Setup Guide

Setup Guide Automation AIS-Cloud and Uplink v 2.1

Updated: Date 2020-09-25

Contents

1 Introduction

Addovation provides a cloud service integration platform that is located either in a professional hosted environment, located within the borders of Norway or Sweden, Microsoft Azure or in your local in-house environment. All that is required is an Internet Information Server and an SQL Server database (2008+). All communication is done via REST-based interfaces; hence it is perfect for enabling collaboration between IFS and the outside world. No passwords are stored in Addovation Cloud, and all communication through the Cloud is encrypted.

1.1 Technical information

Addovation Cloud can work as self-hosted service or as Windows service. It runs three WCF services – Client service and two Data services.

1.1.1 Client Service

Client service is a WCF REST service, which receives all the mobile clients' requests. It uses HTTP binding with transport-level security (HTTPS communication provides confidentiality and integrity protection for the messages that are transmitted over the wire). It will be available on address "https://server:48081/Addovation.Cloud/ClientService/" by default.

1.1.2 Data Service

Data service is a WCF service, which provides possibility to perform requests to IFS databases. It uses NET TCP binding (socket endpoints) and NET HTTPS binding (websocket endpoints) with both transport and message security configured and duplex communication (duplex contracts are supported) with Uplink service. It will be by default available on address "net.tcp://server:48080/Addovation.Cloud/DataService/" for NET TCP binding and on address "wss://server:48079/Addovation.Cloud/DataServiceWss/" for NET HTTPS binding.

2 Prerequisites

These prerequisites are to make sure that all install packages and libraries are the same version (revision number).

2.1 Cloud Manager & Uplink Manager

For example, the installation package name is “AutomationServer 2.0.0.28106 x86.msi”. Check the last digits of the version in the file properties window.

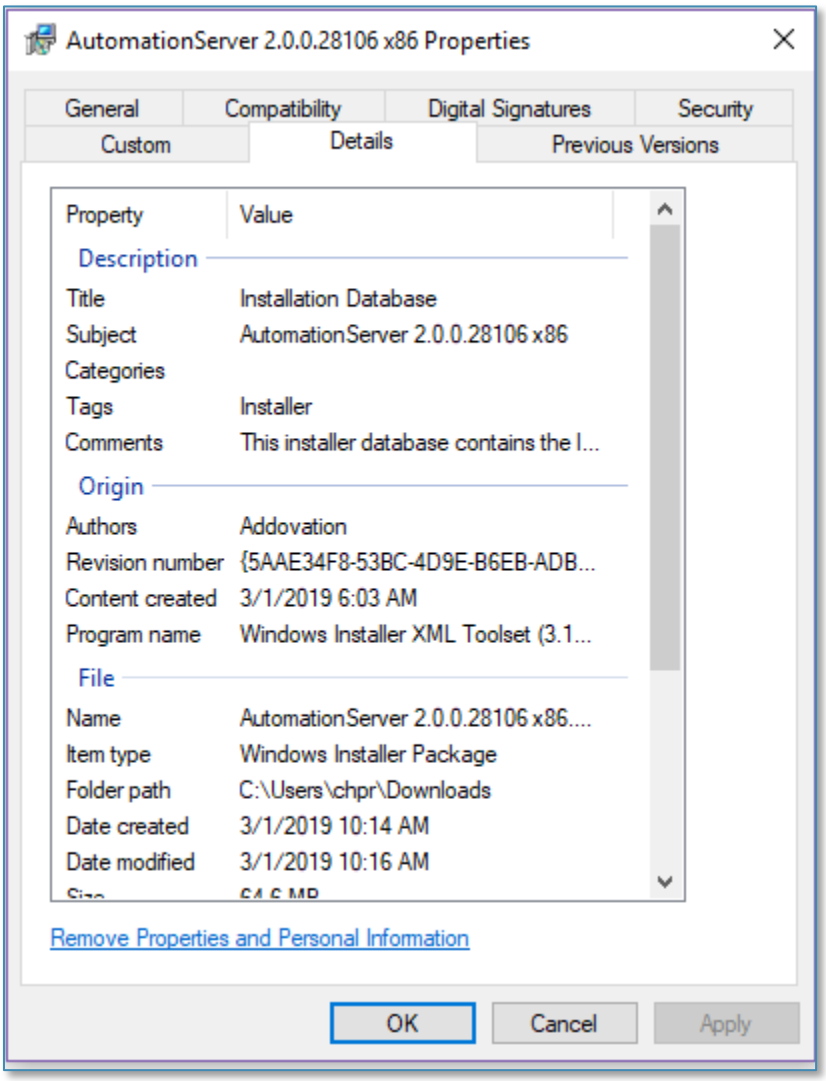

Figure 1 - Properties

Run the installation package and check the same digits in the main installation window.

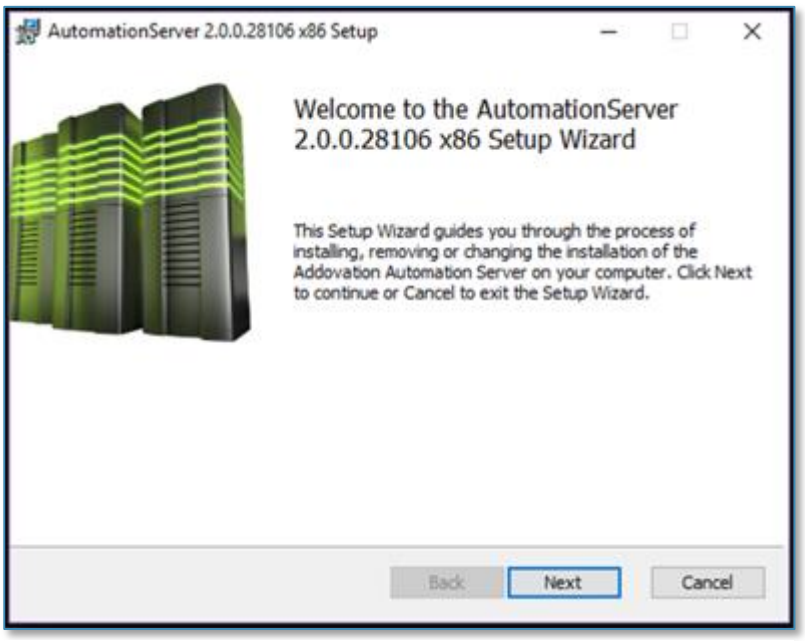

Figure 2 - Start setup wizard

2.2 AddoResources library

Addo Resource files will be installed in the following location by the installer.

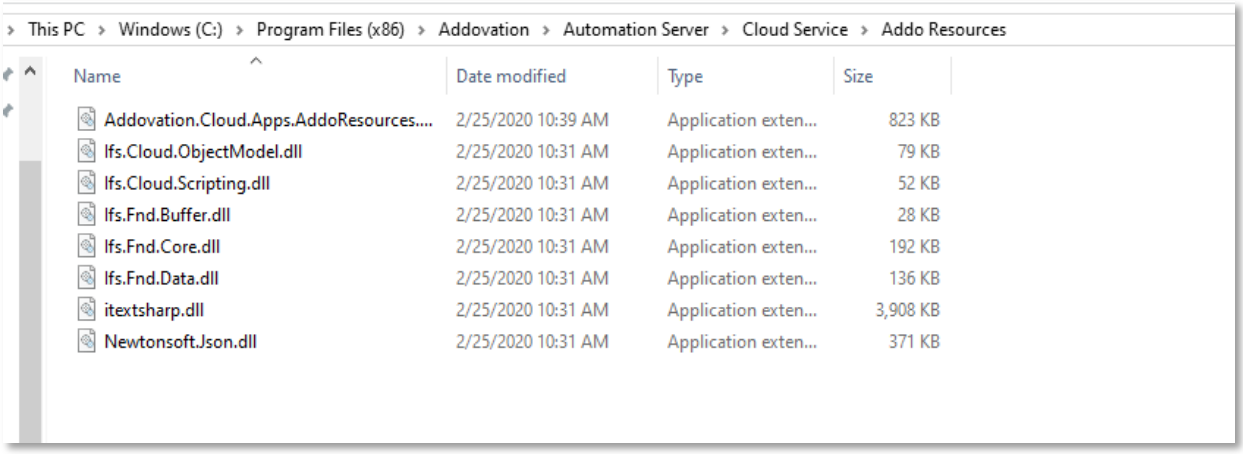

Figure 3 - AddoResources

For example, the library file name is “Addovation.Cloud.Apps.AddoResources.dll”. Check the last digits of the version in the file properties window.

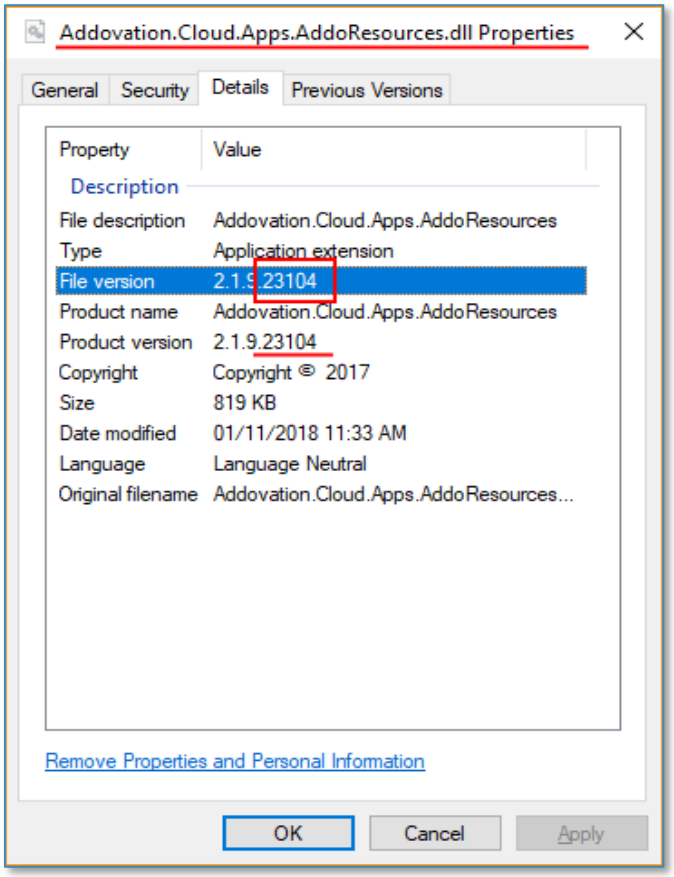

Figure 4 - Properties

3 Installation

3.1 Uplink Manager

Copy the installation package “AutomationServer 2.0.0.28106 x86.msi” to the server, which is going to be used for the Uplink Manager and run it.

Click “Next” on the Welcome screen.

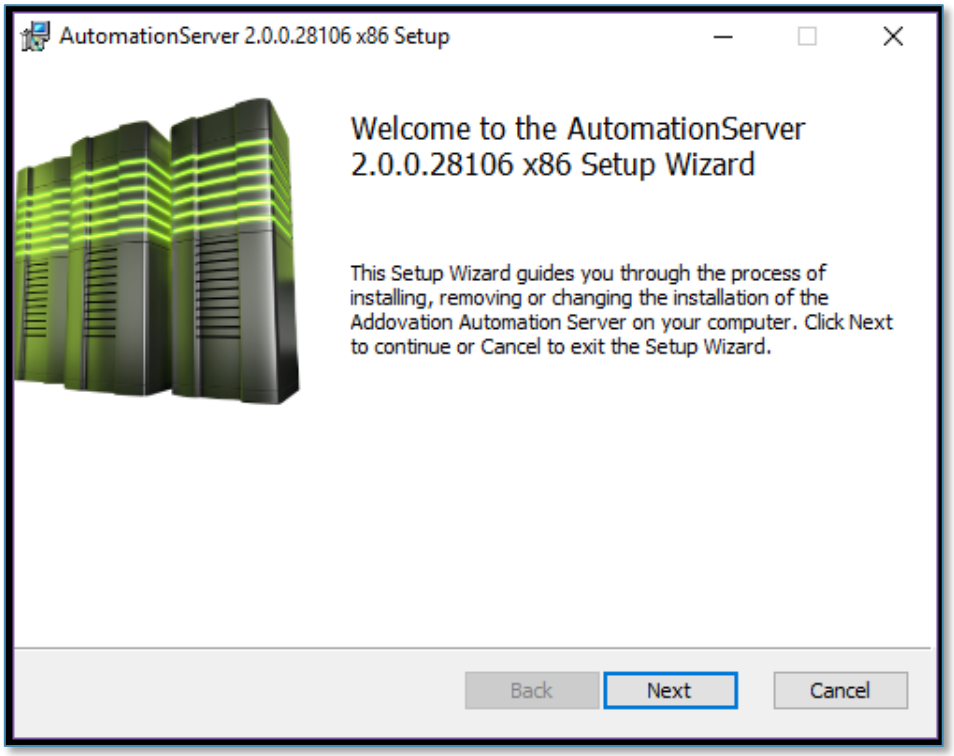

Figure 5 -Start setup

Review the license agreement and accept it, click “Next”.

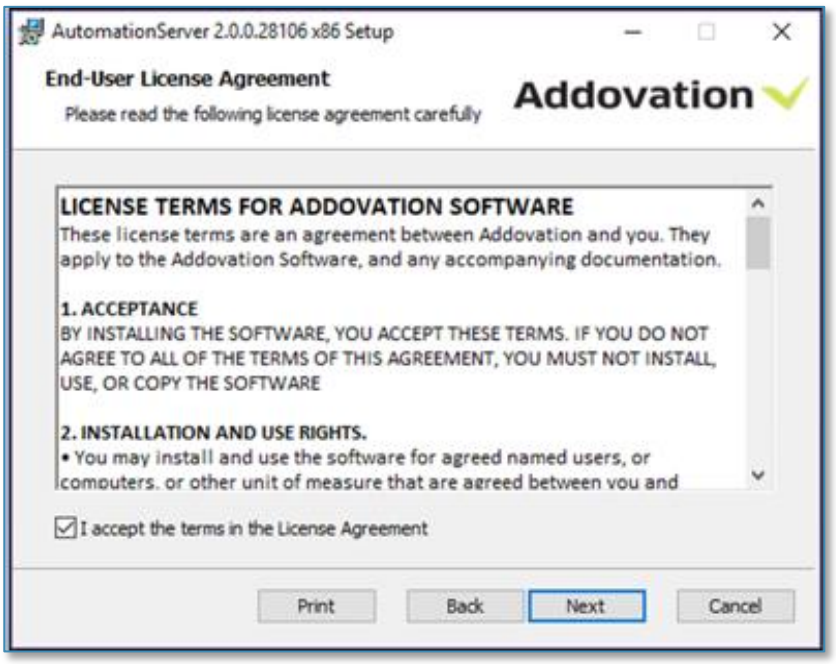

Figure 6 – End user license agreement

Click “Next” on “Environment configuration” screen without entering any configuration settings.

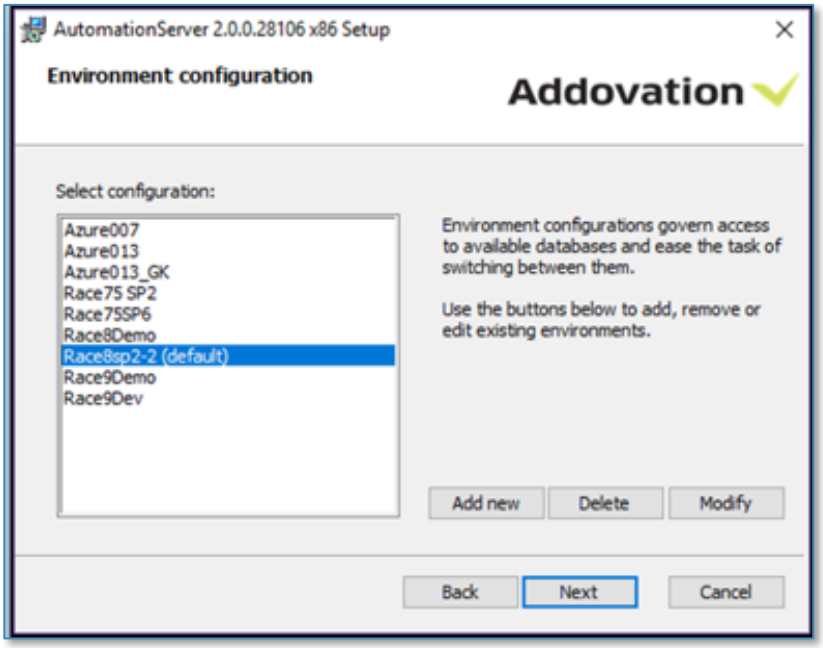

Figure 7 – Environment Confgiuration

Enter a valid license key for AIS Uplink and click “Next”.

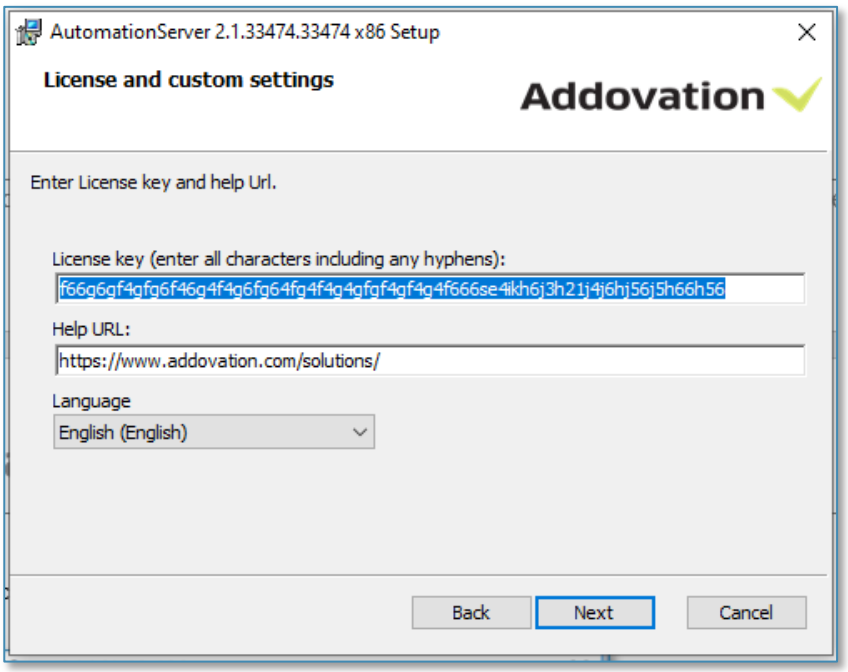

Figure 8 - License and custome settings

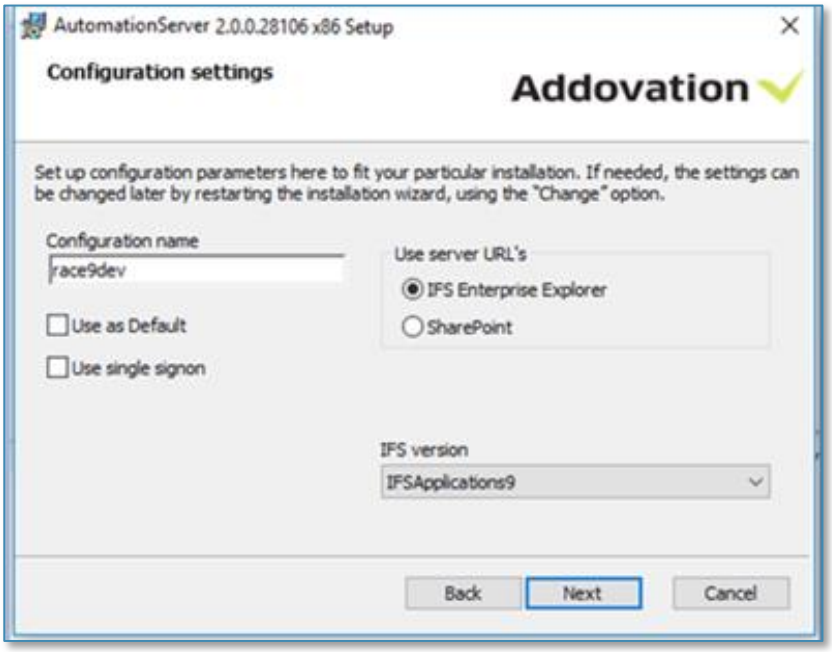

Figure 9 – Configuration settings

Verify that the chosen license key is not expired and valid for AIS Uplink. Click “Next”.

