ADSS Go>Sign Desktop

Installation Guide

ASCERTIA LTD

JUNE 2022

Document Version- 7.1

CONTENTS

TABLES

FIGURES

1 Introduction

1.1 Scope

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

1.2 Intended Readership

This manual is intended for end users and system administrators responsible for the installation. 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	https://www.ascertia.com/products/knowledge-base/adss-server/
FAQs	https://ascertia.force.com/partners/login

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 version number and build date.
- ADSS Go>Sign Desktop log files.

2 System Requirements

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

Component	Minimum Requirements
Operating System	• Windows 7/8/10 (x86 and x64) • Mac OS X 10.4 Tiger and above
CPU/RAM	A modern fast CPU with 1 GB RAM

Table 1 - System Requirements

2.1 Installation Notes

ADSS Go>Sign Desktop relies on TLS communication with the business application i.e. **SigningHub**. This is secured using a TLS certificate having 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) to itself.

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

- **Windows OS:** *C:\Windows\System32\Drivers\etc\hosts*
- **Mac OS:** *Macintosh HD/private/etc/hosts*

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

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

3 Overview

Although there is tremendous interest now in the use of remote (central) signing, there are still a large number of users needing to sign using keys and certificates held locally on smartcards, USB tokens, Virtual CSP keys/certificates held centrally and of course local software key stores. To enable web-applications to be able to sign using these keys and certificates, Ascertia has a Windows and MacOSX installable middleware product called ADSS Go>Sign Desktop. ADSS Server Go>Sign Service communicates with Go>Sign Desktop using JavaScript and supports any modern HTML5 browser.

By default, ADSS Go>Sign Desktop application accepts connections from any application. For tight security Ascertia can provide an organisation specific version which allows the local security team to state their business application domain URLs, e.g. https://www.ascertia.com, https://web.signinghub.com As part of license and support services Ascertia will create a client specific version of ADSS Go>Sign Desktop using access control list that locks down on security and will only accept communication from the defined URLs, ask Ascertia sales and support about this option:

- Access control list (ACL) is a network filter utilized by Go>Sign Desktop application to permit and restrict data flows into and out of the application. The ACL contains a list of items, known as Access Control Entities (ACE), which holds the security details of each “trustee” (IP addresses or port numbers) with system access. By default, ADSS Go>Sign Desktop has following entries in its ACL:

  127.0.0.1, 0:0:0:0:0:0:0:1, http://localhost:8766, *

Note the following:

1. *For legacy clients with active support contracts, Ascertia still supports older versions of Go>Sign Applet, the forerunner of Go>Sign Desktop*
2. *Go>Sign TLS Server certificate is issued from GlobalSign Validation CA which is rooted to GlobalSign Root CA.*

3.1 Packaging Details

ADSS Go>Sign Desktop is bundled with ADSS Client SDK. The ADSS Client SDK package must 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-Win64.msi (Windows x64)*
- *ADSS-Go-Sign-Desktop-vx.x-Win32.msi (Windows x86)*
- *ADSS-Go-Sign-Desktop-vx.x.zip (Mac)*

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:

- Manual rollout
- Remote Installation using Group Policy

4.1 Manual Rollout

ADSS Go>Sign Desktop can be deployed manually at each desktop/workstation. This approach is only recommended for small trials and single-machine usage. However, if there is no Domain or alternative solution this might be the only approach.

NOTE: By default, User Account Control Settings (UAC) are enabled in windows. ADSS Go>Sign Desktop needs user permissions to make changes on the installing device. Windows always prompt a dialog to get the user permissions if user granted the permissions then ADSS Go>Sign Desktop would be installed on the device.

