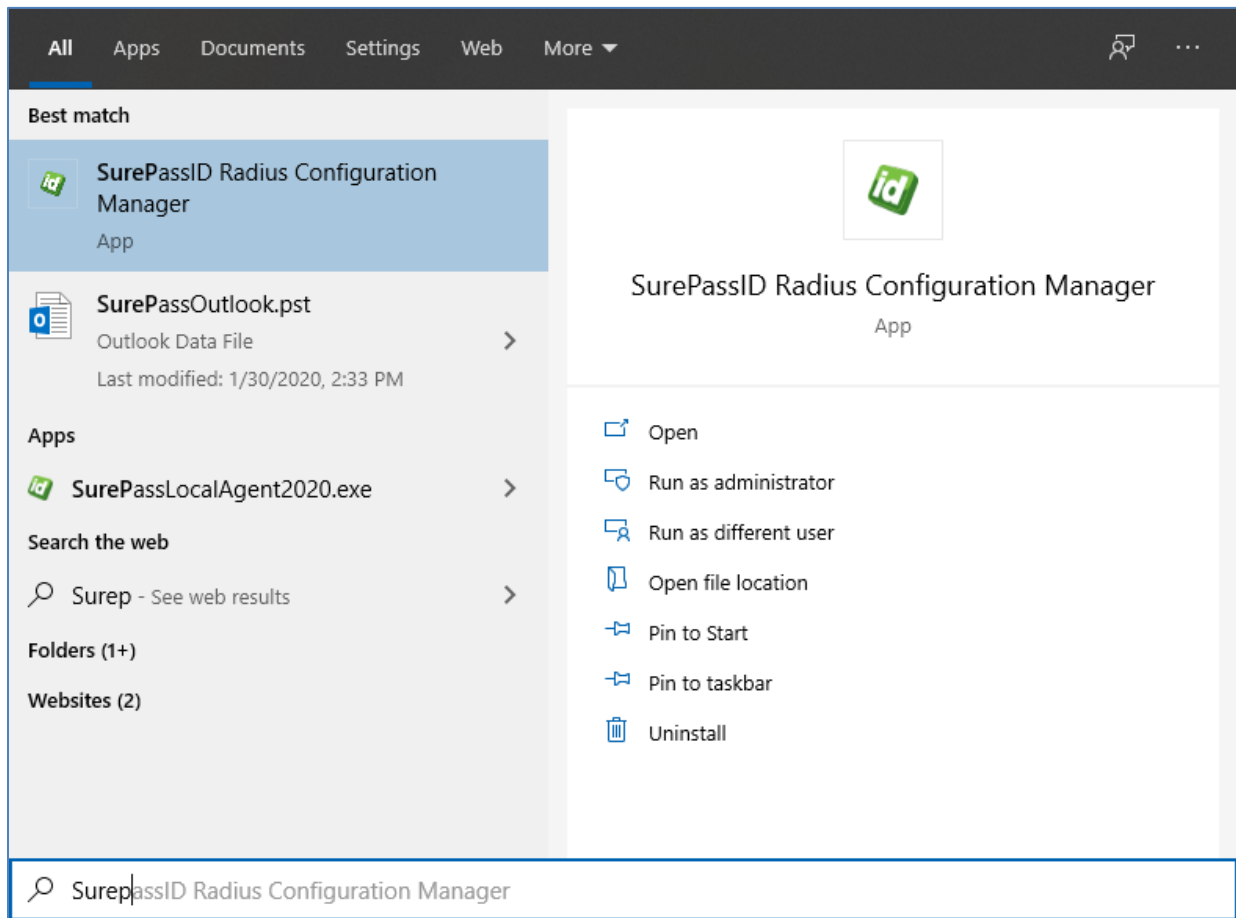
The **RADIUS Server** also supports the pushing authentication requests to the user's phone. If the user accepts the request, the user is allowed to login with just username and password. The choices are:

- **Push Authentication** – Send a message to the SurePassID Mobile Authenticator App to confirm or reject authentication.

- **IVR Authentication** – Call the user’s phone (including land lines) let them confirm or reject authentication with their key pad.
- **SMS Question** – Push a question is sent to the user’s mobile device via SMS text asking the user to confirm or reject authentication with their key pad system.

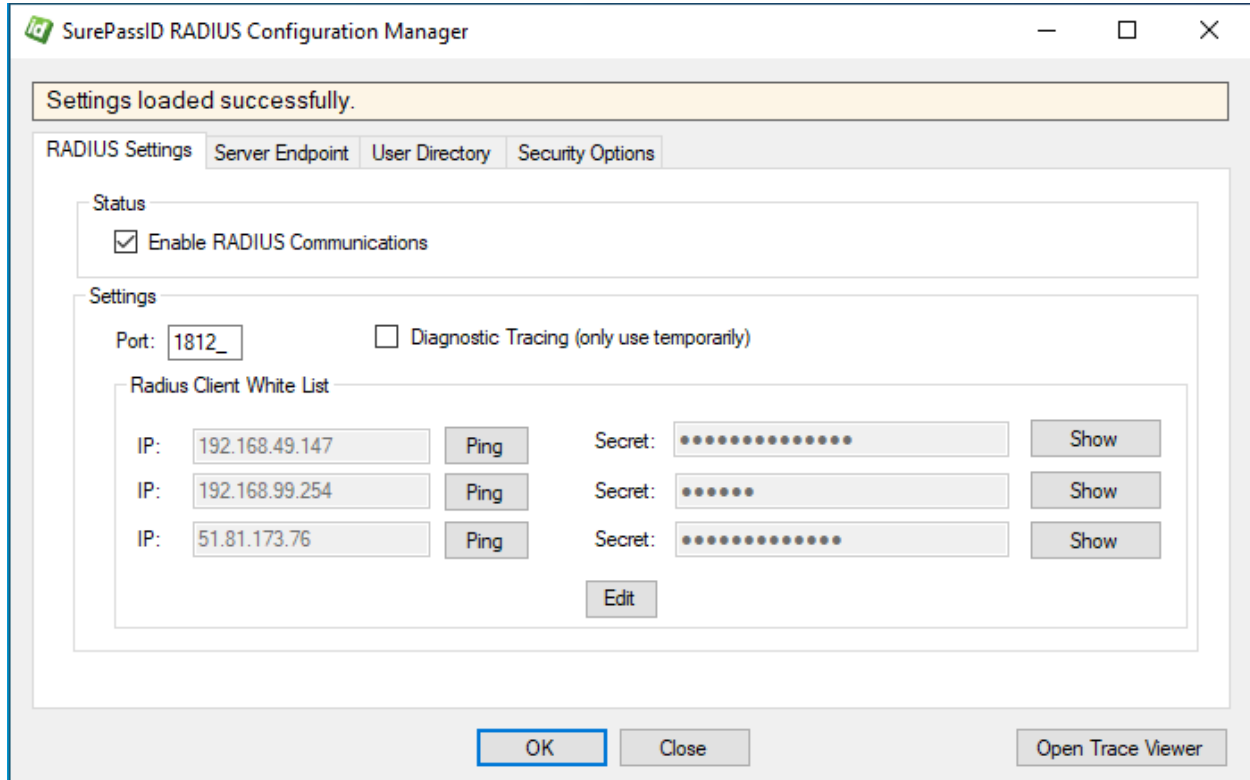
**HINT: All messages sent to the user can be tailored to your company’s needs in the SurePassID portal using the Customize SMS Messages and Customize Email Messages menus.**

