-

CONFIGURE R2CP PC

Software HowTo´s

Author: **Mate, L.** EPDM Created by **Team Leader Software .Net** **Date: 08/11/2021**	**Reviewed:** **Sanchez, Angel** EPDM Revised by **Ingeniero Software .Net** **Date: 10/11/2021**	**Approved:** **Sanchez, Angel** EPDM Approved by **Ingeniero Software .Net** **Date: 10/11/2021**

Digitally signed by
radmin
Date: 2021.11.10
08:38:56 +01:00
Reason: Grupo Sedecal
Location: Algete - Madrid

Table of Updates

Revision	Date	Changes / Remarks	Affected Sections	Author
A	12/06/2020	Document created	All	Lucia Maté
B	08/11/2021	New File Manager Service	1, 4 and 8	Angel Sánchez

TABLE OF CONTENTS

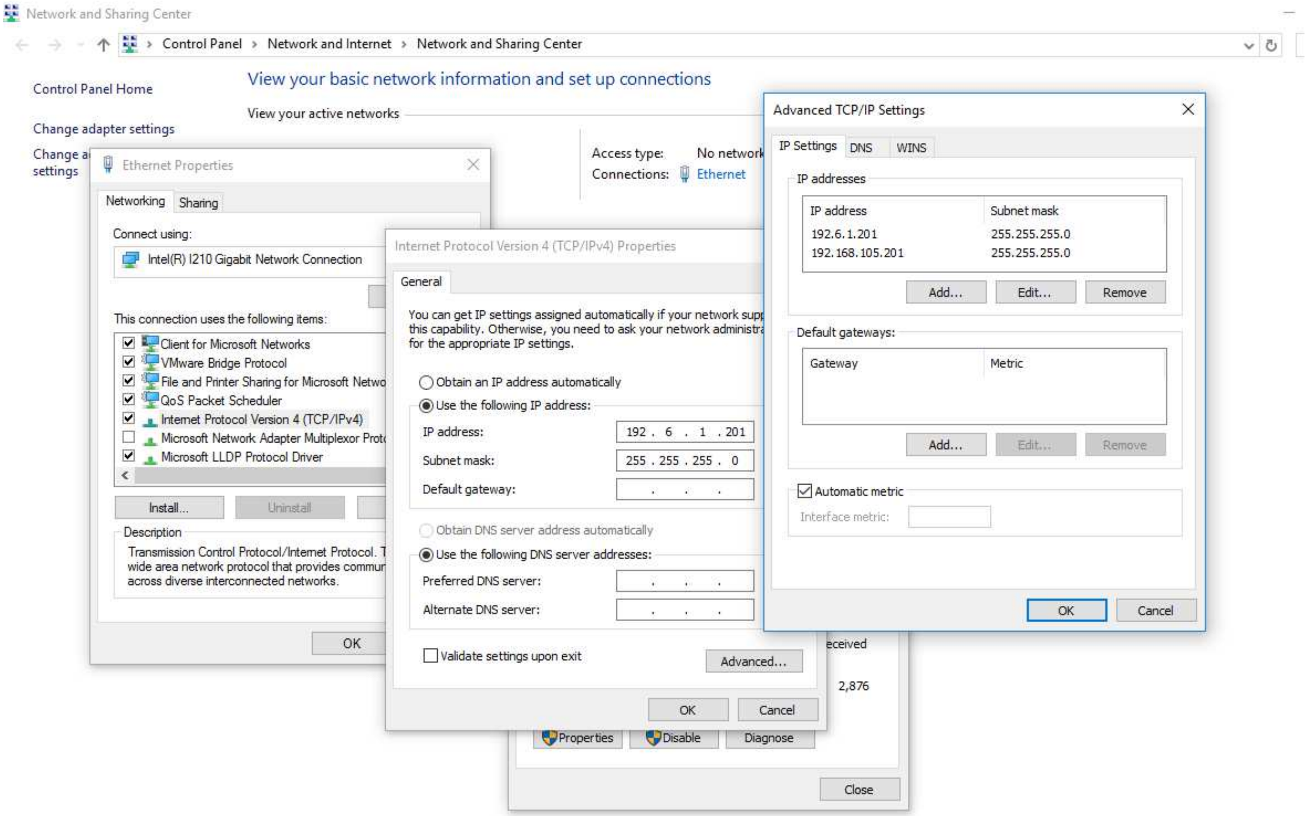
1. Introduction

This document describes PC basic custom configuration for R2CP integration. It will have installed a *Windows 10 with .NET 4.8* Framework included.

