SurePassID LDAP Secure Gateway Guide

SurePassID Authentication Server 2020

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

SurePassID, Corp.
13750 W. Colonial Drive
Winter Garden, FL 34787
www.SurePassID.com

Table of Contents

Table of Figures

Introduction

This guide explains how to install and configure the SurePassID LDAP Secure Gateway 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 LDAP Secure Gateway?**
  - A brief introduction to the SurePassID LDAP Secure Gateway.
- **Installing and Configuring SurePassID LDAP Secure Gateway**
  - Detailed explanations for installing the SurePassID LDAP Secure Gateway 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 LDAP Secure Gateway?

The SurePassID LDAP Secure Gateway is a LDAP Secure Gateway service that adds Two Factor Authentication (2FA) to any LDAP based system. The SurePassID LDAP Secure Gateway protects laptops, desktops, and servers from attacks when locally logging into a Windows device or login via Windows Remote Desktop Services (RDS).

The SurePassID LDAP Secure Gateway works with any SurePassID server (cloud, on-premises) and supports all the SurePassID 2FA supported OTP devices.

SurePassID LDAP Secure Gateway also supports the following directories for single-factor (username and password) authentication:

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

The SurePassID LDAP Secure Gateway supports the sending of One-Time Codes to the user as well as pushing authentication requests to the SurePassID Mobile Authenticator mobile app.

Send OTP Options:

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

Push Authentication Options (uses cellular network, not SMS, except for Push SMS question):

- **Push SMS Question** – A question is sent to the user's mobile device asking the user to confirm a request to allow access to the system. If the user responds positively, the user is allowed to login with just username and password.
- **Push Question -** A question is sent to the user's mobile device (via cellular notification) asking the user to confirm a request to allow access to

the system. If the user responds positively, the user is allowed to login with just username and password.

- **Push OTP -** An OTP is sent to the user's mobile device via cellular notification, not SMS). The OTP can be used as if it were an OTP from a soft token, or hard token (fob or card).
- **Push Voice Question -** A voice call is made to the user's phone asking the user to confirm access to the system. If the user responds positively, the user is allowed to login with just username and password.

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

Prerequisites

SurePassID LDAP Secure Gateway can be installed on the following 64-bit Windows versions:

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

SurePassID LDAP Secure Gateway requires a SurePassID MFA server. This can be the cloud version or on-premises version.

Post Configuration Steps

Here are a few recommended items to consider after installing the SurePassID LDAP Secure Gateway.

- Configure LDAP Gateway Server Configuration

These suggestions are discussed in subsequent sections.

Installing the LDAP Secure Gateway

The LDAP Secure Gateway can be downloaded from the following URL:

https://sandbox.surepassid.com/downloads/LG/SPLG.zip

The SurePassID LDAP Secure Gateway installer will install all of the LDAP Secure Gateway components and prerequisites.

To start the installation you must first download the installation file SPLG.zip unzip the file and run **SurePassIdLdapGateway2019.exe** on one of your Windows servers and you will see the following installation form:

Figure 1: Installation Welcome

Click **Next** and the SurePassID LDAP Secure Gateway License Agreement will be displayed.

