ESMIG U2A

Qualified Configurations

V1.2

Author

Version	1.2
Date	26/07/2021
Status	Final
Classification	Unclassified
Accessible	
Classified until	

History of releases

RELEASE	DATE	ISSUES	STATUS[1]
1.0	01/03/2021	First version. Applicable for TIPS	Draft
1.0.1	06/04/2021	Second version, clarifications on support for terminal servers	Draft
1.1	05/05/2021	Third version. Extension to CLM and RTGS GUIs	Final
1.2	26/07/2021	Added terminal server support for Ascertia client. Extension to ECMS. Ascertia client URLs changed. Minor clarifications on U2A configurations. Added section in the annex concerning the GSD multi-user solution	Final

[1] Status value : Draft, Open, Final, Dismiss

Table of content

1 INTRODUCTION 4

1.1. PURPOSE AND OBJECTIVES 4
BACKGROUND REMARKS 4
QUALIFIED CONFIGURATIONS 4

1.2. TECHNICAL REQUIREMENTS AND RECOMMENDATIONS 5
DOWNLOAD MECHANISM 5
GO>SIGN DESKTOP CLIENT REQUIREMENTS 6
OTHER TECHNICAL REQUIREMENTS 7

1.3. RUNNING THE APPLICATION GO-SIGN-DESKTOP 8
VERIFYING GO>SIGN APPLICATION RUNNING 9

1.4. TROUBLESHOOTING INFORMATION - 10
LOGGING INFORMATION 10
CHANGING LOGGING LEVEL 10

2 ANNEX Errore. Il segnalibro non è definito.

2.1 GOSIGN DESKTOP (GSD) CLIENT – TERMINAL SERVER INSTALLATION GUIDE 11
SETUP GSD SINGLE USER CLIENT 11
COPY GSD EXECUTABLE INTO GSD CLIENT INSTALLATION PATH 15
UPDATE LOG FOLDER PATH 16
CONFIGURE GO-SIGN-DESKTOP AS WINDOWS SERVICE 16
PUBLISH APPLICATIONS GSD.EXE AND CHROME IN CITRIX FARM 19

1 INTRODUCTION

1.1. Purpose and Objectives

This document describes the general configuration that ESMIG users shall be complaint with in order to access TIPS, ECMS, RTGS, CLM and CRDM GUI via the ESMIG web portal. A specific section is devoted to describe the technical framework needed to fully implement the non-repudiation of origin functionality (NRO). This solution will be implemented in TIPS via the Change Request TIPS-0034-SYS, when the applet technology will be decommissioned in favour of a browser's java plugin independent solution. In RTGS and CLM GUIs the same solution will be implemented according to the official plan.

Background remarks

The aim of the ESMIG qualified configurations is to provide ESMIG users with a specific configuration that is proved to be fully working.

As already mentioned, the NRO solution, based on the Ascertia Go>Sign Desktop application, will be the unique U2A NRO solution to be adopted for TARGET services, therefore only one version of the Go>Sign Desktop client will be used and distributed across the different services.

Important also to hightlight that Go>Sign Desktop client applications are already in use in TARGET2 for Internet Access and Contingency Network and 4CBs will guarantee that no different versions are needed by the relevant services using the client, before the go-live of CSLD project.

Qualified configurations

As already mentioned, the 4CB has qualified a specific subset of the NSPs compatibility matrix. These configurations have been extensively tested and support on them is guaranteed.

NSP	SWIFT	SIA-COLT
OS	Windows 10	
Browser	Google Chrome 88.0+, Firefox 78.0+	
Go>Sign Desktop	> 6.0.0.14	

These cryptographic key stores, used to access the signing keys, are supported:

- PKCS#11 for hardware-based tokens

The Ascertia solution based on the Go Sign Desktop client is currently not fully compatible with Servers/Citrix Terminal Server solutions; this means, in details, that such solutions can be used by a

single user at a time only. In order to cope with such specificity, customers may want to configure/provide smaller server instances to their operators, so that they can be used as single-user workstations. The 4CB cannot provide detailed instructions on the configuration/deployment of such scenario as it is highly dependent on the local infrastructural setup.

A new version of the client supporting multi user environment is being developed by Ascertia and it has been made available to the external users for early installation first (see Annex). 4CB will be testing the effectiveness of the changes on their Citrix terminal server infrastructure only, before sharing the final multi-user client with the market.

The Citrix Virtual Desktop solution is, on the other hand, already fully supported by Ascertia, allowing the implementation of a jump host to be used to connect to the relevant TARGET Service (i.e. not directly from the operator workstations).

The 4CB will ask customers running a software version lower than that qualified to upgrade to a qualified version in order to proceed with problem investigation.

The 4CB will investigate issues experienced by customers while running a software version higher than that qualified: If the root cause is linked to the specific software version, then the 4CB will attempt to find a workaround (which may involve customers downgrading their software to a qualified version). The 4CB will evaluate whether a fix for the issue can be included in a future relevant TARGET Service GUI release.

Customers using totally or partially different system components or versions than those mentioned are then responsible to verify the full compatibility with the relevant TARGET Service GUI in the test environments and the system. The 4CB will in any case, provide support to the maximum extent possible for checking / testing alternative configurations in order to support troubleshooting process.

The local customer system set-up, i.e. adaption of the local firewall and security policies in order to enable the client installation, HTTPS transfer communication, access to the certificates on the USB tokens from the client machines (either physical or remote workstations) is under the sole responsibility of the end users (that may also need to involve their internal IT Dept. as well as external providers, in case of product specific issues).

1.2. Technical requirements and recommendations

Download mechanism

The client is available for download at the following URLs on the ESMIG portal:

EAC PORTAL

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/32bit_client

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/32bit_client

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/64bit_client

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client

UTEST PORTAL

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/32bit_client

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/32bit_client

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/64bit_client

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client

PROD PORTAL

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/32bit_client

https://portal.emip.swiftnet.sipn.swift.com/gosign/download/32bit_client

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/64bit_client

https://portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client

The full installation guide provided by Ascertia is distributed separately and it can be used as reference for specific needs (e.g. automated installations).

Downloading and installing the Go>Sign Desktop client is a mandatory step to sign U2A requests. Installation requires administrative privileges; local IT support must be involved to make sure the installation correctly ends.

Please make sure the correct version Go>Sign desktop is installed. To check this please right click on the go sign icon and choose "about". After that the following window appears:

Go>Sign Desktop Client Requirements

The client invocation on user side will be triggered by the web application (via Javascript) with the first attempt to sign an instruction (and each time the user needs to sign one) and is transparent to users.

ADSS Go>Sign Desktop relies on TLS communication only with the web application (port 8782). This communication is secured using a TLS server certificate having hostname:

client.go-sign-desktop.com.