The **SurePassID RADIUS Configuration Manager** application is used to configure the RADIUS and Directory Authentication Services. To configure the services, select **SurePassID RADIUS Configuration Manager** from the Windows Start menu as shown below:



### Start Configuration Application

# SurePassID RADIUS Configuration Manager



## RADIUS Settings

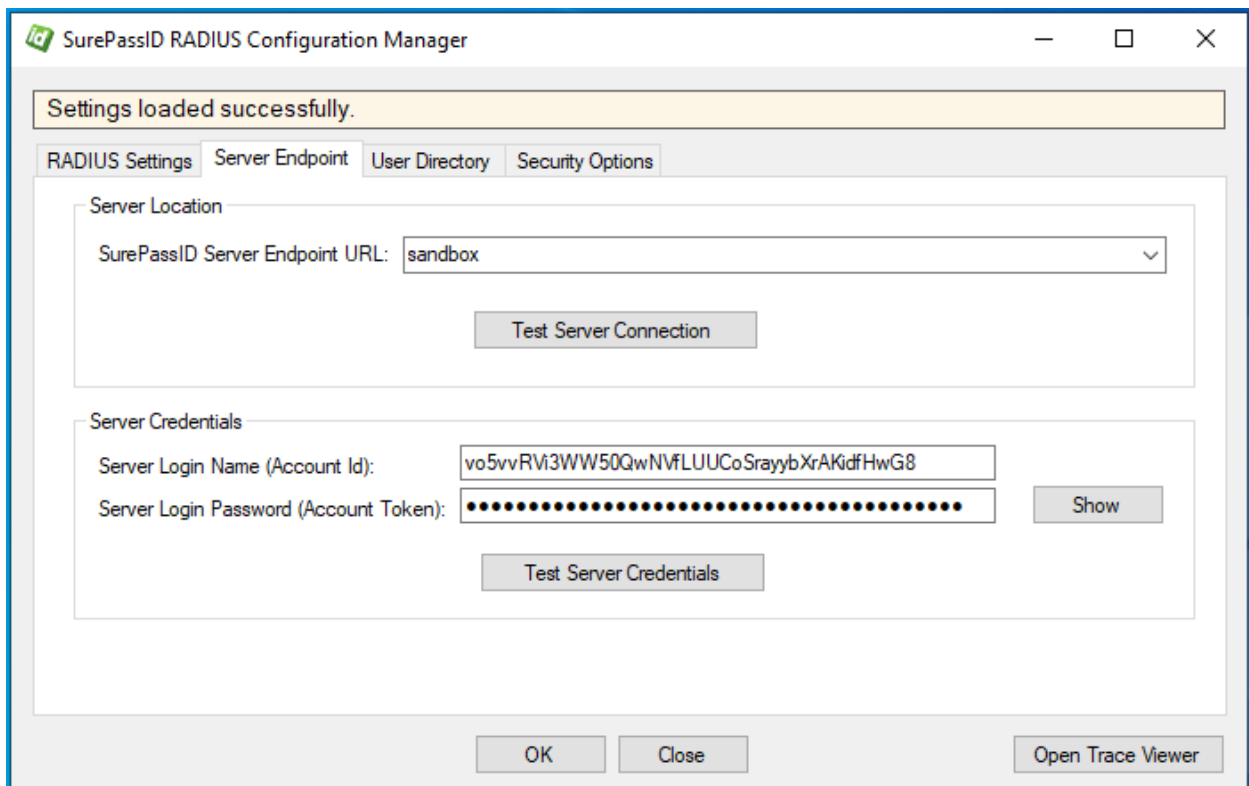
The application has four folder tabs. These tabs are:

- **RADIUS Settings** – Configuration settings for the SurePass RADIUS Server specific.
- **Server Endpoint** - Configuration settings for identifying your SurePassID account.
- **User Directory** - Configuration for User Directory.
- **Security Options** - Configuration for Permitted MFA Methods, User Active Directory Security Groups, and Additional Options.

The **RADIUS Settings** tab has the following fields:

- **Enable RADIUS Communications** – Check this box to enable the RADIUS server.

- **Port** – The UDP port that the RADIUS server will listen on. The default value is 1812; the standard RADIUS authentication port.
- **Diagnostic Tracing** – This option should only be checked when you are actively troubleshooting an issue. Leaving this option checked negatively impacts performance and accumulating large amounts of system data can create a potential security issue.
- **\_RADIUS Client White List** – The first three RADIUS devices that are permitted to communicate with the SurePassID RADIUS service.
  - **IP** – The IP of address of the RADIUS client device
  - **Secret** – The shared secret on the RADIUS client device.
- **Edit Button** – Add, update or remove a RADIUS clients from the white list. Only RADIUS clients on the white list that can make requests to the **RADIUS Server**. Each RADIUS client is identified by its IP address and the shared secret used between the RADIUS client. Requests from RADIUS clients that are not on the white list will be rejected.



## Server Endpoint

The **Server Endpoint** tab has the following fields:

- **Endpoint URL** – 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 cloud system.
  - **prod** – The SurePassID production cloud system.
  - **on premises system** – 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**

- **Test Server Connection button** – This button will verify that this server has connectivity to the SurePassID server using TLS (port 443). If this fails, then steps must be taken to determine where the connection fails. Common problems are (1) port 443 is not open in the firewall or TLS is not configured correctly, (2) the SurePassID Endpoint URL is invalid or not able to accept TLS requests, (3) no TCP/IP connectivity, (4) other problems that require trouble shooting.


**NOTE:** Although it is not recommended, for initial testing the system can be configured for port 80 communications removing the TLS requirement. This requires changes to both the **RADIUS Server** configuration and the SurePassID server. Contact SurePassID technical support ([support@surepassid.com](mailto:support@surepassid.com)) for instructions.

- **Server Login Name** – The login name for your SurePassID account.
- **Server Login Password** – The login password for your SurePassID account.
- **Test Server Credentials Button** – This button will verify that the Server Login Name and Server Login Password are correct.

**IMPORTANT:** Before trying this, make sure you have successfully connected to the server via pressing the **Test Server Connection Button**.

- **Open Trace Viewer Button** – This button will display the **RADIUS Server** trace log. This can be useful for verifying initial system connectivity, trouble-shooting system configuration, login failures, and performance related issues.