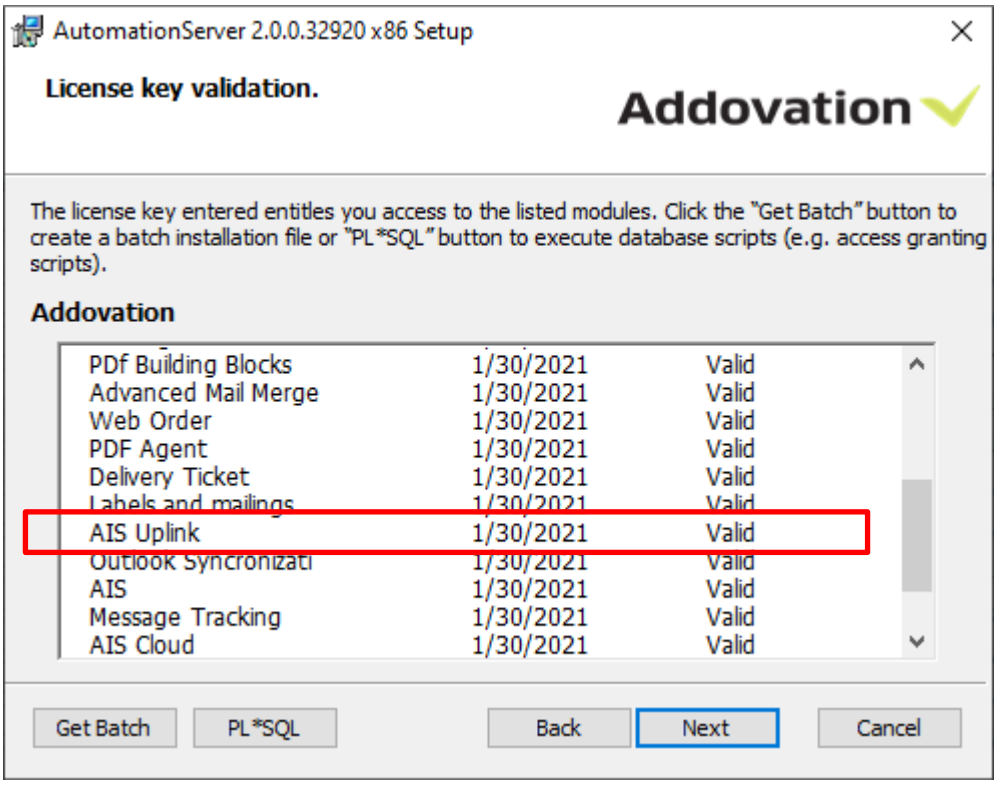

Figure 10License key validation

Choose “Custom” setup to install “Addovation Uplink” only and skip other applications.

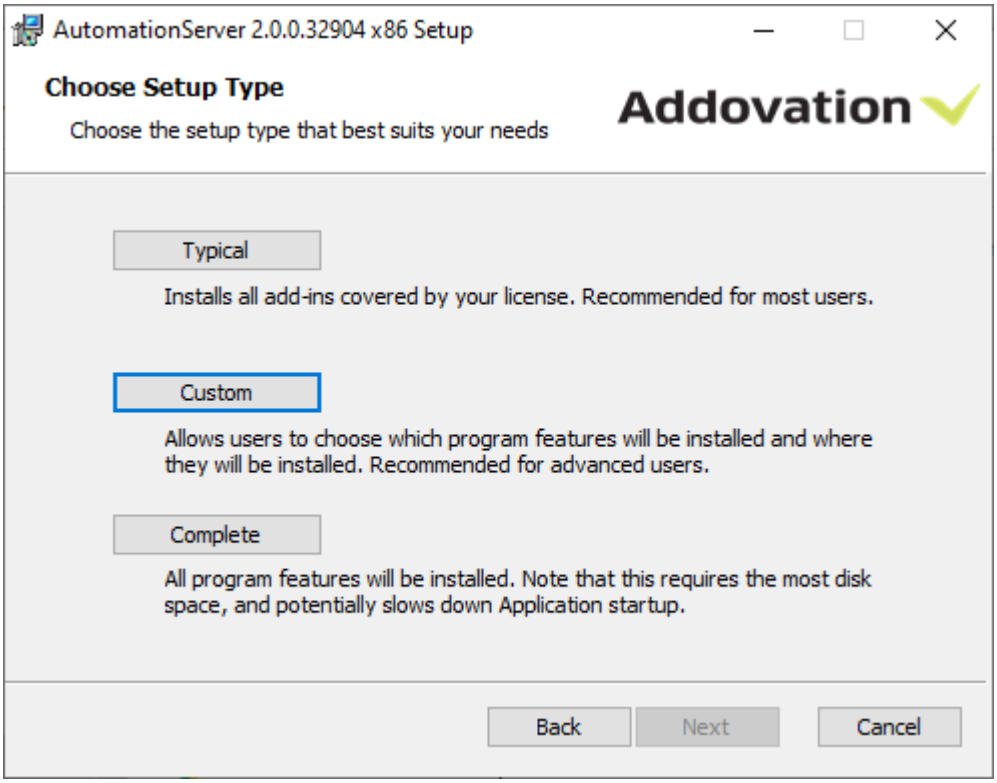

Figure 11 Choose setup type

Disable all other components (if they are not used and installed on that server), except “Addovation Uplink”, and click “Next”.

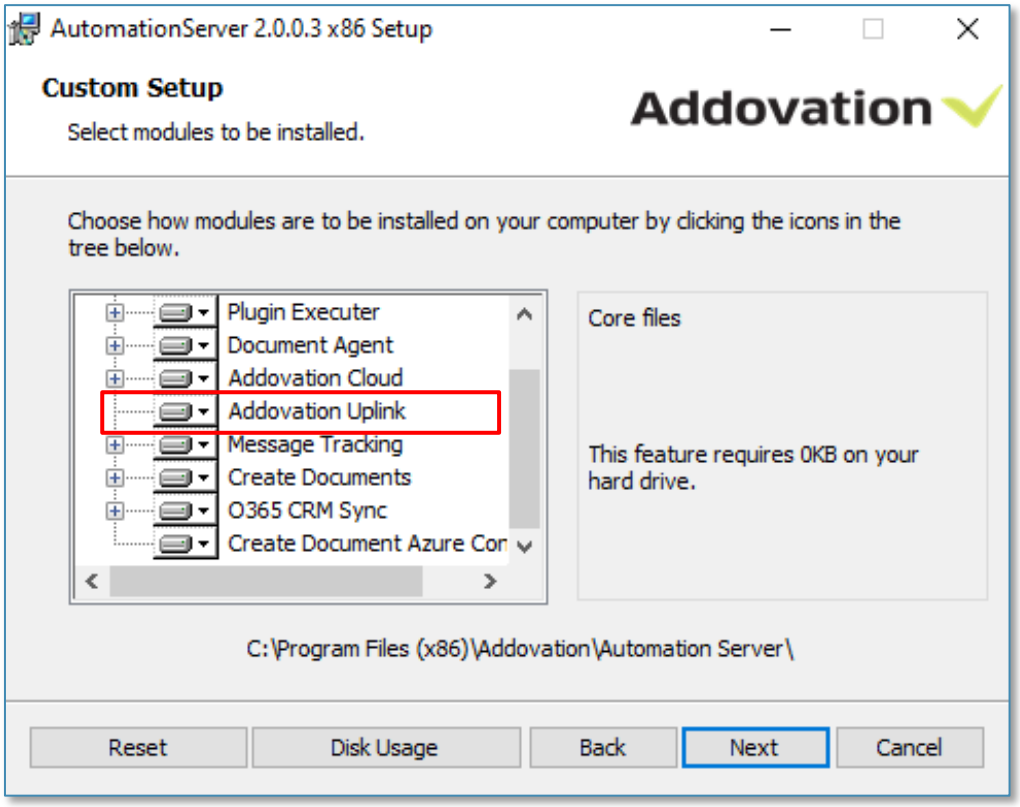

Figure 12 – Custom setup

Click “Install” to start the installation process.

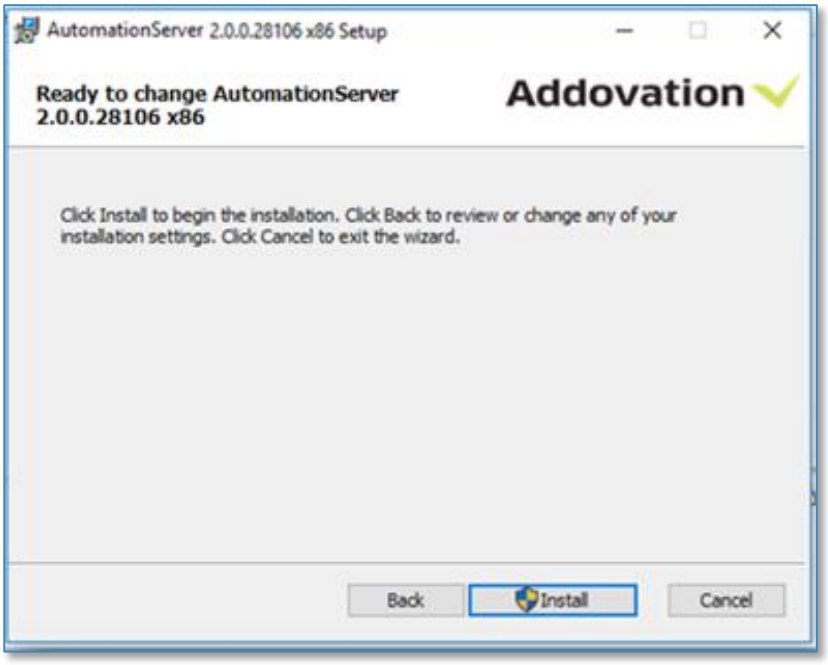

Figure 13 Install

You are done! The Uplink Manager is installed. Click “Finish” to close the window.

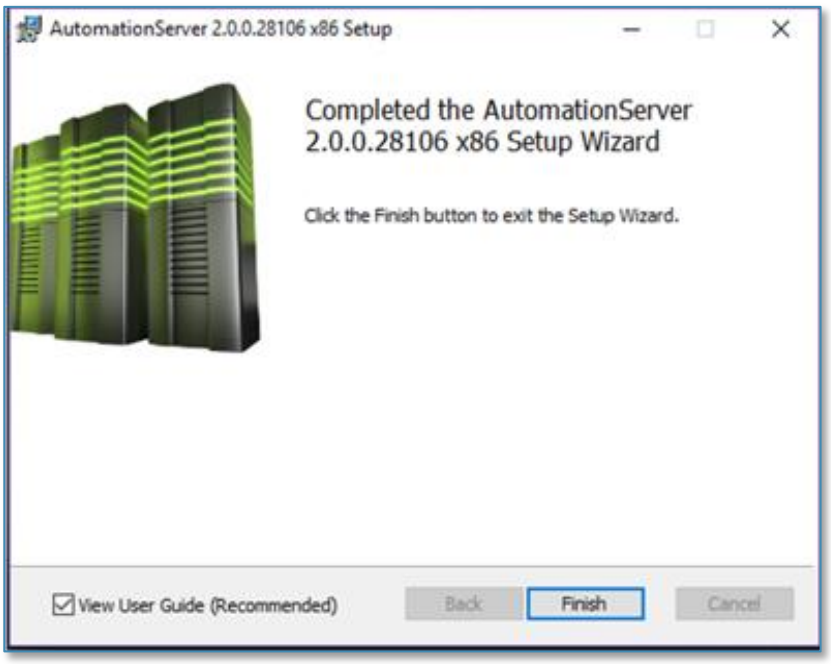

Figure 14 -Finish

By default, the Uplink Manager is installed to “C:\Program Files (x86)\Addovation\Automation Server\Uplink Service” folder. Run “Addovation.Uplink.Manager.exe” to configure Uplink Manager.

3.2 Cloud Manager

Copy the installation package “AutomationServer 1.1.6.23104 x86.msi” to the server, which is going to be used for the Cloud Manager and run it.

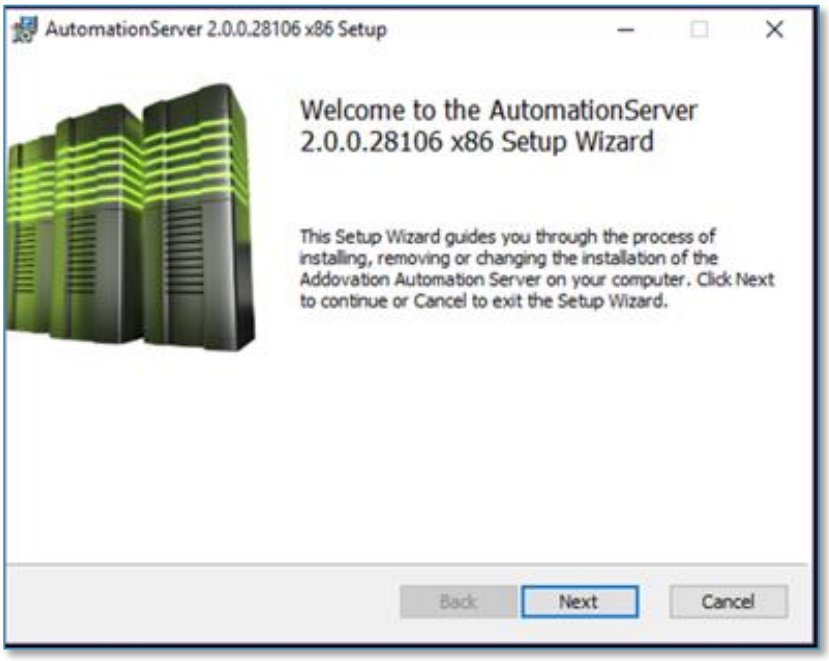

Figure 15 – Start setup

Click “Next” on the Welcome screen.

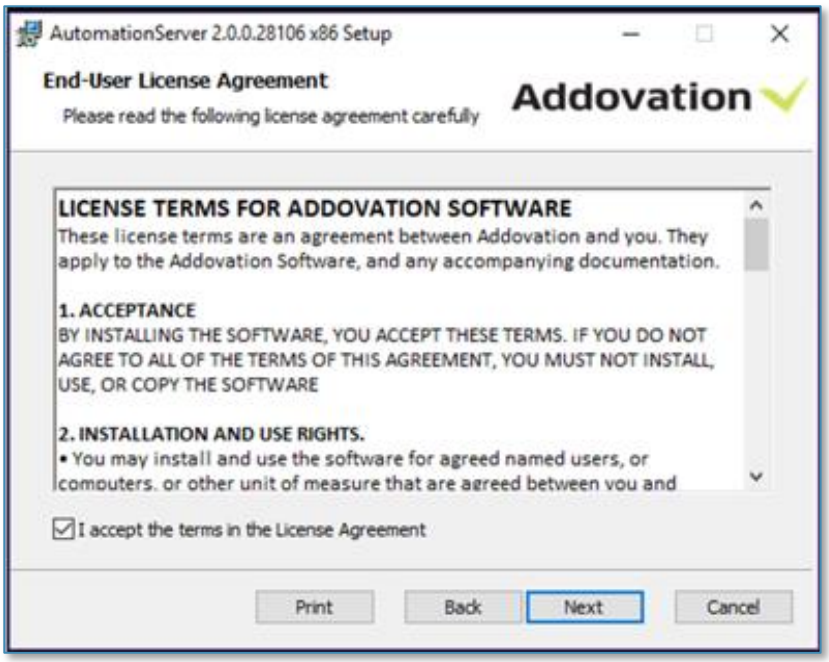

Figure 16 License agreement

Review the license agreement and accept it, click “Next”.

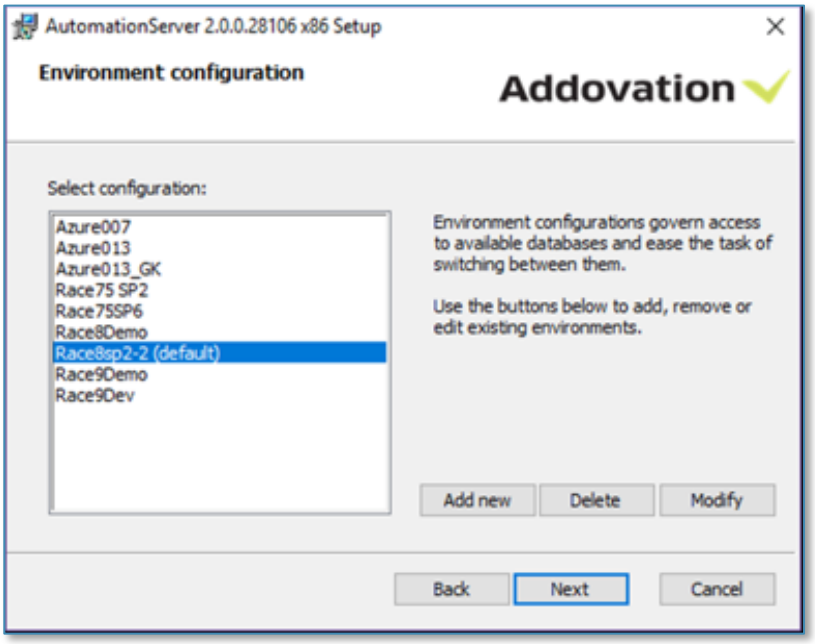

Figure 17 Environment confgiuration

Click “Next” on “Environment configuration” screen without entering any configuration settings.

