SurePassID LDAP Gateway Guide

SurePassID Authentication Server 23.1

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

SurePassID, Corp.
360 Central Avenue
First Central Tower
Suite 800
St. Petersburg, FL 33701
USA
+1 (888) 200-8144
www.surepassid.com

Table of Contents

Table of Figures

Introduction

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

The SurePassID LDAP Gateway functions as a proxy between an LDAP based application and an LDAP based directory enhancing it to support Multi-Factor Authentication (MFA) to any LDAP based system/application.

The SurePassID LDAP Gateway uses the native LDAP directory for first factor authentication and requires any SurePassID MFA server (cloud, on-premises) for all multi-factor authentication. One SurePassID LDAP Gateway can support many different LDAP applications. Alternatively, you can have a different LDAP gateway for each LDAP application.

The SurePassID LDAP Gateway can be added to any load balancer backend application pool such as F5, NGINX, Azure Load Balancer, AWS (Amazon Web Services) Load Balancer for scale and server fail-over, disaster recovery.

The system supports the majority of SurePassID MFA capable authentication methods as described below:

Legacy send OTP Options (not recommended by NIST or SurePassID):

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

Push Authentication Options:

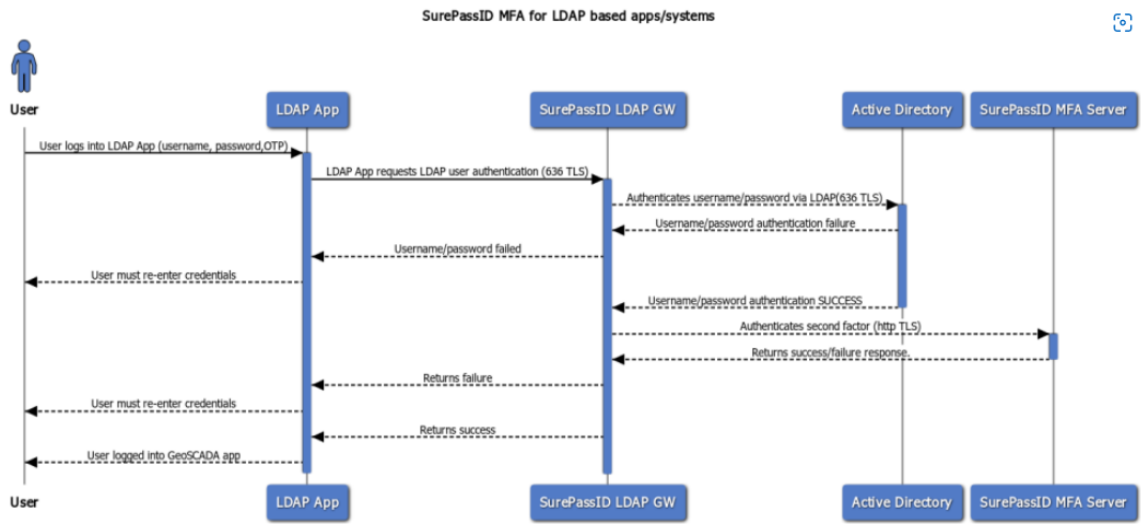
- **Push SMS Question** – A question is sent to the user's mobile device asking the user to confirm a request to allow access to the system. If the user responds positively, the user is allowed to login with just username and password. Requires SMS support turned on in the SurePassID MFA server.
- **Push 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 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 SurePassID portal using the Customize SMS Messages and Customize Email Messages menus.

SurePassID LDAP Gateway supports the following directories:

- **SurePassID Directory** – For use with other cloud systems or external users that are not part of the existing enterprise Active Directory.
- **Active Directory (LDAP)** – For companies that use Windows Active Directory.
- **LDAP Native Directory** – For companies that use a native LDAP directory such as OpenLDAP.

The product architecture is shown in the diagram below is for securing all LDAP applications:



Product Architecture

Prerequisites

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

- Windows 2012 – All versions (Microsoft End-of-Life 10/23/2023)
- Windows 2016 – All versions
- Windows 2019 – All versions
- Windows 2022 – All versions

Post Configuration Steps

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

- Configure LDAP Gateway Server Configuration

These suggestions will be discussed in subsequent sections.

Installing the LDAP Gateway

The LDAP Gateway can be downloaded from the following URL:

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

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

The SurePassID LDAP Gateway is installed as a Windows service.

To start the installation, you must first download the installation file SPLG.zip **file,** unzip the file, and run **SurePassId_LdapGateway2023.exe** on one of your Windows servers and you will see the following installation form:

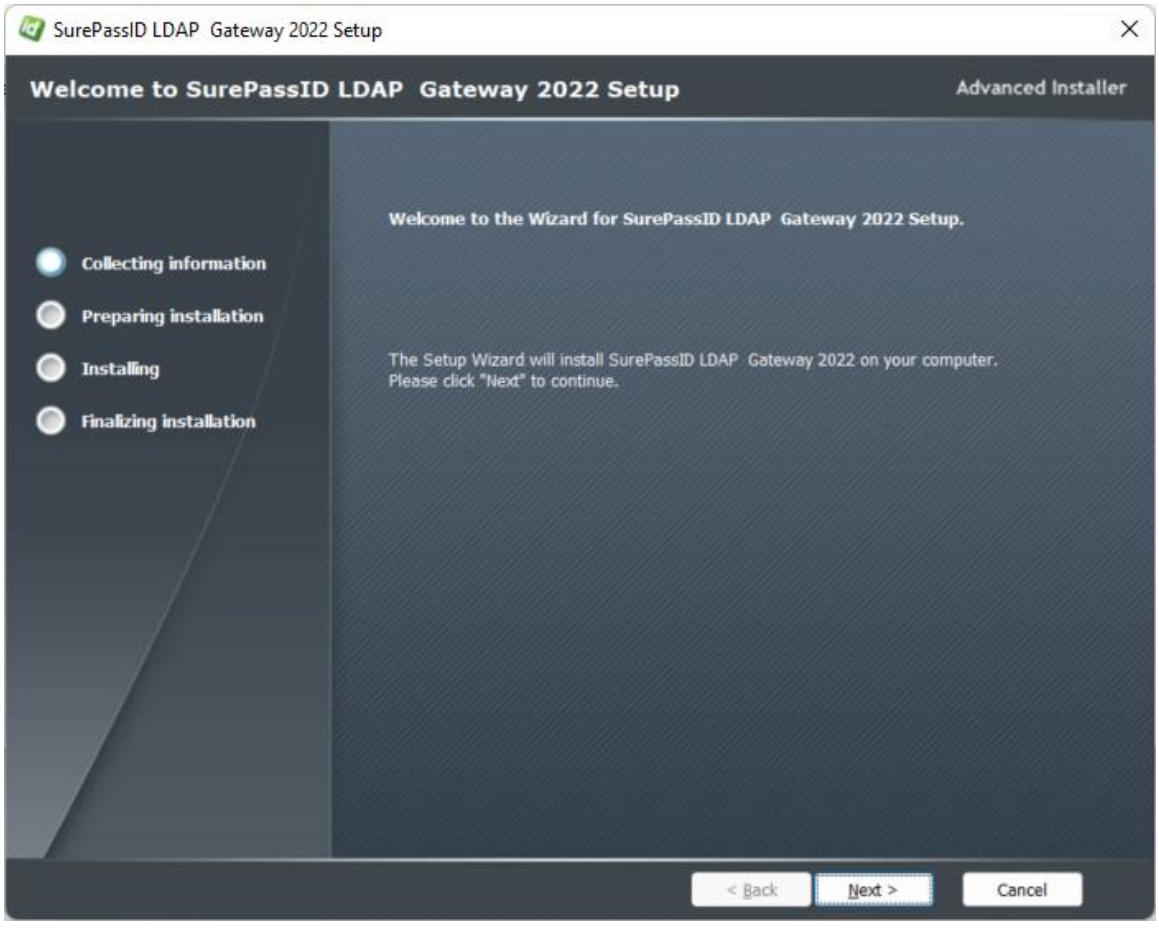


Figure 1: Installation Welcome

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

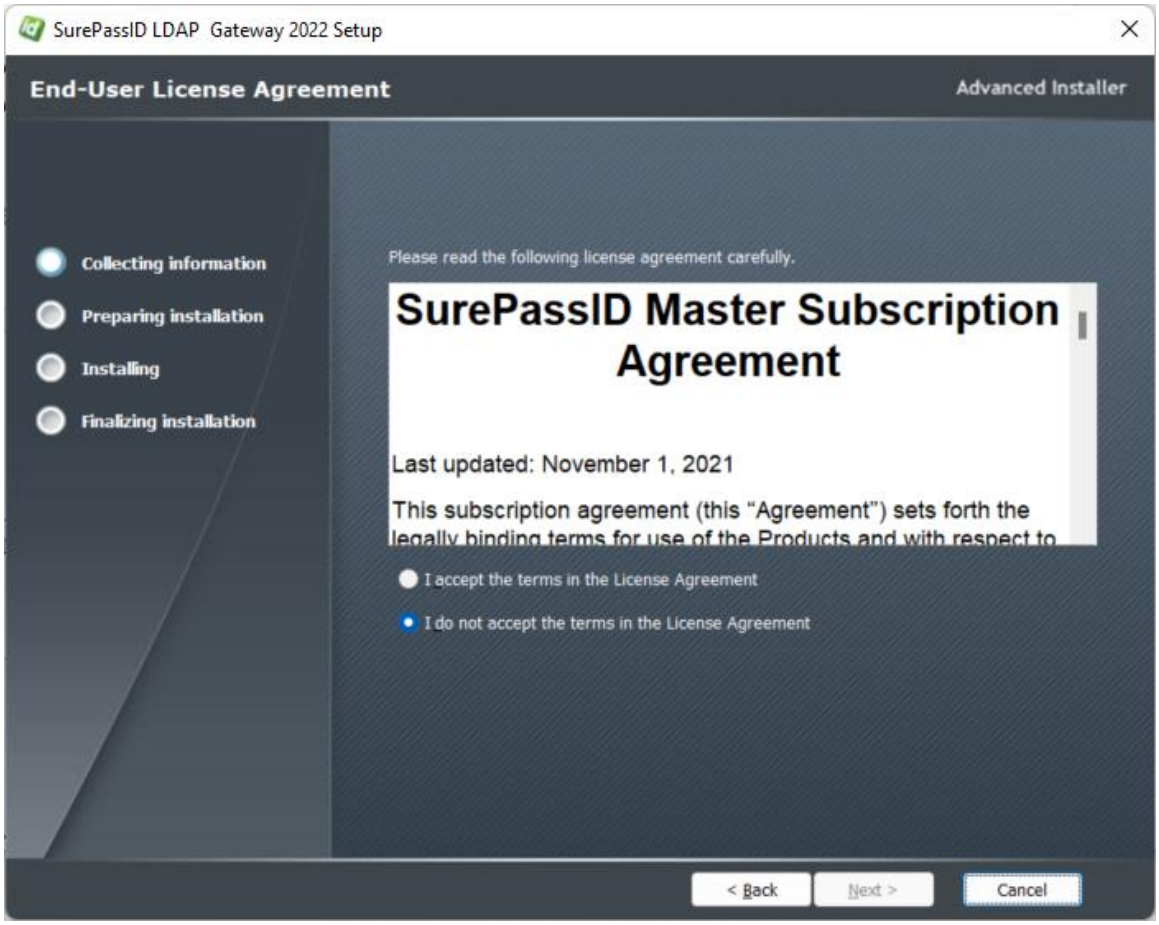


Figure 2: License Agreement

Read the Master Subscription License Agreement and if you accept the terms then click the **Next** button and you will see the installation folder form.