The **Server Login Name** and **Server Login Password** can be retrieved from your SurePassID account as shown below. To view the password, click the 'Show' link to show the display of the password and 'Hide' link to hide the password:

**SurePass** 

Home | Users | Tokens | Audit Trail | SSO | volansys.com | Andy Gill(Admin) | Logout

Account | Settings | Customize Email Messages | Customize Mobile Messages | Fido U2F | Fido UAF

### Update Account [New](#) [Update](#) [Close](#)

**Account Information**

Account:

Company Name:

Printed Serial Number Prefix:

**Account Credentials**

Server Login Name (Account Id): vo5vvRvi3WW50QwNVfLUUCoSrayybXrAKidfHwG8

Server Login Password (Account Token): 0wAaNurG8LtenEsJcE1GULhctip4KYzkFfjkhPbv [Hide](#)

Data Protection:

**SurePassID Licensing**

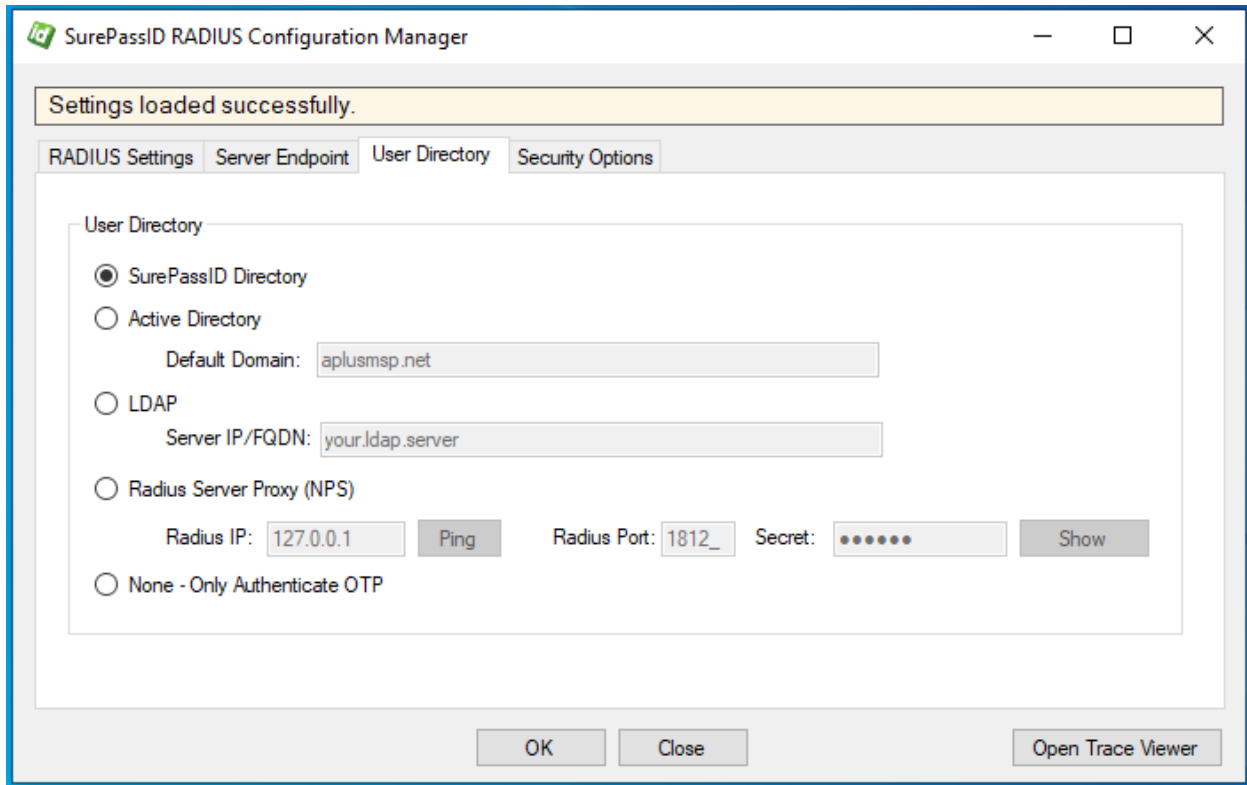
License Type:

**Authenticate Calling IP Address**

White List (allow access only to) these IP addresses :

## SurePassID Account Settings

User Directory tab has the following fields:



## User Directory

- **User Directory** – Check the appropriate User Directory to validate the user’s name and password.
  - **SurePassID Directory** – Check this box to use the SurePassID directory
  - **Active Directory** – Check this box to use Active Directory.
    - **Default Domain** - You can specify the default domain for all users. Leaving this field blank will default to the current domain of the RADIUS server.
 

**NOTE:** For enterprises that have multiple domains, users can override the default domain when logging in by entering their username in the form of **domain/username** or **username@domain**.
  - **LDAP** – Check this box to use an LDAP directory.
    - **ServerIP/FQDN** – You must enter the IP or Fully Qualified Domain Name (FQDN) of the LDAP server
  - **None – Only authenticate OTP** – Check this box to instruct the RADIUS Server to only check the OTP. This means the RADIUS client (VPN/firewall/etc.) will validate the username locally or with some external

