

# SurePass

## SurePassID Directory Sync Guide

SurePassID Authentication Server 2024



© 2013-2024 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.**

360 Central Avenue

First Central Tower

Suite 800

St. Petersburg, FL

USA

+1 (888) 200-8144

# Table of Contents

<b>Table of Figures.....</b>	<b>4</b>
<b>What is the Directory Sync Application? .....</b>	<b>5</b>
<b>Installing the Directory Sync Application .....</b>	<b>5</b>
<b>Configuring the Directory Sync Application.....</b>	<b>8</b>
Security Considerations.....	9

# Table of Figures

No table of figures entries found.

## What is the Directory Sync Application?

The SurePassID User Synchronization App allows you to 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.

## Installing the Directory Sync Application

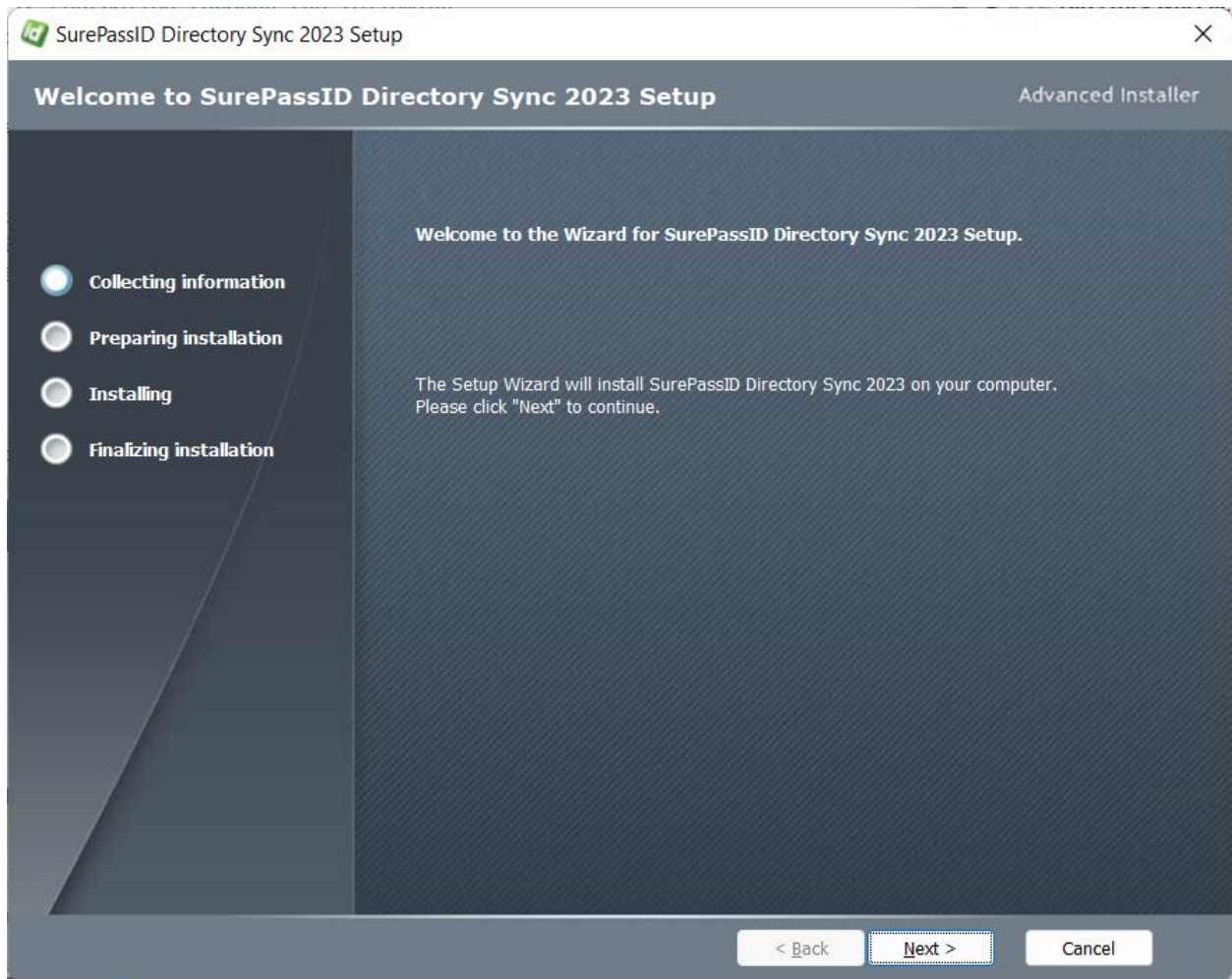
To install the Directory Sync application, you must first download and unzip the installer from here:

<https://downloads.surepassid.com/DS/SPDS.zip>

After downloading the file unzip, unzip the file and run the installer file **SurePassID\_DirSync2023.exe**.