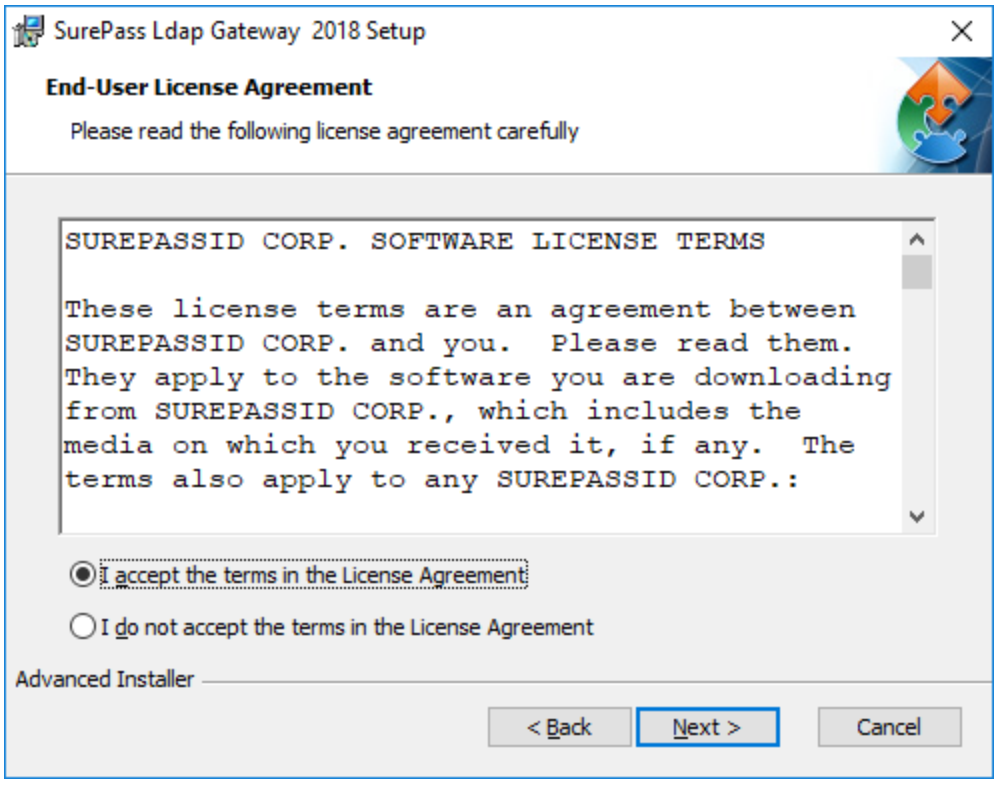

Figure 2: License Agreement

Read the License Agreement and if you agree then click the **Next** button and you will see the installation folder form.