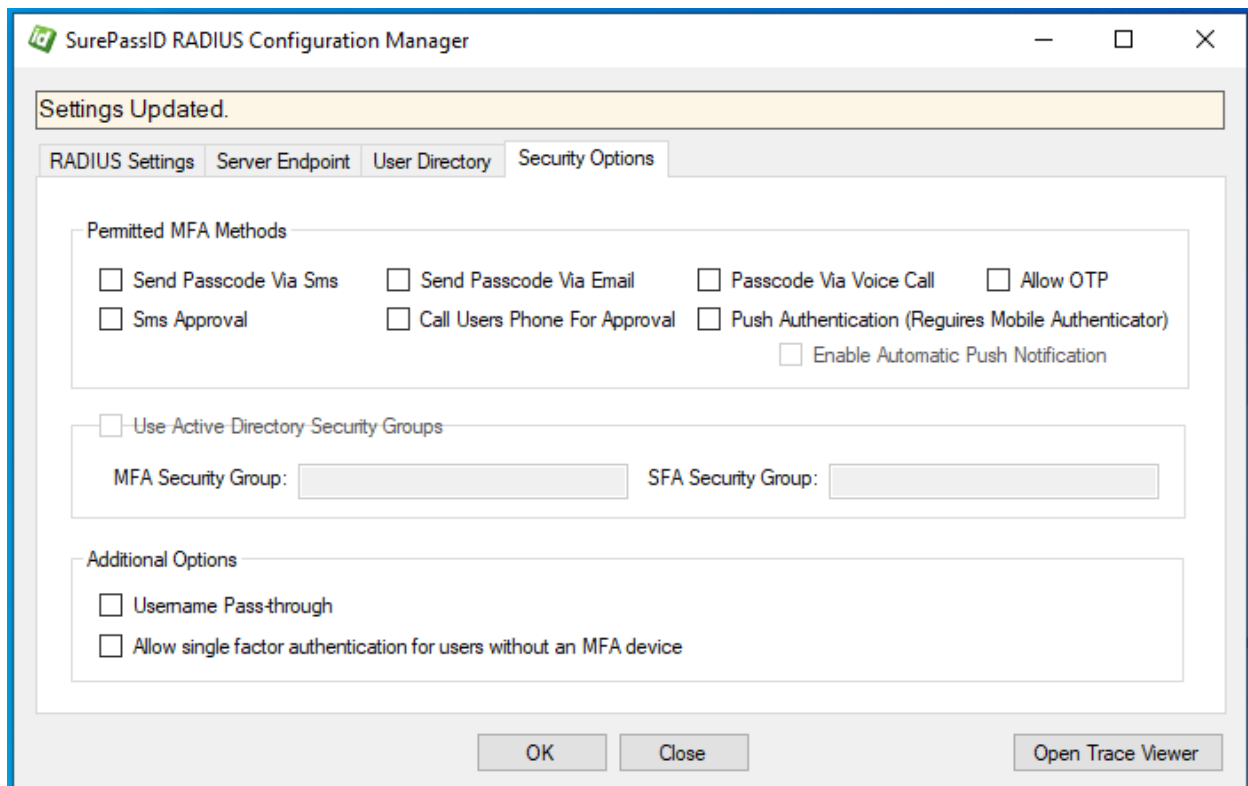


directory such as Active Directory/LDAP first and then prompt the user for the OTP and send it to RADIUS Server for validation.

After making changes, you can start the **RADIUS Server** windows service. If the service is already running the **RADIUS Server** will automatically pick up the changes.

**NOTE:** When authenticating users, the username (without domain information if present) entered at RADIUS login must be defined in the SurePassID directory regardless of the **User Directory** selected.

The **Security Options** tab has the following fields:



The screenshot shows the 'SurePassID RADIUS Configuration Manager' window with the 'Security Options' tab selected. A yellow message bar at the top indicates 'Settings Updated.' The 'Security Options' tab contains the following sections:

- Permitted MFA Methods:** A group box containing seven checkboxes: 'Send Passcode Via Sms', 'Send Passcode Via Email', 'Passcode Via Voice Call', 'Allow OTP', 'Sms Approval', 'Call Users Phone For Approval', and 'Push Authentication (Requires Mobile Authenticator)'. There is also an unchecked checkbox for 'Enable Automatic Push Notification' below the main group.
- Use Active Directory Security Groups:** An unchecked checkbox with two text input fields below it: 'MFA Security Group:' and 'SFA Security Group:'.
- Additional Options:** A group box containing two unchecked checkboxes: 'Username Pass-through' and 'Allow single factor authentication for users without an MFA device'.

At the bottom of the window are three buttons: 'OK', 'Close', and 'Open Trace Viewer'.

### Security Options

- **Permitted MFA Methods** – Select the MFA methods your users can use to login. If you do not select an MFA method users will not be able to login.

- **Send Passcode Via Sms** - One time passcode is sent to the users mobile phone via an SMS text message. The user enters that code.
- **Send Passcode Via Email** - One time passcode is sent to the users email. The user enters that code.
- **Passcode Via Voice Call** – The user receives a phone call and the one time passcode is spoken to the user. The user enters that code.
- **Allow OTP** - The user enters OTP from the mobile authenticator application with password.
- **Sms Approval** – A question is sent to the users mobile phone via an SMS text message. The user accepts to login or refuses the request.
- **Call Users Phone For Approval** - The user receives a phone call and the user is asked a question. The users answers the question to accepts to login or refuses the request.
- **Push Authentication (Requires Mobile Authenticator)** - The user receives a push notification on their mobile phone. The users accepts to login or refuses the notification request.
- **Enable Automatic Push Notification** - This option will get enabled when user selects Push Authentication MFA method. After the user enters a valid username and password they will automatically be sent a push.
- **User Active Directory Security Groups** - This option will get enabled when user selects Active Directory from the User Directory tab.
  - **MFA Security Group** – You can mention MFA user’s security group name. The users from the mentioned group will be allowed to connect to the RADIUS server.
  - **SFA Security Group** – You can mention SFA user’s security group name. The users from the mentioned group will be allowed to connect to the RADIUS server.

If both groups are mentioned then users that do not belong to any of the above groups will not be allowed access to RADIUS server.

If this option is not checked then all authentication requests will be processed by the RADIUS server.

- **Allow single-factor authentication for users without a two factor device** – Check this box if you will have some users logging in that will not have a two-factor authentication token. Users who are assigned a two-factor authentication token must provide the second factor of authentication.

- **Username Pass-through** - Check this box when AD username normalization is not needed.

## Configuring RADIUS Clients

Once the SurePassID **RADIUS Server** is configured and running. You need to configure your RADIUS clients to use it for secure authentication.

When configuring the RADIUS clients' settings there are only a few parameters that are important to the SurePassID **RADIUS Server**.

**RADIUS Server IP** – Set this IP to the SurePassID **RADIUS Server** IP. Make sure that the IP of the RADIUS client is in the SurePassID **RADIUS Server** white list.

**RADIUS Server Port** - Set this port to 1812 which is the standard for RADIUS authentication/. This needs to match

**RADIUS Secret** – This must match the secret assigned to each whitelist port in the SurePassID **RADIUS Server**. If these are not correct the RADIUS client and SurePassID RADIUS Server will not be able to communicate and

**RADIUS Authentication Protocol** – The typical default is PAP. If the option is offered by the RADIUS client then select PAP. Selecting any other option will not work.

**Secondary Authentication** – Most RADIUS clients allow you to select a primary and secondary authentication methods. We suggest you consider all factors that might occur and prevent your RADIUS client from connecting to the primary RADIUS server (SurePassID **RADIUS Server**) such as internal network outages, external network outage, VM issues, etc. and pick a secondary method that eliminates these potential bottle necks so that a limited number of users can authenticate and access the system remotely in times of need. The SurePassID **RADIUS Server** can be deployed as a load balancer. You can also configure multiple instances of the SurePassID RADIUS Server on multiple servers for fault tolerance and additional scalability.

## Timeouts and Retries

We recommend a RADIUS authentication timeout of 10 seconds and 3 retries if you are using hard/soft tokens.

Out of band authentication such as sending an email, sms, or push authentication can take time for the user to respond and you do not want your users to get cut-off before they authenticate and then retry. Depending on your network latency, authentication

methods and SurePassID MFA Server install options (cloud vs. on-premises) this timing can vary. We recommend a minimum RADIUS timeout of 30 seconds and zero retries as a starting point. You can always make this longer or shorter depending on your needs.

SurePassID natively supports out of band timeouts. This is required for systems that do not have timeouts like RADIUS. This timeout value is specified in the SurePassID admin portal. It is important that your RADIUS timeout value is greater than SurePassID mobile timeout by 5 seconds. This variance is to account for the RADIUS authentication overhead.

If you have any additional questions, please call or email [support@surepassid.com](mailto:support@surepassid.com) assistance.