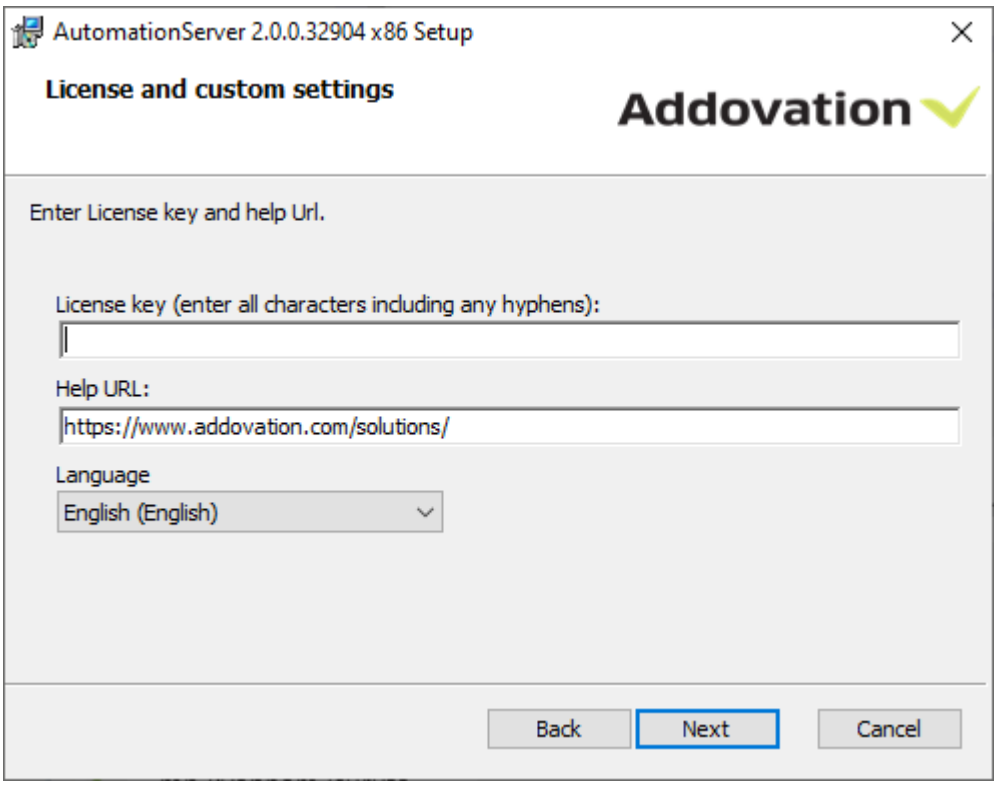

Figure 18 Licese and custom settings

The license key is not a mandatory field for Cloud Manager – you may skip it and click “Next”. If the license key field is empty, you may see a window with this warning:

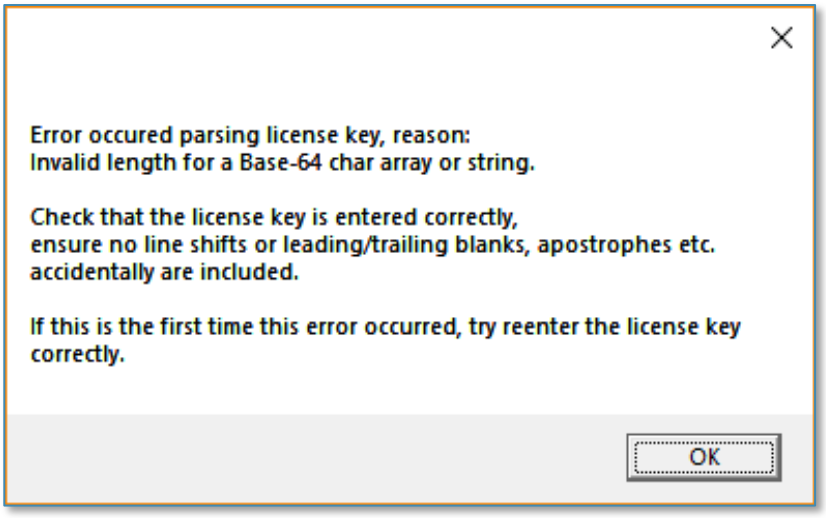

Figure 19 Warning

You can safely ignore this warning and click OK.

Click “Next” on the “License key validation” window.

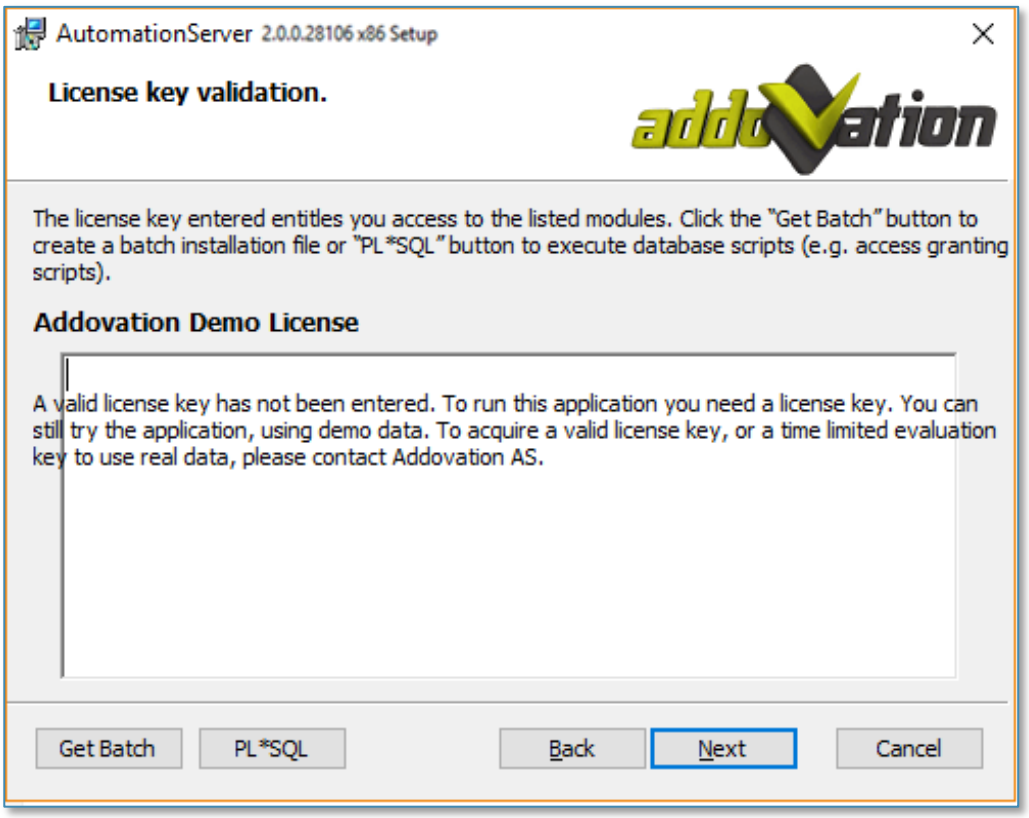

Figure 20 - License key validation

Choose “Custom” setup to install “Addovation Cloud” only and skip other applications.

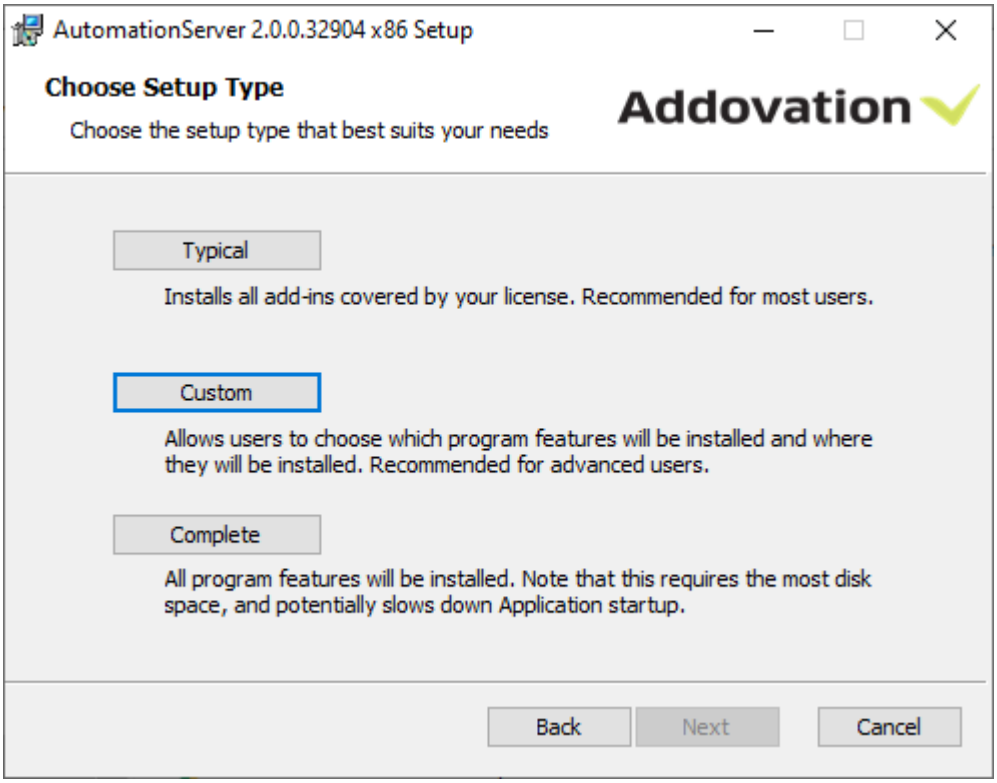

Figure 21 Setup Type

Disable all other components (if they are not used and installed on that server), except “Addovation Cloud”, and click “Next”.

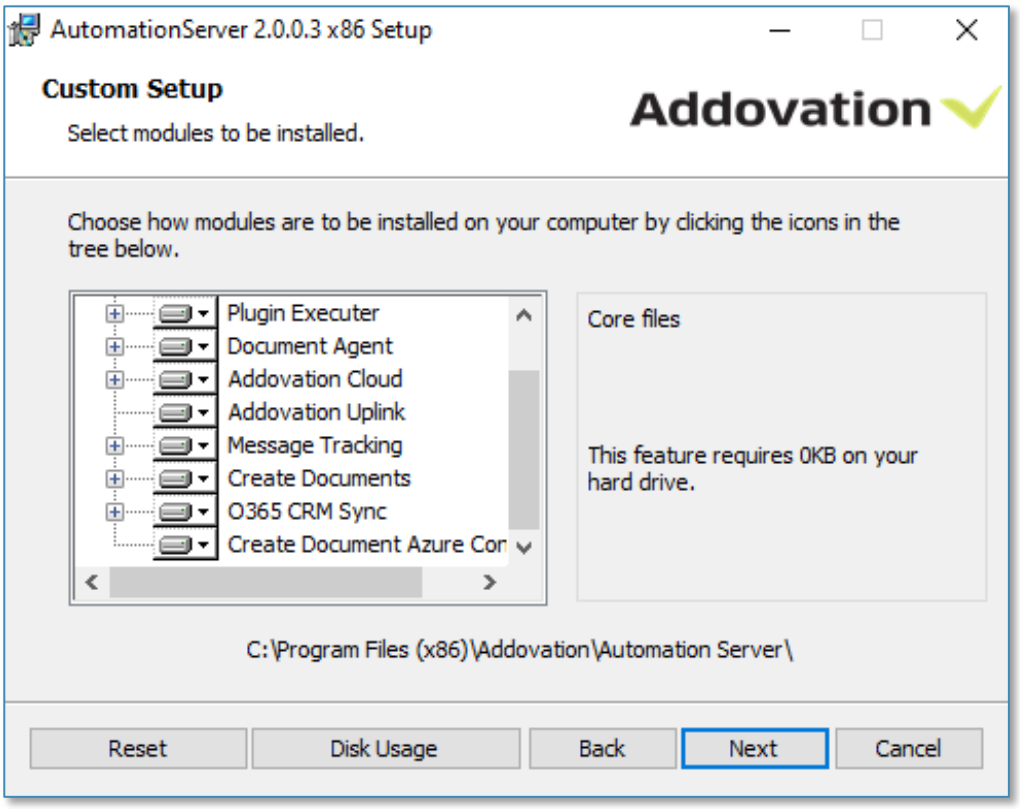

Figure 22 Custom Setup

Click “Install” to start the installation process.

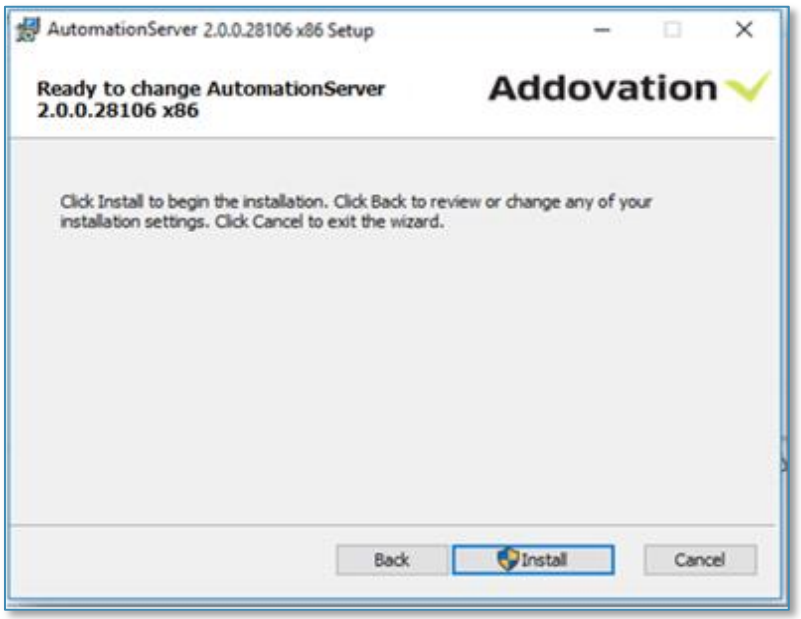

Figure 23 - Install

While installing the application, you may see this warning again:

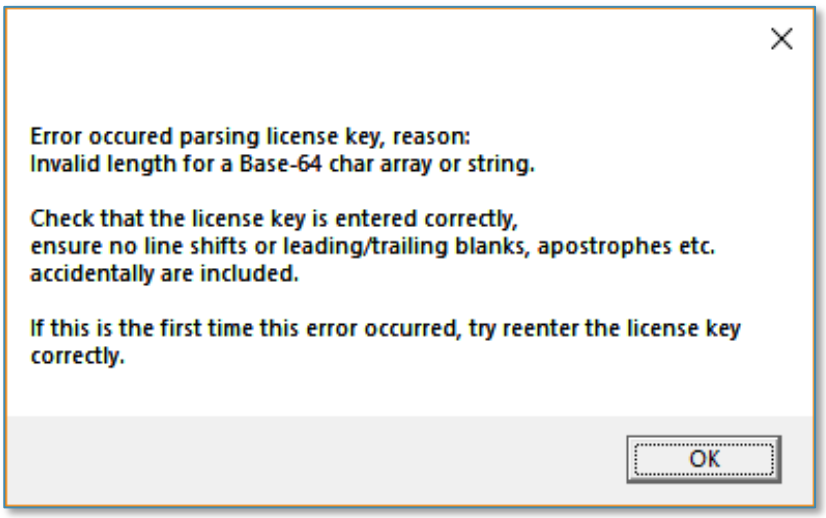

Figure 24 Warning

Don't pay attention to it, just skip it by clicking "OK".

You are done! The Cloud Manager is installed. Click "Finish" to close the window.

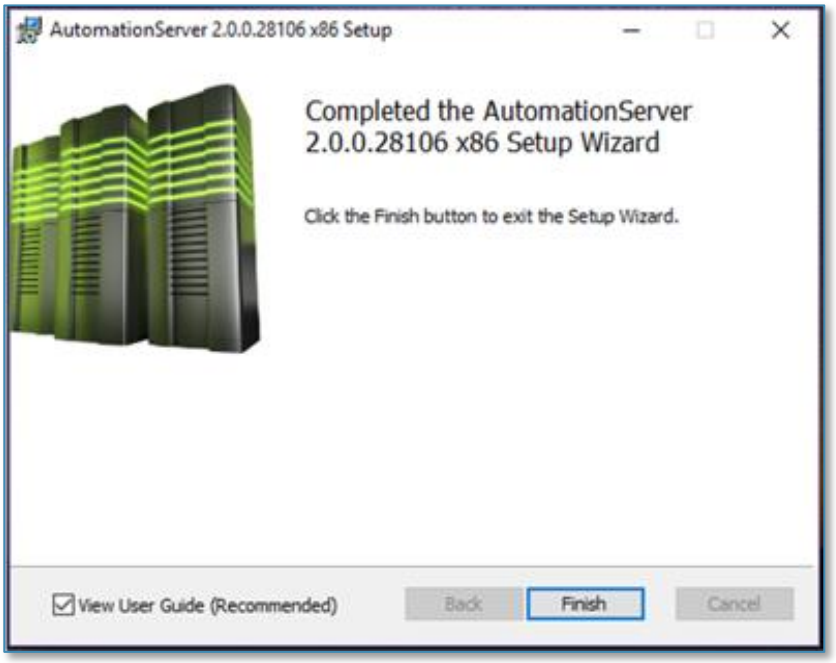

Figure 25 - Finish

By default, the Cloud Manager is installed to "C:\Program Files (x86)\Addovation\Automation Server\Cloud Service" folder. Run "Addovation.Cloud.Manager.exe" to configure Cloud Manager.

3.3 AddoResources library

The AddoResources library together with the referenced libraries should be registered in the Cloud Manager application. Choose “File / Manage Resources” in the menu as shown below.