Therefore, the local client machine must be able to resolve this FQDN (Fully Qualified Domain Name complete domain name for a specific computer, or host, on the internet) to itself.

In order to achieve this, the standard procedure foresees that the Go>Sign Desktop Installer automatically adds the entry :

127.0.0.1 client.go-signdesktop.com

in the Operating System host file to register the client.go-sign-desktop.com as a local domain (Windows OS: C:\Windows\System32\Drivers\etc\hosts).

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

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

The TLS server certificate will be self-signed and different for each workstation where the client will be installed. Once loaded into Windows OS, it is expected to be found in the Root CA keyring (i.e. and not in the personal certificate keyring).

The end users have to ensure that the security settings of their institutions, i.e. firewalls, allow for installation of the applet/desktop client as well as for code signing certificate revocation check, if not generally disabled. 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.

Other technical requirements

Here following a list of items to be checked before starting the test sessions or in case of exceptions that may block the testing. Internal IT support may be needed to perform these checks because security restrictions may be in place preventing the end users to complete them autonomously.

- As a general remark, please make sure that the configurations listed in the relevant NSPs documentation are applied (as a not exhaustive example, the mandatory changes on the pac file). For further details please refer to the "SWIFT's Solution for ESMIG U2A Setup Guide Step-by-Step" document and the " SIAnet.XS Connectivity Services for ESMIG U2A User Guide"
- In case of certificate exceptions in the browser during first interaction with new Ascertia infrastructure: add DSS host certificates in browsers keyring (e.g Chrome and Firefox). Host names following for information:

SIA TST	esmig-tst-dss.u2a.sianet.sia.eu
SIA CRT	esmig-cert-dss.u2a.sianet.sia.eu

SIA PRD	esmig-dss.u2a.sianet.sia.eu
SWIFT TST	esmig-tst-dss.emip.swiftnet.sipn.swift.com
SWIFT CRT	esmig-cert-dss.emip.swiftnet.sipn.swift.com
SWIFT PRD	esmig-dss.emip.swiftnet.sipn.swift.com

The same above URL may need to be added to the browsers trusted sites.

- In case of Cross-Origin Resource Sharing (CORS) issue during first interaction with new Ascertia infrastructure, please temporarily disable CORS checks both in Chrome and/or FF

a. FF --> https://addons.mozilla.org/es/firefox/addon/access-control-allow-origin/ + Toggle ON

b. Chrome --> "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security --user data-dir="C:\.....\Chrome"

- Check windows host file for the definition 127.0.0.1 client.go-sign-desktop.com

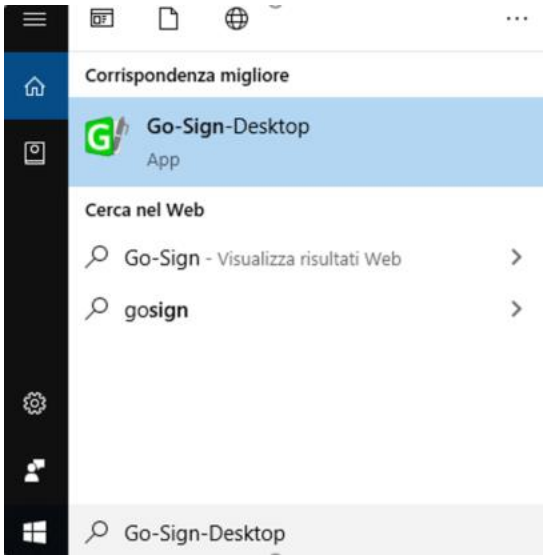
- Check installation / install "client.go-sign-desktop.com" certificate in Chrome and Firefox explicitly (or check first if it is in all browsers keyring after GSD client installation). Without this exception error code 404 is displayed.

It is finally suggested to ensure that one token at time is connected to a workstation during signing operation.

1.3. Running the Application Go-Sign-Desktop

Once the application is installed, it is usually configured to run automatically when a Windows session is started. However, due to specific security settings, this might not happen, resulting signature attempts to end with a similar error "Go>Sign desktop not running/installed".

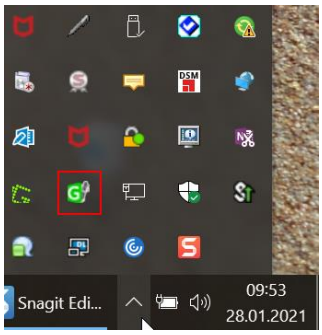
In this case, it is necessary to run it manually before initiating a browsing session in ICM. It is possible to lookup for the Go>Sign via the Windows Search bar:



If the icon is not found, this can be probably linked to problems occurred during the installation. The local IT support needs to be involved in this case.

Verifying Go>Sign application running

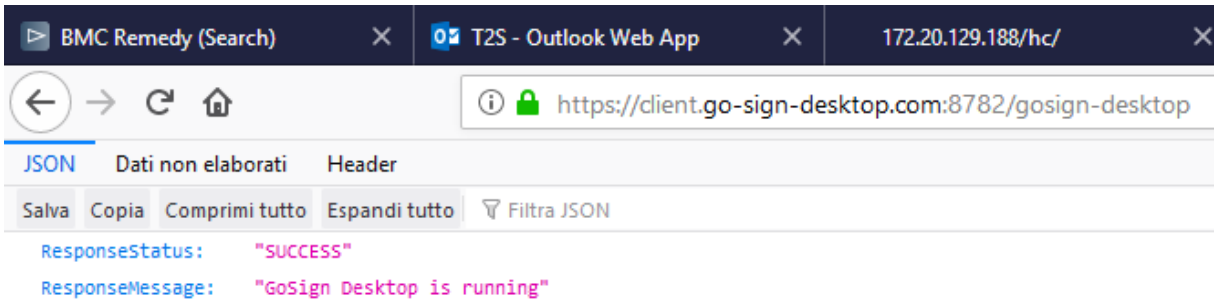
Ensure that the Go>Sign icon is featured in the system tray.



In addition, it is requested to verify that Go>Sign is running properly, by accessing the URL

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

The screenshot below is the expected result with Mozilla Firefox:



1.4. Troubleshooting information - Logging information

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. For Windows OS and go>sign client configuration, users can view ADSS Go>Sign Desktop application logs at:

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

and should send the send the "GoSignDesktopLog.txt" when opening the incident to 4CB Service Desk.