## Fortinet Notes

Most VPN appliances let you configure the default timeout value using their user interface. This is not the case for the Fortinet. The Fortinet appliance has a default timeout of 5 seconds, which will fail for anything other than OTP passcode authentication. The timeout can be increased only using the Fortinet Command Line Interface (CLI) as described below:

The following [global changes](#) need to be made to the Fortigate as per Fortigate Forum [RADIUS Time-Out | Fortinet Technical Discussion Forums](#):

CLI:

```
config system global
set remoteauthtimeout <seconds>
end
```

The following changes need to be made to [each SurePassID RADIUS server](#) on the Fortigate as documented in the Fortigate Forum [Repeated RADIUS Requests | Fortinet Technical Discussion Forums](#):

```
config user radius
edit <radius_server_name>
set timeout <seconds>
```

We recommend you start with <seconds> = 30. We recommend setting the SurePassID Mobile notifications setting to match the <seconds>.

## Configuring Your Proxy Server

If your company uses a proxy server to monitor outbound traffic from your network you will need to configure the RADIUS server to use that proxy. Follow these steps:

- a. Edit SurePassRadiusServerService.exe.config located in the same folder as SurePassRadiusServerService.exe.
- b. You will need to make the following changes under the <configuration> element add the following xml.

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://myproxy:80"
      usesystemdefault="true"
      bypassonlocal="true"
      autoDetect="true" />
  </defaultProxy>
</system.net>
```

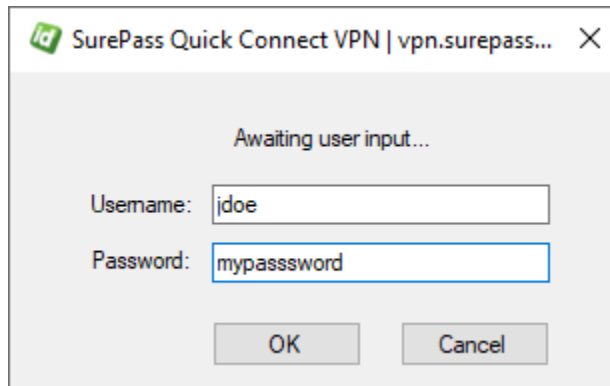
- c. You need to modify myproxy:80 to your proxy server:port. Do not remove the leading http://.
- d. Restart the SurePassID RADIUS server.

## VPN End-User Login Overview & Examples

### Example 1 – Login Using Single-Factor

Logging into your VPN with single-factor authentication is a fairly straight forward and legacy process that requires only the username and password. Typically, you follow these steps:

1. Start VPN client software
2. Enter username
3. Enter password



#### Single-Factor VPN Login

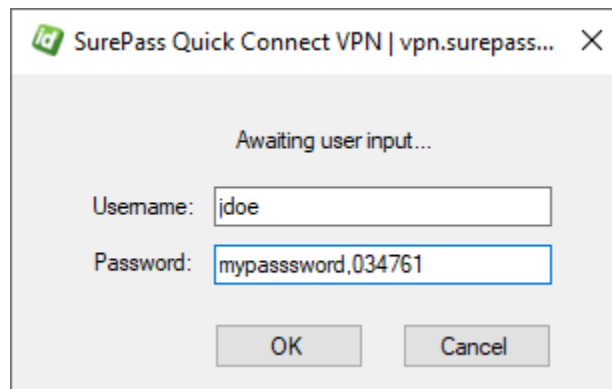
4. Press **OK** button to authenticate

When you use two-factor authentication, the process changes slightly because you will need to enter the second factor code in addition to the username and password.

### Example 2 – Login Using Code from Hard or Soft Token

You will follow these steps if you have a device that displays a second factor code such as a hard token (OTP display smart card, key fob, etc.) or a soft token (SurePassID desktop token, mobile OTP apps such as Google Authenticator, Nymi Companion App, etc.)

1. Start VPN client software
2. Enter username
3. Enter password and concatenate the second factor code that is displayed from the device. In this example, the number displayed on the device is 034761 as show below:



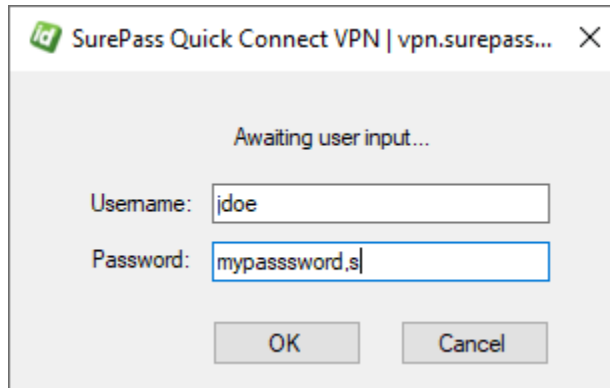
### Two-Factor Authentication with Token

4. Press **OK** button to login.

### Example 3 – Login Using Sending OTP via SMS, Email or Voice Code

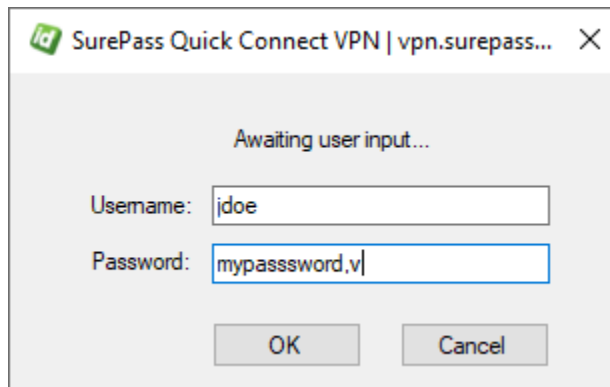
You will follow these steps if you want to have a second factor code sent to you via SMS Text, Voice Call, or Email:

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a method to send yourself a passcode to login.
  - Enter **s, 0,** or **SENDSMS** to have a code sent via text to your cell phone.



### Two-Factor Authentication with SMS Text Code

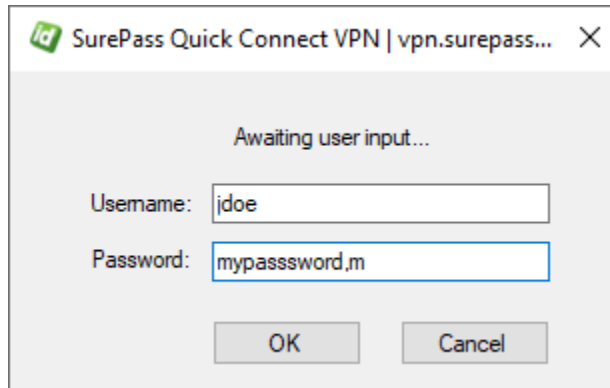
- Enter **v, 2, or SENDVOICE** to have an automated voice call made to your cell phone that will tell you a code.



### Two-Factor Authentication with Voice Call

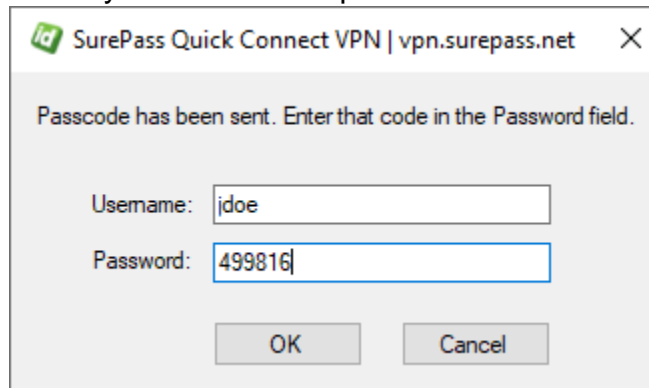
- Enter **m, 1, or SENDEMAIL** to have a passcode sent via email.



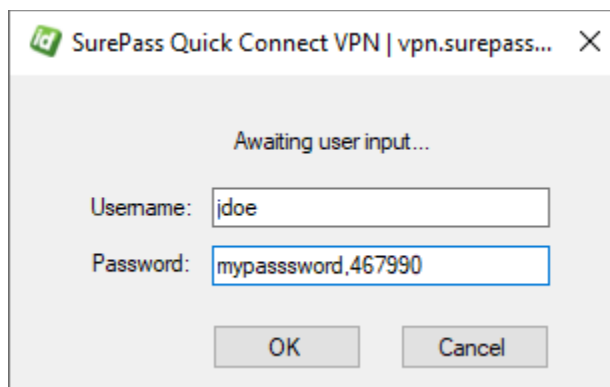


### Two-Factor Authentication with Email

4. If your VPN supports RADIUS challenge/response, then you will receive the following message. Enter your code in the password field.