2. Ethernet interfaces configuration

Configure IP addresses as follows:

- R2CP Interface: IP: 192.6.1.201.



Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center

Control Panel Home

Change adapter settings

Change a settings

View your basic network information and set up connections

View your active networks

Access type: No network

Connections: Ethernet

Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) I210 Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Netwo
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Prot
- ☑ Microsoft LLDP Protocol Driver

Install... | Uninstall

Description

Transmission Control Protocol/Internet Protocol. T wide area network protocol that provides commur across diverse interconnected networks.

OK

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supp this capability. Otherwise, you need to ask your network administra for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 6 . 1 . 201

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK | Cancel

Properties | Disable | Diagnose

eceived

2,876

Close

Advanced TCP/IP Settings

IP Settings | DNS | WINS

IP addresses

IP address	Subnet mask
192.6.1.201	255.255.255.0
192.168.105.201	255.255.255.0

Add... | Edit... | Remove

Default gateways:

Gateway	Metric

Add... | Edit... | Remove

☑ Automatic metric

Interface metric:

OK | Cancel

3. SNTP Server (clock sync.) configuration

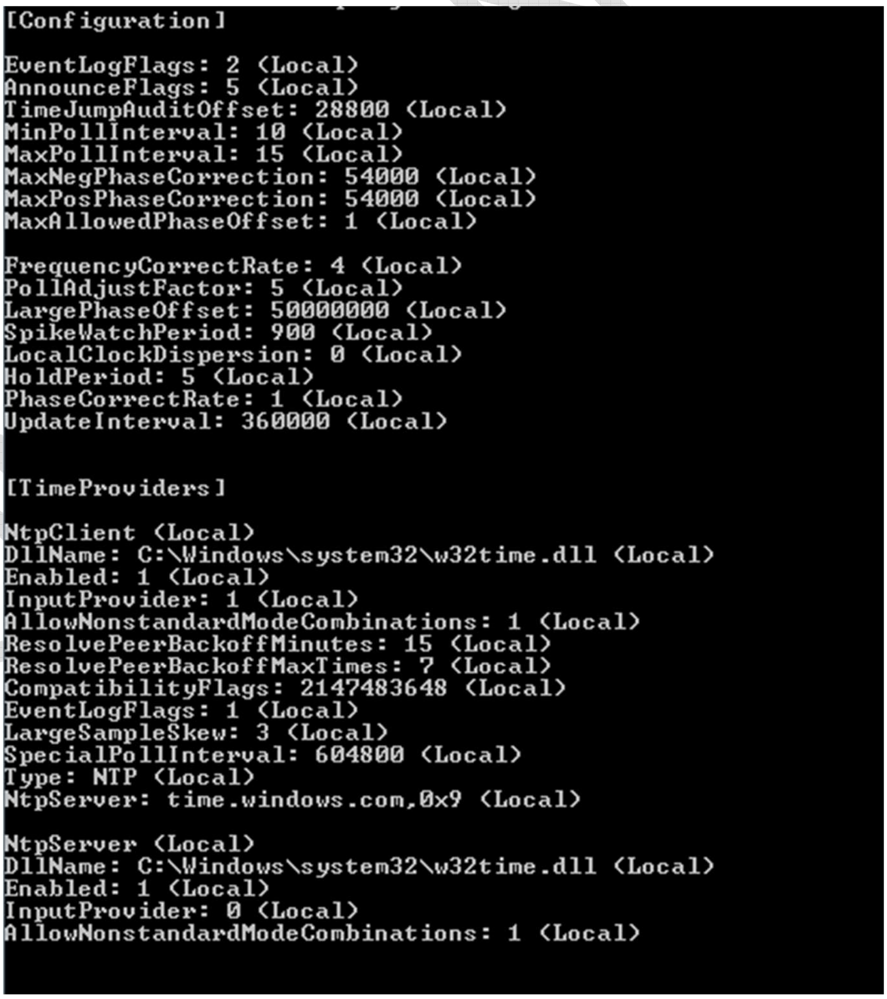
As a consequence of working in a distributed system scenario we need to provide time synchronization between all the components-nodes of our X-Rays system. In order to achieve this synchronization, we will use the SNTP as a networking protocol for clock synchronization between computer systems.