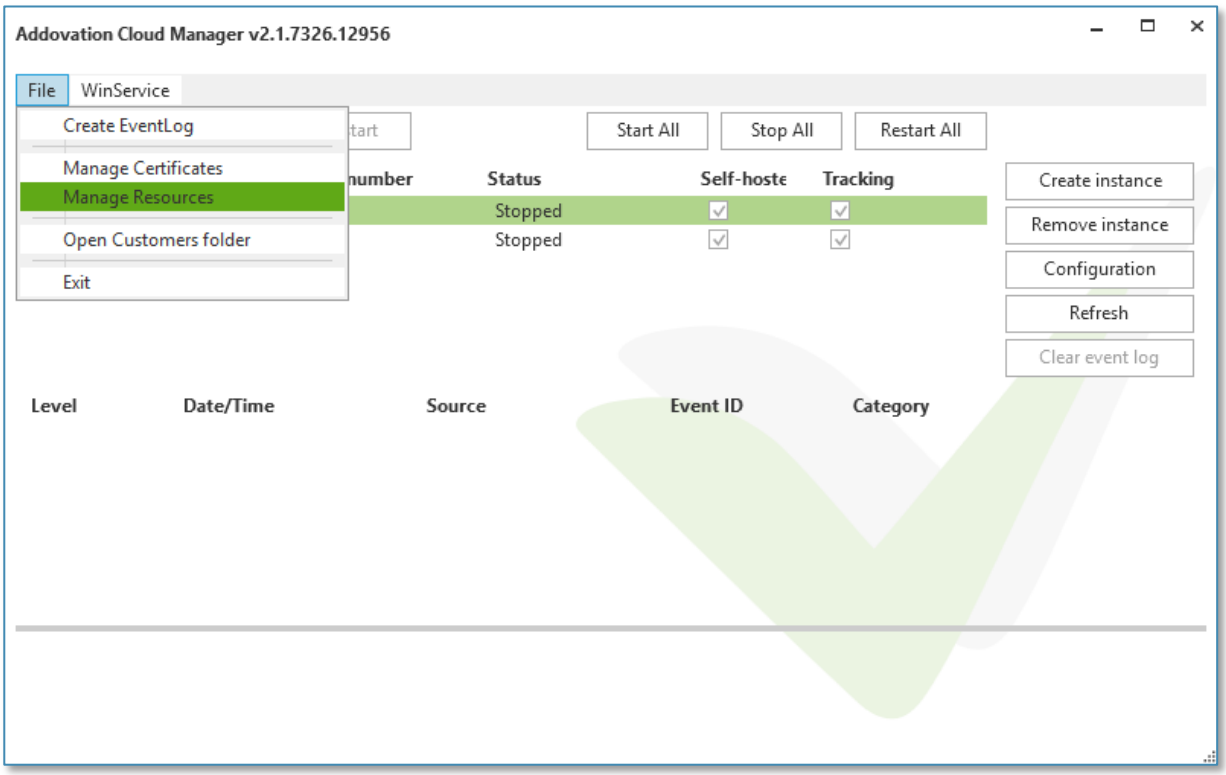

Figure 26 – Cloud Manager resources

Right click on the left-hand panel and choose “Add Customer” in popup menu to register a new Customer in the system.

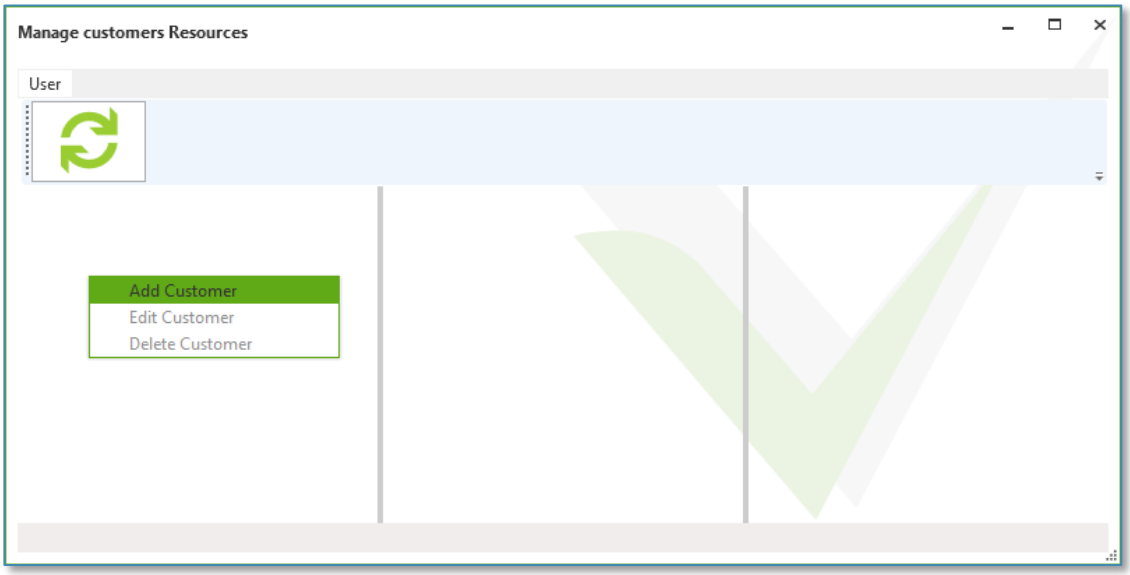

Figure 27 – Customer resources

Enter customer's name and click "OK".

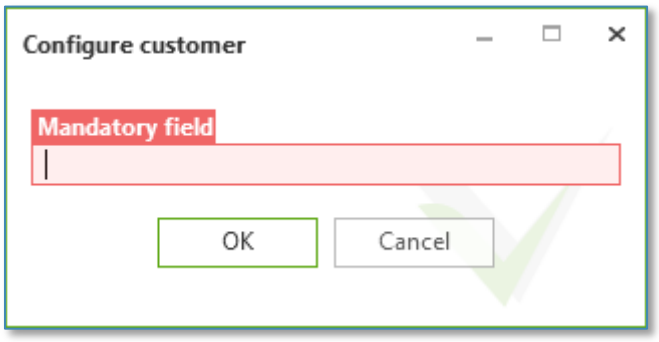

Figure 28 – Configure customer

Right click in the middle panel and choose "Add System ID" to register a new System ID for the chosen Customer.

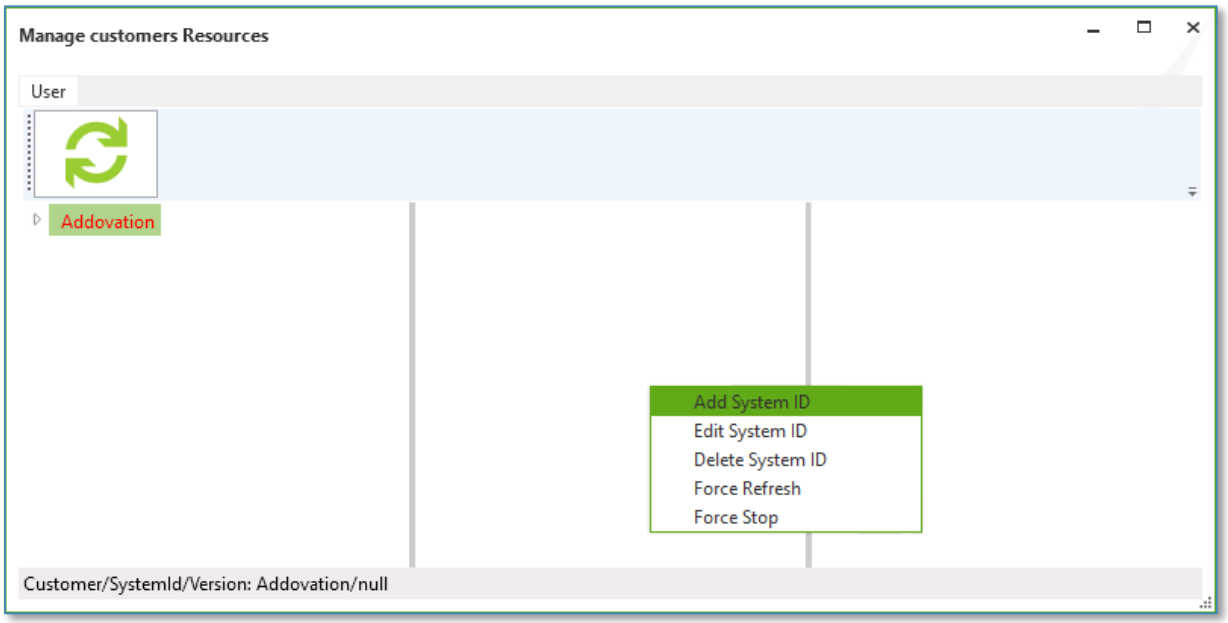

Figure 29 – System IDs

Enter the preferred System ID and click “OK”. The certificate field may be configured later to assign System ID with the corresponding SSL certificate.

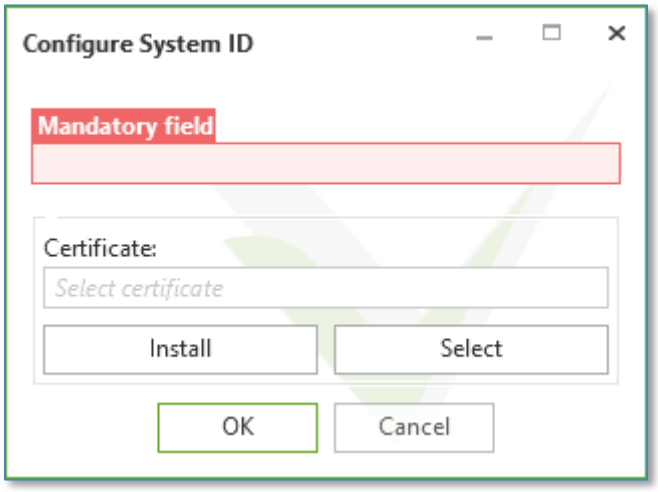

Figure 30 – Configure system ID

Right click in the right-hand panel and choose “Add Resource” to register the AddoResources libraries for the chosen System ID.

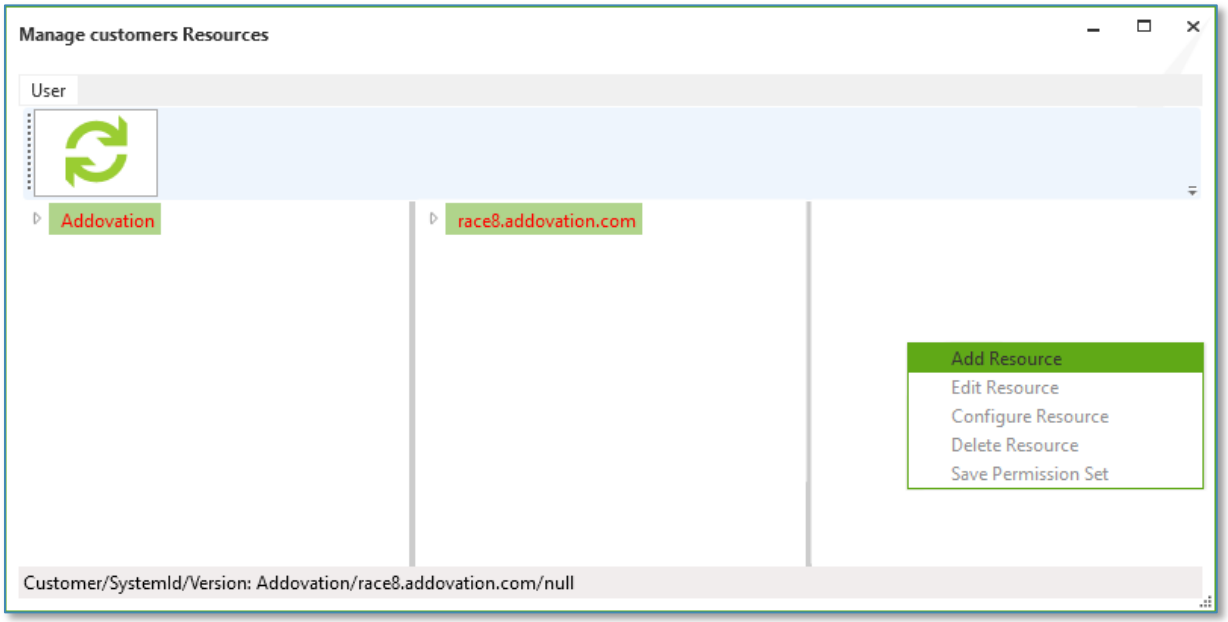

Figure 31 – Manage customer resources

Enter the version number of AddoResources library (this version number is provided by Addovation). Click “Add file” and choose all the files related to the AddoResources library. Click “OK” to finish installing new AddoResources library.

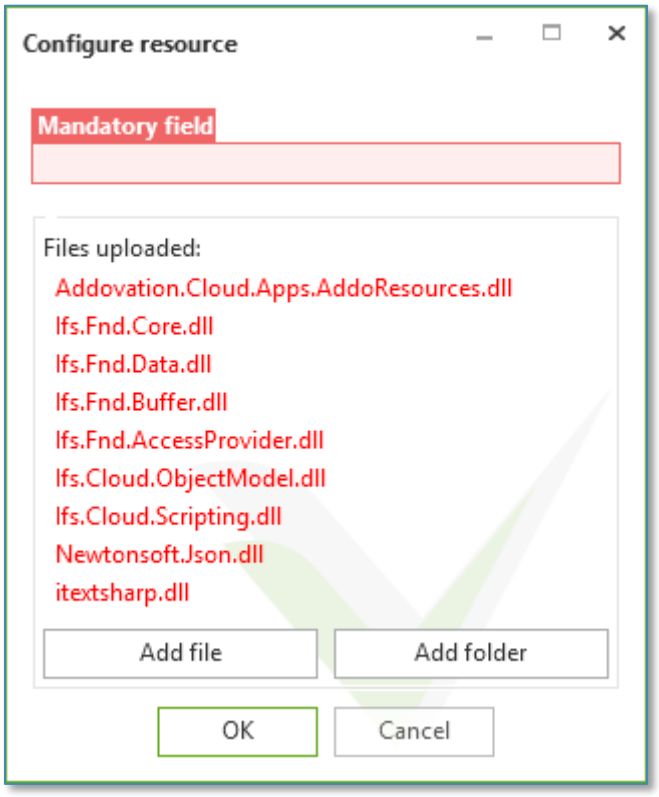

Figure 32 – Configure resources

4 Configuration

This is a two-part configuration: for Uplink Manager and for Cloud Manager.

4.1 Uplink Manager configuration

Open Uplink Manager application. Click on “Create instance” button to add new uplink service.

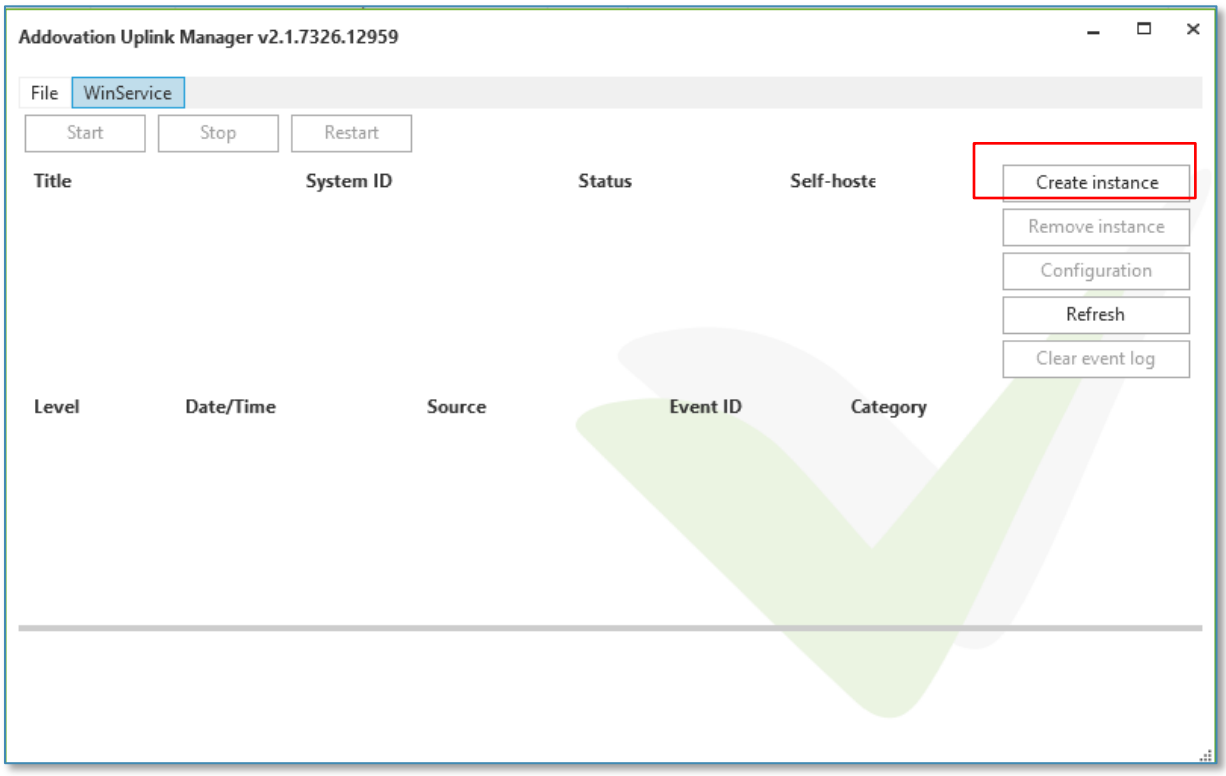

Figure 33 – Uplink manager

Enter the Instance name, System ID, IFS database URL and choose IFS database version for the new uplink service.