5. If your VPN does not support challenge response, then enter the password followed by a comma, followed by the code you have just received (no spaces after the password).

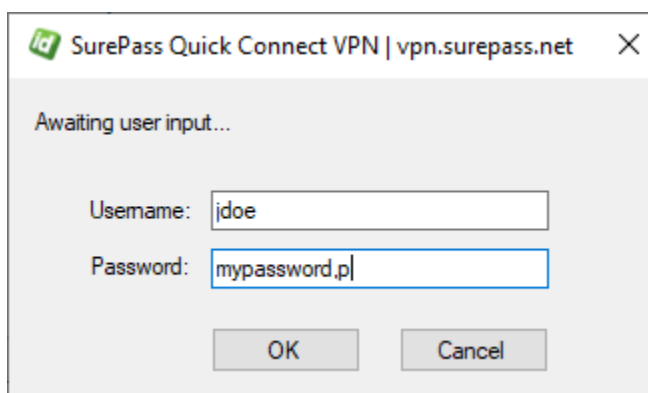


6. In either case press **OK** button to login.

## Example 4 – Login Using SMS Question

You will follow these steps if you want to secure yourself via an SMS approval question and not have to enter a code.

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **p, ??, or PUSHSMS** to have an approval question sent via SMS text to your phone number on your account. You only need to reply **y** or **yes** (not case sensitive) to the text message to have the second factor authenticated. If you did not request to be authenticated, you can respond with any other answer (such as **n** or **no**) and access will be denied.



The image shows a screenshot of a Windows-style dialog box titled "SurePass Quick Connect VPN | vpn.surepass.net". The dialog box has a close button (X) in the top right corner. The main text inside the dialog box says "Awaiting user input...". Below this text, there are two input fields: "Username:" with the value "jdoe" and "Password:" with the value "mypassword,p". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

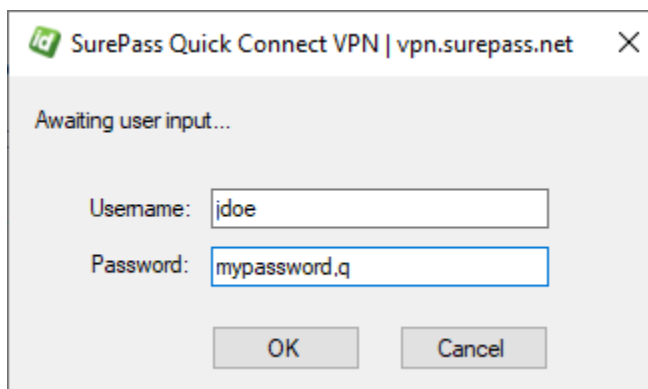
### Two-Factor Authentication with SMS Question

4. Press button **OK** to send you a question.
5. Wait for the question to be delivered via SMS to your mobile device.
6. Reply Yes (or Y) to the question to allow you to login in.
7. Wait for confirmation from the server that you have been authenticated on your phone.
8. You will be logged in without further action.

## Example 5 – Login Using Push Authentication

You will follow these steps if you want to secure yourself via a push notification question and not have to enter a code. This authentication method requires that you have registered your token with SurePassID Mobile Authenticator and your account/token was configured for push notifications.

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **q**, **?** or **PUSHAPPQUESTION** in the passcode to have a push notification request sent to your phone.



Screenshot of the SurePass Quick Connect VPN login dialog box. The window title is "SurePass Quick Connect VPN | vpn.surepass.net". The text "Awaiting user input..." is displayed. The "Username:" field contains "jdoe". The "Password:" field contains "mypassword,q". There are "OK" and "Cancel" buttons at the bottom.

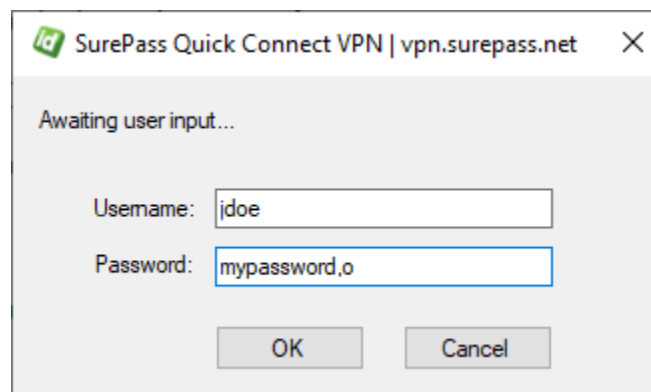
### Two-Factor Authentication with Push Notification

4. Wait for the push notification question to be delivered to your mobile device.
5. On your mobile click **Authenticate** to approve the request or click **Cancel** to disallow the request.
6. If you clicked **Authenticate** you will be logged in without further action.

## Example 6 – Login Using Push Voice Call

You will follow these steps if you want to secure yourself via a voice call notification. You will not have to enter a code. This requires that your account has been configured for to allow phone call to be made to your phone number

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **o (the letter)**, **#** or **PUSHVOICE** in the passcode to have a push notification request sent to your phone.



### Two-Factor Authentication with Voice Call Notification

4. Wait for the call on your phone.
5. Answer the call, listen to the message and take the required actions to allow or deny the request.
6. Wait for confirmation on your phone you have been authenticated on your phone and hang up.
7. You will be logged in without further action.

# Configuring the Directory Sync Application

The Directory Sync application is a command line application that synchronizes user Active Directory user information with the SurePassID directory. The Directory Sync application (DirectorySync.exe) is located in the SurePassID Local Agent\Directory Sync folder.

To run the Directory Sync application, use the following syntax:

```
DirectorySync [-ln=loginname]  
[-lp=loginpassword]  
[-add=activedirectorydomain]  
[-adf=activedirectoryfilter]
```

where

**-ln** – SurePassID account login name

**-lp** – SurePassID account login password

**-activedirectorydomain** – Active Directory domain to synchronize.

**-activedirectoryfilter:** – Active Directory filter to synchronize a subset of the Active Directory domain.

The Directory Sync application synchronizes the following data:

- Username (same as account name)
- First Name (given name)
- Last Name (surname)
- Email (email)
- Mobile Number (mobile)

The Directory Sync application by default uses https for transport security. If you need a greater level of security, please contact SurePassID technical support and we can assist in setting up message level security using X509 certificates.

## Configuring the Event Log Sync Application

The Event Log Sync application is an application that pulls information from the SurePassID Audit Trail and sends it to a number of different logging systems referred to as targets. Event Log Sync application is delivered as a command line application or an Azure Web Job.

The system supports the following targets:

- Windows Event Log
- Syslog Format – TCP (TLS and plain text transports)
  - Splunk
  - Loggly
  - Elastic Search
  - All Syslog based listeners

Event Log Sync only retrieves specific events that your SurePassID account is configured for. This allows you to only retrieve a subset of audit log information (such as errors only) and not all audit trail records. The audit events that are eligible for synchronization are set in your SurePassID Account Settings as highlighted in green below:

[Home](#) | [Accounts](#) | [Users](#) | [Tokens](#) | [Audit Trail](#) | [SSO](#)

[Account](#) | [Settings](#) | [Customize Email Messages](#) | [Customize SMS Messages](#) | [Fido U2F](#) | [Fido UAF](#)

### Update Settings [SurePassId] [Update](#) [Close](#)

Account Limits

Maximum Users Licensed:

Maximum Tokens Licensed:

Account Expiration Date:

Culture and Time Zone

Time Zone:

Current Culture:

Security

Allowable Failed OTP Validations Per Token:

Account Password Expiration:

OTP Lifetime

SMS OTP is valid for: Minutes:  Seconds:

Email OTP is valid for: Minutes:  Seconds:

Temporary OTP is valid for: Minutes:  Seconds:

User Authentication Directory

User Authentication Method:

Event Log Synchronization Filters

Synchronize These Events:

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Severe	Warning	Success	Action Required
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Informational			

EventLogSync.exe creates a trace log each day it runs. This file is good for trouble shooting connectivity issues, reviewing process health, etc. The trace logs are stored in the trace folder and there is a new file created each day. The location of the trace folder is:

**C:\Program Files (x86)\SurePassID Corp\SurePassID Local Agent 2021\EventLogSyncClientConsole\Trace\**

## Running Event Log Sync

To run the application, use the following syntax:

EventLogSync [-ln=login-name]  
[-lp=login-password]  
[-dbconnection=sqlserver-connection-string]  
[-syncapi=api-protocol]  
[-restendpoint=sp-server-endpoint]  
[-targettype=log-target-type]  
[-targetendpoint=log-target-endpoint]  
[-targetport=log-target-port]  
[-maxsyncitems=record\_count]  
[-sd=syslog\_account-identifier]  
[-runoption=run-option]  
[-continuousrunwaittime=wait-time-between-runs]

The command line parameters are explained below.

## MFA Server

- **-ln** – SurePassID account login name
- **-lp** – SurePassID account password
- **-dbconnection** – SQL Server database connection string. All the possible connection string options are documents here: [SQL Server Database Connections](#).

NOTE: It is strongly recommended that you create a unique SQL Server account (limited access) to the MFA server database. See **Database User Permissions** in a subsequent section.

- Sample SQL Server authentication:  
**Data Source=<sqlserver\_server>;**  
**Initial Catalog=<surepassid\_database>;**  
**User id=EventLogSync\_User;**  
**Password=<surepassid\_sqlserver\_password>;Integrated Security=false**



- Sample SQL Server windows authentication (service or managed service accounts):  
**Data Source=<sqlserver\_server>;**  
**Initial Catalog=<surepassid\_database>;**  
**Integrated Security=true**
- **-restendpoint** – SurePassID Authentication server endpoint URL. In most cases, you will not need to change this unless you are using a custom SurePassID installation. Not required if you are using **-dbconnection**. The values are:
  - **sandbox** – The SurePassID sandbox cloud system.
  - **prod** – The SurePassID production cloud system.
  - **on premises system** – The on-premises or custom SurePassID server endpoint. The format of this parameter is usually:

**https://<surepassid-server>/AuthServer/REST/OATH/OathServer.aspx**

## Synchronization Targets

- **-targettype** – The log target to sync with.
  - **e**=Windows Event Log,
  - **s**=syslog,
  - **l**=log4net.

## Synchronization Process Options

- **-maxsyncitems** – Count of records that EventLogSync will process in each processing run. 0=process all records that are eligible for sync. The default is 0.
- **-runoption** – EventLogSync can be configured to perform one processing run and stop, or it can be configured to run continuously performing an endless number of processing runs. Regardless, it will always try to process **maxsyncitems** records each time it runs. If running continuously, EventLogSync can sleep between processing runs. The amount of time that it sleeps is determined by **continuousrunwaittime**. o=run once, c=continuous. Default is run once.

**-continuousrunwaittime** – The count of seconds that EventLogSync to wait between processing runs when operating in continuous mode.

## Syslog Specific

- **-targetendpoint** - The IP of the target system listener endpoint.
- **-targetport** - The port that target system listener endpoint. Default is 6514.
- **-sd** - Syslog systems can require that the calling entity must provide an account identifier as part of the [Structured Data Element](#) to add log records. The form is usually `uuid@41058`. However, this value can be anything and is determined by

target syslog provider. For systems that require this (such as Loggly) you must provide this parameter (to identify your Loggly tenant) or syncing will fail.

## Database User Permissions

The SQLServer account that will access the MFA database requires the following permissions:

SELECT ON the following tables:

- Partner
- PartnerSettings,
- PartnerUserAudit

SELECT ON the following tables:

- PartnerSettings

If you plan to use SQLServer authentication you would run the following script after creating a strong password and entering it between the single quote following PASSWORD=:

```
CREATE LOGIN [EventLogSync_User] WITH PASSWORD = ',
DEFAULT_DATABASE=[SurePass2013_sandbox],
DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF

CREATE USER EventLogSync_User FOR LOGIN EventLogSync_User WITH
DEFAULT_SCHEMA=[dbo]