SNTP, known as the Simple Network Time Protocol, is a less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time. It is used in some embedded devices and in applications where high accuracy timing is not required.

The SNTP server configuration will be done under a Windows OS in a few steps defined bellow:

1. Launch Regedit windows tool.

2. Locate: HKEY_LOCAL_MACHINE/system/CurrentControlSet/services/W32Time/TimeProviders/Ntpserver
3. Change the value of "**Enabled**" field to 1.
4. Locate: HKEY_LOCAL_MACHINE/system/CurrentControlSet/services/W32Time/Config
5. Change the value of "**AnnounceFlags**" field to 5 (dec).
6. Change the value of "**LocalClockDispersion**" field to 0 (dec).
7. Go to Control Panel – Administrative Tools – Services
   7.1. Start "**Windows Time**" service if it is not already started.
   7.2. Configure **"Windows Time"** service startup type as "Automatic". (Right click on service – Properties menu)
8. Open a command prompt and enter the line:
   a. **w32tm /config /update**
9. Check that this was successfully configured by entering command line:
   a. **w32tm /query /configuration**



```
[Configuration]

EventLogFlags: 2 (Local)
AnnounceFlags: 5 (Local)
TimeJumpAuditOffset: 28800 (Local)
MinPollInterval: 10 (Local)
MaxPollInterval: 15 (Local)
MaxNegPhaseCorrection: 54000 (Local)
MaxPosPhaseCorrection: 54000 (Local)
MaxAllowedPhaseOffset: 1 (Local)

FrequencyCorrectRate: 4 (Local)
PollAdjustFactor: 5 (Local)
LargePhaseOffset: 50000000 (Local)
SpikeWatchPeriod: 900 (Local)
LocalClockDispersion: 0 (Local)
HoldPeriod: 5 (Local)
PhaseCorrectRate: 1 (Local)
UpdateInterval: 360000 (Local)


[TimeProviders]

NtpClient (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 1 (Local)
InputProvider: 1 (Local)
AllowNonstandardModeCombinations: 1 (Local)
ResolvePeerBackoffMinutes: 15 (Local)
ResolvePeerBackoffMaxTimes: 7 (Local)
CompatibilityFlags: 2147483648 (Local)
EventLogFlags: 1 (Local)
LargeSampleSkew: 3 (Local)
SpecialPollInterval: 604800 (Local)
Type: NTP (Local)
NtpServer: time.windows.com,0x9 (Local)

NtpServer (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 1 (Local)
InputProvider: 0 (Local)
AllowNonstandardModeCombinations: 1 (Local)
```

10. Run the following command to define a trigger event that suits our environment:

a. **sc triggerinfo w32time start/networkon stop/networkoff**

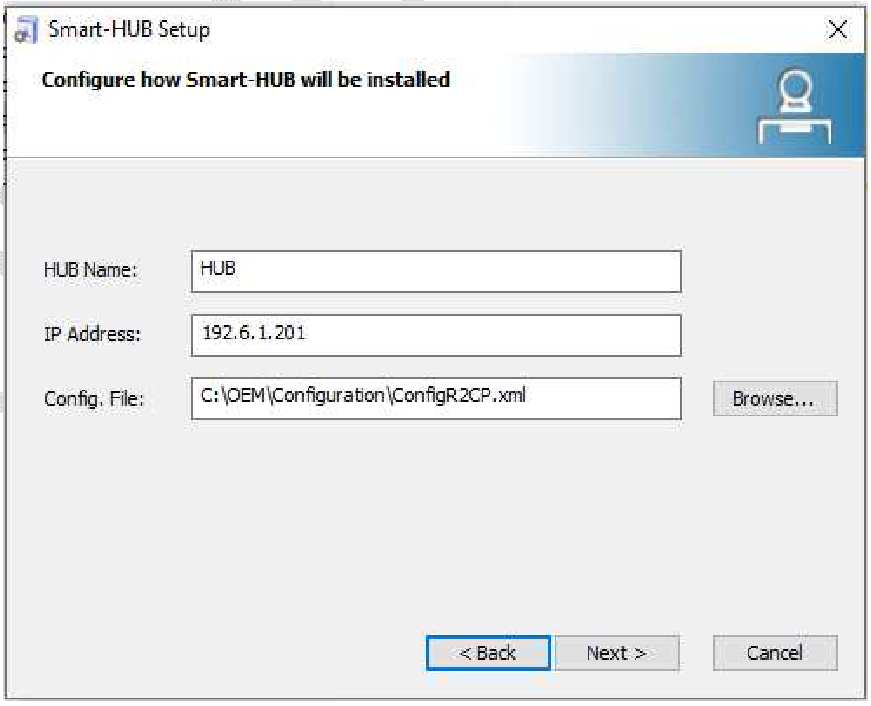
4. Sedecal installers

Execute Sedecal applications installers, **following this order, and reboot the PC afterwards**:

SmartHub	Smart-HUB.Installer.vX.Y.Z.bbbb.exe
Setting Setup	SettingSetup.Installer.Sedecal.vX.Y.Z.bbbb.exe
File Manager	FileManager.Installer.vX.Y.Z.bbbb.exe
Log Service	LogService.Installer.vX.Y.Z.bbbb.exe
Service Tool Console	ServiceTool.Installer.vX.Y.Z.bbbb.exe

Next pictures show some configuration dialogs for installers. The ones not shown here should be configured with their default options:

- SmartHub



Smart-HUB Setup

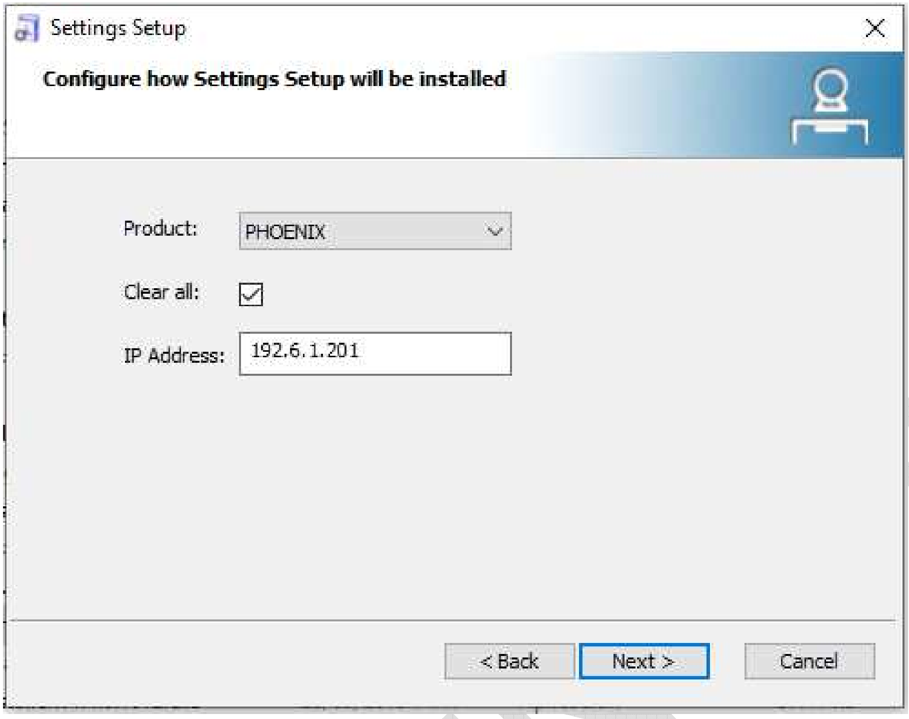
Configure how Smart-HUB will be installed