4.1.1 Installation Steps for Windows OS

Follow these steps to install ADSS Go>Sign Desktop application on Windows OS:

1. Run the desired application file appropriate to your Windows architecture.
2. The installation wizard will prompt and display the following screen:

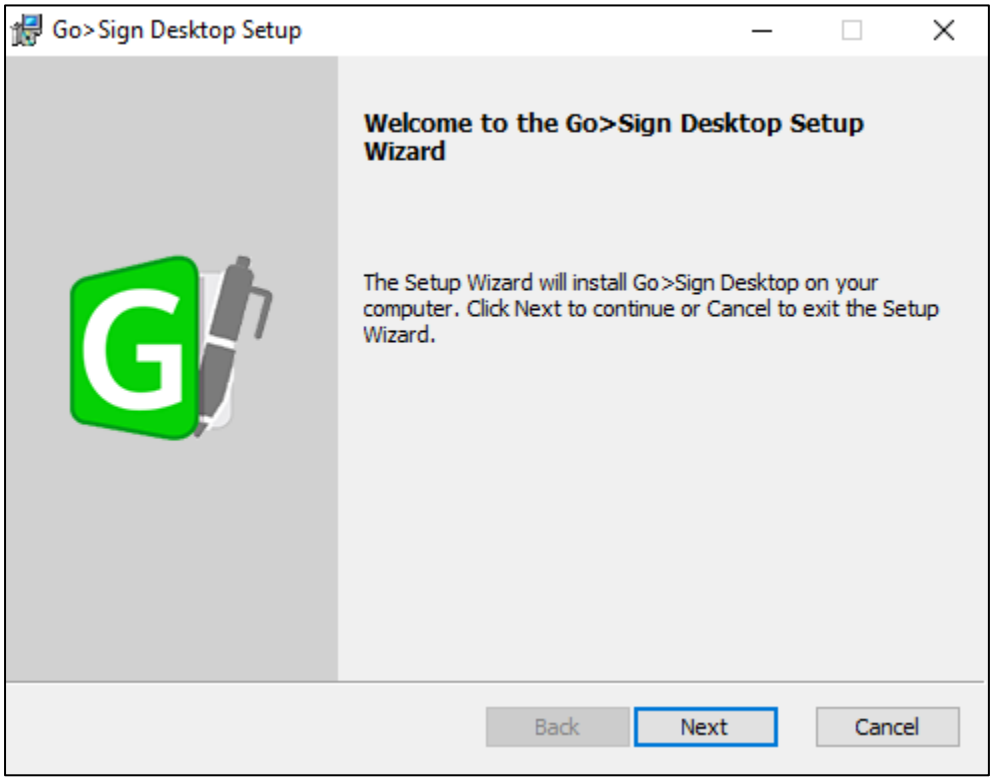

Figure 1 - Windows OS Installer Wizard Introduction

3. Clicking on **Next** button will show the following screen:

Figure 2 - Windows OS Installer Wizard License Agreement

4. If you agree with the displayed terms and conditions, then click **Next** button to continue the installation process otherwise click **Cancel** button to stop the installation process:

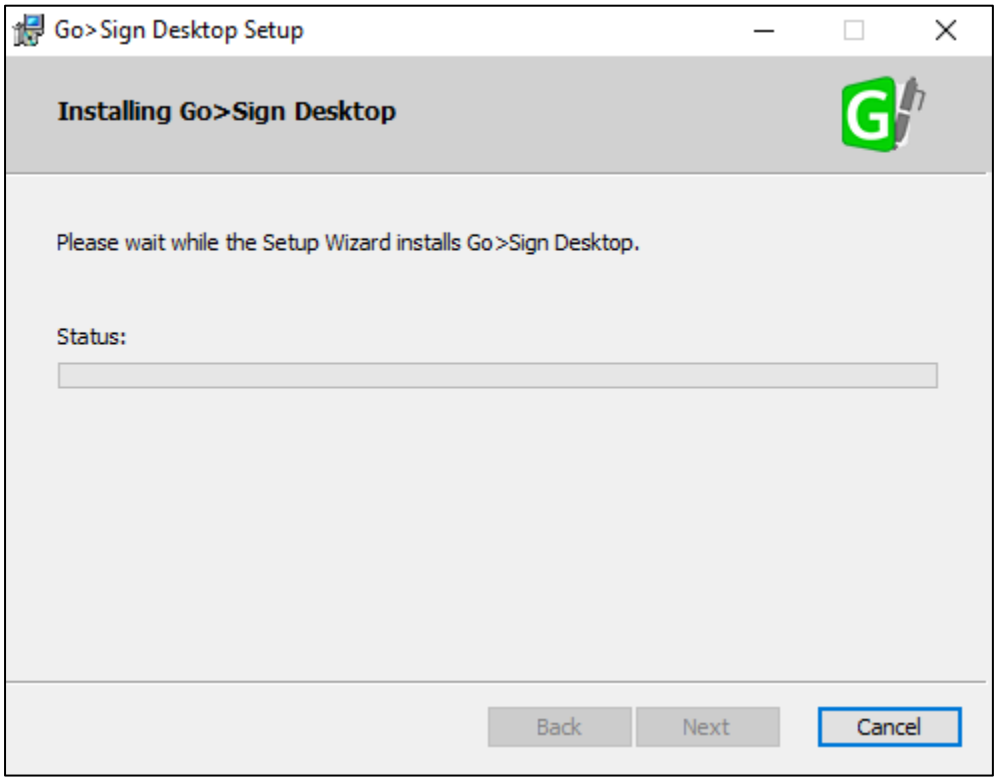

Figure 3 - Windows OS Installer Wizard Installation

5. Once the installation is successful then user will be shown following screen:

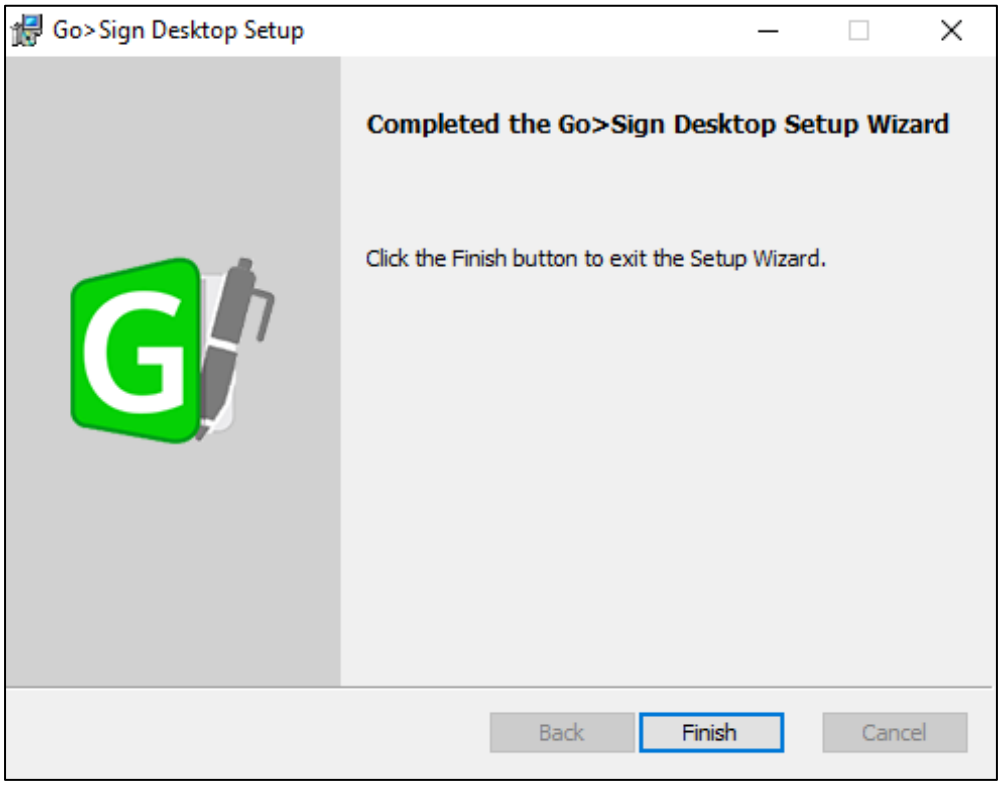

Figure 4 - Windows OS Installer Wizard Summary

6. Click on the **Finish** button to close the installation wizard.
7. After successful installation, you can view the ADSS Go>Sign Desktop application Icon in **Windows System Tray**:

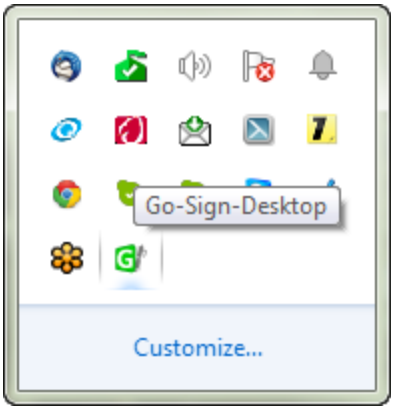

Figure 5 - Windows System Tray

4.1.2 Installation Steps for MAC OS

Follow these steps to install ADSS Go>Sign Desktop application on MAC OS:

1. Extract the zip file and run the package file (.pkg) for Mac OS.
2. The installation wizard will prompt for basic information that must be completed. Running the package displays the **Introduction** screen:

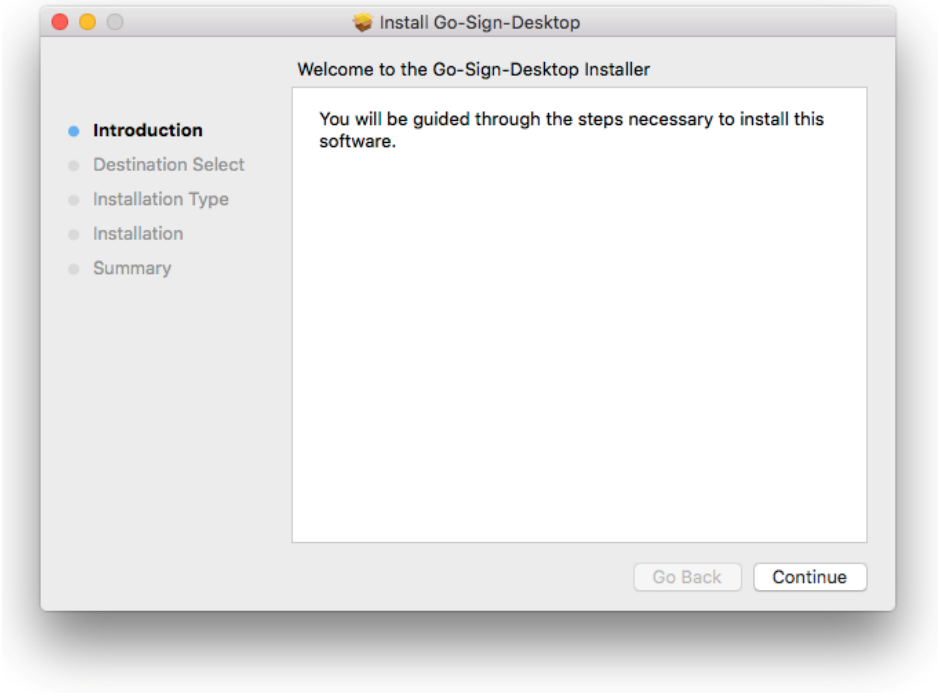

Figure 6 - MAC OS Installer Wizard Introduction

3. Click **Continue** to display the **Destination Select** screen. This allows you to select the target installation disk (there may only be one choice as shown here):