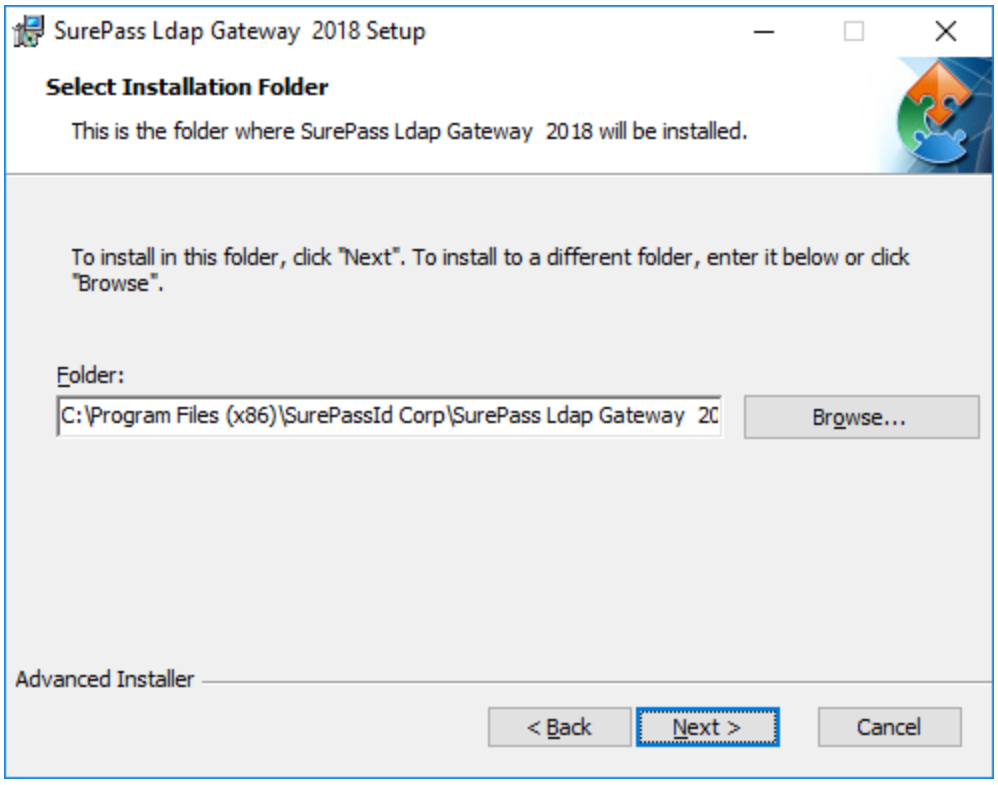

Figure 3: Installation Location: Specify Installation Folder

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

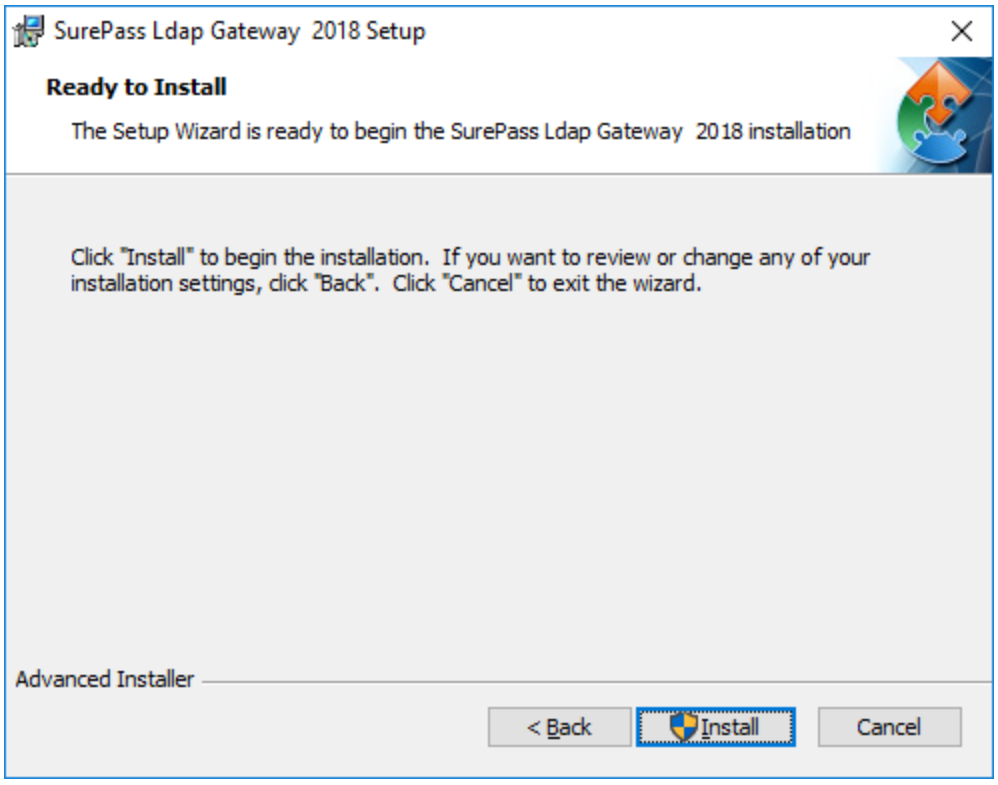

Figure 4: Ready To Install:

Click the **Install** button to start the installation process. You will first be presented with a signed SurePassID verified publisher statement.