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 → C:\Program Files\Ascertia\Go-Sign-Desktop\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 → right click ADSS Go>Sign Desktop application icon and select the option Quit.
5. Start ADSS Go>Sign Desktop application → Start Menu

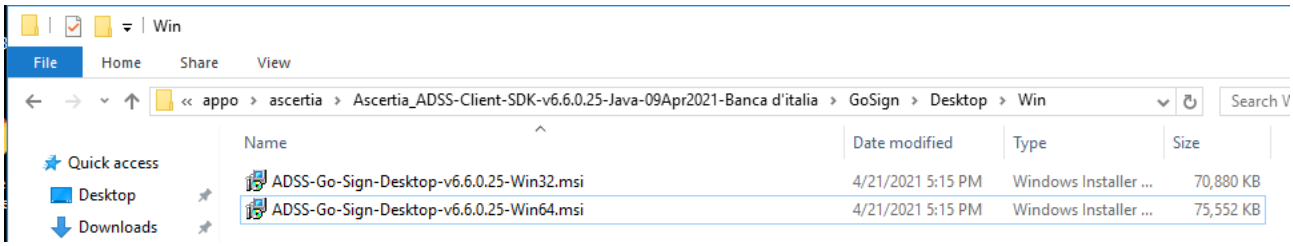
2 ANNEX

GoSign Desktop (GSD) Client – Terminal server Installation Guide

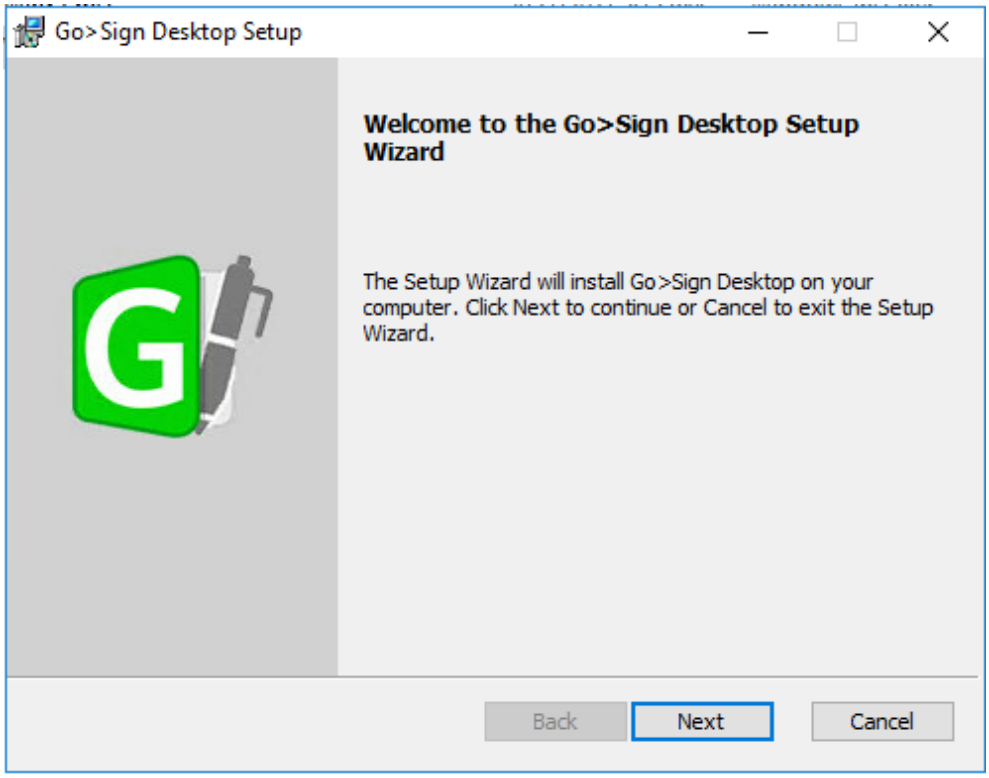
Installation steps are reported in the following paragraph; they may subject to further changes / improvements in order to simplify the overall process.

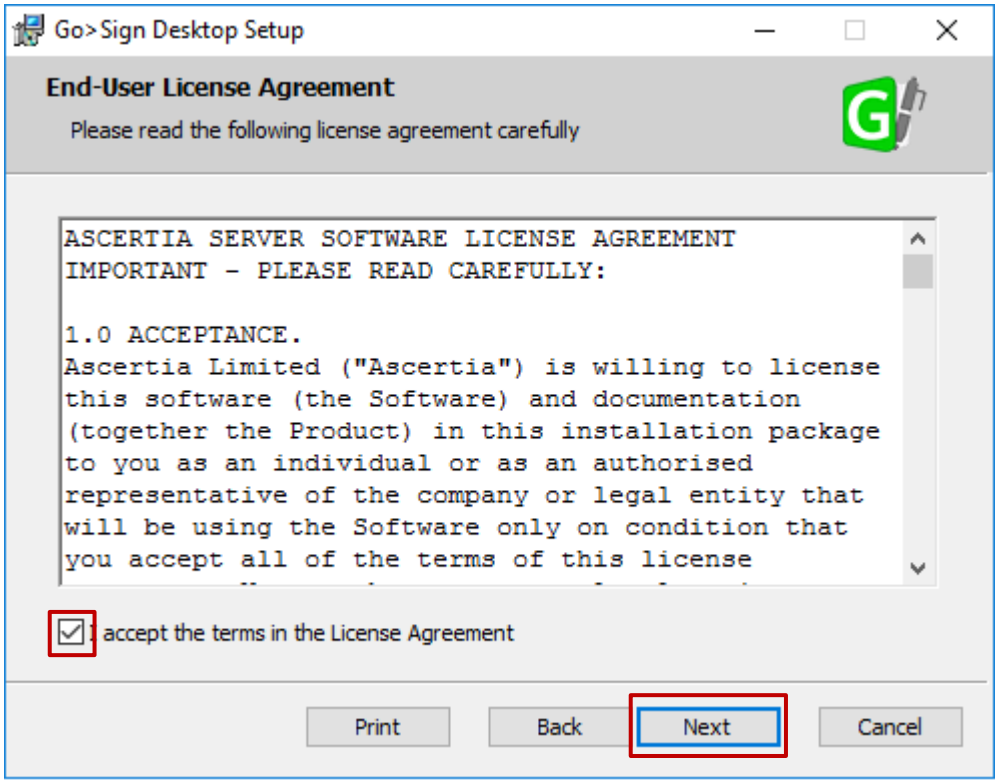
Setup GSD single user client

- Open Command prompt as Administrator
- Execute command: chgusr /install
- then run ADSS-Go-Sign-Desktop-v.6.6.0.xx-win64.msi installation package (currently distributed 6.6.0.14 can be used)