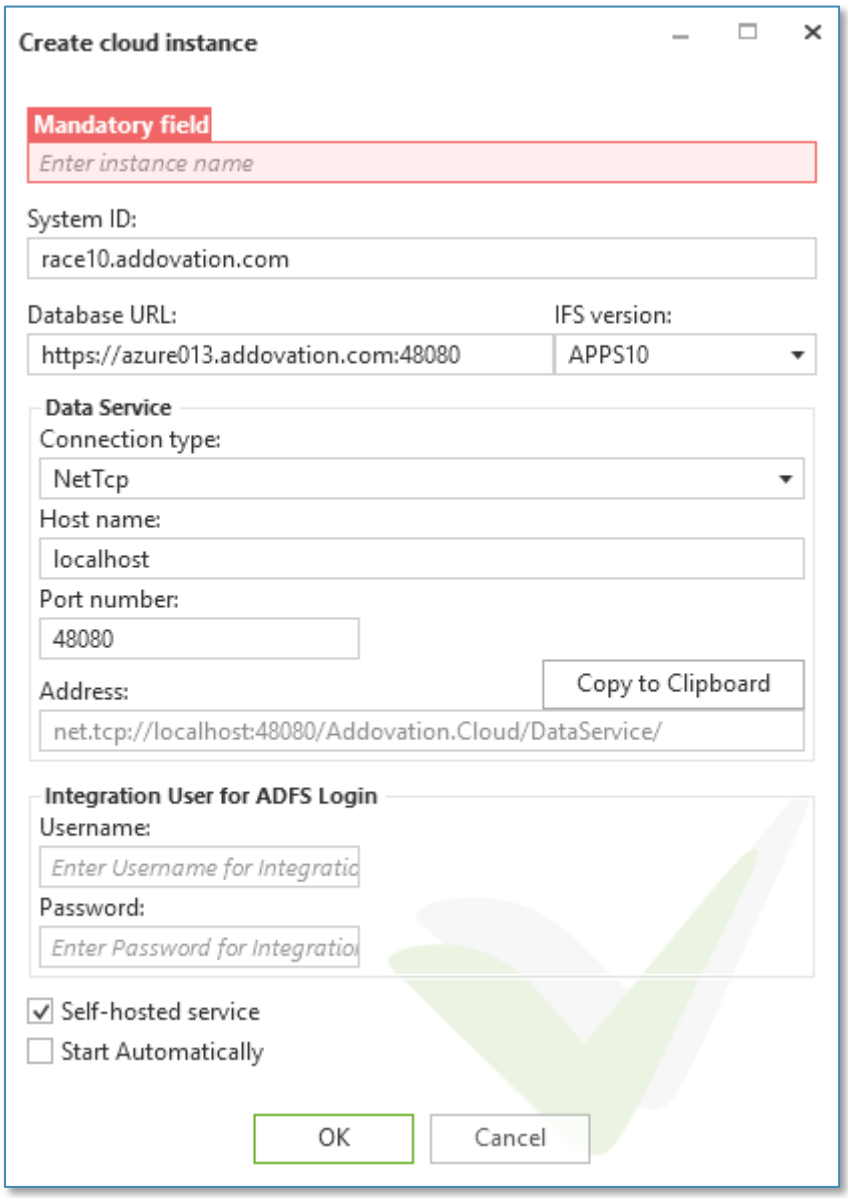

Figure 34 – Create cloud

Configure the connection settings in Data Service section: Connection type, Host name, Port number, Address, or leave it as it is. Click “OK” to create the uplink instance.

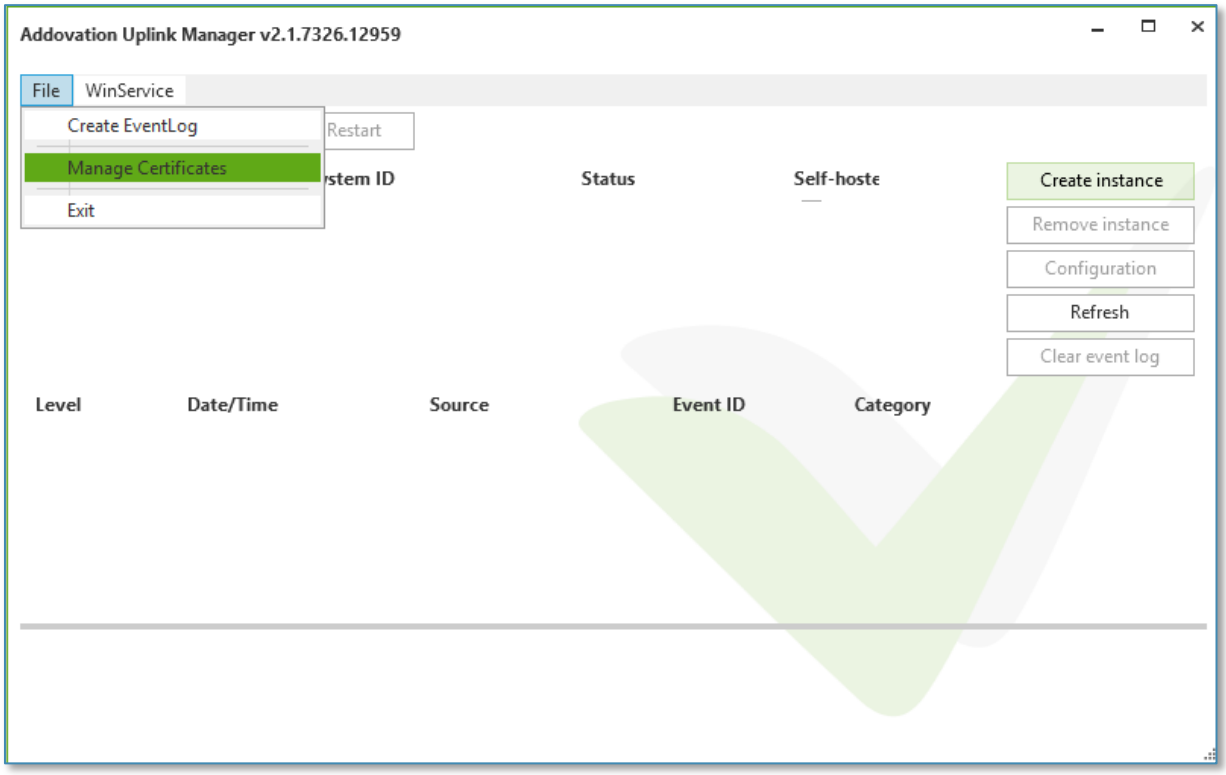

Figure 35 – Manage Certificates

The communication between Uplink and Cloud is encrypted by SSL certificate. Select “File / Manage Certificates” in main menu of the application to create a new SSL certificate for further communication.

Click “Generate new” button to add a new certificate for a particular System ID.

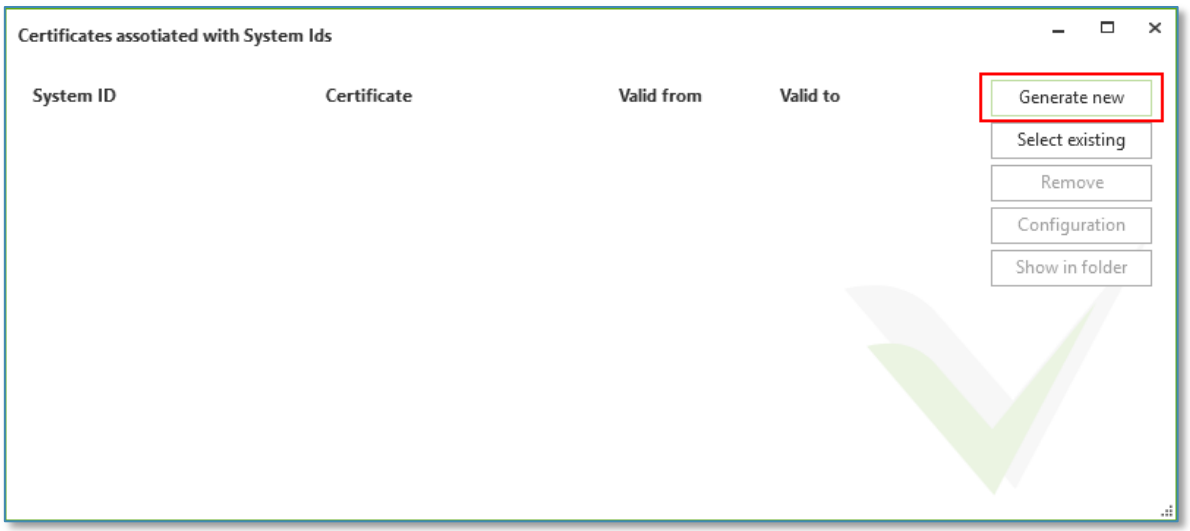

Figure 36 – Generate New

Enter the same System ID and any Certificate subject to identify it, click “OK”. After the certificate is generated and assigned to the System ID, it will appear in the list of the certificates used by the application.

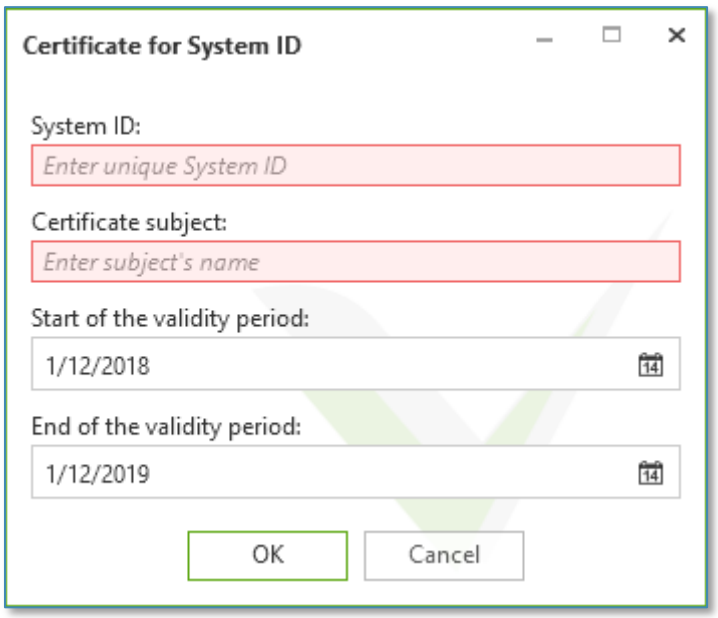

Figure 37 – Create Certificate

This certificate must be copied and registered on the server, which is used for hosting Cloud Manager. Click “Show in folder” button to go to the certificate file and copy this file to the Cloud Manager server.

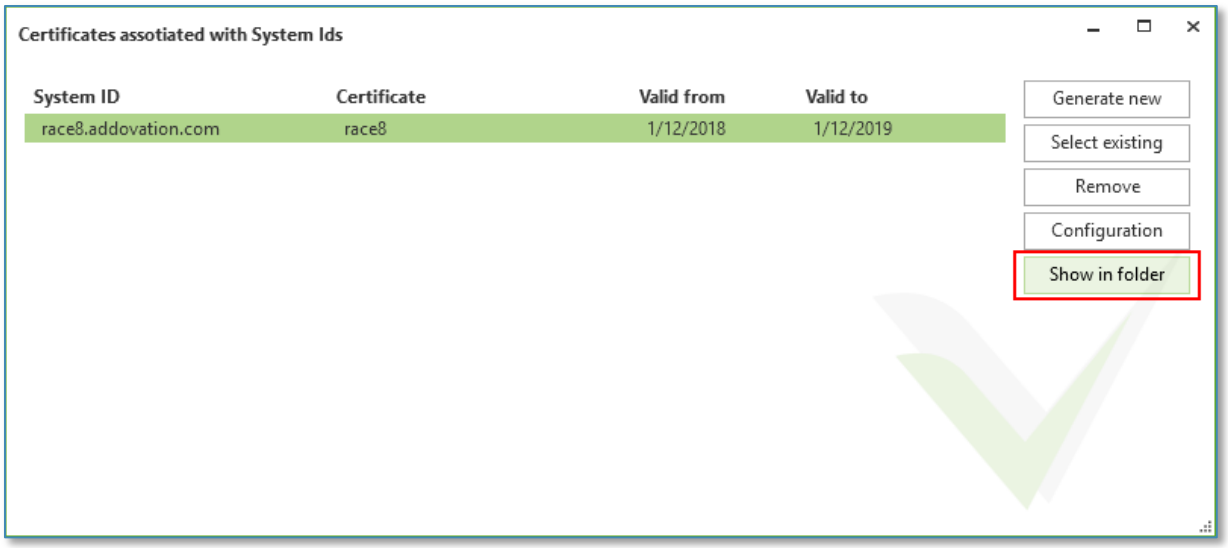

Figure 38 - Certificates

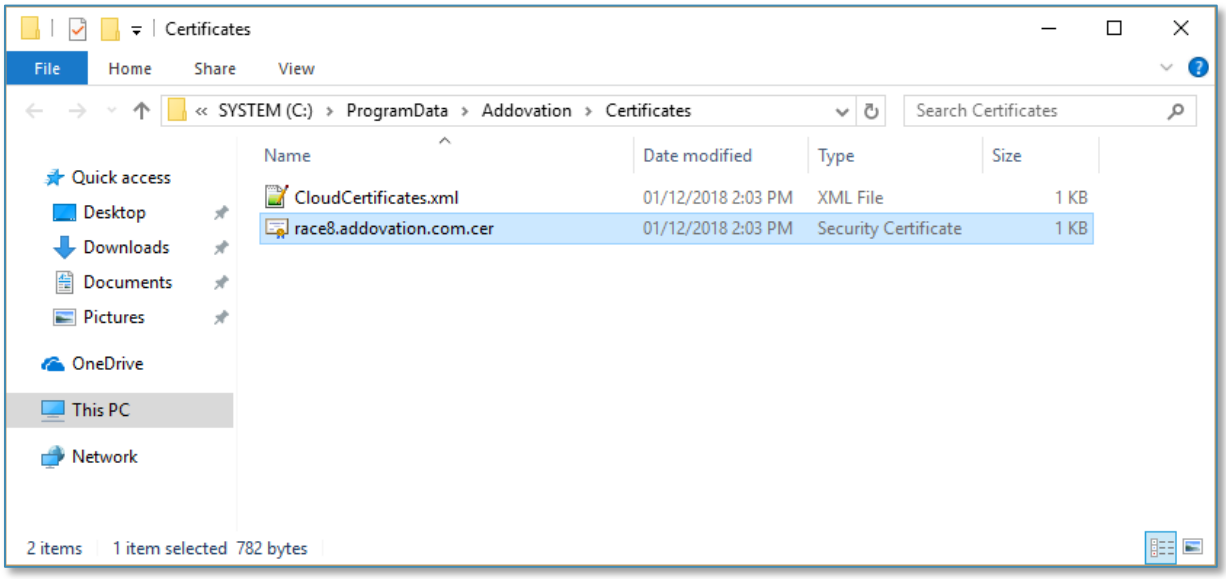

Figure 39 – Created certificates

4.2 Cloud Manager configuration

Open Cloud Manager application. Click on “Create instance” button to add a new cloud service.

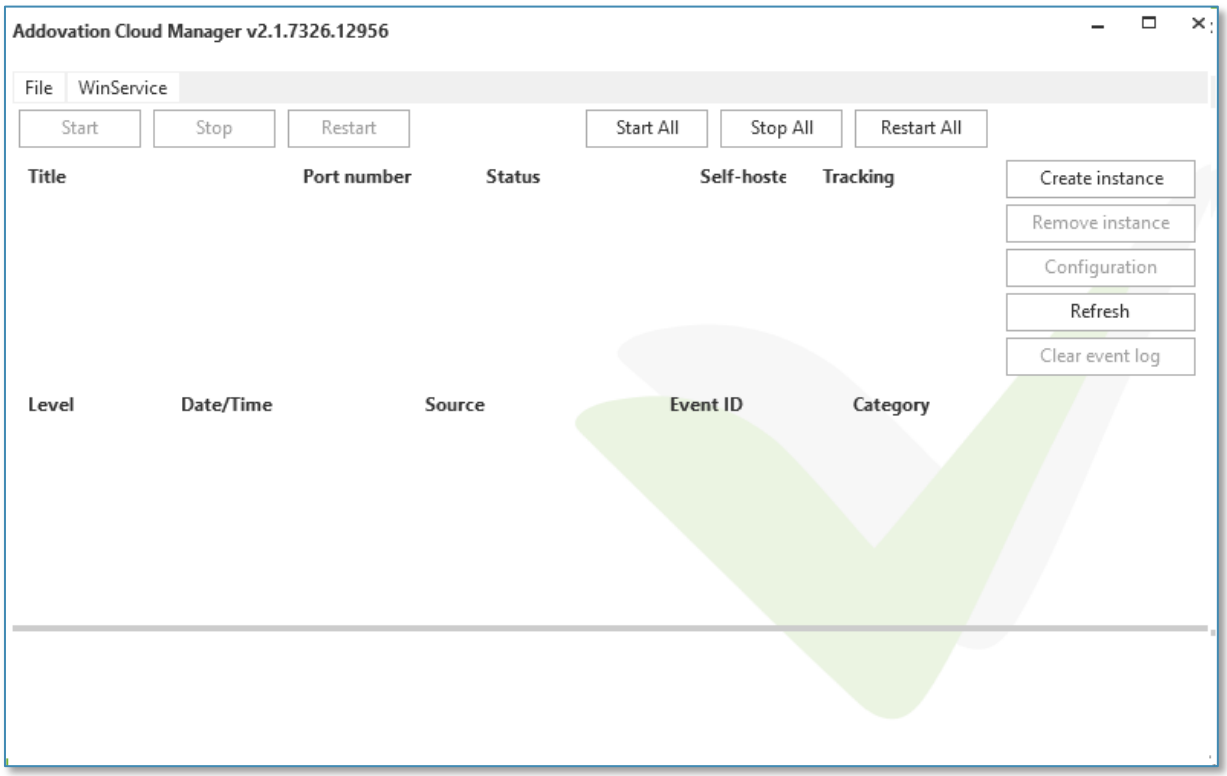

Figure 40 Cloud configuration

Enter the Instance name of new cloud service and Host name (DNS or IP) of the server.

Click “Generate Self-Signed Certificate” or enter SSL Certificate Thumbprint to identify the SSL certificate which will be used to secure client requests to the cloud. Click “OK” to create the cloud instance.