GRANT SELECT ON [Partner] TO EventLogSync_User
GRANT SELECT ON [PartnerSettings] TO EventLogSync_User
GRANT SELECT ON [PartnerUserAudit] TO EventLogSync_User
GRANT UPDATE ON [PartnerSettings] TO EventLogSync_User
GRANT UPDATE ON [PartnerUserAudit] TO EventLogSync_User
EXEC sp_addrolemember 'db_datareader', 'EventLogSync_User'
```

If you plan to use SQLServer authentication you would run the following script after creating a strong password and entering it between the single quotes following PASSWORD=:

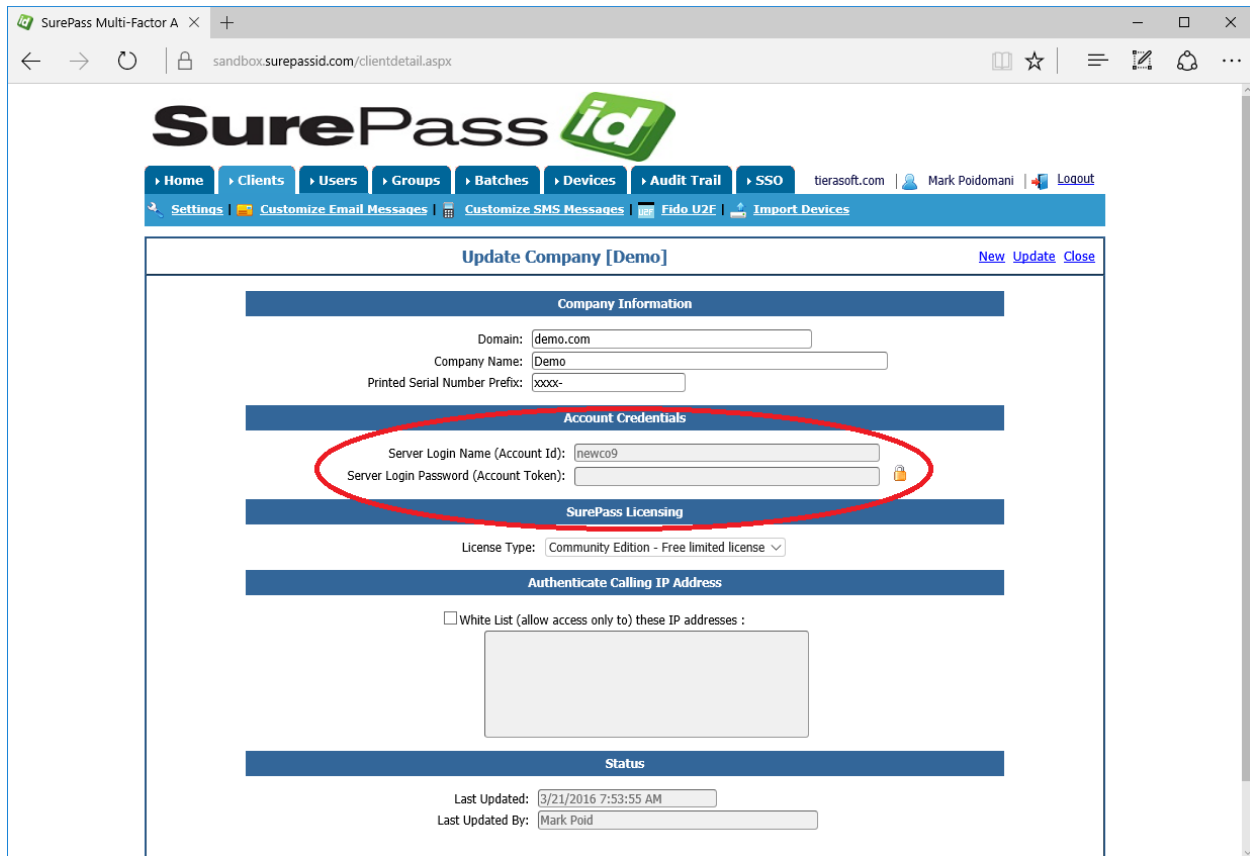
If you plan to use Windows authentication (STRONGLY RECOMMENDED) you would run the following script after adding a windows account (Managed Service Account would be good. e.g. EventLogSync\_User) to allow access to the database:

```
GRANT SELECT ON [Partner] TO EventLogSync_User
GRANT SELECT ON [PartnerSettings] TO EventLogSync_User
GRANT SELECT ON [PartnerUserAudit] TO EventLogSync_User
GRANT UPDATE ON [PartnerSettings] TO EventLogSync_User
GRANT UPDATE ON [PartnerUserAudit] TO EventLogSync_User
EXEC sp_addrolemember 'db_datareader', 'EventLogSync_User'
```

## REST API Sync to SurePassID

To sync events from SurePassID to another event log source you need to identify your SurePassID account. You must specify the **-ln** and **-lp** parameters to identify your account.

The **-ln** and **-lp** parameters 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:



Event Log Sync app will sync events using the SurePassID REST API.

## Direct Connect Sync to SurePassID

SurePassID on-premises users can optionally use the Direct Connect Sync option to sync directly from the SurePassID database to external sync sources. To use Direct Connect Sync you must specify the **-dbconnection** parameter on the command-line. Direct Connect Sync has the following advantages over the REST API Sync:

- More efficient and high throughput rate than the REST API
- More flexible connection options to meet your compliance and governance requirements.
- Capable of syncing additional SurePassID system management specific events not available via the REST API Sync.

The Event Log Sync application (EventLogSync.exe) is located in the Event Log Sync installation folder. The default location is:

**C:\Program Files (x86)\SurePassID Corp\SurePassID Local Agent 2021\EventLogSyncClientConsole.**

## Command line Options for SurePassID REST API Sync

The table below provides the parameters required for log target parameters for each log target:

Parameter Name	Target System	Mandatory/ Optional
-ln	windows event log, syslog	M
-lp	windows event log, syslog	M
-syncapi	windows event log, syslog	M
-restendpoint	windows event log, syslog	M
-targettype	windows event log, syslog	O
-targetendpoint	syslog	M
-targetport	syslog	O
-maxsyncitems	windows event log, syslog	O
-sd	syslog	O
-runoption	windows event log, syslog	O
-continuousrunwaittime	windows event log, syslog	O

## Command line Options for SurePassID Direct Connect Sync

The table below provides the parameters required for log target parameters for each log target:

Parameter Name	Target System	Mandatory/ Optional

-ln	windows event log, syslog	M
-lp	windows event log, syslog	M
-dbconnect	windows event log, syslog	M
-syncapi	windows event log, syslog	M
-targettype	windows event log, syslog	O
-targetendpoint	syslog	M
-targetport	syslog	O
-maxsyncitems	windows event log, syslog	O
-sd	syslog	O
-runoption	windows event log, syslog	O
-continuousrunwaittime	windows event log, syslog	O

## Deployment Configurations

Event Log Sync is a Windows console app that can be deployed in a variety of configurations. Some such configurations are:

- Windows Service
- Scheduled Task
- Azure WebJob
- AWS Lambda
- Any App (via SurePassID API)

Event Log Sync uses the SurePassID Server REST API. You can add the same functionality into any app and deploy it in any manner you require. For instance, you could incorporate event log sync into your app and to send the logs to any log target including databases, text files, etc. on any platform using any programming language.

Alternatively, you could use curl and sync the SurePassID audit trail directory into syslog on a RHEL 7 or Ubuntu platform. The possibilities are unlimited.

## Security Considerations

Event Log Sync Application uses TLS 1.2 for transport security. If you need a greater level of security, please contact SurePassID technical support and we can assist in setting up message level security using X509 certificates.