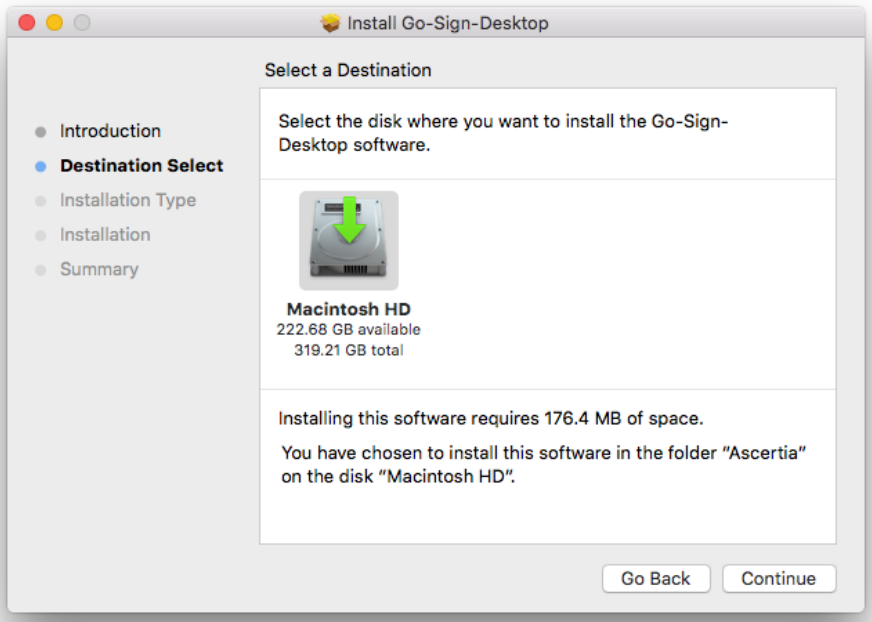

Figure 7 - MAC OS Installer Wizard Destination Select

4. Click **Continue** to move to the next screen **Installation Type** where you can select the target install location:

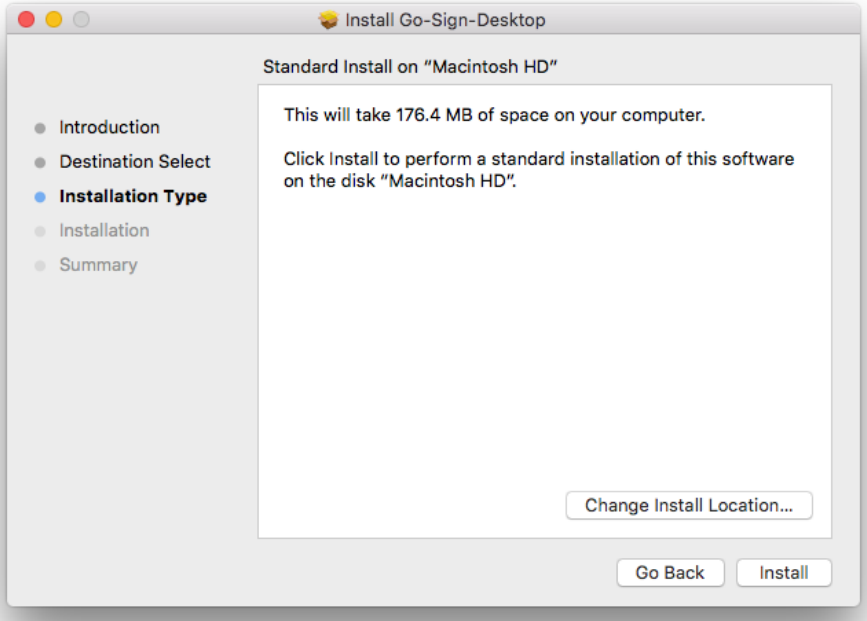

Figure 8 - MAC OS Installer Wizard Installation Type

5. Click **Install** to start the installation process.

6. When the **installer.app** launches, **Administrator Login** dialog pops up. Provide the admin credentials to allow the new software files to be placed in the Applications folder and click **Install Software:**