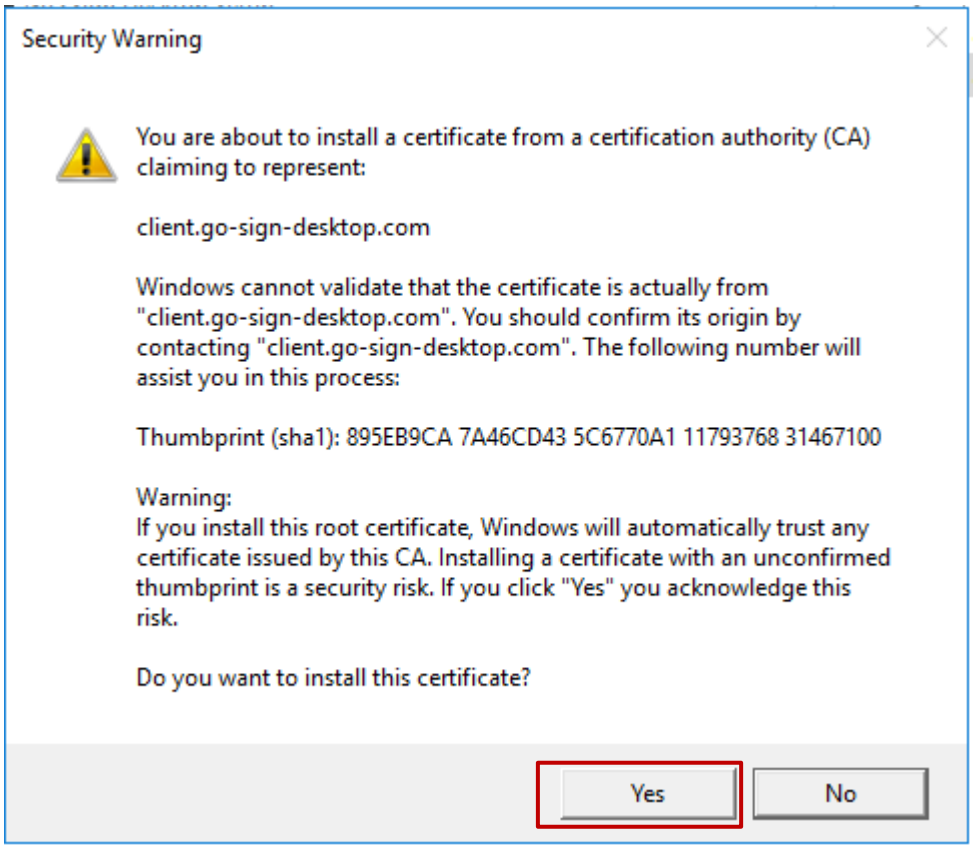


Click Next and accept End User License Agreement

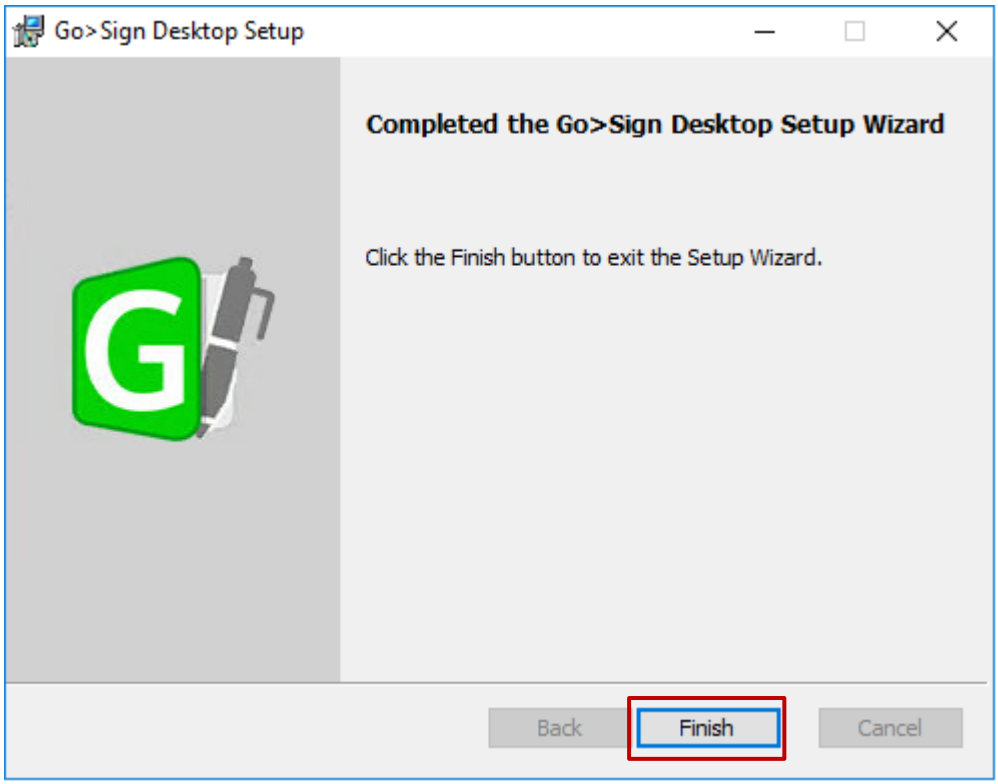




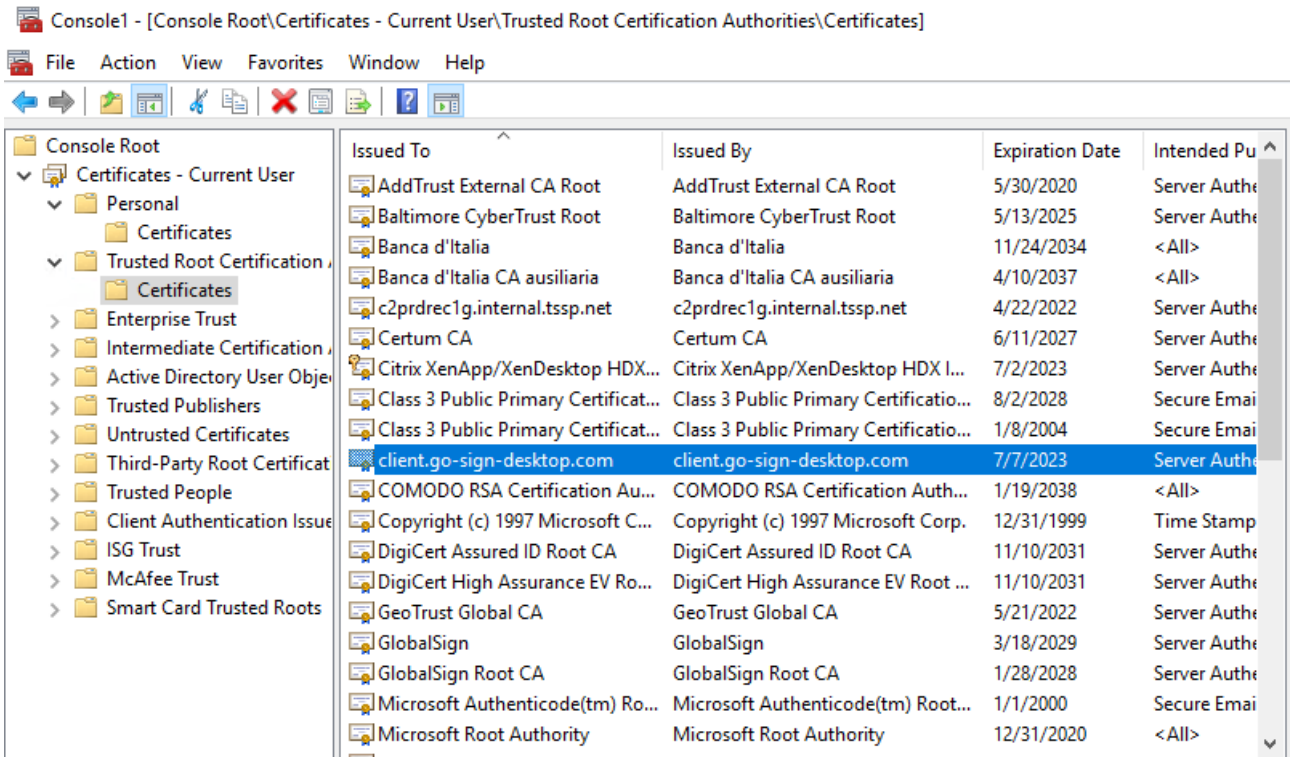
Accept to install certificate:



Select Finish:



Check that certificate client.go-sign-desktop.com is imported in User Certificate store by running *certmgr.msc* tool:

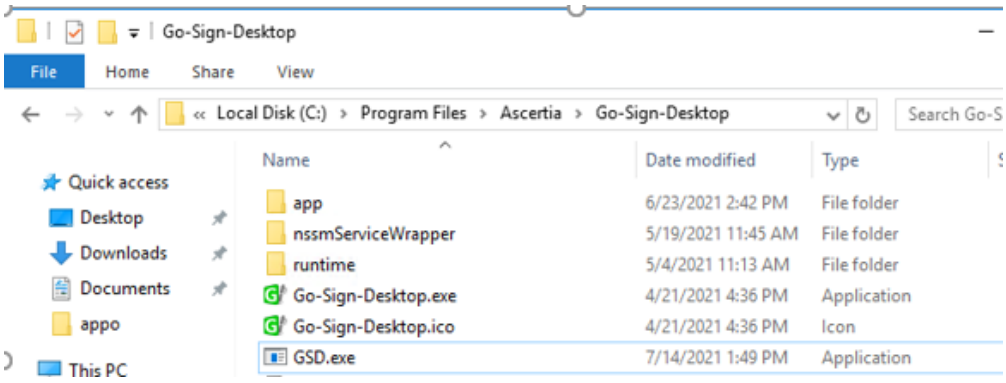


Copy GSD executable into GSD client installation path

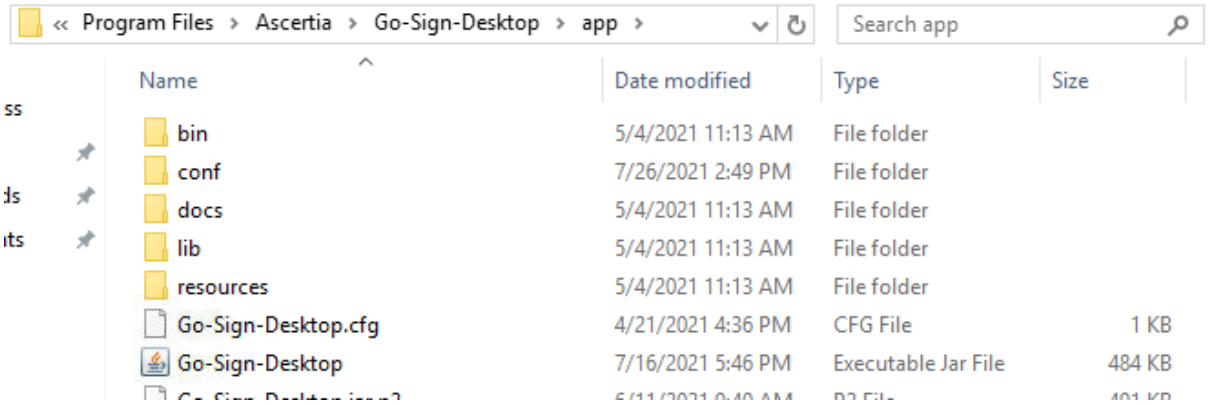
Please note that the following operations need administrative rights.

Download and copy;

- the GSD exe file into GSD installation directory (e.g. C:/Program Files/Ascertia/Go-Sign-Desktop)



- the Go-Sign-Desktop.jar file into <GSD_installation_directory>/app path



The updated code is available for download at the following URLs (directly from the browser):

EAC

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/gsdmu_client

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/gsdmu_client

UTEST

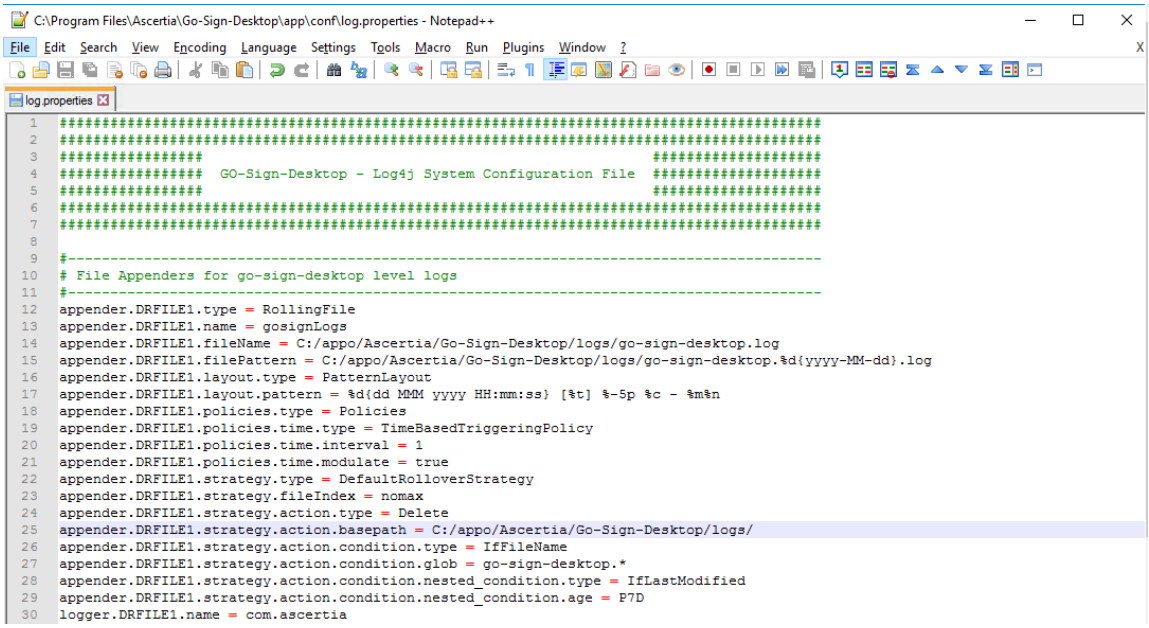
https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/gsdmu_client

