ADSS Server v8.3.11 – Go>Sign Desktop Multiuser Installation Guide

ASCERTIA LTD

APRIL 2025

Document Version- 1.0.0

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Scope

This manual describes how to install the ADSS Go>Sign Desktop Multiser application.

1.2 Intended Readership

This manual is intended for end users and system administrators responsible for the installation of the Go Sign Desktop MultiUser client. It is assumed that the reader has a basic knowledge of standard installation procedures, and for system administrators, proficiency in deploying software using Microsoft Windows Group Policy.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- **Bold text** identifies menu names, menu options, items you can click on the screen, file names, folder names, and keyboard keys.
- `Courier New` font identifies code and text that appears on the command line.
- **`Bold Courier New`** identifies commands that you are required to type in.

1.4 Technical Support

If technical support is required, Ascertia has a dedicated support team that provides debug and integration assistance, and general customer support. Ascertia Support can be reached in the following ways:

Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	Ascertia Community Portal

In addition to the free support service describe above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

A Product Support Questionnaire should be completed to provide Ascertia Support with further information about your system environment. When requesting help, it is always important to confirm:

- System Platform details
- ADSS Server version number and build date
- Details of specific issue and the relevant steps taken to reproduce it
- Database version and patch level
- ADSS Go>Sign Desktop Multi-User version number and build date
- ADSS Go>Sign Desktop Multi-User log files

2 System Requirements

The following table summarizes the minimum requirements for ADSS Go>Sign Desktop MultiUser:

Component	Minimum Requirements
Operating System	• Windows 7/8/10/11 (x86 and x64) • Windows Server 2016/2019/2022 (x64)
CPU and RAM	A modern multi-core CPU such as the Xeon E3-xxxx or E5-xxxx or E55xx or E56-xx or similar are recommended, with 16 GB RAM (min 6GB RAM) and 100 GB disk space (the required disk space can vary depending upon the number of child instances).

Table 1 - System Requirements

2.1 Installation Notes

ADSS Go>Sign Desktop MultiUser relies on TLS communication with the business application. This is secured using a TLS certificate with hostname: **client.go-sign-desktop.com**. Therefore, the local client machine must be able to resolve this FQDN (complete domain name for a specific computer, or host, on the internet).

In order to achieve this, the Go>Sign Desktop MultiUser Installer will add the entry **127.0.0.1 client.go-sign-desktop.com** in the Operating System host file in order to register the **client.go-sign-desktop.com** as local domain in the following location:

- *C:\Windows\System32\Drivers\etc\hosts*

*The default value **client.go-sign-desktop.com** must not be changed*

This will ensure the FQDN **client.go-sign-desktop.com** resolves to IP address **127.0.0.1**.

3 Overview

When Go>Sign Desktop is installed as a single user application, each user installs Go>Sign Desktop individually and performs the required signing operation. When Go>Sign Desktop is installed as a multiuser application, the installation takes place at a common server and multiple users can access the same server using their own credentials. The required signing operations can be performed at a common server, ensuring a server side solution.

Go-Sign Desktop Multiuser works via the following mechanism:

- The Go>Sign Desktop Multiuser application must be executed by an administrator permission privileged account
- The common server where Go>Sign Desktop Multiuser is installed is called the "Parent instance"
- Each user "Child instance" will login to the common servers to access Go>Sign Desktop Multiuser using their own credentials
- A child client called "GSD" will be executed automatically whilst interacting with the business application for signing
- Each of the child instances are registered in the database against its application id, therefore the parent Go>Sign Desktop tracks which instances are registered and forwards the request to the required instance accordingly

3.1 Pre-Requisites

When the Go-Sign Desktop Application is installed, its IP is mapped to a specific URL, 'http://client.go-sign-desktop.com', which is internally linked to the local host IP (127.0.0.1). This allows the application to run on the local machine but prevents external applications from accessing it, as they cannot recognize the local host.

When a proxy server is enabled for all network traffic, any browser request first passes through the proxy. The proxy then tries to access the Go-Sign Desktop Application via the local host URL. To ensure proper communication, an exception must be made so that 'http://client.go-sign-desktop.com' always directs to the loopback address of the user's device (127.0.0.1), rather than that of the proxy server.

Without this exception, the proxy server will redirect 'http://client.go-sign-desktop.com' to its own 127.0.0.1 address instead of the local machine. Since this local host URL is not public, the proxy server won't be able to communicate with the Go-Sign Desktop Application, leading to service disruptions.

To resolve this issue, the Go-Sign Desktop Application's URL ('http://client.go-sign-desktop.com') must be whitelisted, ensuring that the proxy server can effectively access and communicate with the application.

3.2 Packaging Details

ADSS Go>Sign Desktop is bundled with the ADSS Client SDK. The ADSS Client SDK package should be unzipped in a suitable directory. You will find following ADSS Go>Sign Desktop installation packages at **[ADSS Client-SDK Directory]/GoSign/Desktop/**

- *ADSS-Go-Sign-Desktop-vx.x-MU-Win64.msi (Windows x64)*

x-x is the version of the ADSS Go>Sign Desktop

4 Deployment Options

There are two deployment options available for ADSS Go>Sign Desktop Multiuser:

- Manual Installation
- Remote automated installation via Group Policy

4.1 Manual Installation

ADSS Go>Sign Desktop Multiuser can be deployed manually for a single server. The child instances are logged-in using their own credentials, connected to the same server on which Go>Sign Desktop Multi-User is deployed, and performs the required signing operations.

NOTE: By default, User Account Control Settings (UAC) are enabled in windows. ADSS Go>Sign Desktop Multiuser needs user permissions to make changes on the installing device. Windows will prompt a dialog to acquire the user permissions. When the user grants the permissions the ADSS Go>Sign Desktop Multiuser will be installed on the device.