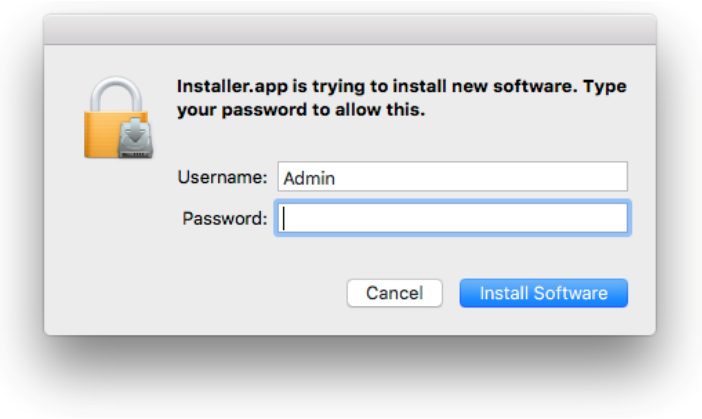

Figure 9 - MAC OS Administrator Password Prompt

7. The **Installation** process takes between 2-3 minutes to complete:

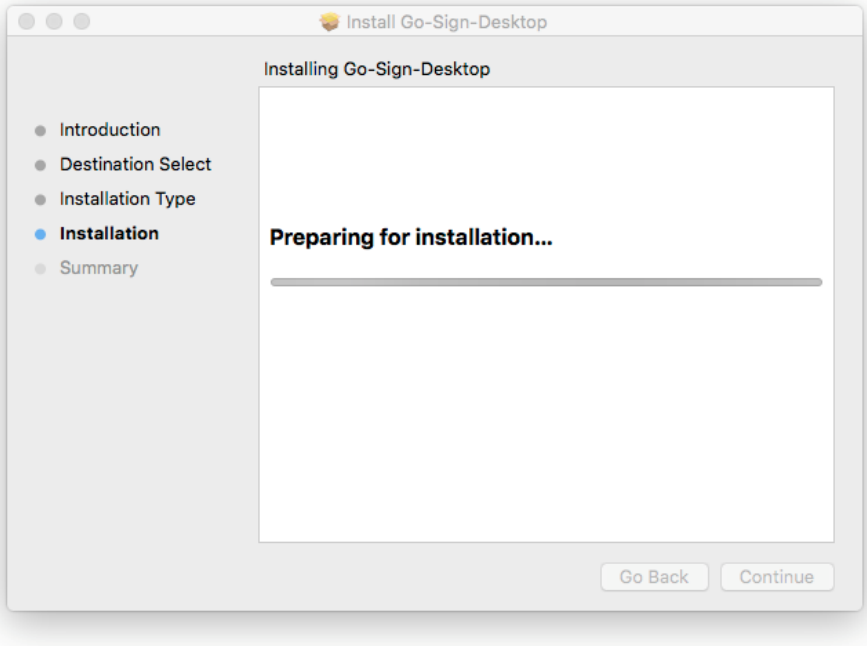

Figure 10 - MAC OS Installer Wizard Installation

8. Once the software has installed, the **Summary** screen will be displayed.
9. Click **Close** to complete the process:

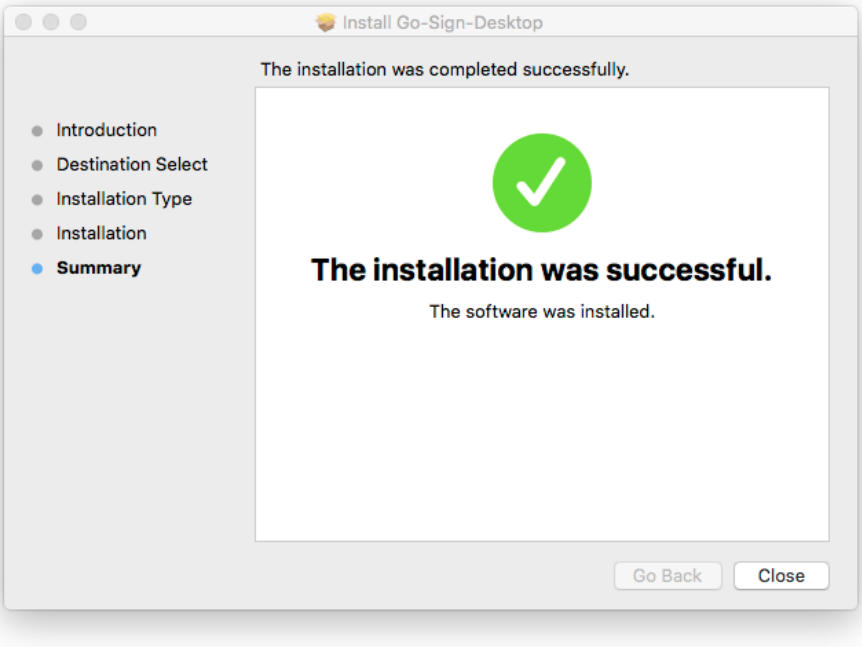

Figure 11 - MAC OS Installer Wizard Summary

10. After successful installation, you can view the ADSS Go>Sign Desktop application Icon in the **Dock** bar:

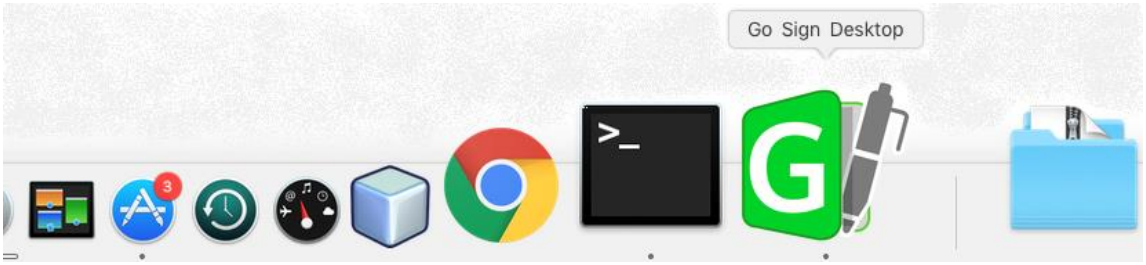

Figure 12 - MAC OS Dock Bar

4.2 Remote Installation Using Windows Group Policy

Follow these steps to deploy ADSS Go>Sign Desktop with Windows Group Policy. This process will either automatically install ADSS Go>Sign Desktop application to client 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 the computer. When the user first runs the program, the installation is completed. 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 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 or install the package to the distribution point. For example, to distribute Microsoft Office XP, 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. Start **Active Directory Users and Computers** snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click **Group Policy** tab, and then click **New**.
4. Type a name for this new policy (for example, “ADSS Go>Sign Desktop” distribution), and then press **Enter**.
5. Click **Properties**, and then click the **Security** tab.
6. Clear **Apply Group Policy** check box for the security groups that you don't want this policy to apply to.
7. Select **Apply Group Policy** check box for the groups that you do want this policy to apply to.
8. When you are finished, click **OK**.

4.2.3 Assign a Package

To assign a program to computers that are running Windows Server 2008, Windows Server 2012, Windows 7, or Windows 10, or to users who are logging on to one of these workstations, follow these steps:

1. Start **Active Directory Users and Computers** snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click **Group Policy** tab, select the policy that you want, and then click **Edit**.
4. Under **Computer Configuration**, expand **Software Settings**.
5. Right-click **Software installation**, point to **New**, and then click **Package**.
6. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, `\\file server\share\file name.msi`.

Important: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared installer package.