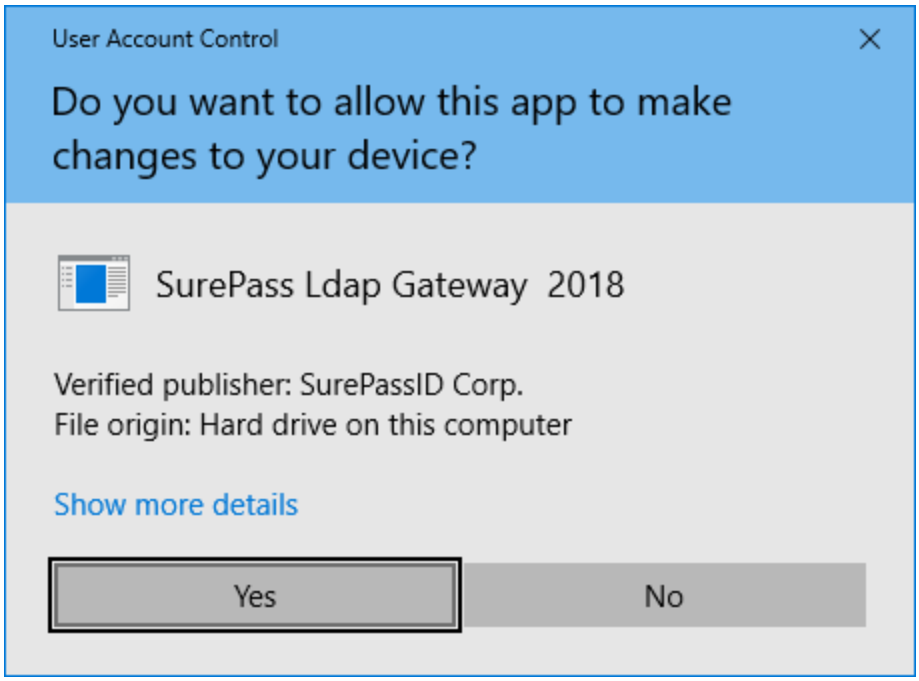

Figure 5: Installation App: Verify Publisher

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

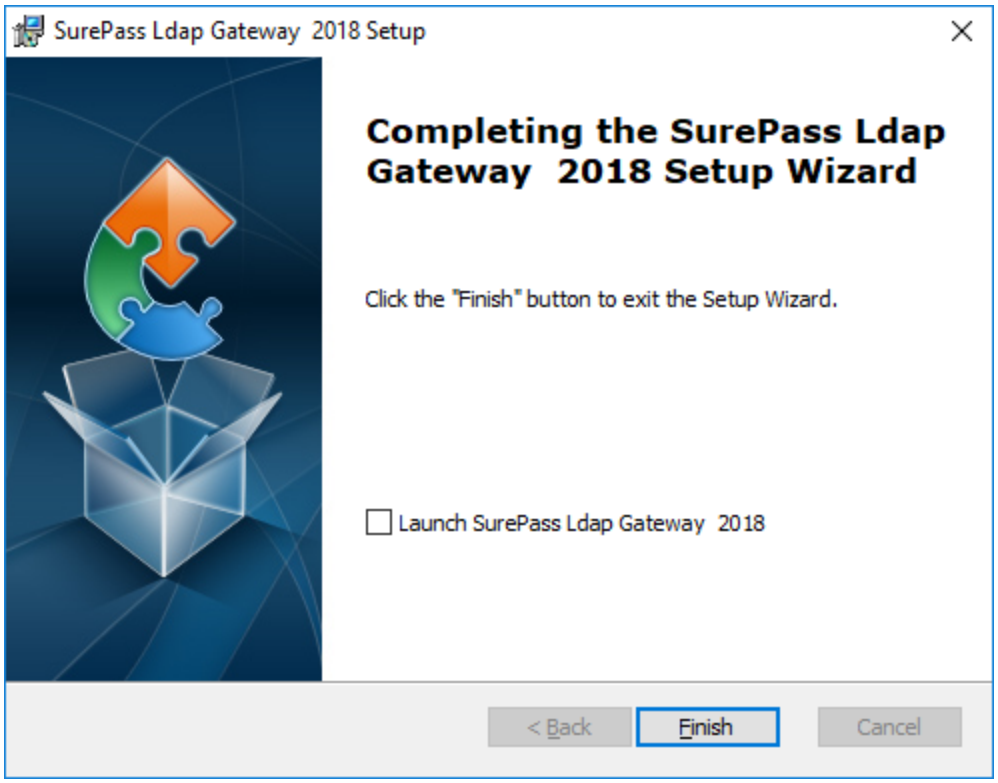

Figure 6: Complete Installation

Installation is complete. You are now ready to configure the system.

Configuration Settings

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

Step1: Configure SurePassID LDAP Secure Gateway Settings

The ldap.conf configuration file is comprised of the following parameters:

```
AuthServerURL=https://sandbox.surepassid.com/AuthServer/REST/OATH/OATHServer.aspx
AuthServerToken=<your account token>
AuthServerKey=<your account key>
AllowSMS=0
AllowEmail=0
AllowCall=0
AllowPushApp=0
AllowPushSMS=0
AllowPushOtp=0
AllowPushAppU2F=0
AllowPushVoice=0
PushAppName=Remote Access
PushAuthnReason=Login
RelyingPartyUrl=
TraceOn=0
LdapAdminDn=cn=Administrator, cn=Users, dc=sptestdomain,dc=local
LdapServerEndPointPort=3899
LdapEndPoint=pookie.homedns.org
LdapEndPointPort=389
TargetDirectory=2
AdDefaultDomain=none
```