**The installer and application is digitally signed by SurePassID. You must verify that as part of the installation.**

Then you will see the following installation screen.

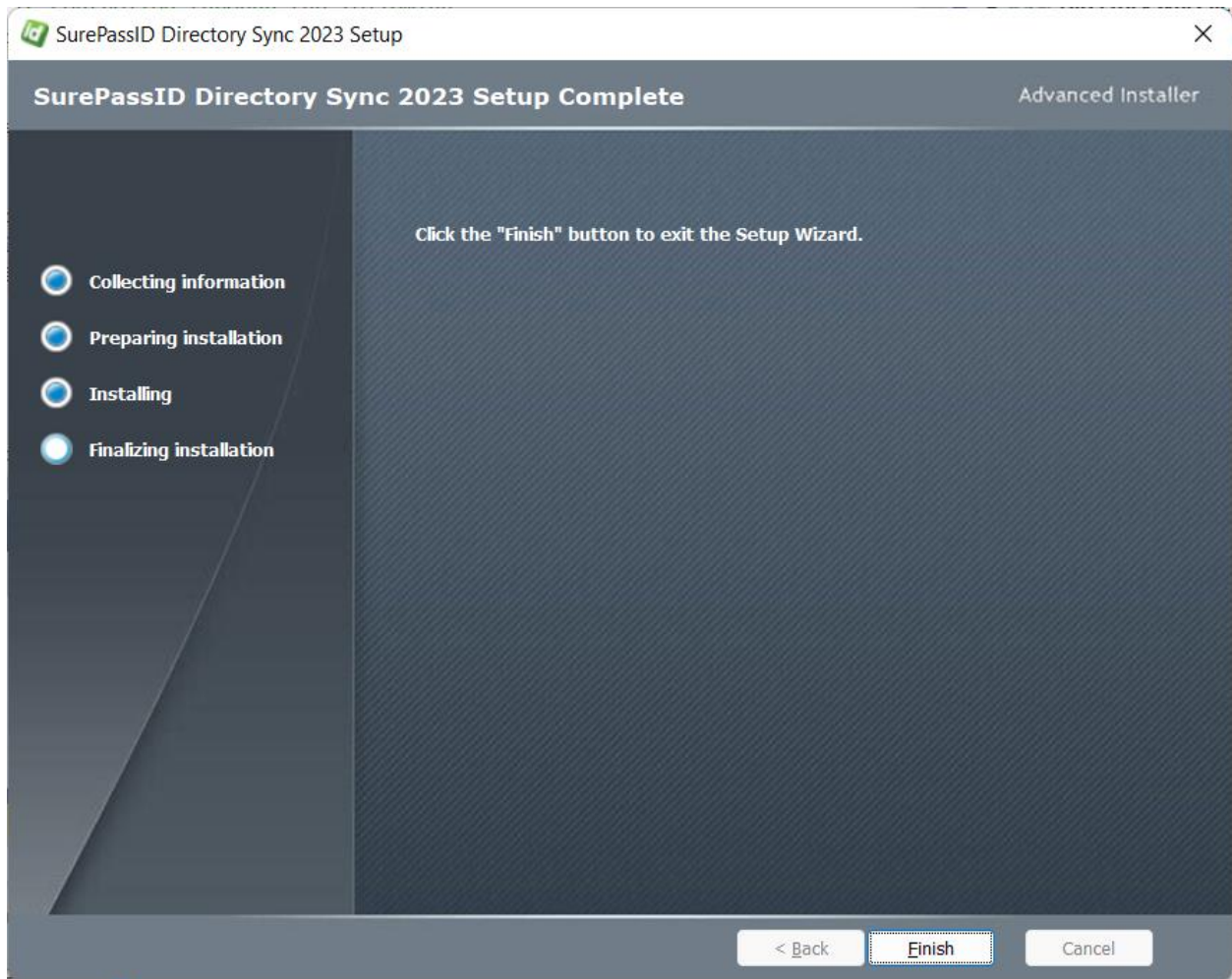


Follow the prompts until you get to the **User Access Control** screen.

**You must verify that the publisher is SurePassID Corp. If not, then press the No button.**

When you press the **Yes** button the application will be installed.