7. Click **Open**.
8. Click **Assigned**, and then click **OK**. The package is listed in the right-pane of the **Group Policy** window.
9. Close the **Group Policy** snap-in, click **OK**, and then close the Active Directory Users and Computers snap-in.
10. When the client computer starts, the managed software package is automatically installed.

4.2.4 Publish a Package

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

1. Start **Active Directory Users and Computers** snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click **Group Policy** tab, click the policy that you want, and then click **Edit**.
4. Under **User Configuration**, expand **Software Settings**.
5. Right-click **Software installation**, point to **New**, and then click **Package**.
6. In the **Open** dialog box, type the full UNC path of the shared installer package that you want. For example, \\file server\share\file name.msi.

   Important: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared installer package.
7. Click **Open**.
8. Click **Publish**, and then click **OK**.
9. The package is listed in the right-pane of the **Group Policy** window.
10. Close the **Group Policy** snap-in, click **OK**, and then close the **Active Directory Users and Computers** snap-in.
11. 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 XP, click **Start**, and then click **Control Panel**.
    - Double-click **Add or Remove Programs**, and then click **Add New Programs**.
    - In **Add programs** from your network list, click the program that you published, and then click **Add**. The program is installed.
    - Click **OK**, and then click **Close**.

4.2.5 Redeploy a Package

In some cases, you may want to redeploy a software package (for example, if you upgrade or change the package). To redeploy a package, follow these steps:

1. Start **Active Directory Users and Computers** snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click **Group Policy** tab, click the **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 you 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 **Redeploy application**. You will receive the following message:

   Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?
7. Click **Yes**.
8. Quit the **Group Policy** snap-in, click **OK**, and then close the **Active Directory Users and Computers** snap-in.

4.2.6 Remove a Package

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

1. Start **Active Directory Users and Computers** snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
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 you 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 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

6 Uninstalling ADSS Go>Sign Desktop App

6.1 Windows OS

Users can uninstall ADSS Go>Sign Desktop application by using one of these options:

- *Windows Control Panel > All Control Panel Items > Programs and Features*
- *Running the **uninstall.bat** using **Run as administrator** option from location **C:\Program Files\Ascertia\Go-Sign-Desktop\uninstall.bat**.*

6.2 MAC OS

User can uninstall the ADSS Go>Sign Desktop application by running the **"uninstall.command"** file from the following destination:

- Applications > Ascertia > Go-Sign-Desktop.app > Contents > Java > app > bin

On Go-Sign-Desktop.app right-click and select "show package contents" to get in to the Contents folder.

7 Logging

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

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

- **Windows OS:**

  C:\Users\[User_Name]\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs

- **MAC OS:**

  Applications>Ascertia>Go-Sign-Desktop.app>Contents>Java>Ascertia>Go-Sign-Desktop>logs

7.1 Changing Logging Level

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

1. Go to ADSS Go>Sign Desktop installation path:
   - **Windows:** *C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf*
   - **Mac OS:** */Applications/Ascertia/Go-Sign-Desktop.app/Contents/Java/app/conf*
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. Stop ADSS Go>Sign Desktop application:
   - **Windows System Tray**:

     Right click ADSS Go>Sign Desktop application icon and select the option **Quit.**
   - **Mac OS Dock/Menu bar**:

     Right click ADSS Go>Sign Desktop application icon and select the option **Quit.**
5. Start ADSS Go>Sign Desktop application:
   - For **Windows >Start Menu**
   - For **Mac OS > Dock/Menu bar**

8 Listening Ports

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

8.1 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 or UNIX daemons to have the changes take effect.

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 8 during initial communication with the browser.*

8.2 ADSS Go>Sign Desktop Changes

Once the above changes are done in ADSS Server Console, users must be informed of the new settings to update the ports in the respective file **"gosign_desktop.properties"** located in the directory:

- **Windows OS:** *C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf*
- ***Mac OS*:** */Applications/Ascertia/Go-Sign-Desktop.app/Contents/Java/app/conf/*

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 ***