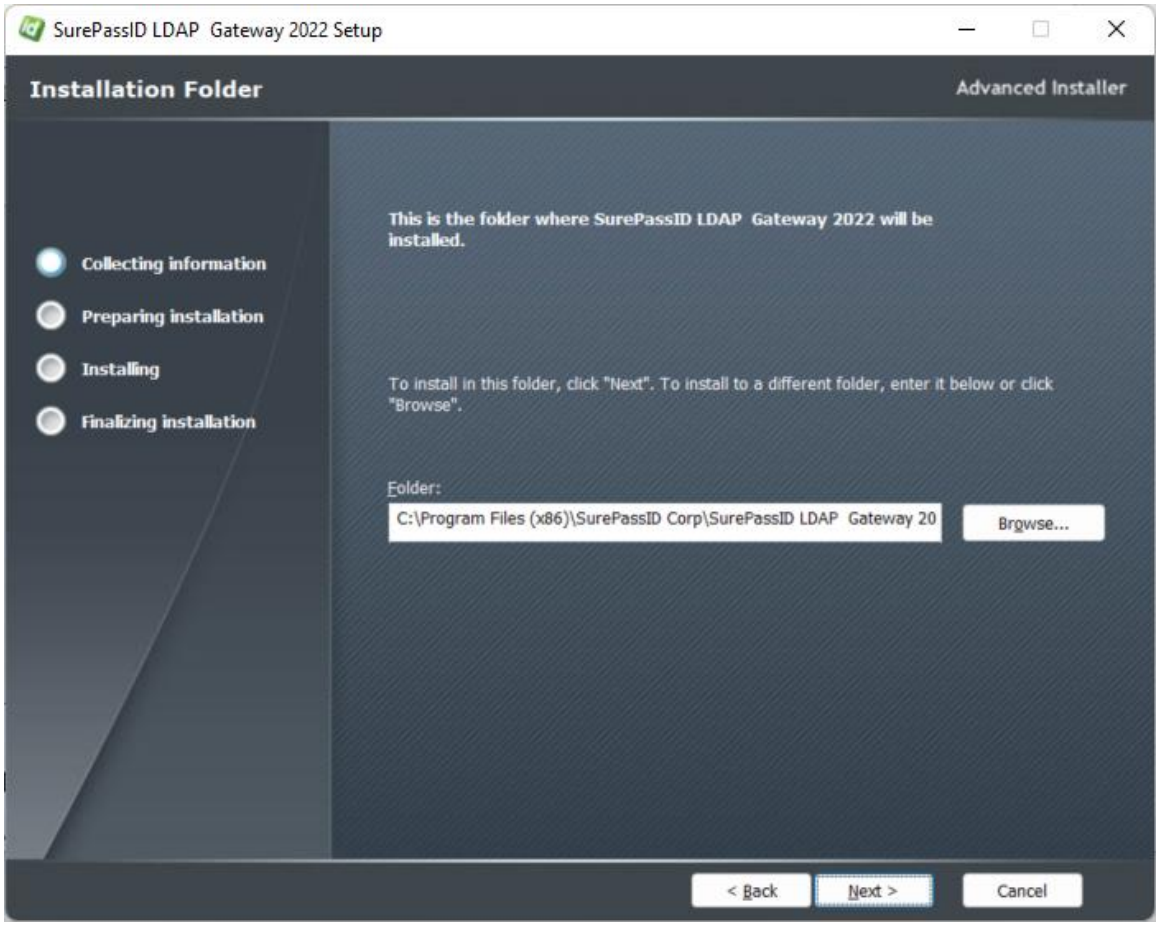


Figure 3: Installation Location: Specify Installation Folder

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

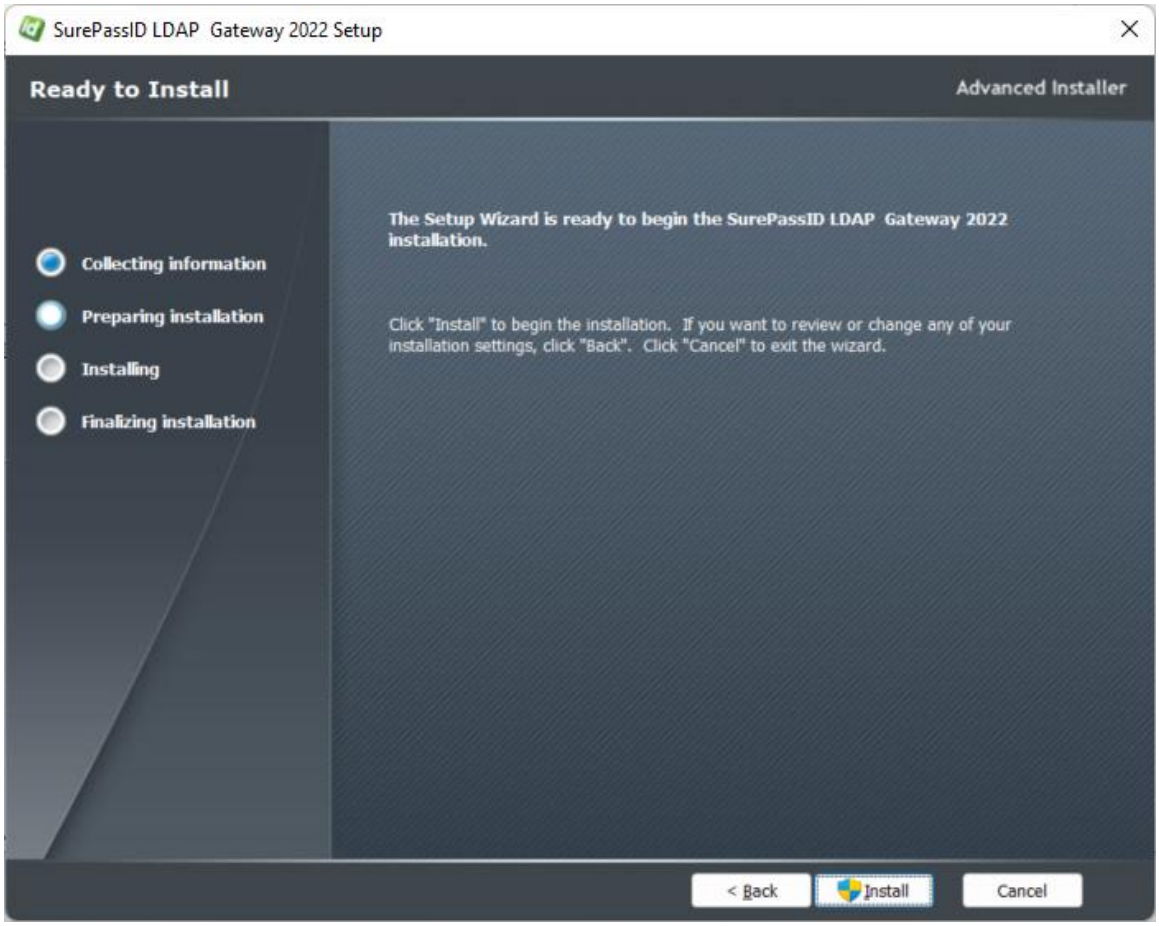


Figure 4: Ready to Install:

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

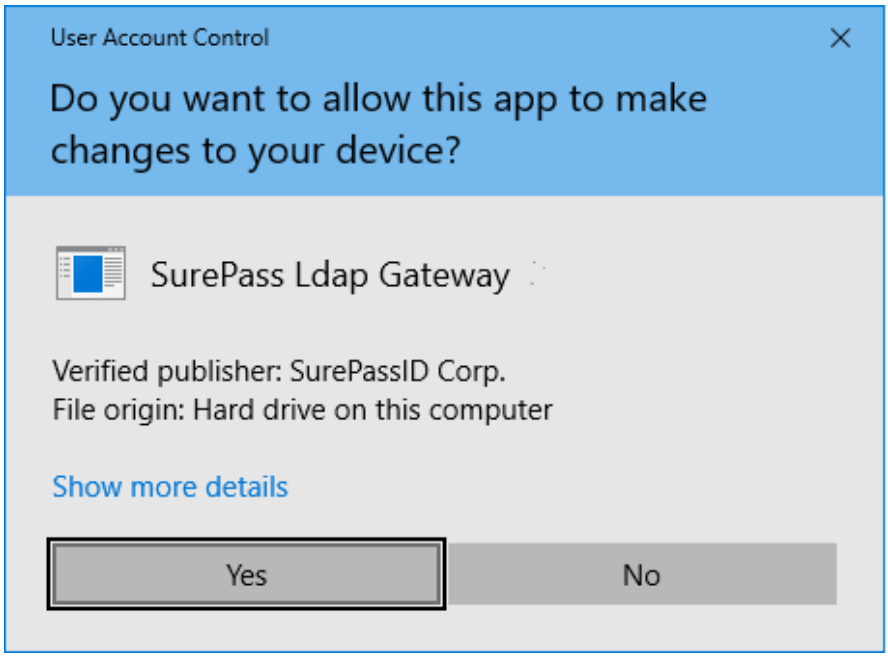


Figure 5: Installation App: Verify Publisher

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

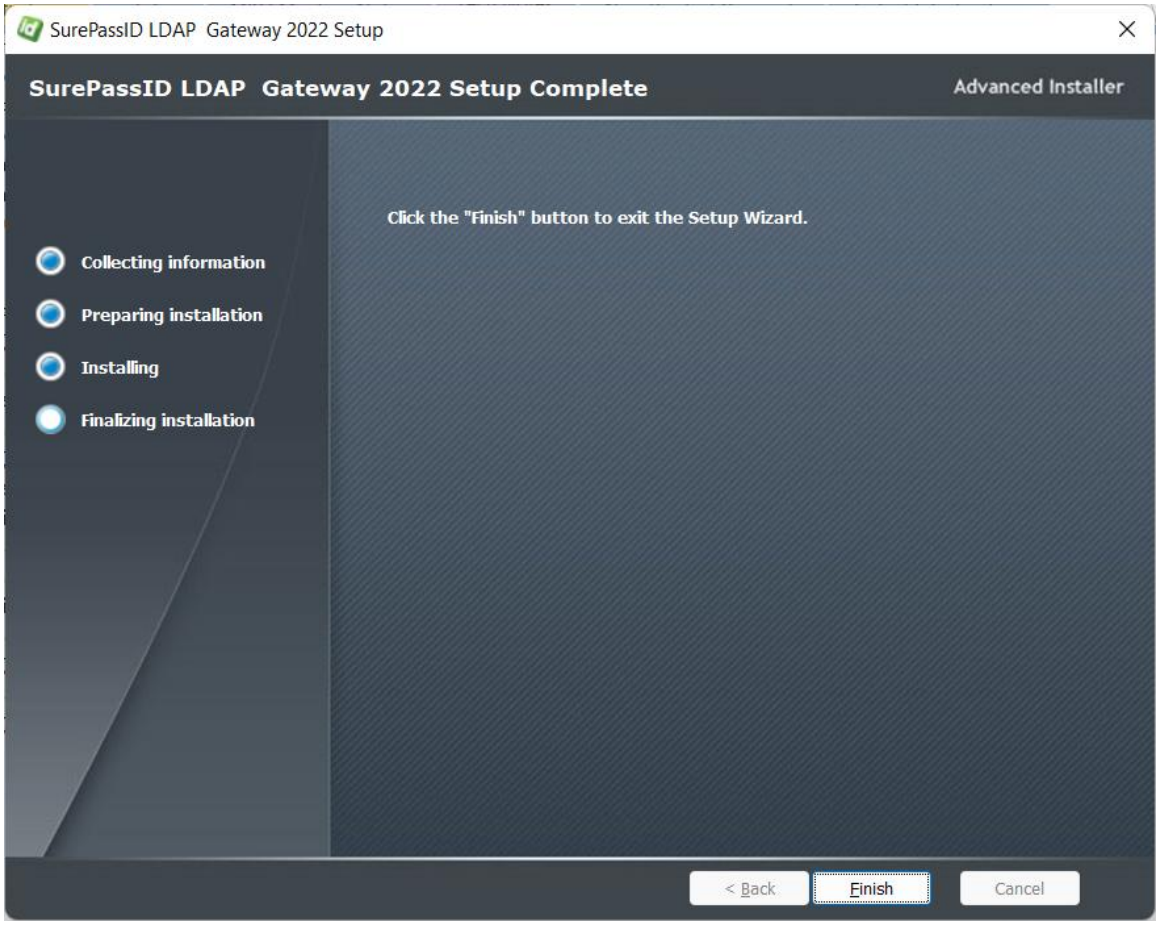


Figure 6: Complete Installation

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 2022.

Step1: Configure SurePassID LDAP Gateway Settings

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

```
//SurePassID MFA Server Settings
'AuthServerURL=https://sandbox.surepassid.com/AuthServer/REST/OATH/OATHServer.aspx
AuthServerURL=https://cloud2.surepassid.com/AuthServer/REST/OATH/OATHServer.aspx
AuthServerKeyIdentifier=<you must fill this in with the appropriate application id>
AuthServerKey=<you must fill this in with the appropriate application key>
AllowSMS=0
AllowEmail=0
AllowCall=0
AllowPushApp=0
AllowPushSMS=0
AllowPushVoice=0
PushAppName=Ldap App Access
PushAuthnReason=Login
//Ldap Server Settings
LdapBaseDn=
LdapEndPoint=<fill this in with your real LDAP server endpoint>
LdapUseTls=true
LdapEndPointPort=636
LdapTargetDirectory=ActiveDirectory
'LdapReceiveTimeoutSeconds=
'LdapSendTimeoutSeconds=
// SurePassID Gateway Settings
LdapGatewayPort=636
LdapGatewayServiceAccount=CN=readonly_service_acct,OU=OU,DC=your_domain,DC=us
LdapGatewayServiceAccountPw=<fill this in with the password for ServiceAccount>
'LdapGatewaySslCertificatePfxPath=SP_LDAP_TEST_CERT.pfx
LdapGatewaySslCertificatePfxPw=test_cert_do_not_use
LdapGatewaySslCertificateThumbprint=D98FFD8B00871987A6046EF20B19A30793182D7C
TraceLevel=0
```

Figure 7: Sample LDAP Gateway Configuration File

The format of the configuration file is one setting per line, each setting is a combination if an option name and value are separated by an equal (=) sign. Lines proceeded with an apostrophe are used as comments.