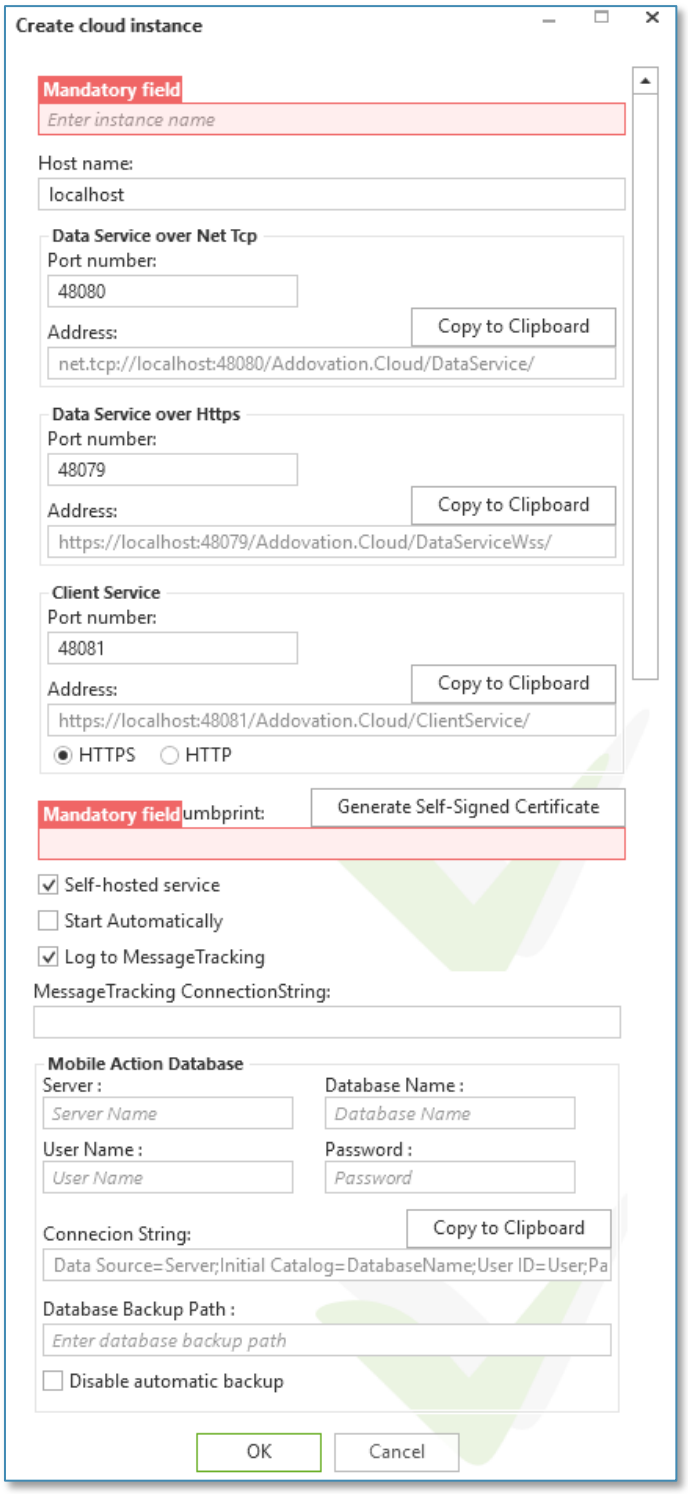

Figure 41 – Create cloud instance

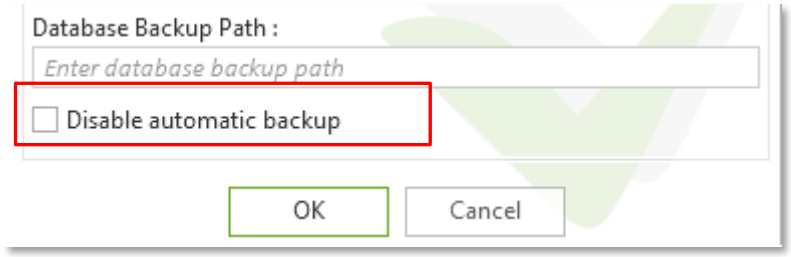

Figure 42 - Disable automatic backup

To avoid unnecessary complications, *'Disable Automatic Backup'* option is provided users to skip the backup when user doesn't want backups to be executed automatically on Mobile Action database update.

If the option is unchecked , backup will be executed to the place where the user has defined or targeting the default folder (C:\Addovation\Backups).

The communication between Uplink and Cloud is encrypted by SSL certificate. Select "File / Manage Certificates" in main menu of the application to register the existing SSL certificate which was copied from Uplink server.

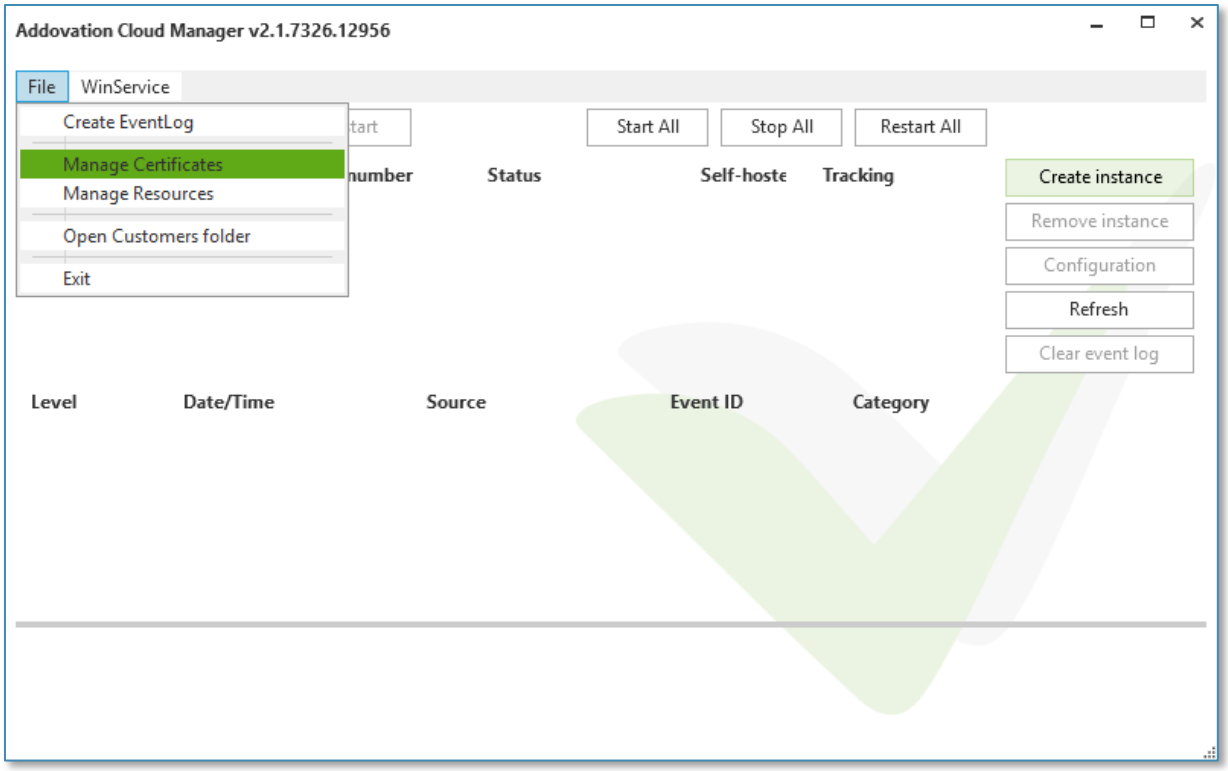

Figure 43 – Manage certificates

Click “Select existing” button.

Figure 44 – Select existing

Find, choose, and select the copied SSL certificate (it is copied from Uplink server).

Now you can manage each version of AddoResources for each System ID of the particular Customer. Select “File / Manage Resources” in main menu of the application.

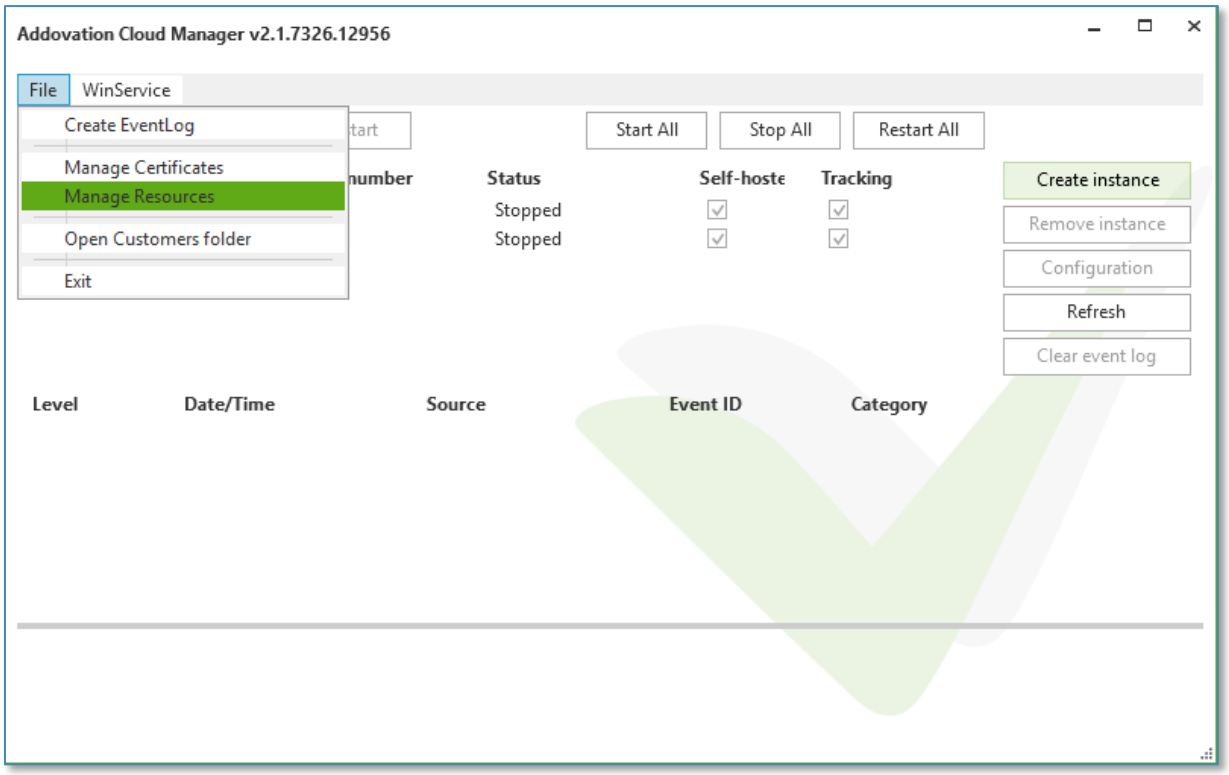

Figure 45 - Manage Resources

Choose the Customer and select the item with the particular System ID. Do right mouse button click on it and choose “Edit System ID”.

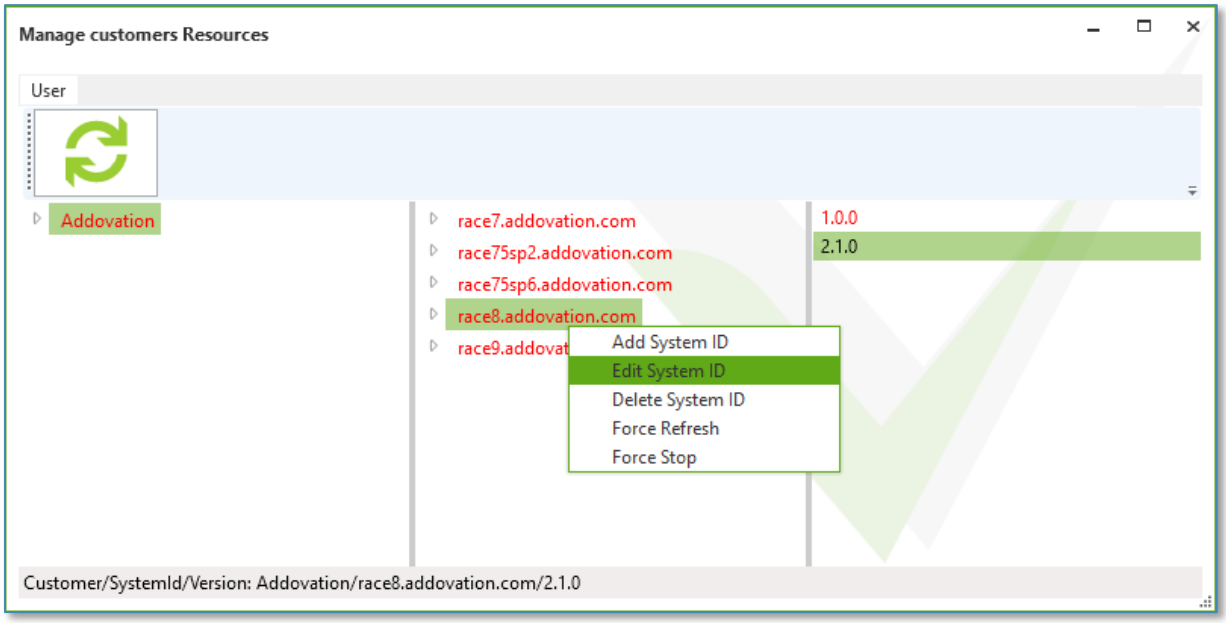

Figure 46 – Edit System ID

In the opened “Configure System ID” window the SLL certificate must be assigned to that System ID.

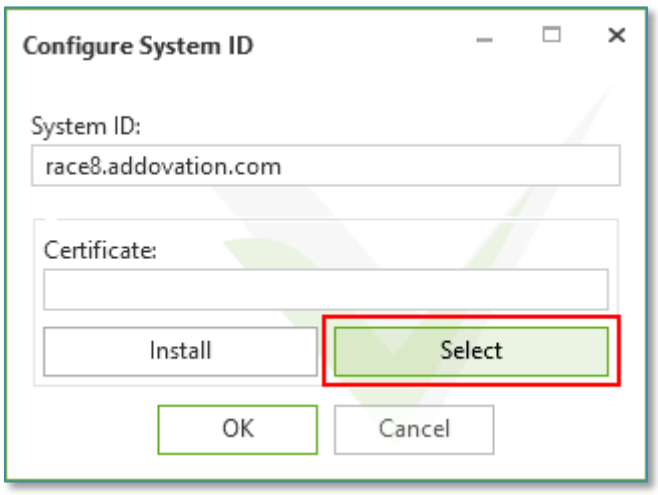

Figure 47 – Configure system ID

Click “Select” button and choose the item with the corresponding certificate, which was registered in the Cloud Manager before (in the Manage Certificates section).

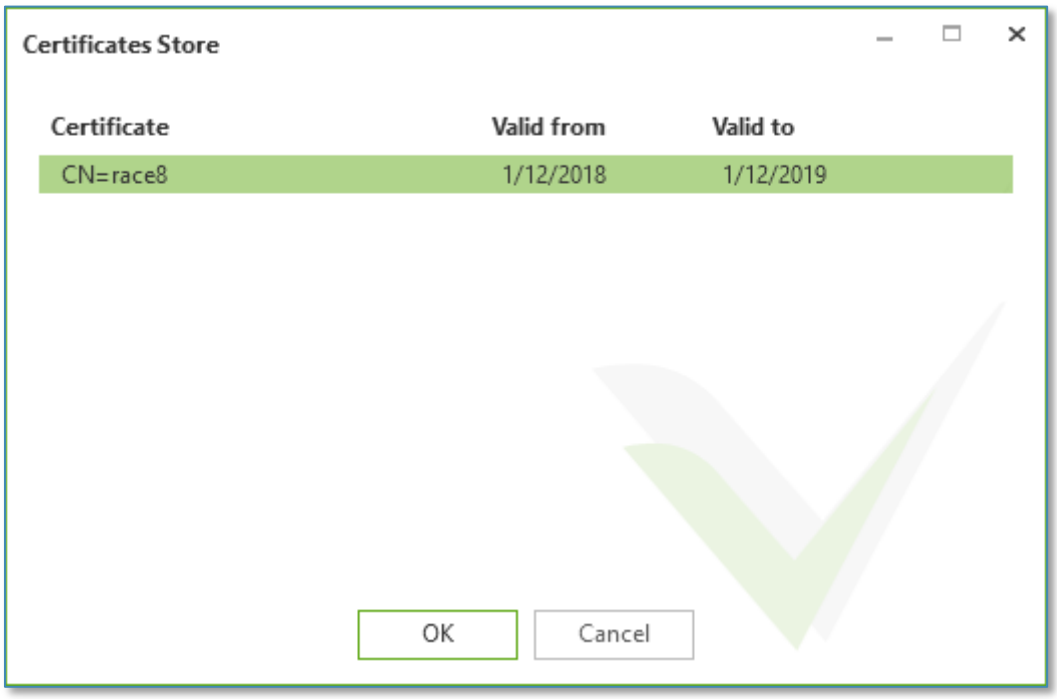

Figure 48 – Certificate store

Click “OK”. The chosen certificate is assigned to the selected System ID.

Select the item with the particular AddoResources version number. Do right mouse button click on it and choose “Configure Resource”.

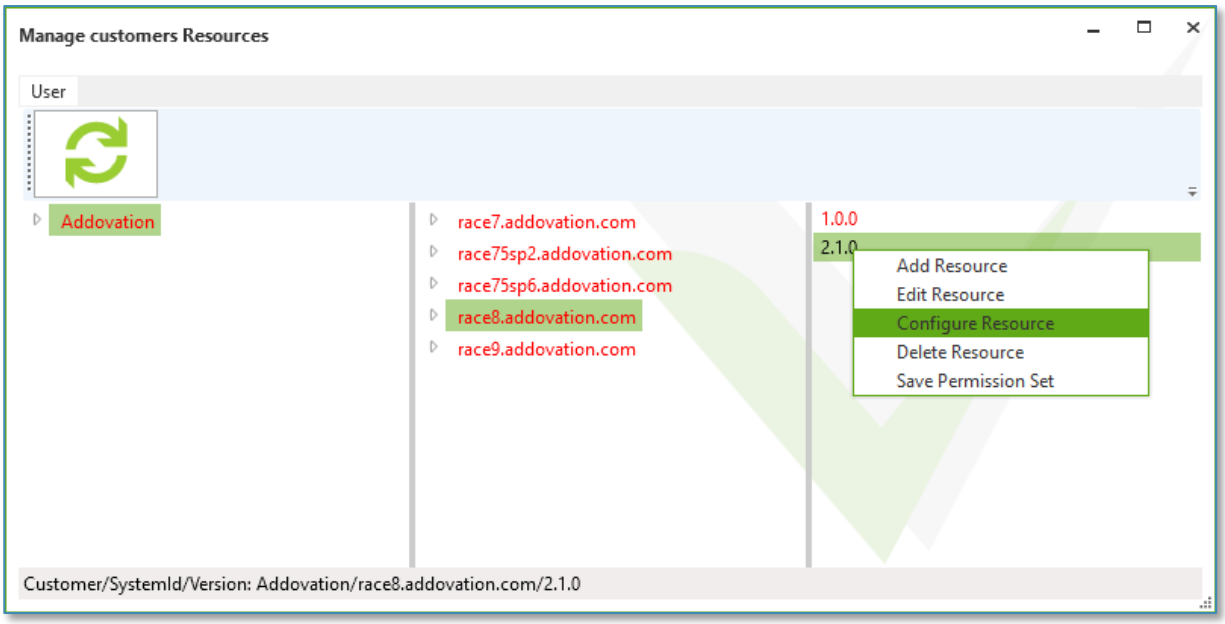

Figure 49 – Customer resources

The opened window allows to customize configuration for each version of AddoResources used for the selected System ID. The configurations are grouped into several sections for each Addovation mobile product.

Enter or change the settings. Enter any connection strings if required and click “Save Configuration”.

