

SurePass

SurePassID Directory Sync Guide

SurePassID Authentication Server 2025



© 2013-2025 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

www.surepassid.com

Table of Contents

Table of Figures.....	4
What is the Directory Sync Application?	5
Installing the Directory Sync Application	6
Configuring the Directory Sync Application.....	9
Running the Directory Sync Application	9
Using the Directory Sync App with SurePassID MFA Server	14
Creating LDAP Filters (-sync_source=AdLdapFilter).....	16
Using Active Directory Groups (-sync_source=AdGroup)	17
Security Considerations	17

Table of Figures

No table of figures entries found.

What is in this document?

This guide explains how to install, configure, and use the SurePassID Directory Sync application to synchronize user data from existing directory services.

- **Directory Sync Application:** Updates user information like names, phone numbers, and emails; does not sync passwords.
- **Installation:** Download, unzip the installer from the link, verify the digital signature.
- **Configuration:** Sync Active Directory user info with SurePassID via command line or config files.
- **Running the App:** Document provides command line syntax and options for user management and token creation.
- **SurePassID MFA Server:** API keys needed for user sync and permissions when creating tokens.
- **Security:** Requires TLS 1.2 or TLS 1.3 for secure data transmission.

What is the Directory Sync Application?

The SurePassID Directory Sync App updates user details like First Name, Last Name, Phone Number, and Email from existing directory services. Note that SurePassID never synchronizes passwords.

Installing the Directory Sync Application

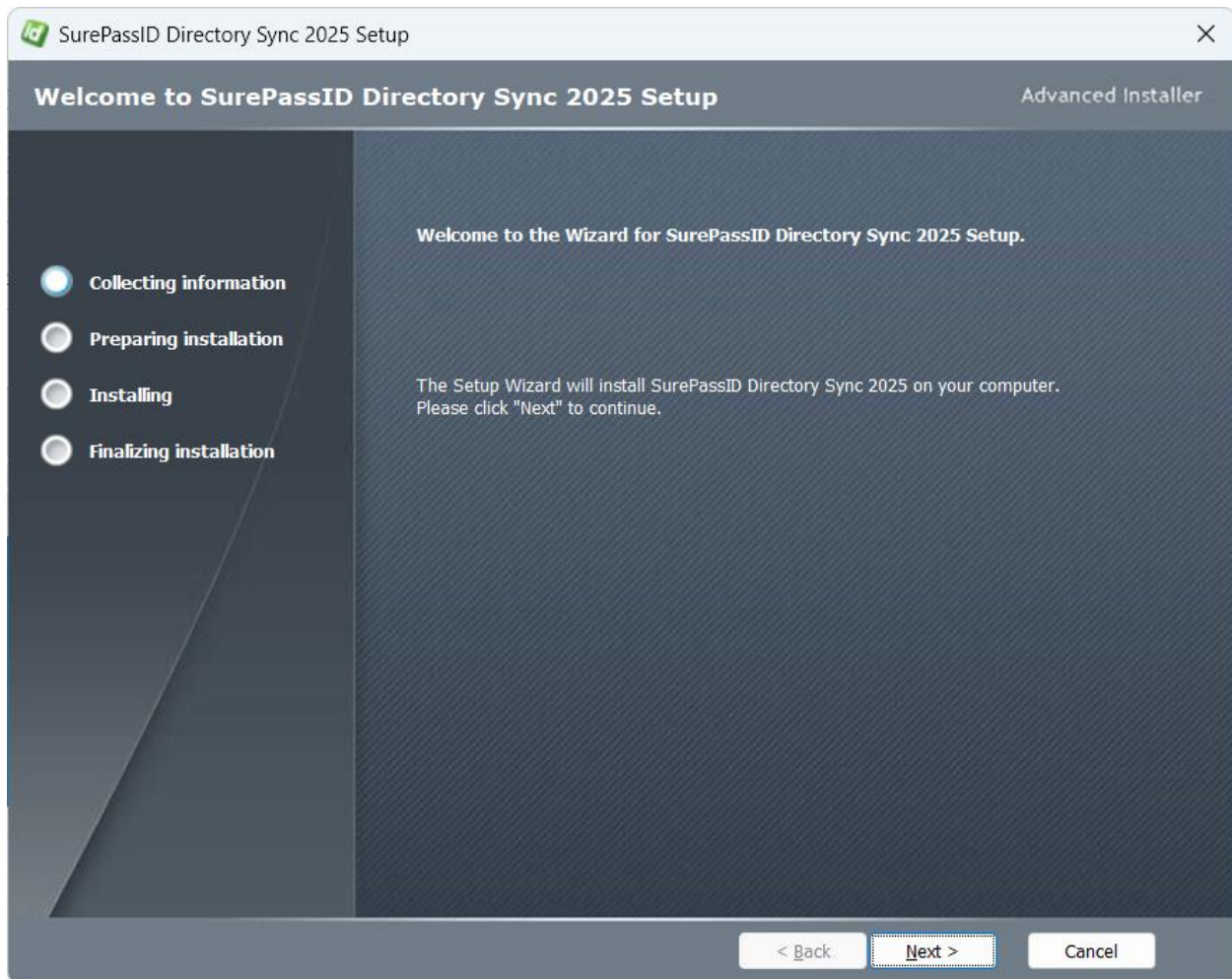
To install the Directory Sync application, you must first download and unzip the installer from here:

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

After downloading the file, uncompress the file and run the installer file.

The installer and application are digitally signed by SurePassID. Verify this during installation.

Next, the installation screen will appear.

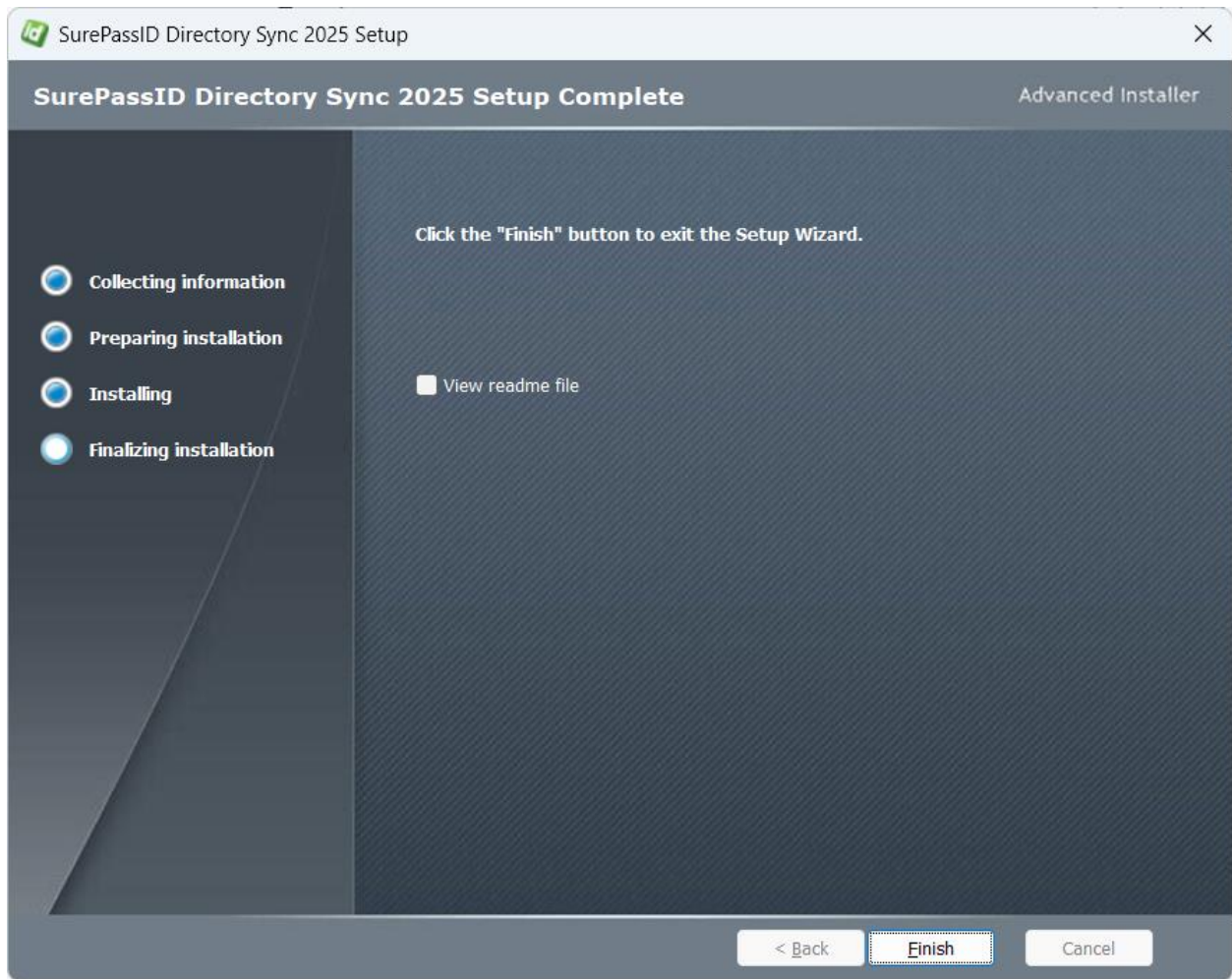


Follow the prompts until you get to the **User Access Control** screen.

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 app synchronizes Active Directory user info with the SurePassID directory. It's located in the SurePassID Directory Sync folder as DirectorySync.exe. The app can also create mobile tokens for users and notify them via email or SMS, streamlining onboarding and termination processes.

Directory sync options can be set via the command line or by editing the DirectorySync.exe.config file in the installation directory. The use_command_line option in this config file determines the method used. If set to true, all sync options must be specified on the command line, ignoring other config values.

```
<?xml version="1.0"?>
<configuration>
  <appSettings>

<!-- =====+-->
<!-- Run DirectorySync from coomand line to get a list of options and values -->
<!-- =====+-->

<add key="use_command_line" value=" true" /> <!-- true=options are specified on command line
false=use the options in this file -->
```

Running the Directory Sync Application

C:\Program Files (x86)\SurePassID Corp\SurePassID Directory Sync 2025

To run the **Directory Sync** app from the command line use the following syntax:

Usage: Directory Sync [options]

Outlined below are the available options. Bold values represent the default selections if no preferences are specified:

Setting	Description	Values
---------	-------------	--------

-use_command_line	Where to get options for the sync	token
-sync_api	API to access SurePassID MFA server.	rest
-sync_source	Options for pulling users into SurePassID:	AdLdapFilter AdGroup Xml
	<ul style="list-style-type: none"> • AdLdapFilter: Follow ldap-filter and ad_domain_fqdn instructions. • AdGroup: Use the provided AD group. See ad_group below. • Xml: Use a properly formatted XML file. Refer to xml_path. 	
-api_key_id	SurePassID application keyid for your tenant.	
-api_key	SurePassID application key for your tenant.	
-rest_endpoint	SurePassID MFA server rest endpoint. For example: https://surepassid-server/api/mfa/v1	
-xml_path	This is the path of the xml file to pull users inSurePassID from. Only used when sync_source = Xml	
-ad_domain_fqdn	This is the Active Directory domain controller FQDN. file to pull users in SurePassID from. Only used	