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

- **AuthServerURL** – The SurePassID authentication Endpoint URL. In most cases, you will not need to change this unless you are using a custom SurePassID installation. The values are:
    - **sandbox** - The SurePassID sandbox cloud system.
    - **prod** – The SurePassID production cloud system.
    - **Custom SurePassID MFA 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

- **AuthServerToken** - The login name (**Server Login Name**) for your SurePassID account.
- **AuthServerKey** - The login password (**Server Login Password**) for your SurePassID account.
- **AllowSMS** - Allow the user to request an OTP be sent by SMS to their mobile device. 0=no 1=yes
- **AllowEmail** - Allow the user to request an OTP be sent to their email. 0=no 1=yes
- **AllowCall** - Allow the user to request an OTP be sent by voice call. 0=no 1=yes
- **AllowPushApp** - Allow the user to request that a push authentication be sent (pushed) to their mobile device to confirm their identity. Requires the user to have SurePassID Mobile Authenticator installed on their mobile device. 0=no 1=yes
- **AllowPushSMS** - Allow the user to request that an SMS push question can be sent to their mobile device to confirm their identity. 0=no 1=yes
- **AllowPushOtp** - Allow the user to request an OTP be sent to their mobile device. Requires the user to have SurePassID Mobile Authenticator installed on their mobile device. 0=no 1=yes
- **AllowPushAppU2F** - Allow the user to request that they be authenticated on their mobile device with a Fido U2F token. Requires the user to have SurePassID Mobile Authenticator installed on their mobile device. 0=no 1=yes
- **AllowPushVoice** - Allow users to request a voice call that will allow them to confirm their identity. 0=no 1=yes
- **PushAppName** - For push authentications, the name of the application requesting access. The PushAppName is displayed to the user when they receive a push notification. The default is Remote Access.
- **PushAuthnReason** – For push authentications, the reason why the application is requesting access. The default is Login.
- **RelyingPartyUrl** - The URL of the application that is requesting access in push notifications. Push notifications responses will be sent to this URL.
- **TraceOn** - Turn on tracing. The trace file is stored in Trace folder located in the installation folder. It is recommended you only turn on trace to debug issues with the system. When you are done debugging, turn off tracing and delete any trace files that are present. 0=no 1=yes
- **LdapAdminDn** – The default admin user in the target LDAP directory. This user will be used by the server for requests that require administrative access such as LDAP importing. E.g**. cn=Administrator, cn=Users, dc=sptestdomain, dc=local**
- **LdapServerEndPointPort** – The port the SurePass LDAP Gateway server listens on. Default is 3899

- **LdapEndPoint** – The FQDN (or IP) of the target AD/LDAP server. See TargetDirectory below.
- **TargetDirectory** – The target directory for validating the username and password. Values are:
    - **1 -** Active Directory
    - **2 -** LDAP
- **AdDefaultDomain** – This is the default AD domain that will be used for authentication if the target directory TargetDirectory is Active Directory and the user name provided for authentication is not a UPN. If a UPN is is used then that will determine the domain for the user.