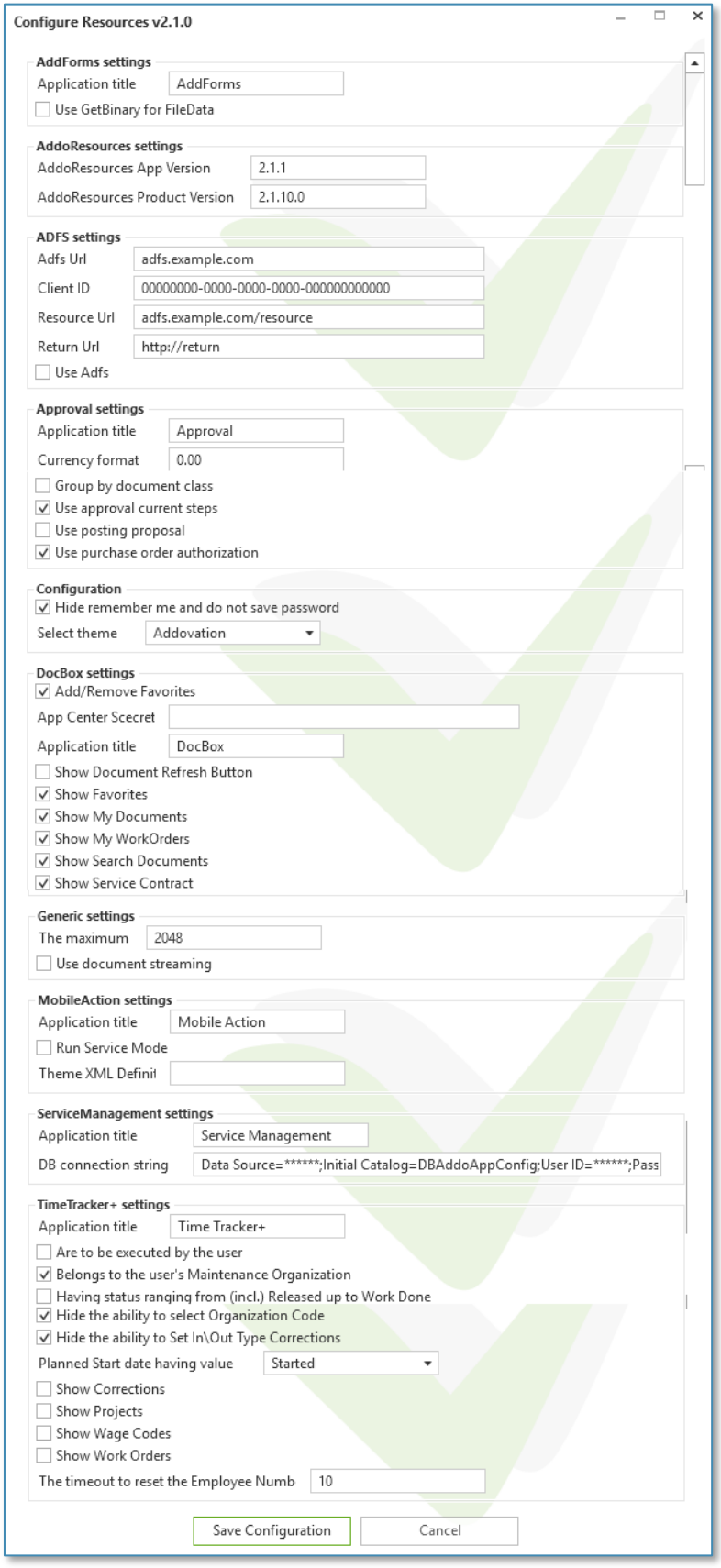

Figure 50 – Configure resources

The Cloud Manager will ask if the cloud service should be restarted to apply the chosen configuration.

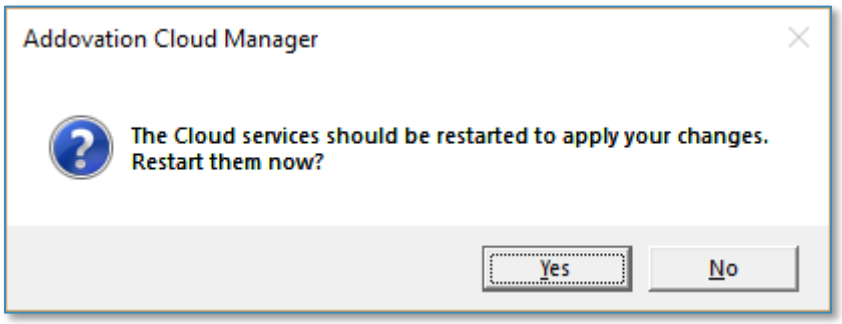

Figure 51 – Restart cloud manger

Click "Yes", if the Cloud service is already started or if you are not planning to restart it manually.

4.3 Start Services

It's possible to run the Cloud Service and the Uplink Service by two ways:

- via Self-hosted application
- via Windows Service

4.3.1 via Self-hosted service

Self-hosted application is a console application, which works in the interactive mode and shows the current user all trace info about the service: when it's started, when it fails, exception and warning messages, connected endpoints, etc.

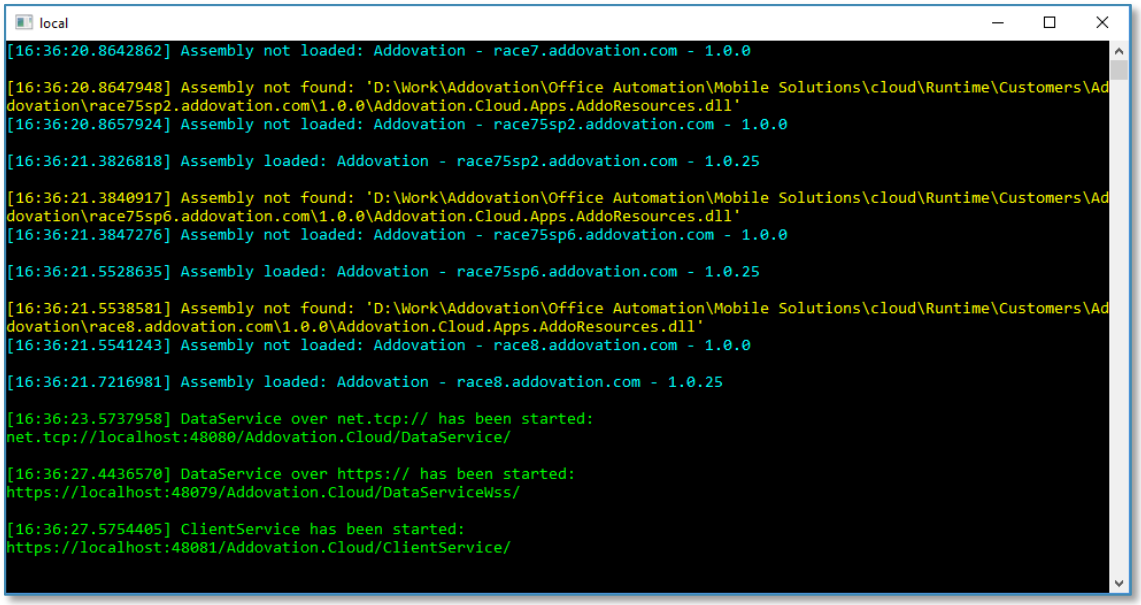

Figure 52 – Service status

To make the service instance start via Self-hosted application, you should go the service instance configuration window (in Cloud Manager or in Uplink Manager) and check the “Self-hosted service” box. Select the service instance item in the list and click “Start” button.

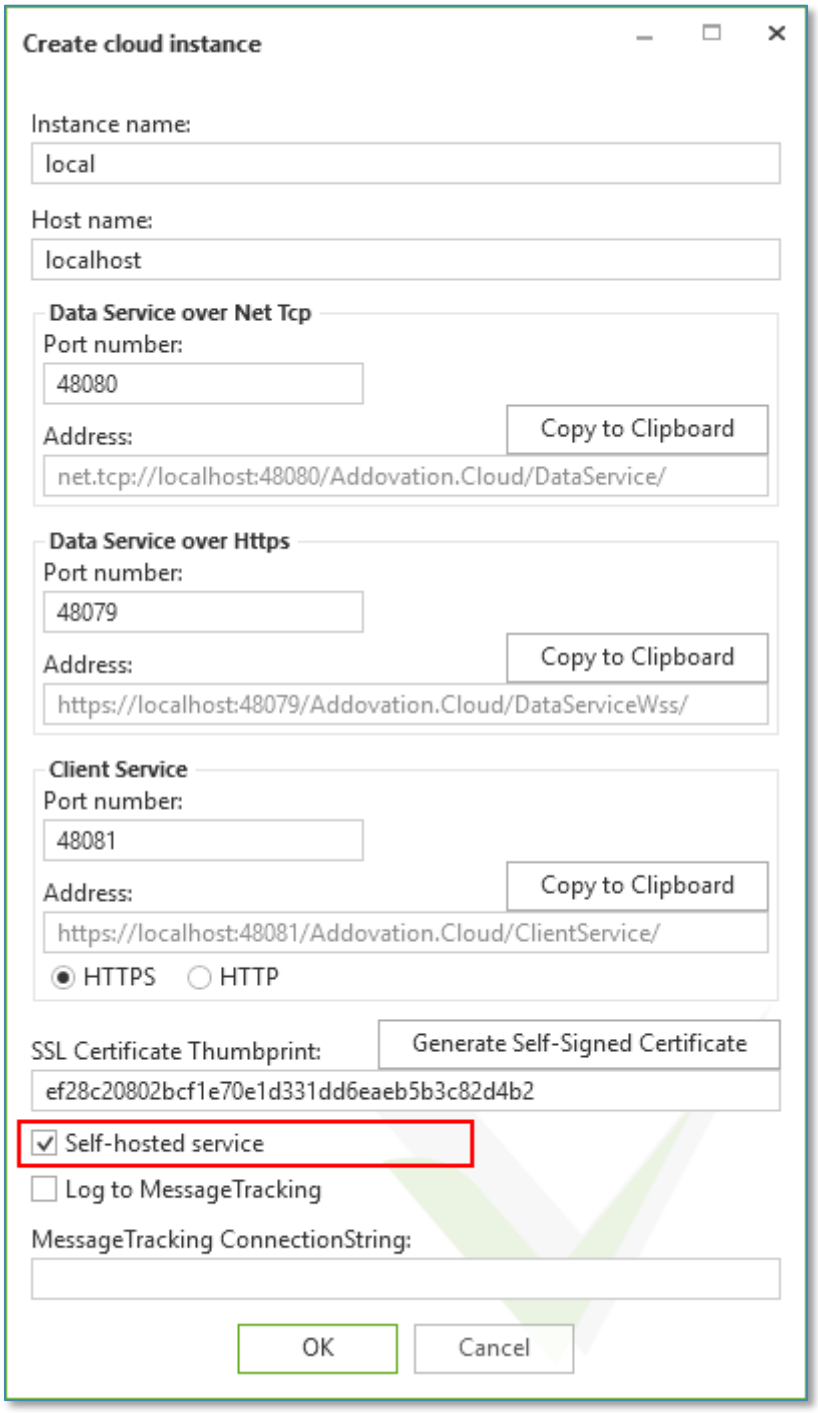

Figure 53 – Self hosted service

4.3.2 via Windows Service

Hosting the service as Windows Service, the user will not be able to see any trace info in the interactive mode. However, the services will start automatically after rebooting the server machine.

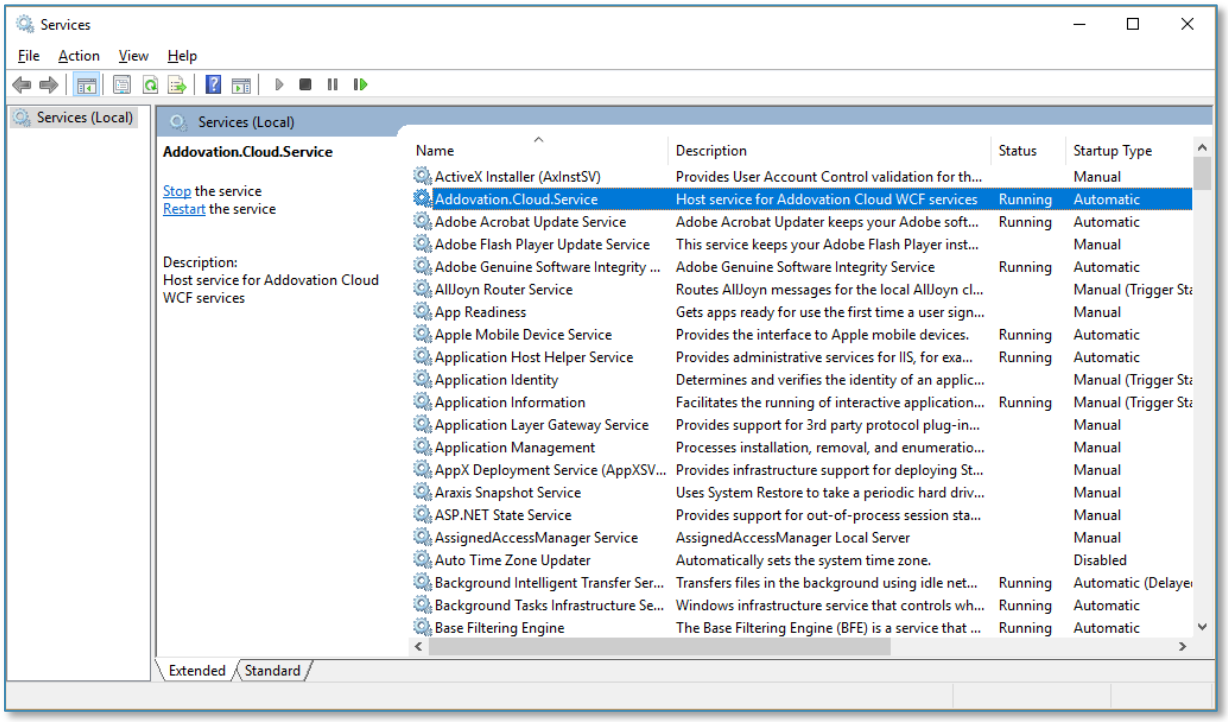

Figure 54 - Services

To make the service instance start via Windows Service, you should go the service instance configuration window (in Cloud Manager or in Uplink Manager) and uncheck the “Self-hosted service” box.

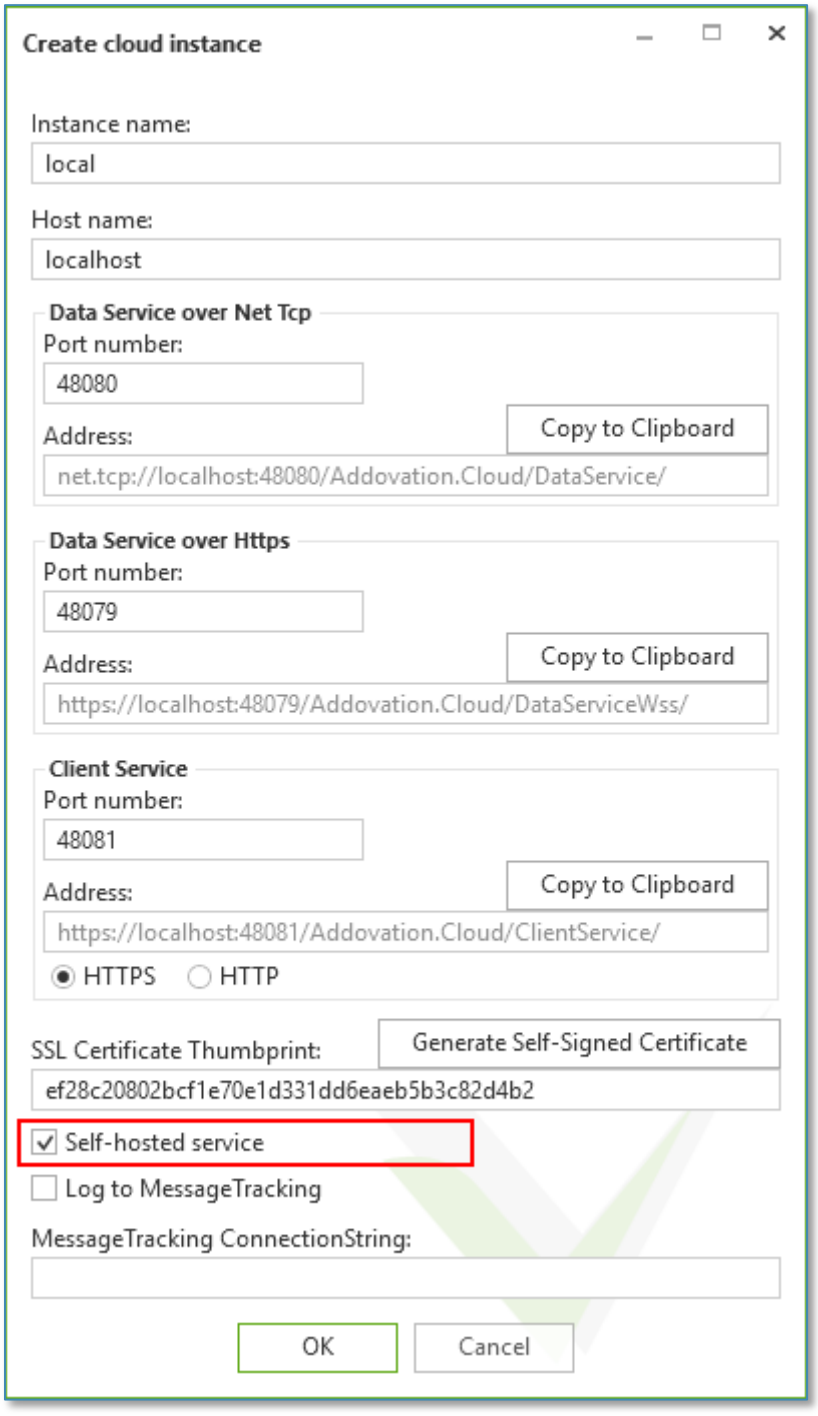

Figure 55 – Uncheck self hosted service

Choose “WinService / Install” in main menu of the application and then click “WinService / Start” to run all service instances via single Windows Service control.