When installation is complete you will see the following screen:



Press the **Finish** button to complete the installation.

# 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 Directory Sync folder.

**C:\Program Files (x86)\SurePassID Corp\SurePassID Directory Sync 2023**

To run the **Directory Sync** app, use the following syntax:

```
DirectorySync -ln=loginname  
-lp=loginpassword  
-add=activedirectorydomain  
[-adf=activedirectoryfilter]  
[-syncsource= AD | XML]  
[-restendpoint=serverendpoint]  
[-xmluserpath=pathofxmluserimportfile]
```

where

**-ln** – SurePassID Key Identifier

**-lp** – SurePassID Key

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

**-activedirectoryfilter:** – Active Directory filter (LDAP format) to synchronize a subset of the Active Directory domain. For a brief tutorial you can look [here](#). Another resource that can be helpful is [here](#). The default value is:  
(&(objectCategory=person)(objectclass=user))

**-syncsource** - AD or XML. The source of user information to sync with the MFA server. AD is ActiveDirectory and XML is an XML source. AD is the default.

**-restendpoint** – SurePassID Authentication server 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 – The on-premises or custom SurePassID server endpoint.  
The format of this parameter is usually:

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

**-xmluserpath** – If you specify **syncsource=XML** the use this parameter to set the full path of the XML file to be imported.

The Directory Sync application synchronizes the following data:

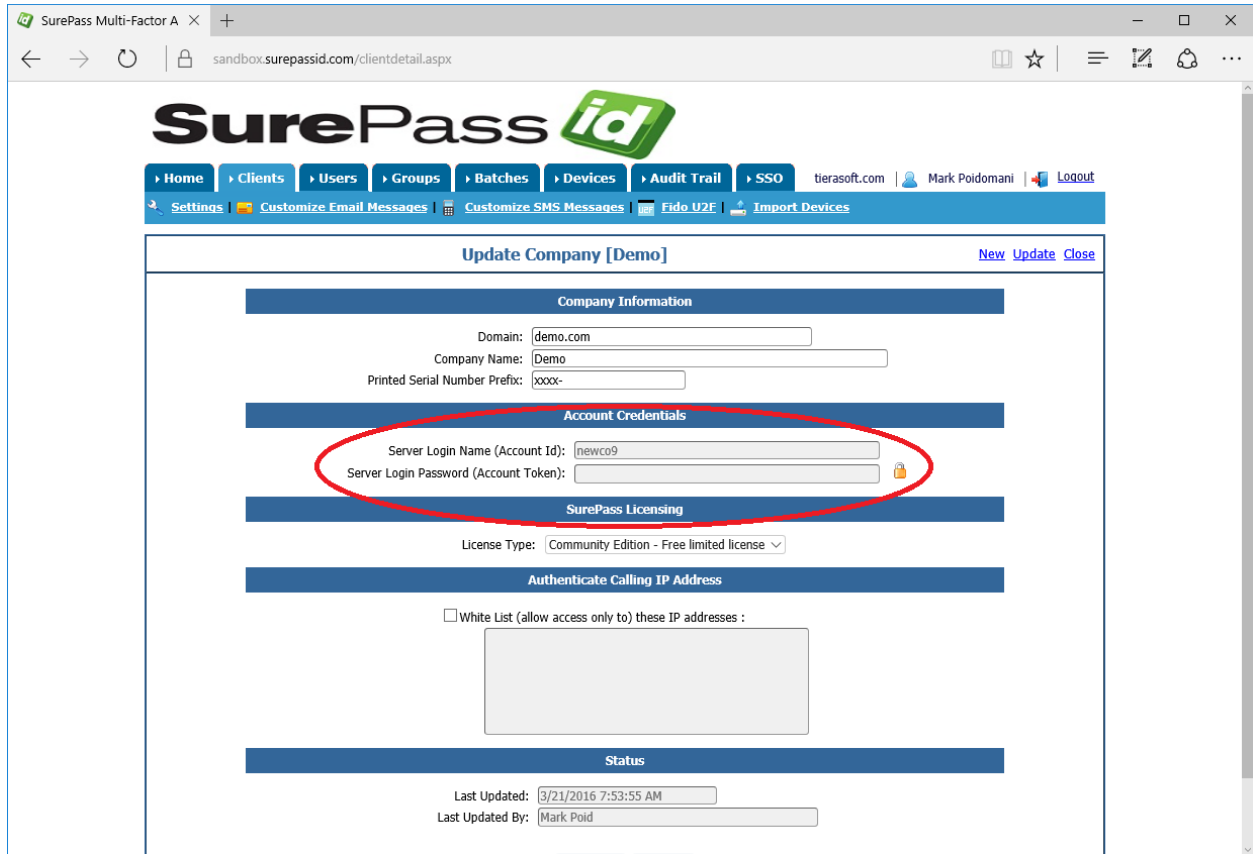
- Username (same as account name)
- First Name (given name)
- Last Name (surname)
- Email (email)
- Mobile Number (mobile)

The **Directory Sync** app 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.