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

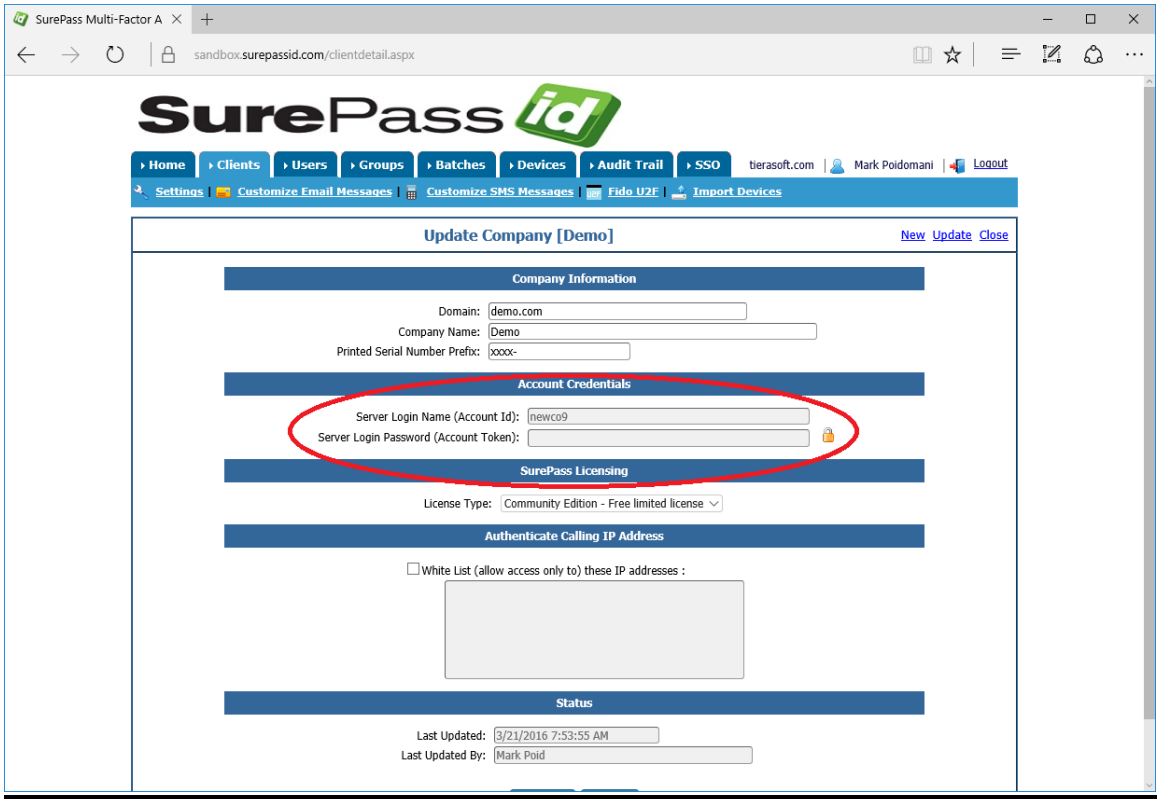

Figure 7: SurePassID Account Settings

Step2: Configure LDAP Application

When using the SurePassID LDAP Secure Gateway the LDAP application is configured the same way as you would for any LDAP server. LDAP applications can vary and if you need help setting up your LDAP application contact SurePassID support and we can assist you to get it up and running.

Step3: Using the LDAP application

After setting up your application to use LDAP Secure Gateway Guide you can try logging into the system. You will need two factors to login. There are several ways to do this and the following examples illustrate this.

LDAP End-User Login Overview & Examples

Example 1 – 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 LDAP 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 254865 as show below:

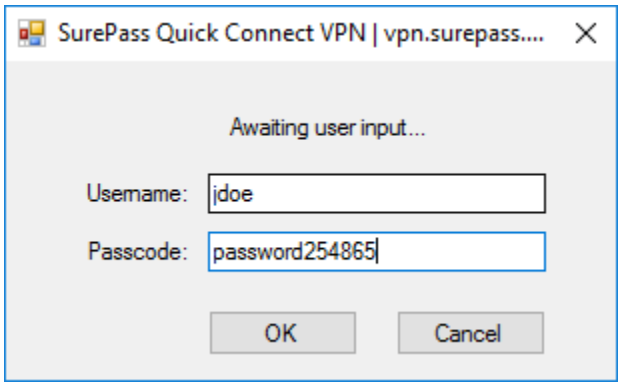

Figure 8: Two-Factor Authentication with Token

4. Press **OK** button to authenticate

Example 2 – Login Using 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 LDAP client software.
2. Enter username.
3. Enter a command in the password field. You can enter these values:

   - # (or **SENDSMS**) to have a code sent via text to your cell phone.