4.1.1 Installation Steps

Follow these steps to manually install ADSS Go>Sign Desktop Multiuser application:

1. Run the .exe file appropriate to the Windows operating system where it's being installed.
2. The installation wizard will prompt and display the following screen:

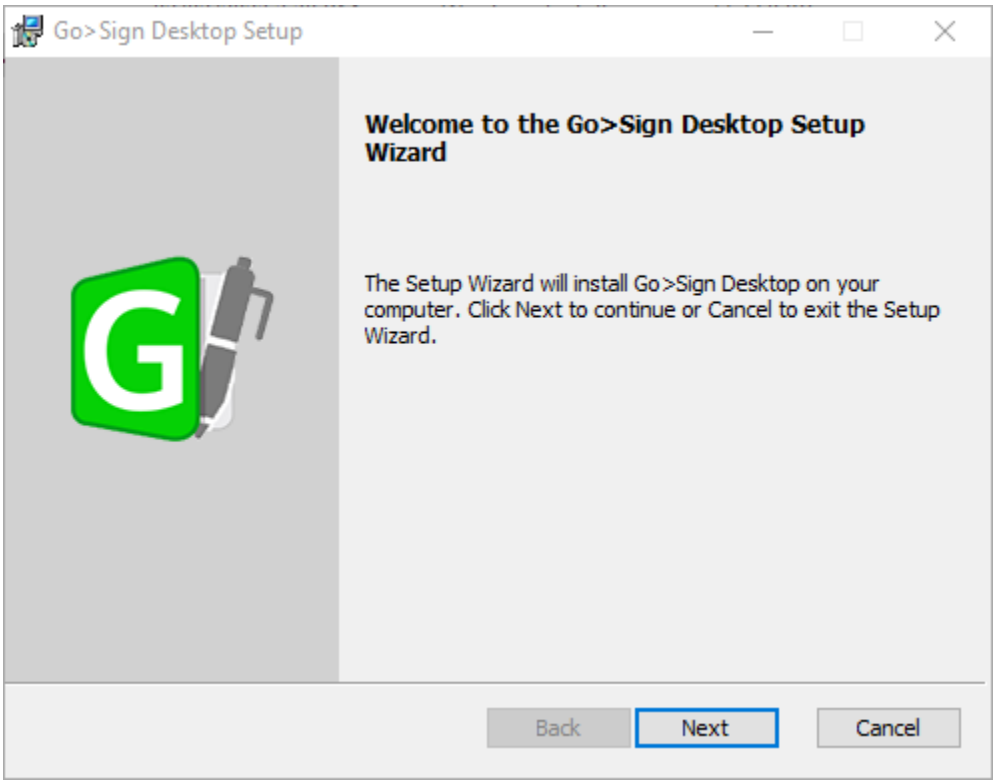

Figure 1 - Windows OS Installer Wizard Introduction

3. Click on the **Next** button to continue the installation process, otherwise click **Cancel** button to stop the installation process:

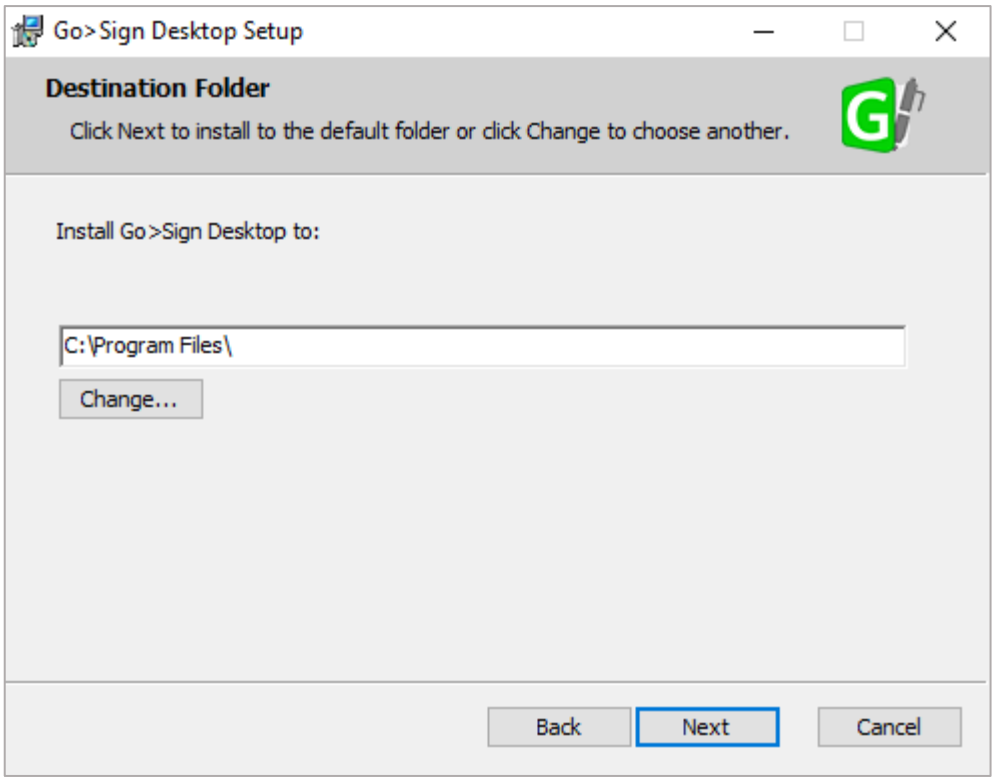

Figure 2 - Destination Folder

4. In the above screen, the user can click on the Change button and select the required installation path from the file system.

   Limitation: If the user tries to enter the required path itself, without clicking on the Change button, then the installation file will be installed at the default location i.e.'C:\Program File\'. Hence, it is recommended to click on the Change button in order to install the file at the desired location.