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/gsdmu_client

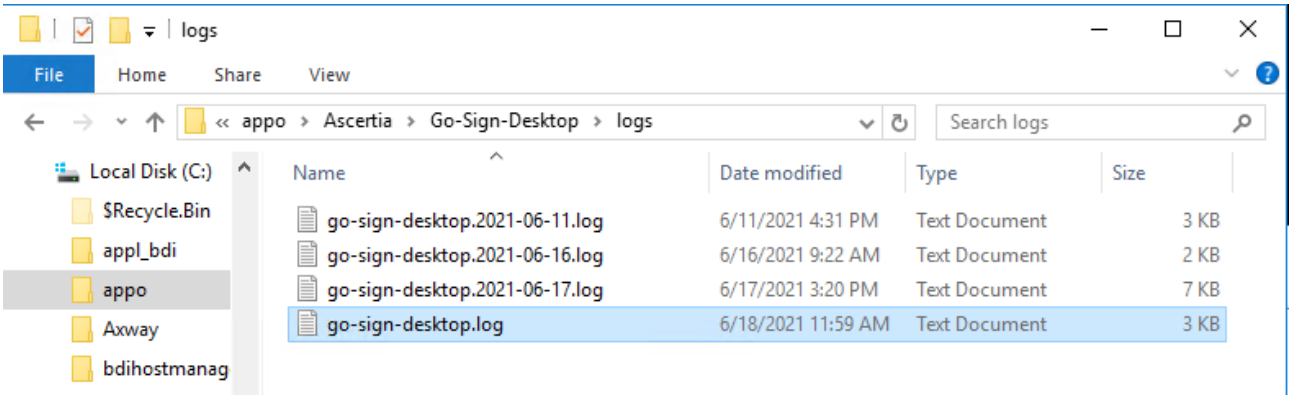
Update Log folder path

Log files are stored by default in user/%appdata% folder.

To change log file configuration modify the file "C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\log.properties" specifying the location where you want to store logs



Check the log file are in the right folder after starting GSD; logs will be collected in this log file/folder, for the moment.



Configure Go-sign-desktop as Windows Service

Current implementation foresees to have Go>Sign Desktop running as a Windows Service via a Service Wrapper which wraps the Go>Sign Desktop executable binary into a Windows Service via the NSSM opens source software available at https://nssm.cc/.

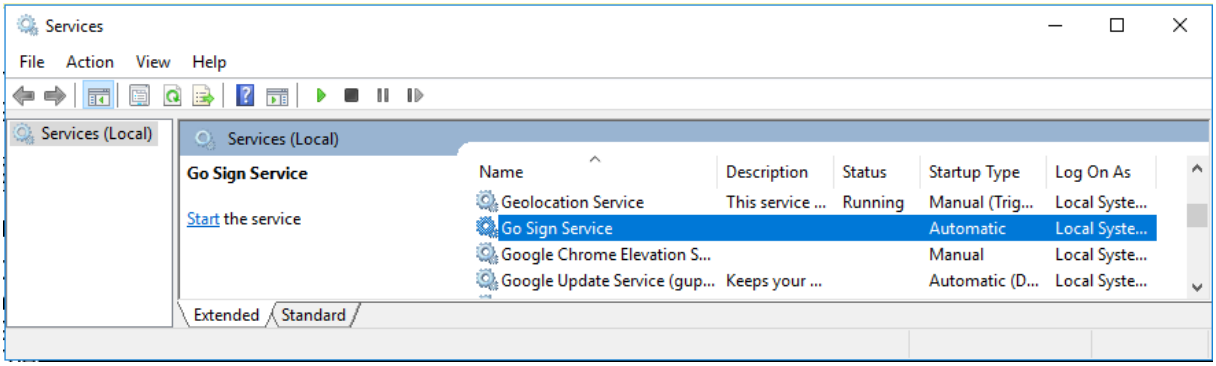
To configure service:

1) Extract archive content "nssmServiceWrapper.zip" to the C:\Program Files\Ascertia\Go-Sign-Desktop\ nssmServiceWrapper

2) Run Command Prompt with Administrator permissions and enter the following line with respect to the real location of Go>Sign Desktop:

"C:\Program Files\Ascertia\Go-Sirgn-Desktop\nssmServiceWrapper\win64\nssm.exe" install "Go Sign Service" "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-Sign-Desktop.exe"

3) Open Services.msc and locate the Go Sign Service just installed:



- Right-click Go Sign Service and choose Properties.
- Ensure "Startup type" is set to Automatic.
- Open the Log On tab and change "Log on as" to this account, then specify the account NETWORK SERVICE and leave the password blank