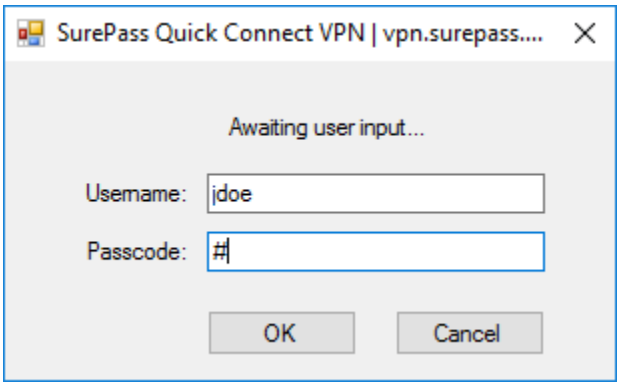

Figure 9: Two-Factor Authentication with SMS Text Code

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

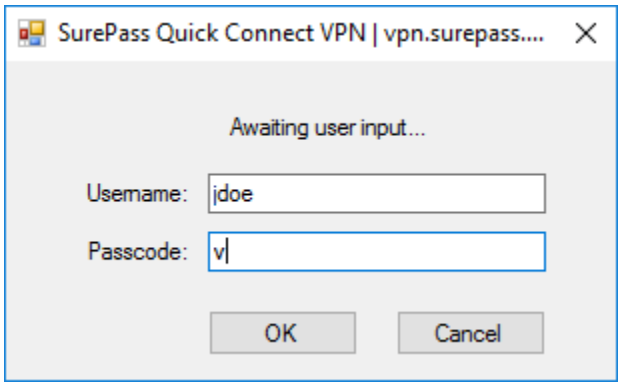

Figure 10: Two-Factor Authentication with Voice Call

   - **m** (or **SENDEMAIL**) to have a code sent via email.

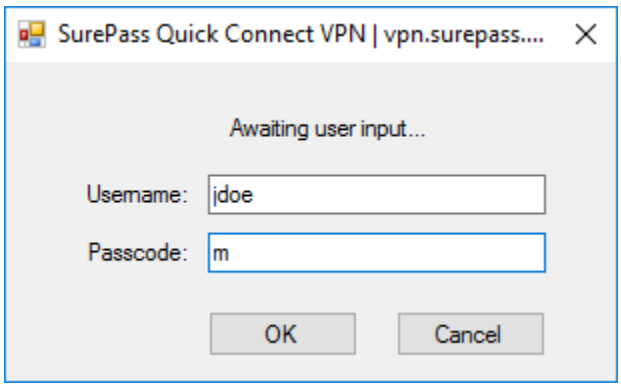

Figure 11: Two-Factor Authentication with Email

4. Press **OK** button to send code.
5. Wait for the code to be delivered to you.
6. Enter the password and concatenate (append) the code you have just received (no spaces after the password). Press **OK** button to authenticate.

Example 3 – Login Using Push SMS/Push Voice

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

1. Start LDAP client software.
2. Enter username.
3. Enter **?** (or **PUSHSMS**) to have a question sent via text to your phone. 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.

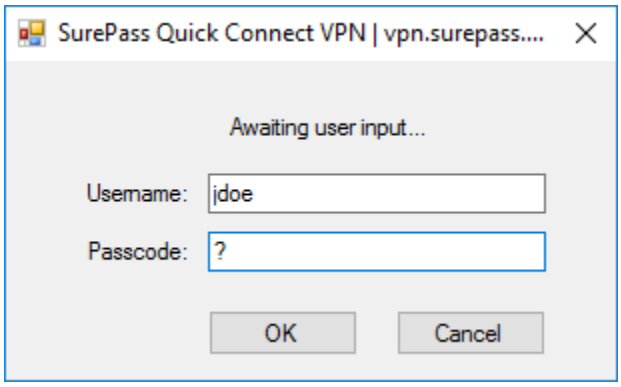

Figure 12: Two-Factor Authentication with SMS Question Part 1

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 authenticate.
7. Wait for confirmation from the server that you have been authenticated.
8. Enter password.

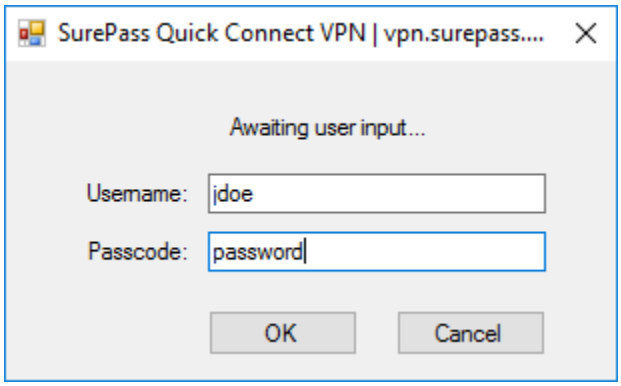

Figure 13: Two-Factor Authentication with SMS Question Part 2

9. Press **OK** button to authenticate.