	when sync_source = AdLdapFilter	
-ldap_scheme	The ldap scheme name. Only used when sync_source = AdLdapFilter	ldap://, ldaps://
-ad_group	This is the Active Directory group used to pull users into SurePassID. It is only applicable when sync_source = AdGroup . An example could be: Domain Admins	
-ldap_filter	This LDAP filter retrieves users for SurePassID when sync_source = AdLdapFilter .	
-ad_disable_group	This group contains users in SurePassID who are to be automatically disabled. Terminated users can be moved into this group and will be disabled in SurePassID.	
-silent	Tracing is suppressed.	true false
-mode	The mode allows you to choose whether users update in SurePassID (live) or not (preview). Use preview to test ldap filters and Active Directory groups, review the results, and then go live when the filter is perfect.	preview live

-sync_user_enabled	Set the status of the users account to enabled (true) or disabled (false).	true false
-sync_user_group	The SurePassID group new users will be assigned to. Leave blank for no group assignment in SurePassID.	
-create_soft_token	When syncing a new user in SurePassID create a new token (true) or not (false). The following options are only used if create_soft_token = true .	true false
-token_type	Soft token to create for the user	SurePassIDAuthenticator GoogleAuthenticator Fido2
-token_usage_otp	Creates a soft token that can use OTP.	true false
-token_usage_push	The soft token created can use push authentication.	true false
-token_usage_push_type	For soft token created that allow push authentication, specify the push authentication type. Yes/No push authentication (push) or fido2 push authentication (fido).	push fido
-token_otp_type	The type of OTP token.	event time
-token_event_otp_window	For event based, tokens, the token windows size.	any integer 30
-token_time_otp_drift	For time based, tokens specify the time windows drift in time units.	any integer 3
-token_enabled	Set the token to enabled (true) or disabled (false).	true false

	Disabeld tokens cannot be used until they are enabled.	
-token_activation_notification	How to notify the user that their new soft token is ready and how to set it up. For email notifications, the server can be configured for either text and HTML formats.	none email sms
- token_fido2_type	Specify the type of Fido token for the user. Required if token_type is Fido.	Passkey SecurityKey

Using the Directory Sync App with SurePassID MFA Server

To sync users from external sources into SurePassID, specify your SurePassID account by using the Application Key Identifier (**-api_key_id**) and Application Key (**-api_key**) options.

It is advisable to generate a new application key for Directory Sync, enabling more straightforward identification of synchronization activities.

If you are syncing users without creating tokens for them, the API Key must be granted the following permissions:

- FindUser (find_user)
- AddUser (add_user)

If you are adding soft tokens for these users, ensure the following permissions are allowed:

- AddOathDevice (add_oath_device)

Here's how to add an API key:

SurePassID Admin Console first last (Super) Settings Sign out

Home Accounts Users Tokens Audit Trail SSO

Account Settings App Configuration File Customize Email Messages Customize Mobile Messages

Update Application Key DirectorySync Update Close

Application Key Status Information

Key Name: DirectorySync

Key Identifier: vmWSix5EqGjo2rVmHToqK7UqrUAVh219KWVPhQY81 [Copy](#)

Key: *****k0hVAB0BCSRc9

Created Date: 5/27/2025 4:04:35 PM

Last Used:

Last Used From:

Application Key Access

Permission Templates: Custom Access Rights (you pick em) ▼

Allow	Access Right ▲	Application Request Type	Access Ca ▲
<input checked="" type="checkbox"/>	AddOathDevice	add_oath_device	Token Managem
<input type="checkbox"/>	AddU2FDevice	add_u2f_device	Token Managem
<input checked="" type="checkbox"/>	AddUser	add_user add_oath_user	Directory Manag
<input type="checkbox"/>	ChangeUserPassword	change_user_password	Directory Manag
<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 Managem
<input type="checkbox"/>	DeleteUser	delete_user	Directory Manag
<input type="checkbox"/>	DeviceActivation	active_oath_device	Token Managem
<input type="checkbox"/>	DeviceAssignment	assign_device unassign_device	Token Managem
<input type="checkbox"/>	DeviceStatus	enable_device disable_device	Token Managem
<input type="checkbox"/>	DirectorySync	directory_sync_start	Directory Manag
<input type="checkbox"/>	EventLogSync	event_log_sync_start	Event Log Mana
<input type="checkbox"/>	ExpireSessionToken	expire_session_token	Session Manage
<input type="checkbox"/>	Fido2Assertion	api/fido/v2/assertion/options/result	FIDO Authentica
<input type="checkbox"/>	Fido2Attestation	api/fido/v2/attestation/options/result	FIDO Authentica
<input type="checkbox"/>	Fido2Delete	api/fido/v2/authenticator/delete	FIDO Authentica
<input type="checkbox"/>	Fido2List	api/fido/v2/authenticator/list	FIDO Authentica
<input type="checkbox"/>	FidoU2FDelete	delete_key delete_all_keys	Token Managem
<input type="checkbox"/>	FidoU2FEnroll	pre_enroll enroll	FIDO Authentica
<input type="checkbox"/>	FidoU2FSign	pre_sign sign	FIDO Authentica
<input type="checkbox"/>	FindDevice	find_device	Token Managem
<input checked="" type="checkbox"/>	FindUser	find_user	Directory Manag
<input type="checkbox"/>	FindUsers	find_users	Directory Manag
<input type="checkbox"/>	GetVerifyMethods	get_verified_methods	Authentication
<input type="checkbox"/>	ProvisionTokenOta	provision_device provision_oath_device	Token Managem
<input type="checkbox"/>	ProvisionTokenQr	get_oath_device_qrcode	Token Managem ▼

Update Close

For more information about API keys, see this [Knowledgebase Article](#) and associated videos.

Creating LDAP Filters (-sync_source=AdLdapFilter)

Developing AD LDAP filters can be complex and necessitates an understanding of Active Directory specifics. Numerous resources address this subject, making it overwhelming and time-consuming to start from the beginning. For comprehensive information, please refer to the Microsoft article on this topic.

[Creating a Query Filter - Win32 apps | Microsoft Learn](#)

The Active Directory User Interface in Windows is capable of assisting you in the creation of LDAP filters.

[Using Saved Queries in ADUC MMC \(Active Directory User and Computers\) | Windows OS Hub](#)

Here are some useful LDAP filters for the domain bestmfaever.net with root OU=rootOU and SurePassID.

All Domain Admins:

```
(&(objectClass=User)(memberOf=CN=Domain Admins,OU=Groups,OU=rootOU,DC= bestmfaever,DC=net))
```

All Domain Users:

```
(&(objectCategory=person)(objectClass=user)(primaryGroupID=513))
```

All users in the MFA group:

```
(&(objectClass=User)(memberOf=CN=MFA,OU=Groups,OU=rootOU,DC= bestmfaever,DC=net))
```

Is there any easier way to sync users. Yes, there is. [Using Active Directory Groups](#)

Using Active Directory Groups (-sync_source=AdGroup)

Here is a method to configure SurePassID to automatically sync users and optionally add soft tokens for them.

1. Create an Active Directory Group for users requiring MFA, called the MFA group.
2. Schedule a PowerShell script named `PowerShellAddUsersToMFAGroupTask` to automatically add new users to the Active Directory MFA group daily or nightly, depending on your company's requirements.
3. Set up the Directory Sync options:

DirectorySync

```
-rest_endpoint=your_mfa_server  
-api_key_id=apikeyid  
-api_key=apikey  
-sync_source=AdGroup  
-ad_group=MFA  
(add other options that are not included here)
```

4. Please create a scheduled task named `SurePassIDSyncAdUserTask` for the DirectorySync options from step 3. Ensure that this task runs subsequent to the completion of `PowerShellAddUsersToMFAGroupTask`.

Users are automatically on-boarded when added to the Active Directory.

Security Considerations

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