## Using the Directory Sync App with SurePassID MFA Server

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

If you are using an older version of SurePassID MFA server you will see the following info for your account as shown below.



The **Server Login Name** parameter is the **-ln** and the **Server Login Password** parameter is the **-lp**. To view the **Server Login Password**, click the 'lock' icon to toggle the display of the password.

If you are using the latest version of SurePassID you will see the following info for your account:

Home Accounts Users Tokens Audit Trail SSO tiersoft.com Mark Poid (Super) Logout

Account Settings File Configuration Customize Email Messages Customize Mobile Messages



### Update Account DEMO-COMPANY [Update](#) [Close](#) [New Application Key](#)

#### Account Information

Account: \* demo.com  
Company Name: \* demo.com  
Printed Serial Number Prefix: \* DEMO

#### Application Keys

[Delete Selected](#)

Action	Key Name	Key Identifier	Last
<input type="checkbox"/>  	DEMO-API-KEY	fQDOSS5rCo03LpWsOydo7eVCQFbAdErru8MpLo28	

Data Protection: SurePassID Local

All application requests to the MFA Server require an **Application Key**. To create a new **Application Key** just for **DirectorySync** app (recommended) click the **New Application Key** link and see the form below:

Add Application Key
[Add](#) [Close](#)

**Application Key Status Information**

Key Name:

Key Identifier:  [Copy](#)

Key:  [New Copy](#)

Created Date:

Last Used:

Last Used From:

**Application List**

Permission Templates:  ▼

Allow	Access Right	Application	Access Category
<input type="checkbox"/>	AddOathDevice	add_oath_device	Token Manager
<input type="checkbox"/>	AddPushAccount	provision_push_device   add_push_user_device	Push Token Ma
<input type="checkbox"/>	AddU2FDevice	add_u2f_device	Token Manager
<input type="checkbox"/>	AddUser	add_user   add_oath_user   add_u2f_user	Directory Mana
<input type="checkbox"/>	ChangeUserPassword	change_user_password	Directory Mana
<input type="checkbox"/>	CheckSessionToken	is_session_token_valid	Session Manage
<input type="checkbox"/>	CreateServerChallenge	create_server_challenge	Authentication
<input type="checkbox"/>	CreateSessionToken	create_session_token	Session Manage
<input type="checkbox"/>	DeleteDevice	delete_device	Token Manager
<input type="checkbox"/>	DeletePushAccount	delete_push_user_device	Push Token Ma
<input type="checkbox"/>	DeleteUser	delete_user	Directory Mana
<input type="checkbox"/>	DeviceActivation	active_oath_device	Token Manager
<input type="checkbox"/>	DeviceAssignment	assign_device   unassign_device	Token Manager
<input type="checkbox"/>	DeviceStatus	enable_device   disable_device	Token Manager
<input checked="" type="checkbox"/>	DirectorySync	directory_sync_start	Directory Mana
<input type="checkbox"/>	EventLogSync	event_log_sync_start	Event Log Man
<input type="checkbox"/>	ExpireSessionToken	expire_session_token	Session Manage
<input type="checkbox"/>	FidoU2FDelete	delete_key   delete_all_keys	Token Manager

The **Key Name** is the friendly name to identify this key. It is not used for any security purposes. For instance, you could name it **Dir Sync Key**.

Select the **Directory Sync** from the **Permissions Templates** drop down list.

The **Key Identifier** parameter is the **-In** and the **Key** parameter is the **-Ip**. and press the **Add** button.

Copy **Key Identifier** and **Key** for later use when configuring **Directory Sync**. Once you click the **Add** button the **Key** will no longer be viewable. If you forget the **Key**, you can delete this **Application Key** and add a new one.

A word of caution. Once an **Application Key** is deleted any application that is currently using that **Application Key** will no longer be permitted access to the MFA Server and the application will fail. An **Application Key** cannot be recovered. A new one must be created, and the application must be updated to use the new **Application Key**.

## Security Considerations

Directory Sync App requires TLS 1.2 or TLS 1.3 for transport security.