5. Once the installation is successful at the provided path, then, the user will be shown the following screen:

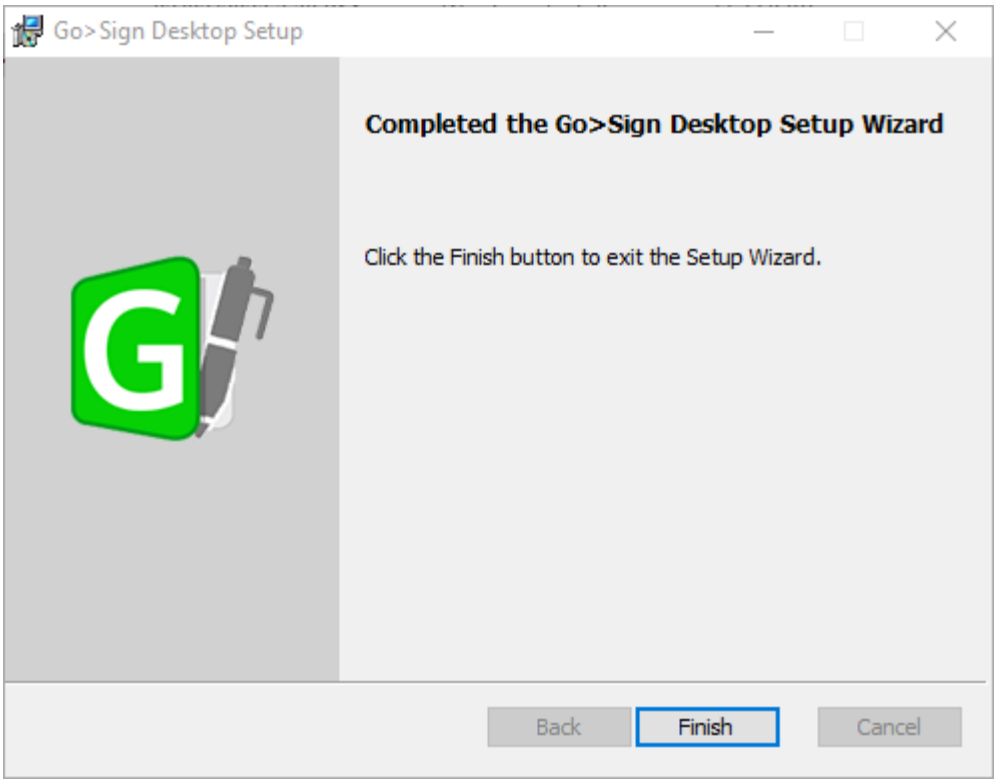

Figure 3 - Windows OS Installer Wizard Summary

6. Click on the **Finish** button to close the installation wizard.
7. Navigate to Local Disk (C:) → Program Files → Ascertia → Go-Sign-Desktop and run the **Go-Sign-Desktop.exe** file manually:

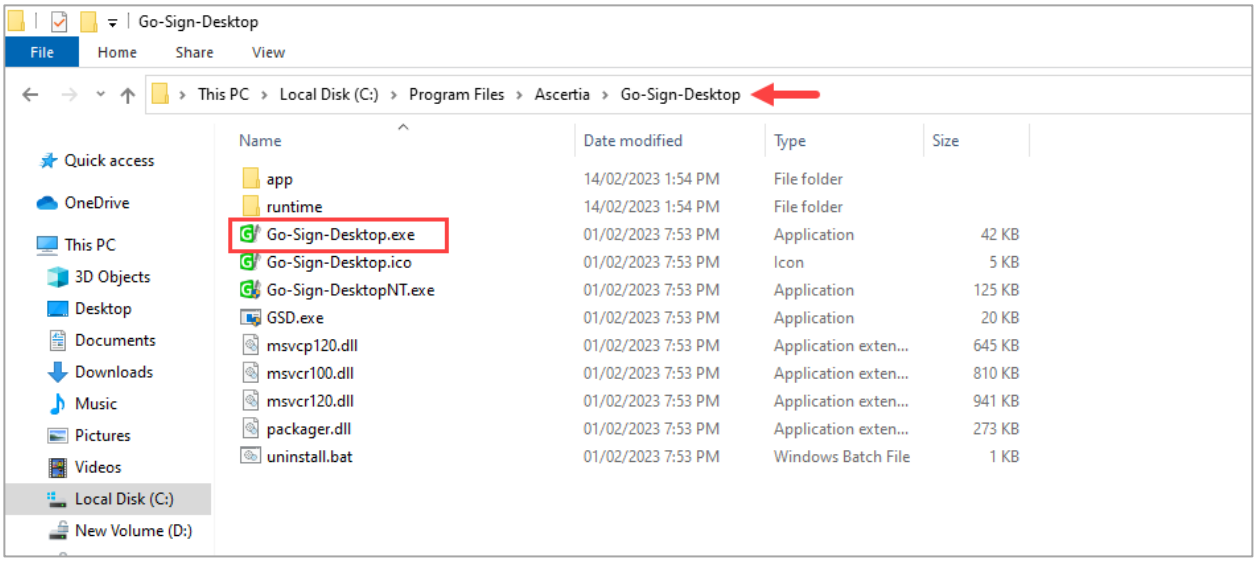

Figure 4 - Windows Explorer

8. Running Go-Sign-Desktop.exe will display the following alert message. Click on the **Yes** button to install the certificate and continue:

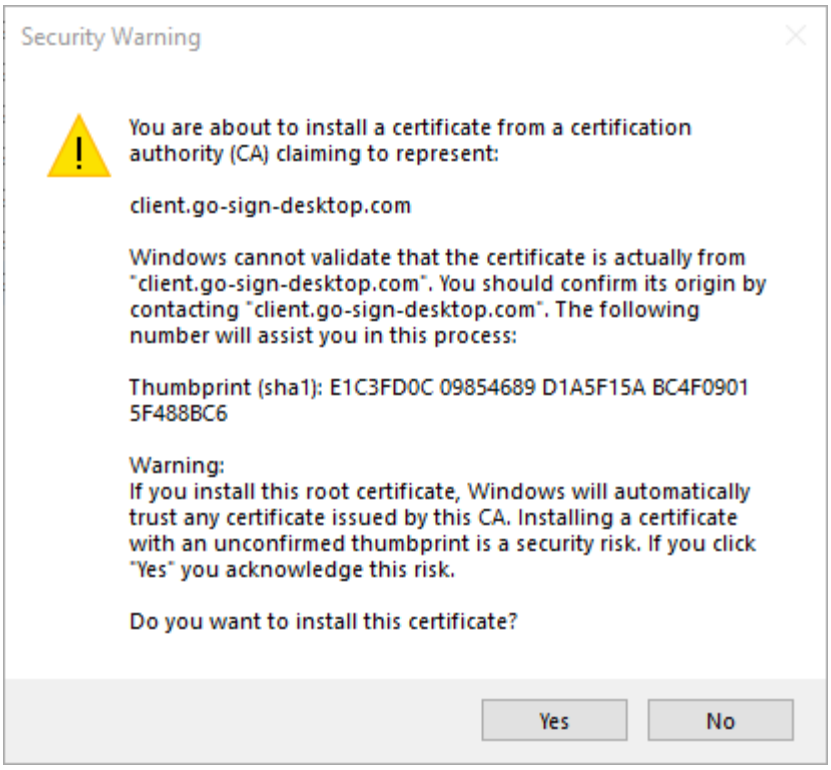

Figure 5 – Warning Message

9. The ADSS Go>Sign Desktop application Icon will be visible in the **Windows System Tray**. Right click on the icon and quit Go-Sign-Desktop:

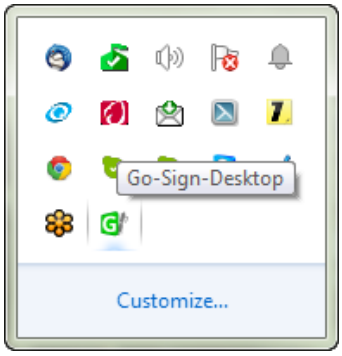

Figure 6 - Windows System Tray

10. Once done, navigate again to Local Disk (C:) → Program Files → Ascertia → Go-Sign-Desktop and execute the **GSD.exe** file:

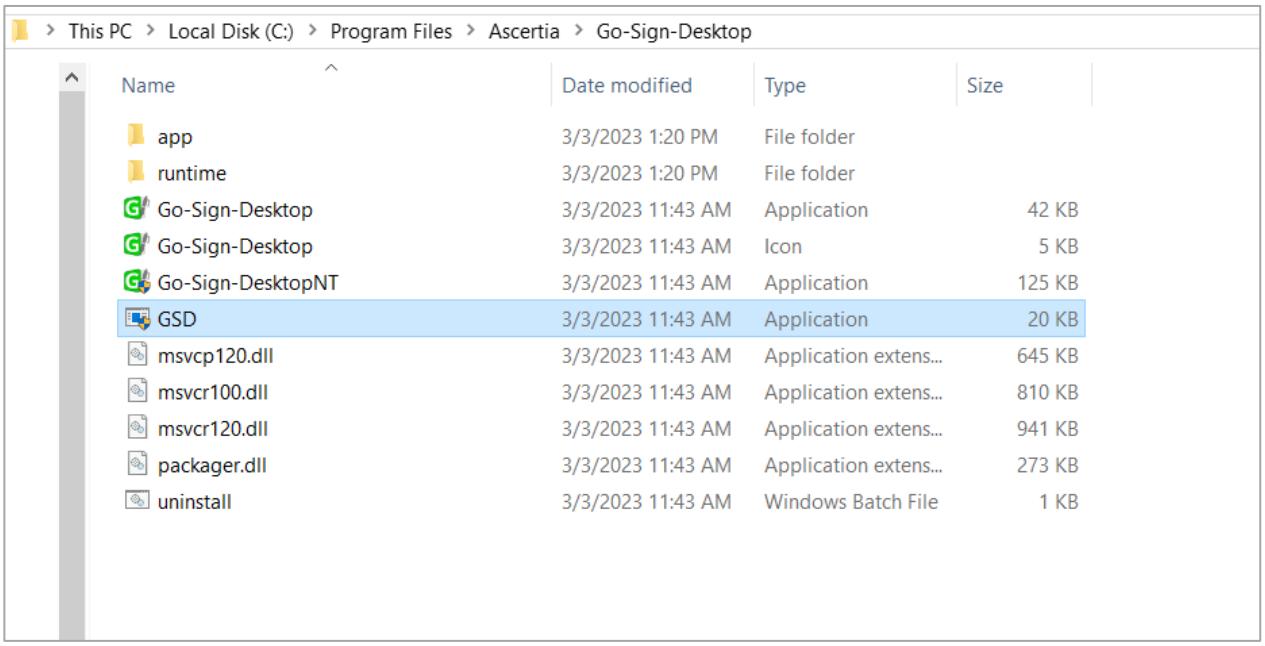

Figure 7 – GSD Exe File

11. Open Windows NT Services and start Go>Sign Desktop Service:

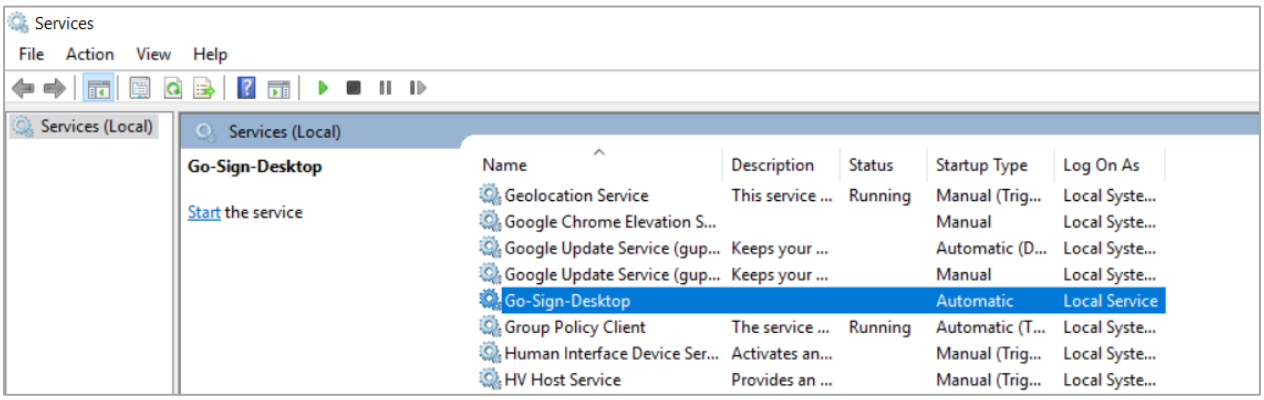

Figure 8 – Windows NT Services

4.2 Remote Installation Using Windows Group Policy

Follow these steps to deploy ADSS Go>Sign Desktop Multiuser with Windows Group Policy. This process will either automatically install ADSS Go>Sign Desktop Multiuser application to the assigned group's computers, or distribute the software for installation. You can use Group Policy to distribute computer programs via the following methods:

- **Assigning Software**

  You can assign a program distribution to users or computers. If you assign the program to a user, it is installed when the user logs on to their computer. When the user first runs the program, the installation is completed automatically. If you assign the program to a computer,

it is installed when the computer starts, and it is available to all users who log on to the computer. When a user first runs the program, the installation is completed.

- **Publishing Software**

  You can publish a program distribution to users. When the user logs on to the computer, the published program is displayed in the Add or Remove Programs dialog box, and can be installed from there.

4.2.1 Create a Distribution Point

To publish or assign a computer program, you must create a distribution point on the publishing server. To do this follow these steps:

1. Log on to the Windows server as an **administrator**.
2. Create a shared network folder like: **`\\file server\share\file name.msi.`** Where you will place the Microsoft Windows Installer package (.msi file) that you want to distribute.
3. Set permissions on the share to allow access to the distribution package.
4. Copy the package to the distribution point. For example, to distribute Microsoft Office 2019, run the administrative installation (setup.exe /a) to copy the files to the distribution point.

4.2.2 Create a Group Policy Object

To create a Group Policy Object (GPO) to distribute the software package follow these steps:

1. Open the **"Group Policy Management"** snap-in. To do this, click **Start**, and search for **"Group Policy Management"** and click to open.
2. In the console forest tree, click on "**Domains**" and right-click the required domain.
3. Click "**Create a GPO in this Domain and link it here"** tab.
4. Type a name for this new policy (for example, **"ADSS Go>Sign Desktop"** distribution), and then press **OK**.
5. The policy named **"ADSS Go>Sign Desktop"** will be created and displayed.

4.2.3 Assign a Package

To assign a program to computers that are running Windows Server 2016, Windows Server 2019, Windows 10 or Windows 11, or to users who are logging on to one of these workstations, follow these steps:

1. Open the **"Group Policy Management"** snap-in. To do this, click **Start**, and search for **"Group Policy Management"** and click to open.
2. In the console forest tree, right-click your policy **"ADSS Go>Sign Desktop"**, and then, click **Edit**.
3. Under **Computer Configuration**, expand "**Policies >>Software Settings"**.
4. Right-click **Software installation**, point to **Properties**. In a General Tab type, the shared path for example **`\\file server\share\file name.msi`** and check the **"Assign"** Option and **Click OK.**

   Important: Do not use the **Browse** button to access the location. Make sure that you use the path of the shared installer package.
5. Right-click **Software installation**, point to **New >> Package.**
6. Select your .msi file and Click **Open**. The package is listed in the right-pane of the **Group Policy** window.

7. Close the **Group Policy Editor** snap-in and in a "**Group Policy Management"** snap-in, select your **OU (Organizational Unit)** on which you want to deploy and **Right-click** on it. Now Click on "Link an Existing GPO".
8. Select your group policy **"ADSS Go>Sign Desktop".** Click ok.
9. When the client computer starts, the managed software package is automatically installed.

Note: In a case if the package does not install. Open "Run" type "gpupdate /force" and press Enter.

4.2.4 Publish a Package

To publish a package to computer users and make it available for installation from the **Programs and features** list in **Control Panel**, follow these steps:

1. Open the **"Group Policy Management"** snap-in. To do this, click **Start**, and search for **"Group Policy Management"** and click to open.
2. In the console forest tree, right-click your policy **"ADSS Go>Sign Desktop"**, and then, click **Edit**.
3. Under **User Configuration**, expand "**Policies >>Software Settings"**.
4. Right-click **Software installation**, point to **Properties**. In a General Tab type, the shared path for example `\\file server\share\file name.msi` and check the **"Publish"** Option and **Click OK.**

   Important: Do not use the **Browse** button to access the location. Make sure that you use the path of the shared installer package.
5. Right-click **Software installation**, point to **New >> Package.**
6. Select your .msi file and Click **Open**. The package is listed in the right-pane of the **Group Policy** window.
7. Close the **Group Policy Editor** snap-in and in a "**Group Policy Management"** snap-in, select your **OU (Organizational Unit)** on which you want to deploy and **Right-click** on it. Now Click on "Group Policy Update".
8. When the client computer starts, the managed software package will be published.

Test the package:

Note because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps:

- Log on to a workstation by using an account that you published the package to.
- In Windows, click **Start**, and then click **Control Panel**.
- Click on **"Programs and Features"** and in the left pane, click on **"Install a program from the network".**
- Click the program that you published, and then click **Install**. The program will be installed.
- Click **OK**, and then click **Close**.

4.2.5 Redeploy a Package

In some cases, there may be a need to redeploy a software package (for example, if the package needs to be upgraded or changed). To redeploy a package, follow these steps:

1. Open the **"Group Policy Management"** snap-in. To do this, click **Start**, and search for **"Group Policy Management"** and click to open.