Descriptions of each option are described in the following sections.

SurePassID MFA Server Settings

- **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 installation of the SurePassId MFA server. The format of this parameter is usually:

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

- **AuthServerKeyIdentifier** - 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
- **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.

LDAP Server Settings

- **LdapTargetDirectory** – The target directory used for first factor (username & passwod) authentication. Values are:
  - **ActiveDirectory** – Native Active Directory connection using the LSA. Must specify the **ActiveDirectoryDomain** paramter.
  - **Ldap –** Any Ldap directory. Must specify the **LdapEndPoint**, **LdapEndpointPort** and **LdapUseTls** parameters.
  - **SurePassID –** SurePassID directory
- **ActiveDirectoryDomain** – The Active Directory domain that will be used to authenticate the users first factor.
- **LdapBaseDN** – The baseDN that will be appended to the DN from the LDAP application. In most cases you can leave this blank.
- **LdapEndPoint** – The FQDN (or IP) of the target AD/LDAP server.
- **LdapEndpointPort** – The port the target LDAP server listens on. Default is 389. Port 389 is the standard port for non-secure LDAP. This is not acceptable for production. You should use port 636 and configure SSL parameters below.

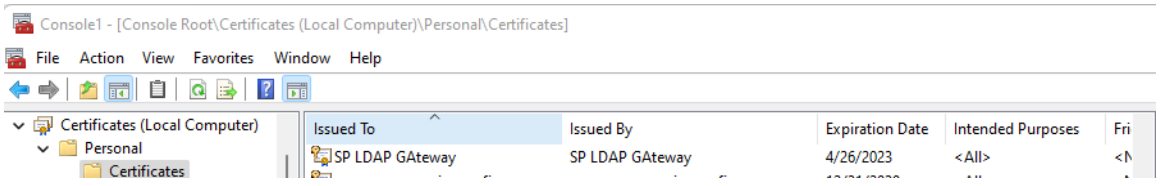
- **LdapUseTls** – Set the gateway to use TLS when communicating with the Ldap server. 0=no 1=yes
- **LdapReceiveTimeoutSeconds** – Setting the maximum number of seconds the gateway will wait to receive data from the LDAP/AD server. Default is 10 seconds.
- **LdapSendTimeoutSeconds** - Setting the maximum number of seconds the gateway will wait sending data to the LDAP/AD server. Default is 10 seconds.

LDAP Gateway Server Settings

```
CN=readonly_service_acct,OU=OU,DC=your_domain,DC=us
```

- **LdapGatewayPort** – The port the SurePassID LDAP Gateway server listens on. Default is 389. 636 is usually used for secure (SSL/TLS) connections.
- **LdapGatewayServiceAccount** – The default user service account in the target LDAP/Active Directory directory. This user will be used by the server for requests that require non-authenticated searches. This user account should have read-only privileges and is specified in distinguished name format. For example:
- **LdapGatewayServiceAccountPW** – The password for the service account (**LdapGatewayServiceAccount**)

- **LdapGatewaySslCertificateThumbprint** – This is the thumbprint for the SSL certificate that is used to secure communications between the LDAP application and the gateway. If you are using port 636 for secure communications (the standard LDAP port for TLS) then you must specify this parameter, or the LDAP application will not be able to connect to the gateway.
- **LdapGatewaySslCertificatePfxPath** – The path to the SSL certificate. If this field is commented out (and it is by default) then the system will look for the certificate in the **Local Computer/Personal/Certificate** store (recommended) as shown below:



- **LdapGatewaySslCertificatePfxPw** – Password for the certificate identified by the **LdapGatewaySslCertificateThumbprint.**

- **TraceLevel** – Sets the level of system tracing. The trace file is stored in the Trace folder located in the installation folder. It is strongly 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. Options are:
    - 0 - No tracing.
    - 1 - Application tracing.
    - 2 – In and outbound tracing packet tracing. **Only for extreme debugging situations and should never be left on. It could expose sensitive information.**

If you are using an MFA server version prior to 2022.2 you can retrieve the **AuthServerKeyIdentifier** from the **Account Id** and **AuthServerKeyToken** from **Account Token** from your SurePassID account as shown below. To view the password, click the 'lock' icon to toggle the display of the password:

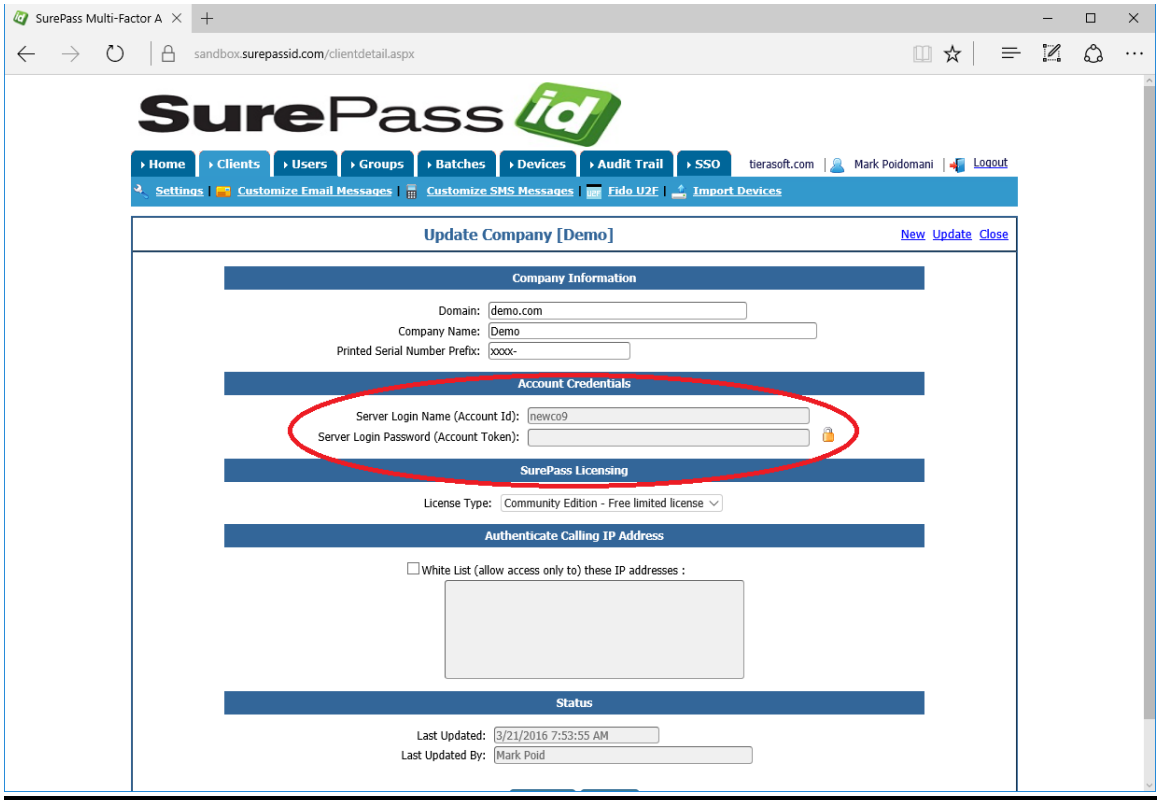


Figure 8: SurePassID Account Settings

If you are using MFA server 2022.2 you can retrieve the **AuthServerKeyIdentifier** from the **Key Identifier** field and

AuthServerKeyToken from **Key** field in your SurePassID account as shown below:

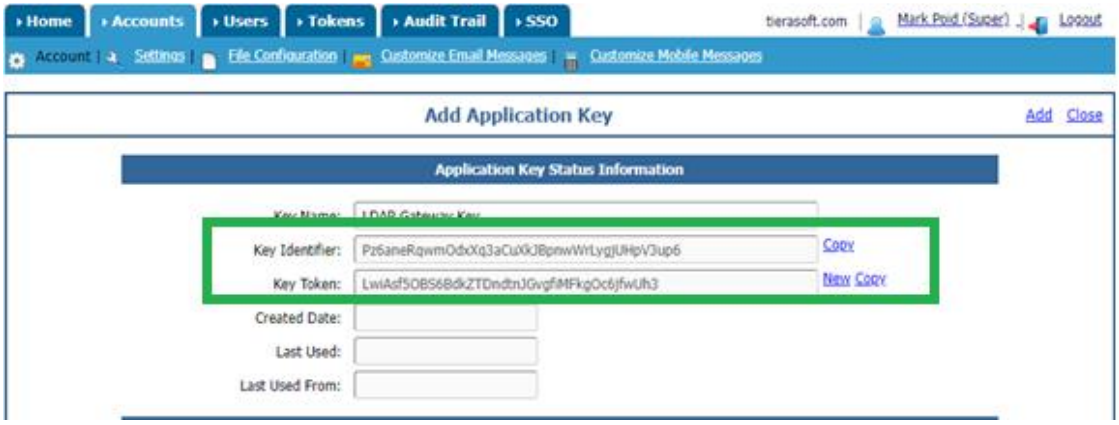


Figure 9: SurePassID Account Settings 2022.4

This requires that you add an LDAP app key as shown below:

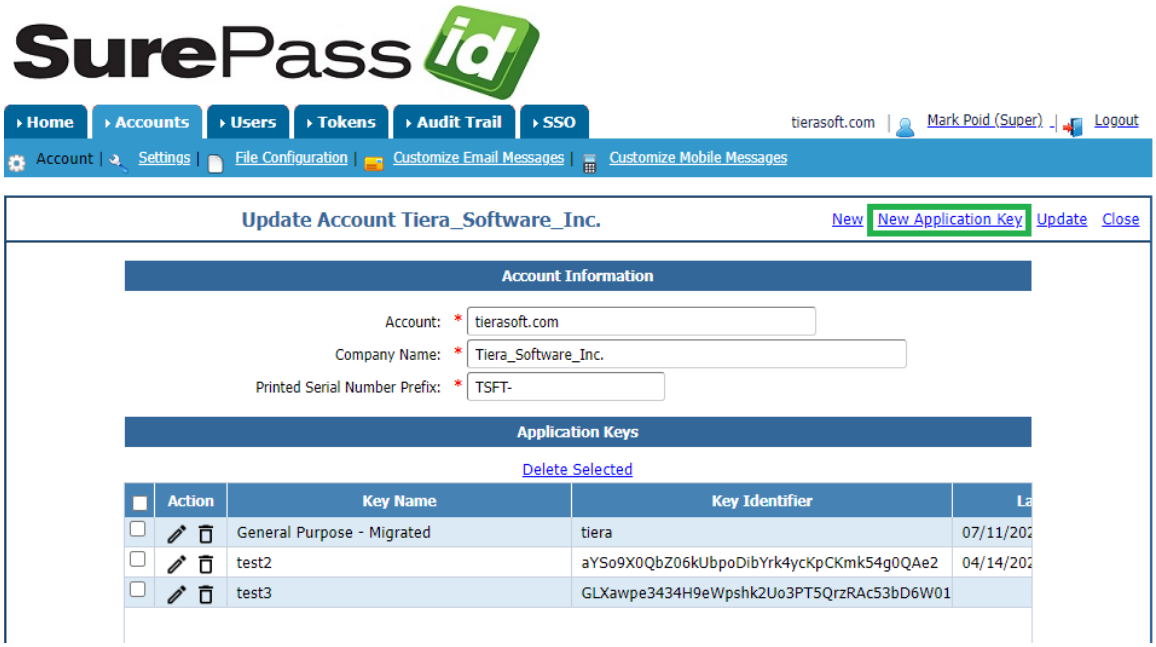


Figure 10: SurePassID Create Application Key 2022.2

Step2: Configure LDAP Application

When using the SurePassID LDAP 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 LDAP application to use SurePassID LDAP Gateway you can test logging into the system. To login You will need two factors. This would be your first factor (username and password which you already know) and second factor (One Time Passcode). The One Time Password (OTP) can come from a hard token (FOB, Display card) or a soft token such as the SurePassID Mobile Authenticator app.

To login securely to you LDAP application that has been configured to use the LDAP Gateway follow these steps:

```
your_current_password,123456
```

1. In the User field enter your username.
2. In the Password field enter your current password followed by a comma and your OTP as shown below:

3. Press the usual button you use to login. If **your_current_password** and OTP are correct, then you will be logged in to the system.

```
your_current_password,push_request
```

You can also use push notifications login to your LDAP application as an alternative/additional two factor method to an OTP. You can do this by changing the format of the password field to the following form:

Where **push_requst** can be one of the following values:

? – Send push authentication
?? -Send MSMS push
– send push voice. Call

When using push authentication, the login flow is:

1. In the User field enter your username.
2. In the Password field enter your current password followed by a comma and your **push_request**. For example, to login using a push notification (assuming your password is Ggg7bb5688&Pw) you would enter:

```
Ggg7bb5688&Pw,?
```

3. When you receive the push notification and approve it you will be logged into your LDAP application. Never approve a notification if it is not requested by you and also look at the notification to verify it is for the LDAP app you are logging into.

SSL/TLS Certificate Set-up

For the SurePassID LDAP Gateway to accepts TLS requests you will need to:

1. Create a certificate with private key using PowerShell
2. Update the ldap.config file to specify the new certificate by its thumbprint.

Step1: Create certificate with private key using PowerShell

To create the certificate and store it in Local Computer/Personal/Certificate use the PowerShell script below. You must run this script as an Administrator. This script (ldap_create_cert.ps1) is also provided in the scripts sub-folder of the installation folder.

NOTE: You can tailor the script to meet your company standards by changing the certificate Expiration Date ($ed) and Subject Name ($sn) variables.

```
$ed = Get-Date -Date "12/31/2025 23:59:59"
$sn = "CN=SurePassID LDAP Gateway TLS"
Write-OutPut "Starting the LDAP Gateway certificate generation process....."

Write-OutPut "Creating self-signed cert and placing it in Local
Computer/Personal/Certificate store…"
$cert=New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -
Subject $sn -NotAfter $ed -KeyExportPolicy Exportable -KeySpec Signature -
KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
Write-OutPut "Certificate created. Please take note of the change to
ldap.conf below:"

$tn=Get-ChildItem Cert:\LocalMachine\my -Recurse | Where { $_.Subject -eq
$sn} | Select Thumbprint

Write-OutPut ""
Write-OutPut "-----------------update ldap.config----------------"
Write-OutPut " Update line:
LdapGatewaySslCertificateThumbprint="$tn.Thumbprint" "
```

Step2: Update the ldap.config file to specify the certificate by its thumbprint.

When the script in Step 1. runs it will give you instructions of how to update the ldap.conf file. Look for:

Update line:
LdapGatewaySslCertificateThumbprint=CERTIFICATE_THUMBPRINT

```
$expirationdate = Get-Date -Date "12/31/2025 23:59:59"
$sn = "CN=SurePassID LDAP Gateway xx"
Write-OutPut "Starting the LDAP Gateway certificate generation process....."

Write-OutPut "Creating self-signed cert and placing it in Local
Computer/Personal/Certificate ...."
$cert=New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -
Subject $sn -NotAfter $expirationdate -KeyExportPolicy Exportable -KeySpec
Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
Write-OutPut "Certificate created. Please take note of the change to ldap.conf
below:"

$tn=Get-ChildItem Cert:\LocalMachine\my -Recurse | Where { $_.Subject -eq $sn} |
Select Thumbprint

Write-OutPut ""
Write-OutPut "-----------------update ldap.config----------------"
Write-OutPut " Update line: LdapGatewaySslCertificateThumbprint="$tn.Thumbprint"
"
```