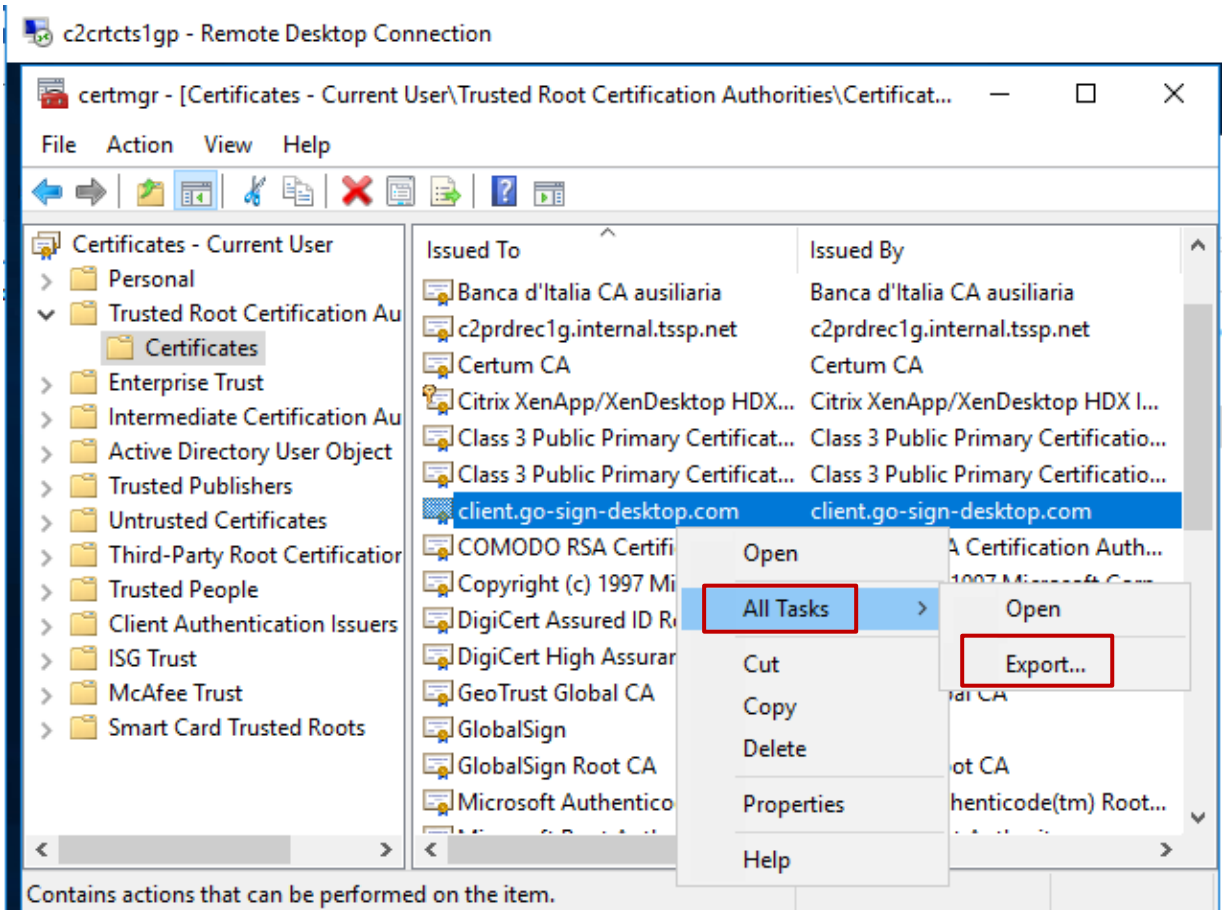
Import client.gosign certificate into Network Service user keystore

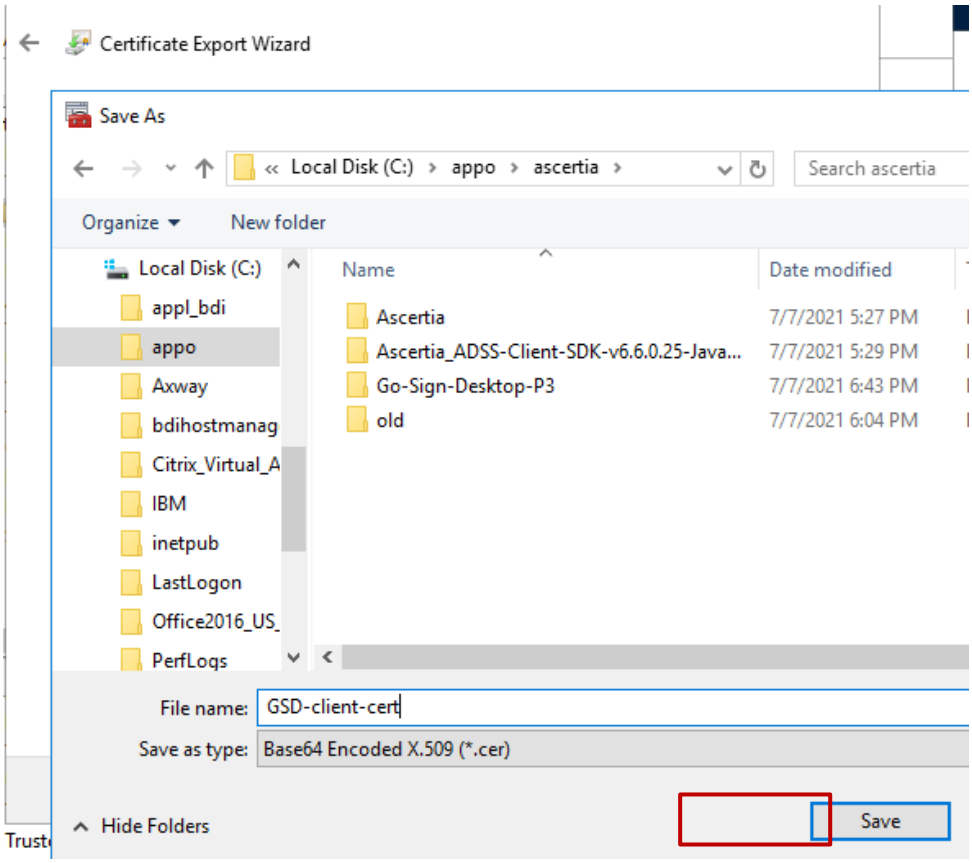
Run *certmgr.msc* tool and import directly the client certificate exported from the Current User Store.

Alternatively, GSD.exe file should be started from a "Network Service" user environment command prompt in order to start the client.gosign certificate (e.g. psexec tool can be used for such scope).

Connect client.gosign into GSD java keystore

Export new client.gosign-desktop certificate from the user store in DER format (certmgr.msc tool):





Update 'cacerts' file located in 'C:\Program Files\Ascertia\Go-Sign-

Desktop\runtime\jre\lib\security' with the certificate Go>Sign Desktop app trusted when it ran for the first time. The following keytool command to be used:

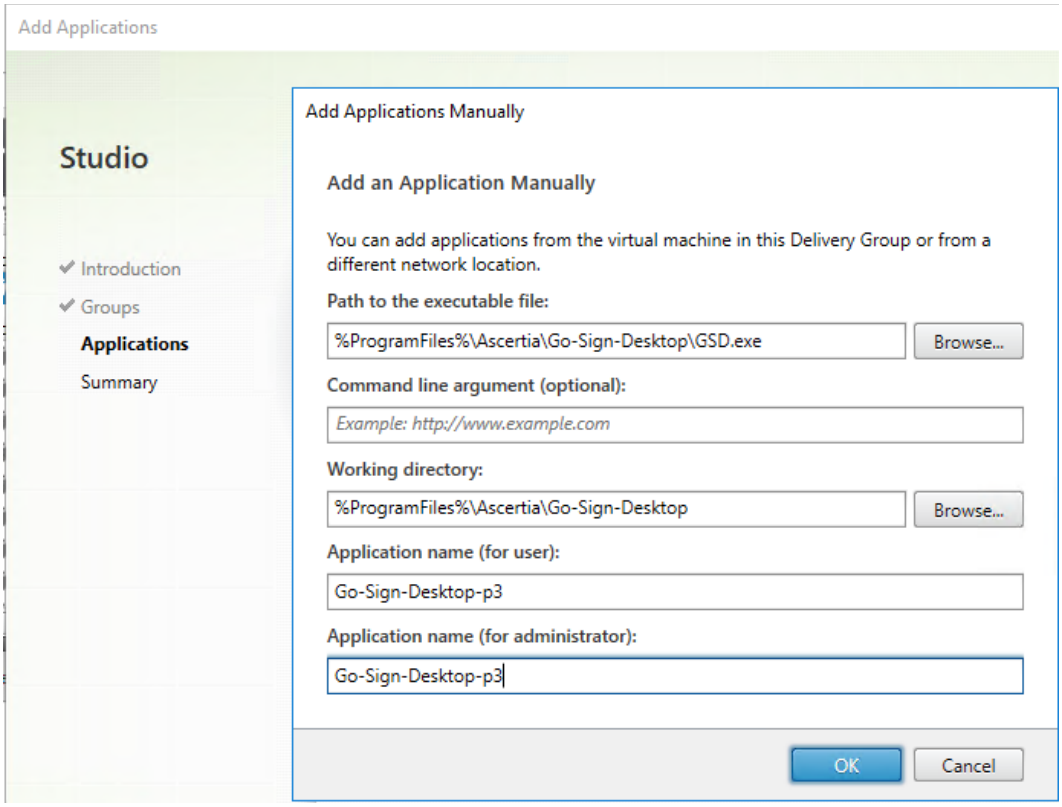
```
keytool -import -alias gosign -file exported-cert-der.cer -keystore "C:\Program Files\Ascertia\Go-Sign-Desktop\runtime\jre\lib\security\cacert"
```

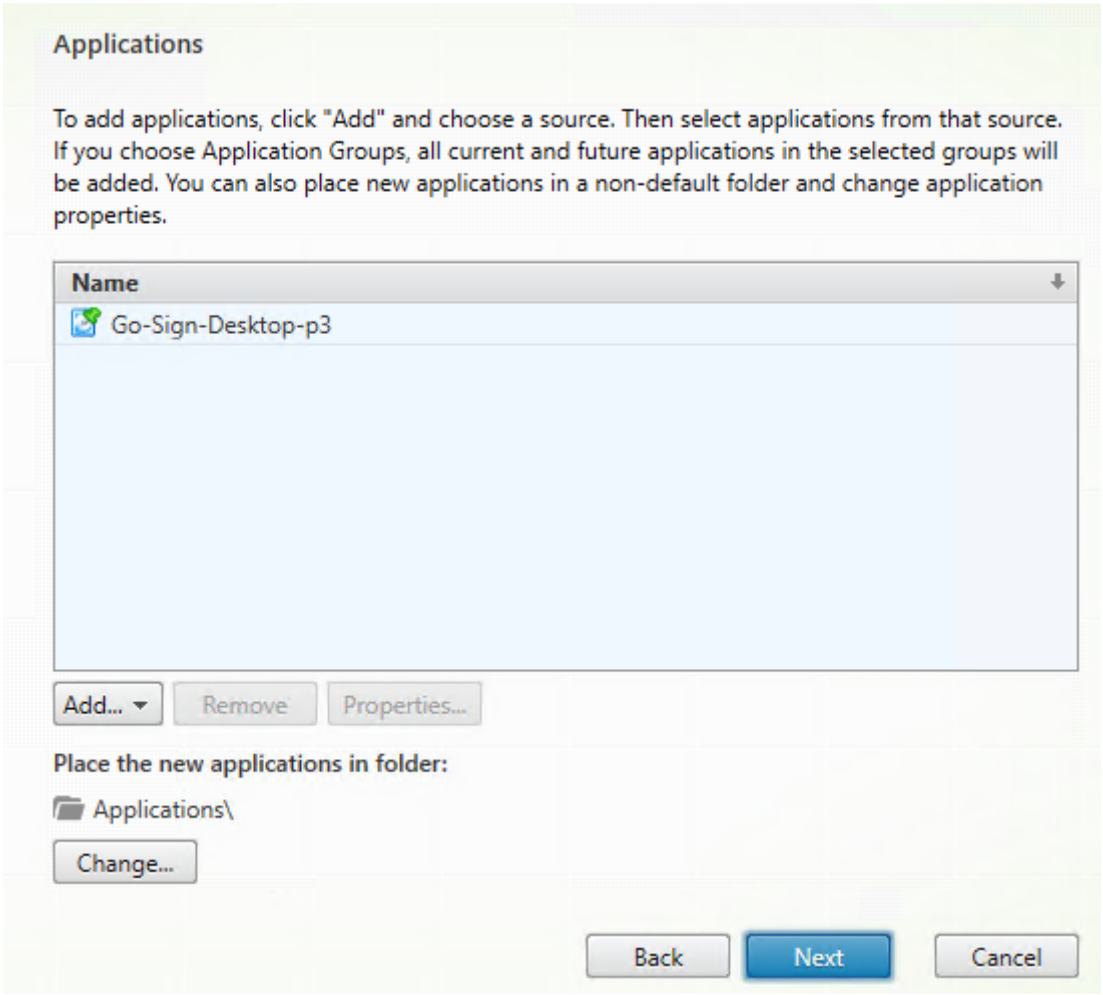
Copy C:\Program Files\Ascertia\Go-Sign-Desktop\runtime\jre\lib\security\cacert from the first server to the other terminal servers (if present).

Publish applications GSD.exe and Chrome in Citrix Farm

Publishing GSD from Citrix Studio

From Citrix Studio console Add a new Application, assign Delivery Group and "add an application manually" as described:


Add Applications
Studio
Introduction
Groups
Applications
Summary
Add Applications Manually
Add an Application Manually
You can add applications from the virtual machine in this Delivery Group or from a different network location.
Path to the executable file:
%ProgramFiles%\Ascertia\Go-Sign-Desktop\GSD.exe
Browse...
Command line argument (optional):
Example: http://www.example.com
Working directory:
%ProgramFiles%\Ascertia\Go-Sign-Desktop
Browse...
Application name (for user):
Go-Sign-Desktop-p3
Application name (for administrator):
Go-Sign-Desktop-p3
OK
Cancel



To be repeated for all the relevant users.

User preliminary actions

From Citrix Studio console Add a new Application, assign Delivery Group and "add an application manually" as described Before using GSD each user must launch one time GSD application on Citrix Portal in order to add in user profile the right registry keys and save the user configuration.

Then open Chrome.