2. In the console forest tree, right-click your policy **"ADSS Go>Sign Desktop"**, and then, click **Edit**.
3. In the console tree, right-click your domain, and then click **Properties**.
4. Click **Group Policy** tab, click the **Group Policy Object** that you used to deploy the package, and then click **Edit**.
5. Expand **Software Settings** container that contains the software installation item that was used to deploy the package.
6. Click the software installation container that contains the package.
7. In the right-pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Redeploy application**. The following message will be presented:

   Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?
8. Click **Yes**.
9. Quit the **Group Policy** snap-in, click **OK**.

4.2.6 Remove a Package

To remove a published or assigned package, follow these steps:

1. Open the **"Group Policy Management"** snap-in. To do this, click **Start**, and search for **"Group Policy Management"** and click to open.
2. In the console forest tree, right-click your policy **"ADSS Go>Sign Desktop"**, and then, click **Edit**.
3. Click the **Group Policy** tab, click **Group Policy Object** that you used to deploy the package, and then click **Edit**.
4. Expand **Software Settings** container that contains the software installation item that was used to deploy the package.
5. Click the software installation container that contains the package.
6. In the right-pane of the **Group Policy** window, right-click the program, point to **All Tasks**, and then click **Remove**.
7. Do one of the following:
   - Click **immediately uninstall the software from users and computers**, and then click **OK**.
   - Click **Allow users to continue to use the software but prevent new installations**, and then click **OK**.
8. Close the **Group Policy** snap-in, click **OK**, and then closet the **Active Directory Users and Computers** snap-in.

5 Testing Go>Sign Desktop Application

The following URL can be used in order to verify that the installed Go>Sign Desktop Multiuser Application is working correctly:

https://client.go-sign-desktop.com:8782/gosign-desktop

6 Use ADSS Go>Sign Desktop App with Firefox

To use Firefox with Go>Sign Desktop, click on the link below:

https://ascertia.force.com/partners/s/article/How-to-trust-TLS-Server-Certificate-with-Go-Sign-Desktop-in-Firefox

7 Uninstalling ADSS Go>Sign Desktop Multi-User App

In order to uninstall ADSS Go>Sign Desktop Multiuser application, follow the instructions below:

1. Navigate to Windows → Control Panel → Programs → Uninstall a program:

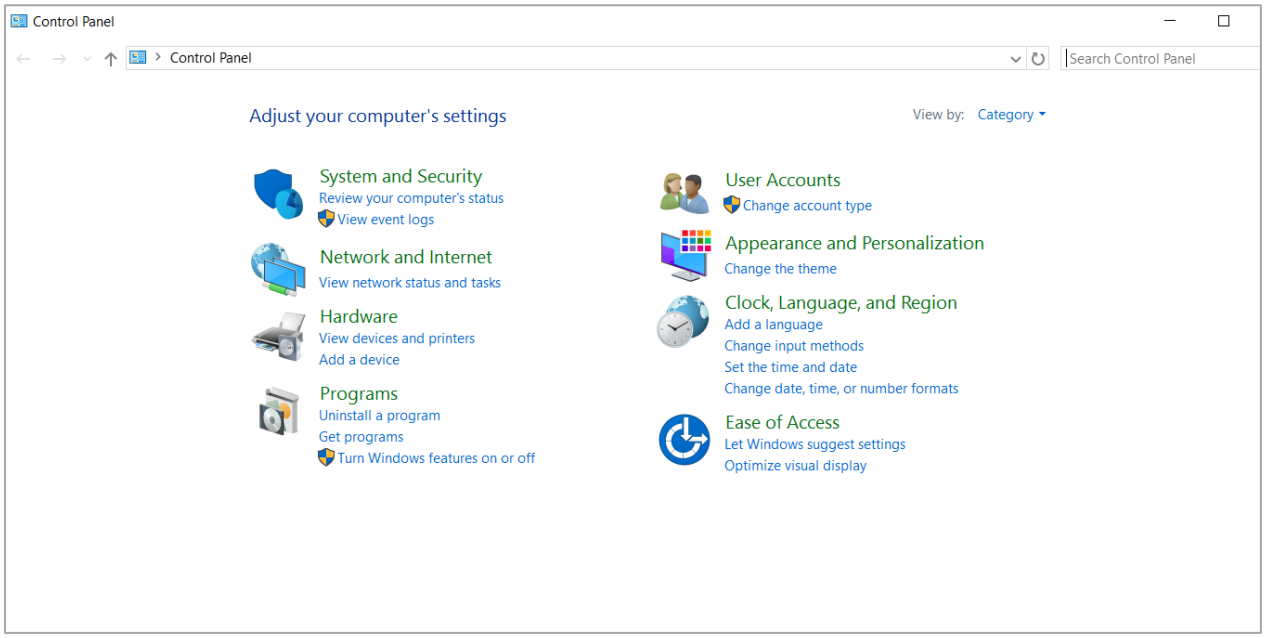

Figure 9 – Control Panel

2. Select and right click on **Go-Sign Desktop**, and then click **Uninstall**:

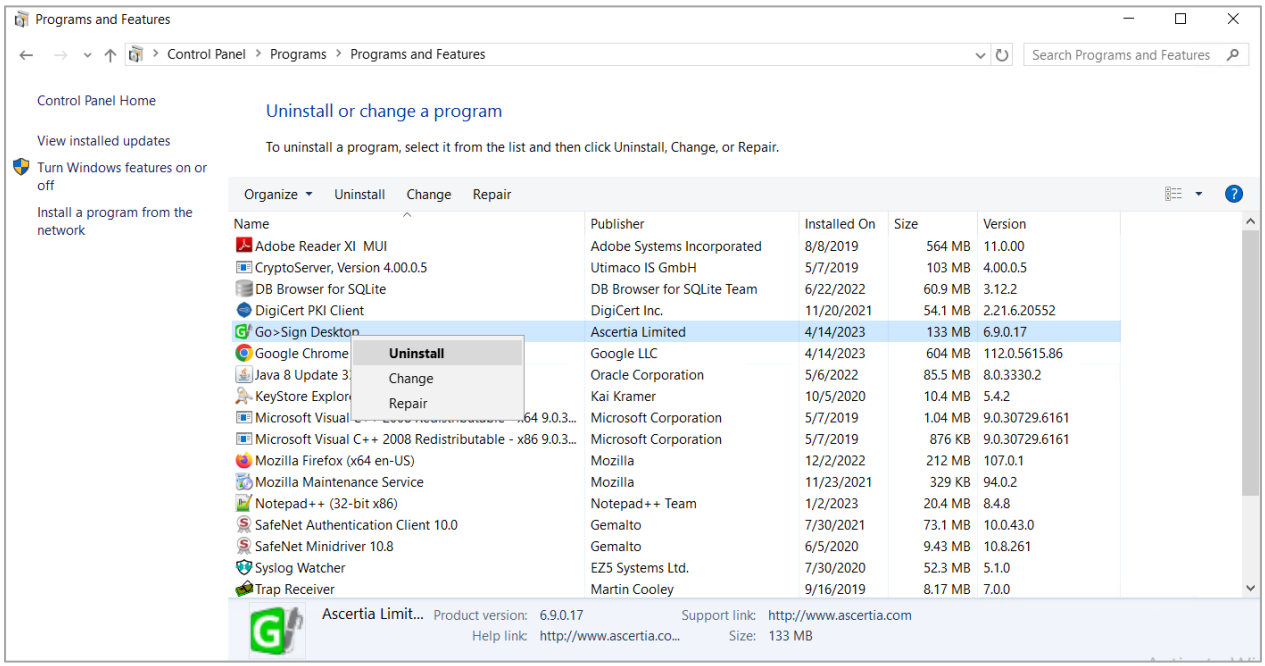

Figure 10 – Control Panel > Go-Sign Desktop

3. A warning message will prompt, click on **Yes** to continue:

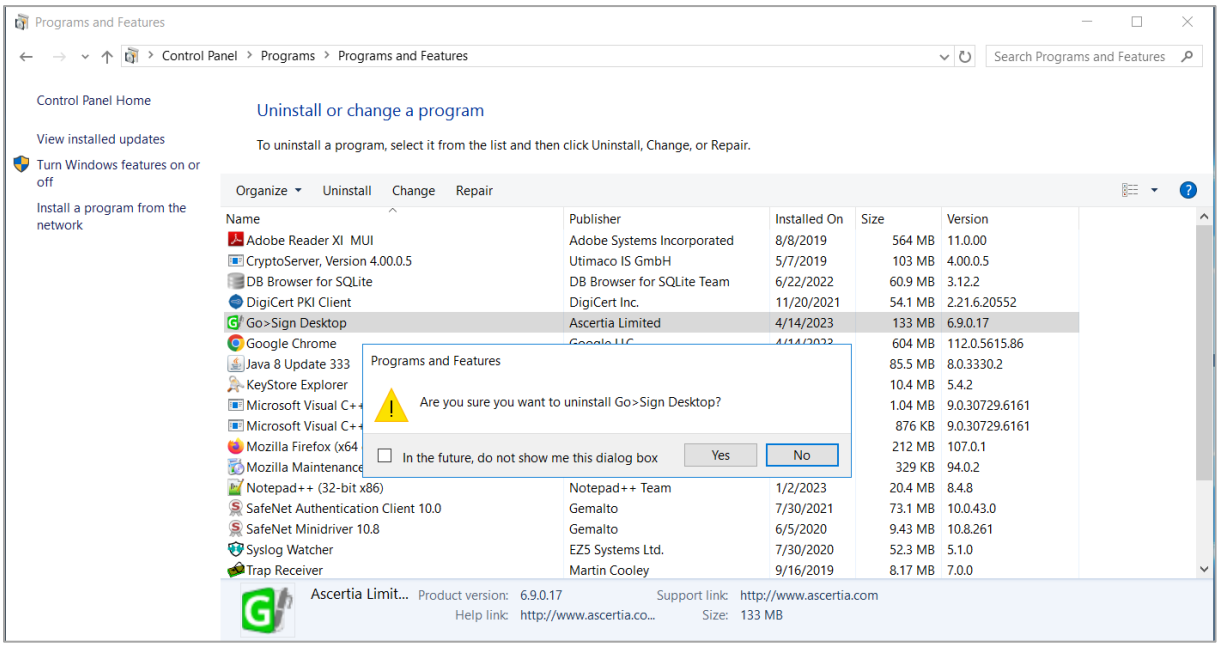

Figure 11 – Control Panel > Go-Sign Desktop > Uninstall

4. A User Account Control message will prompt, click on **Yes** to continue:

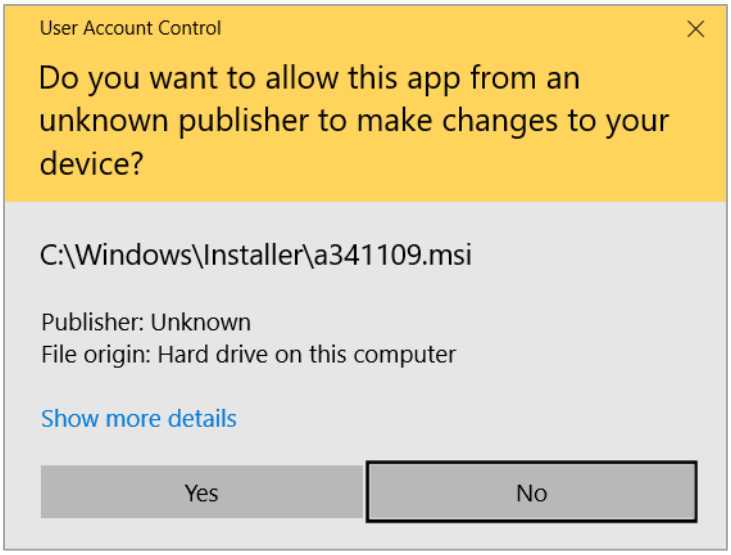

Figure 12 – User Control Account

5. A Root Certificate Store message will prompt, click on **Yes** to continue:

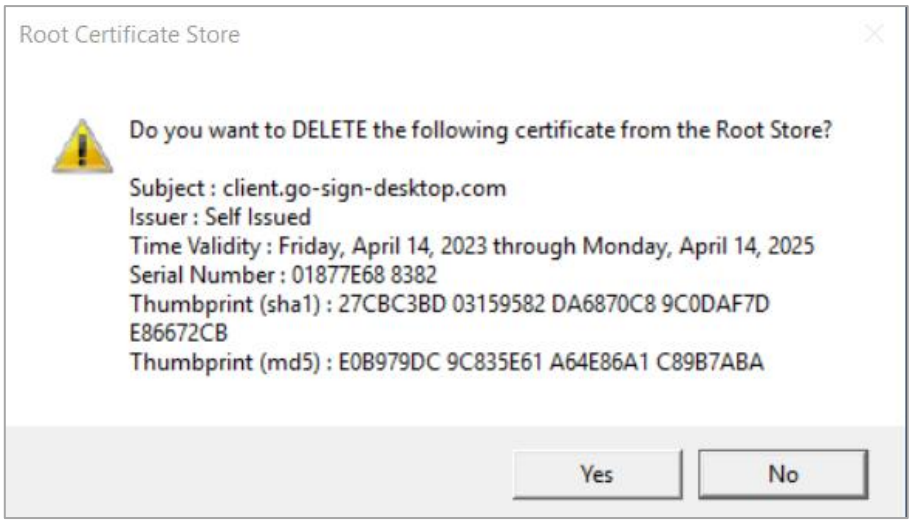

Figure 13 – Root Certificate Store

8 Logging

ADSS Go>Sign Desktop Multiuser application has two log levels. Informational, which is for ordinary use, and debug, which should only be used when investigating performance issues, functionality problems, etc.

Users can view ADSS Go>Sign Desktop Multiuser application logs at:

Parent instance:
C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\logs

Child instance:
C:\Users\[User-Name] \Documents\Ascertia\Go-Sign-Desktop\logs

8.1 Changing Logging Level

By default, ADSS Go>Sign Desktop Multiuser logging level is set to **INFO**. To enable detailed debug logging, follow these instructions:

1. Navigate to the following path:

   C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop

2. Edit the **gosign_desktop.properties** file using a suitable text editor.
3. Change the value of the property **GOSIGN_DESKTOP_LOG_LEVEL** from **INFO** to **DEBUG** and save the file.
4. Restart the Go-Sign Desktop service from Windows NT Services.

9 Listening Ports

9.1 Parent Instance

ADSS Go>Sign Desktop Multiuser listens for JavaScript requests from the web browser on the port 8782 (TLS). Changes to the ADSS Go>Sign Desktop Multiuser ports require the same amendments to ADSS Go>Sign Service:

9.1.1 ADSS Server Changes

1. Launch the ADSS Server Console.
2. Navigate to **Global Settings > Advanced Settings.**
3. From the **Property Type** dropdown menu select the option **Go>Sign**, search and update the value accordingly for the property: **GOSIGN_DESKTOP_HTTPS_PORT**
4. Start the ADSS Server Service instance from Windows services to have the changes take effect.

9.2 Child Instance