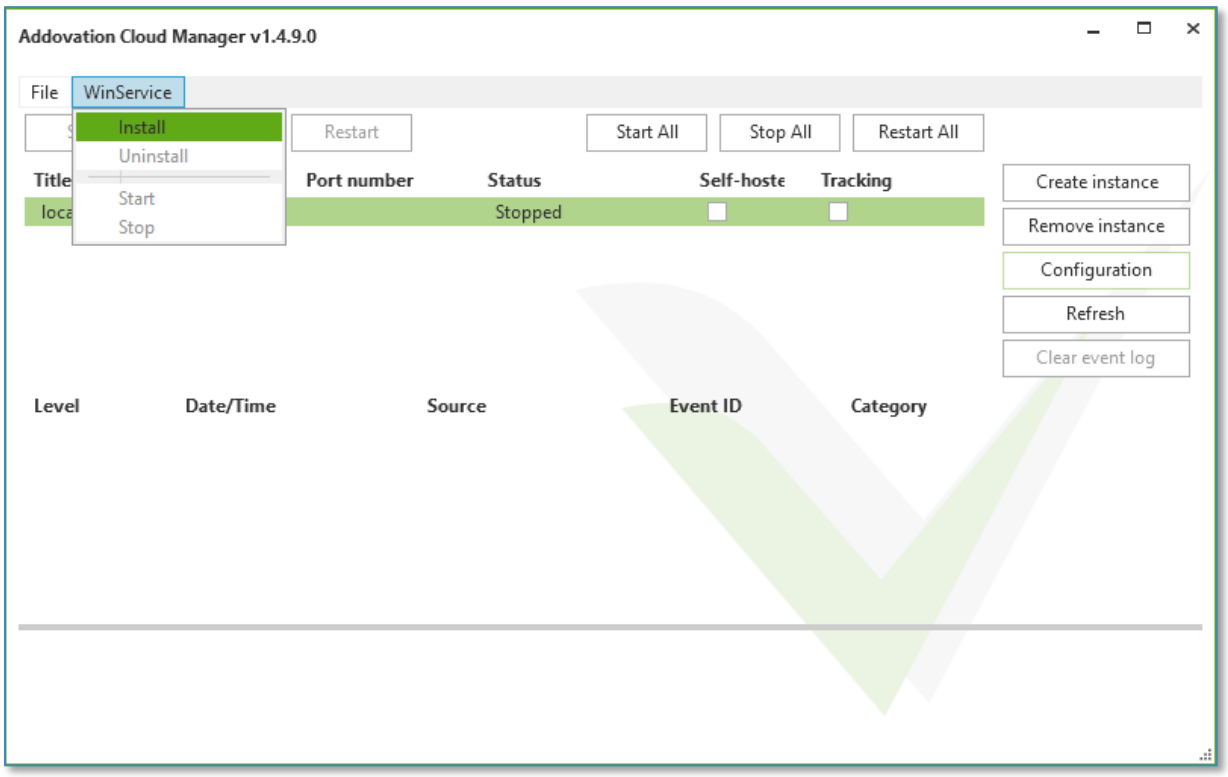

Figure 56 - Install

5 ADFS

With ADFS login integrated into Service Management and Mobile Action you can now login via ADFS or Azure AD instead of an IFS user. Because ADFS tokens are not supported in IFS this works by creating an integration user and running impersonation on top of it. It also supports Multi-Factor Authentication.

The user will first login via the app and after entering the cloud and system id the user will be taken to a secure Microsoft webpage where the user will enter username and password. The webpage requires an SSL certificate to make the connection secure which means that the user either need a local certificate installed on the device or the company can use a global certificate. The ADFS server will check the credentials towards Active Directory and the ADFS server then sends a token to the user if the credentials are correct. This token also allows users to login to the app later without having to login again (depends on configuration in ADFS server). The token contains several claims but the one we are interested in is the UPN value which looks like user@company.com. We use it to login to IFS so make sure it matches the Directory ID.

5.1 ADFS values

The values which are needed to configure ADFS for the mobile application:

Adfs Url: the Url that will connect to the ADFS server or Azure. The value will normally be the name of the server plus an endpoint that points to the authorization method. So it might be https://your-adfsserver-here/adfs/ouath2. Keep in mind that there are more variations.

Client ID: This is the identifier that allows ADFS to identify the app that is being used. It is a GUID that is created in the ADFS server via PowerShell or Azure.

Resource Url: This is an endpoint that controls how the user can login and what values will be passed to the ADFS token. This can be a relaying party trust, a generic resource if you are on Azure or any other value that can handle how a user can login.

Return Url: This is a value that is created in ADFS or Azure that can be anything as long as it is in http format. It is just a value to tell ADFS or Azure that the connection is secure.

6 IFS configuration

First, we create an integration user in IFS.

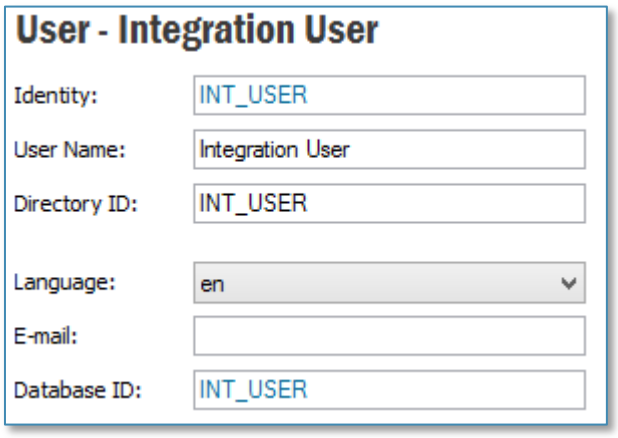

Figure 57 – Integration user

We then create a user in IFS that we will login with a directory id that matches the username in AD or Azure.

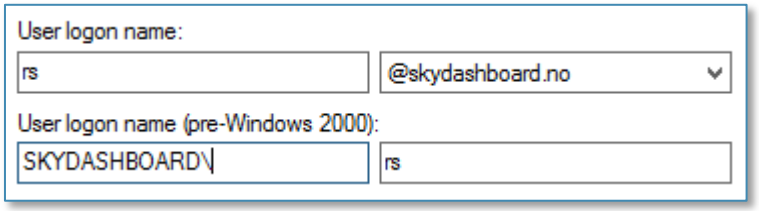

Figure 58 – Logon Details

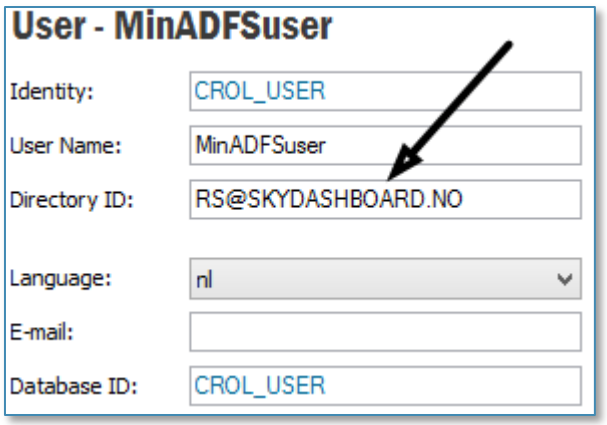

Figure 59 – ADFS user

6.1 Cloud configuration

Go to “File / Manage Resources” in main menu and do “Configure Resource” for the particular version of AddoResources.

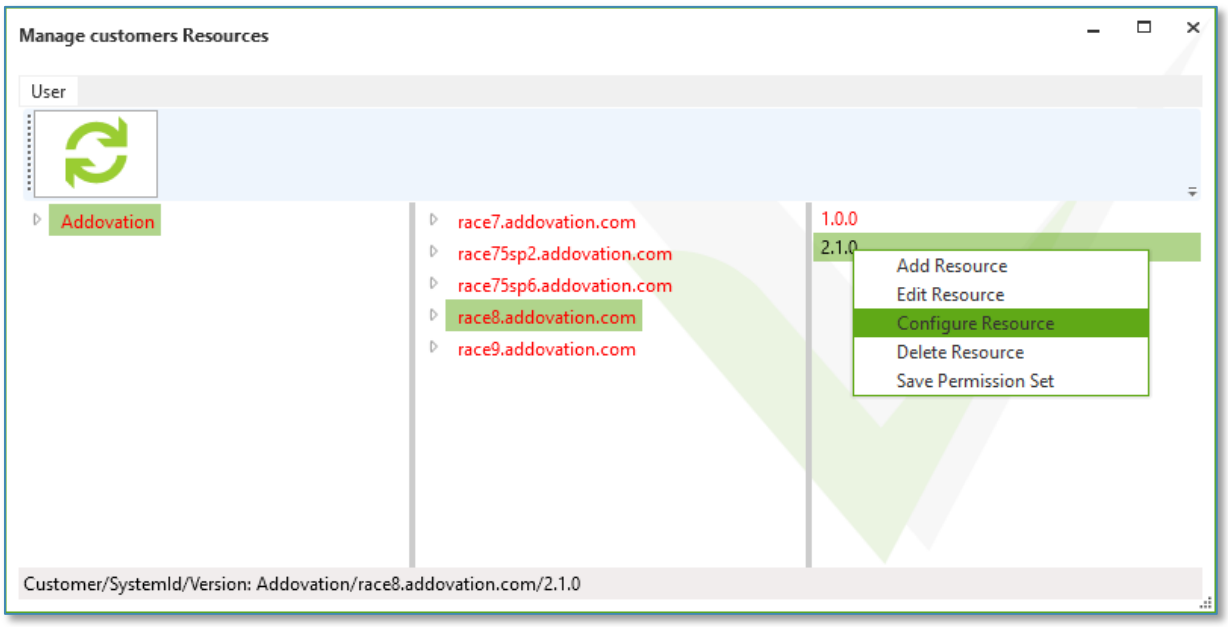

Figure 60 – Configure resources

Enter the values inside “ADFS settings” section and check the “Use Adfs” box to enable ADFS login.

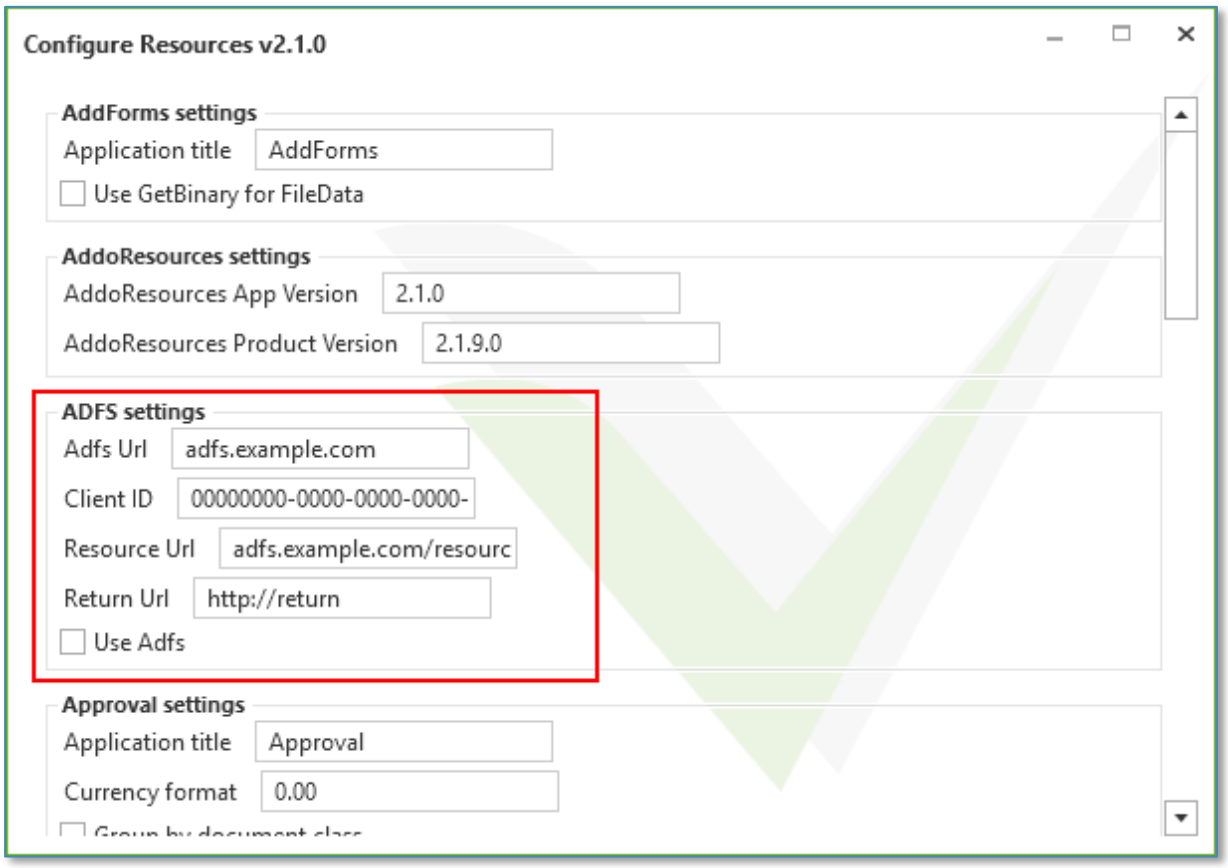

Figure 61 – ADFS settings

6.2 Uplink configuration

The integration user credentials must be entered inside uplink instance configuration window.

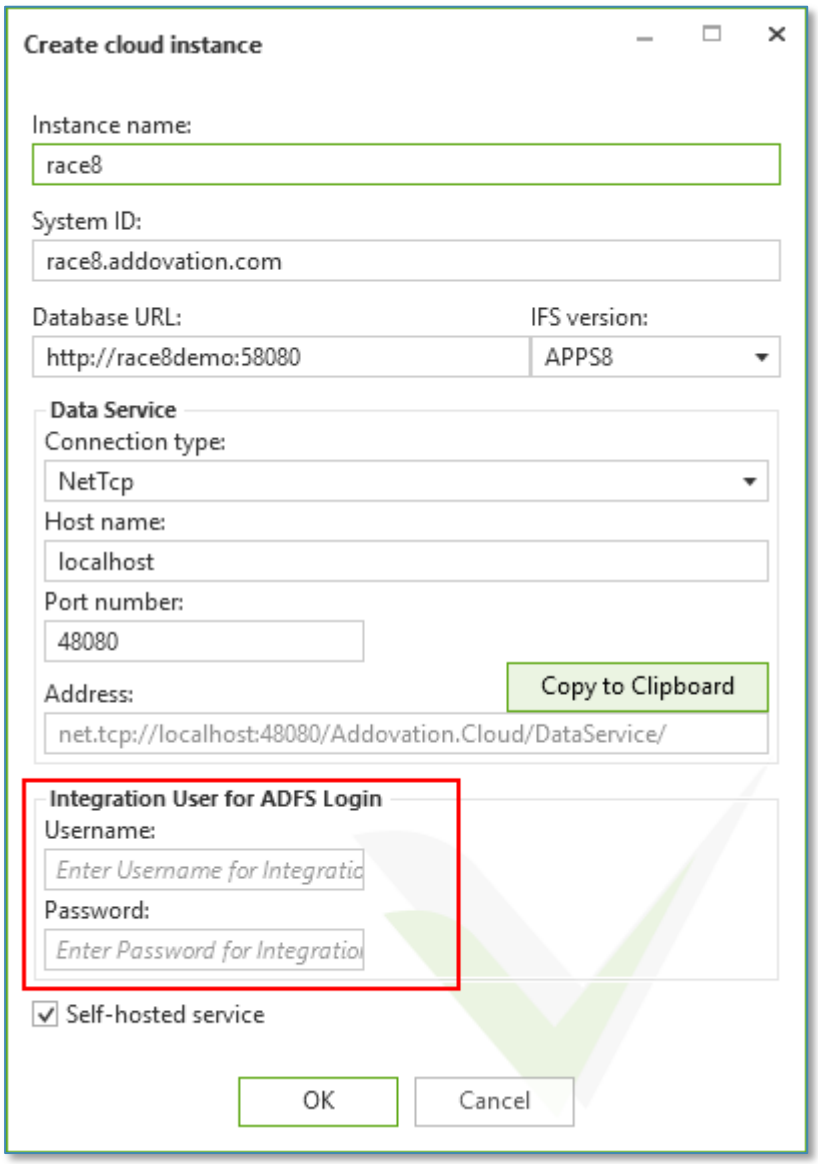

Figure 62 – Create cloud instance

The credentials will be encrypted after saving.

6.3 Authentication

When you enter the Cloud Url and the System ID and if the corresponding AddoResources library is configured to use ADFS, the Username and Password fields are hidden.

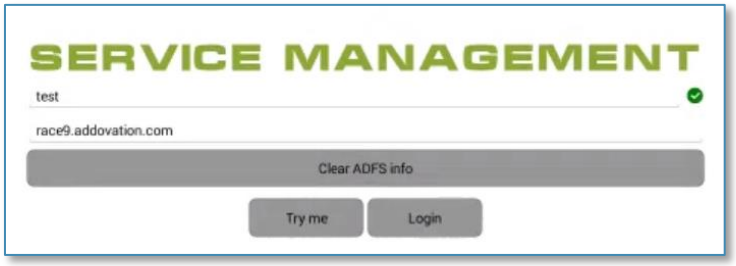

Figure 63 - Authentication

Clicking on “Login” button will redirect you to ADFS login screen. Enter the Username and Password for your AD user.

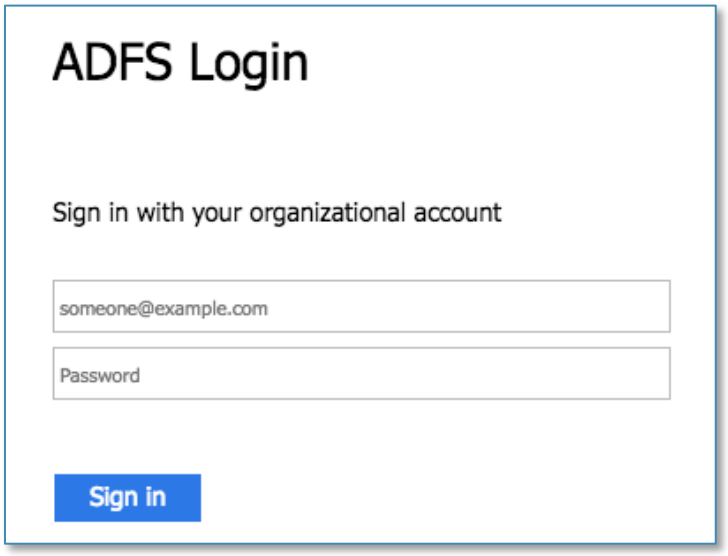

Figure 64 – ADFS Login

Clicking on “Clear ADFS info” button will clear the cached ADFS token, and you will have to pass the ADFS authentication once again in order to enter the application.

7 Upgrade

7.1 Upgrading old versions to Automation Server 2.1. 33715 or higher.

While performing an upgrade, environments and license key should be added again, due to the fact that previously configured environments won't be available during and after the upgrade.