The child instances of ADSS Go>Sign Desktop Multiuser application are pre-registered on the dynamically available ports.

Note the following:

1. *For communication with Go>Sign Desktop, only HTTPS protocol is supported. The default port is 8782.*
2. *TLS v1.2 and TLS v1.3 are used for HTTPS.*
3. *The Go>Sign Desktop application uses default cipher algorithms supported by SUN provider for JRE 11 during initial communication with the browser.*

9.3 ADSS Go>Sign Desktop Multiuser Changes

To make the changes in the Go>Sign Desktop Multiuser application, the properties file needs to be updated. The properties file is located at the following path:

Path: *C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf*

The contents of the file are displayed as:

go-sign-desktop.properties

```
##########################################################################################################
########################                                                  ########################
########################   Go>Sign Desktop - App System Configuration File    ########################
########################                                                  ########################
##########################################################################################################

#----------------------------------------------------------------------------------------------------------
# Application ports configuration
#----------------------------------------------------------------------------------------------------------

GOSIGN_DESKTOP_HTTPS_PORT=8782

GOSIGN_DESKTOP_INSTALLATION_MODE = MULTI_USER

GOSIGN_DESKTOP_LOG_MODE = info

GOSIGN_DESKTOP_PARENT_INSTANCE_THREAD_COUNT = 20

GOSIGN_DESKTOP_LOG_FILE_PATH = default

GOSIGN_DESKTOP_CONF_FILE_PATH = default

GOSIGN_DESKTOP_LOG_FILE_MAX_SIZE = 1 MB

GOSIGN_DESKTOP_LOG_FILE_MAX_COUNTER = 10

GOSIGN_DESKTOP_ENABLE_HEART_BEAT = FALSE

GOSIGN_DESKTOP_MAX_IDLE_TIME = 4

GOSIGN_DESKTOP_MAX_IDLE_INTERVAL = 1

GOSIGN_DESKTOP_MAX_INSTANCES_PER_USER = 2
```

Figure 14 – Properties File

If a single ADSS Server is installed for multiple organizations, then this change will impact all users of ADSS Go>Sign Desktop, i.e. all users must update the port configuration found in the "gosign_desktop.properties" file.

Alternatively, use Group Policy to redeploy ADSS Go>Sign Desktop package as described previously.

*** End of document ***