HUB Name: HUB

IP Address: 192.6.1.201

Config. File: C:\OEM\Configuration\ConfigR2CP.xml

- Setting Setup



Settings Setup

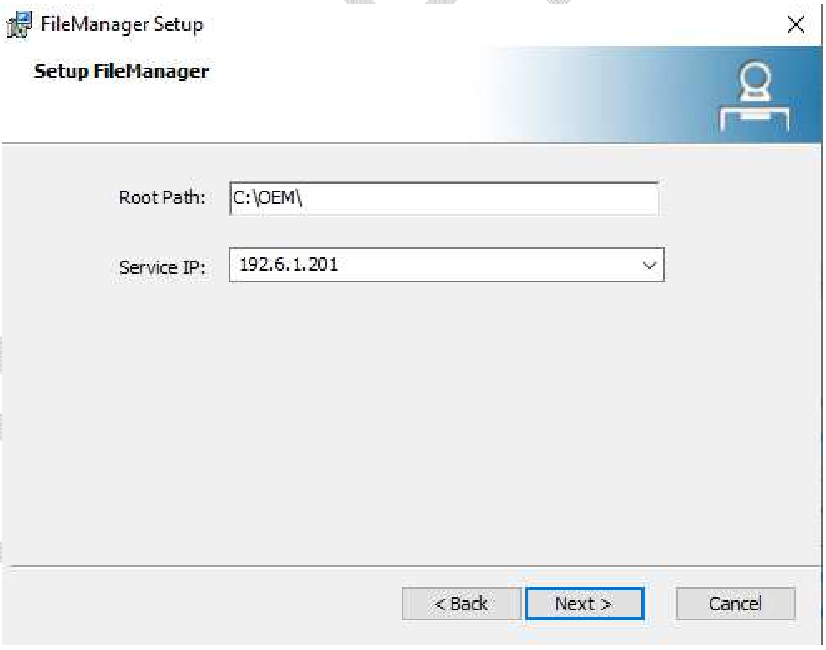
Configure how Settings Setup will be installed

Product: PHOENIX

Clear all: ☑

IP Address: 192.6.1.201

- File Manager



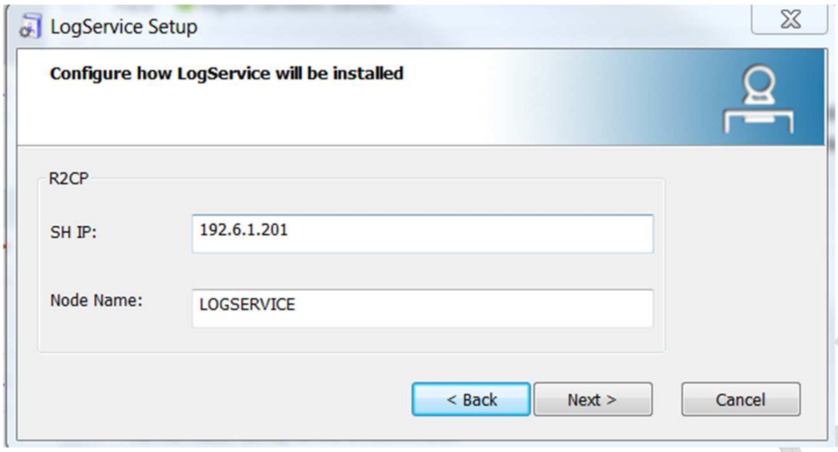
FileManager Setup

Setup FileManager

Root Path: C:\OEM\

Service IP: 192.6.1.201

- Log Service



LogService Setup

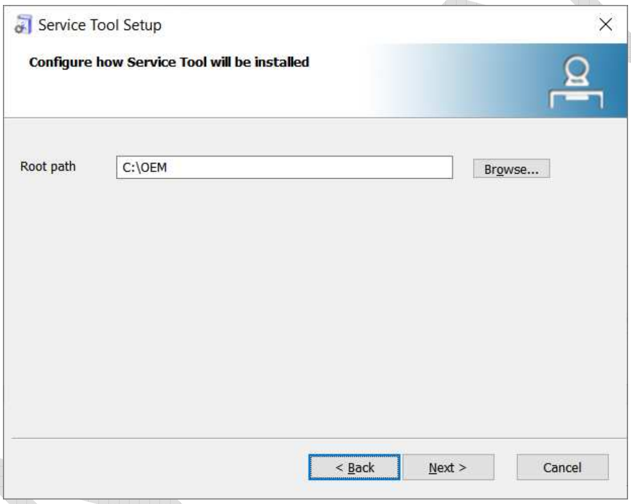
Configure how LogService will be installed

R2CP

SH IP: 192.6.1.201

Node Name: LOGSERVICE

- Service Tool. Root path should be the URL where config files are stored.
  - If Service Tool is installed in the same PC where smarthub is running, set C:\OEM
  - Otherwise, use http://192.6.1.201:8099/FileManagerService.svc/DownloadFile/



Service Tool Setup

Configure how Service Tool will be installed

Root path C:\OEM

5. Touch sensor settings

The right settings for the desired console behavior are as follows:

7.1. Remove blue circles from your cursor

- Run gpedit.msc
- User configuration + Administrative templates + Windows components + Tablet PC + Cursors
- Click “Turn off pen feedback”
- Click “policy settings”
- Select “Enable” and OK.

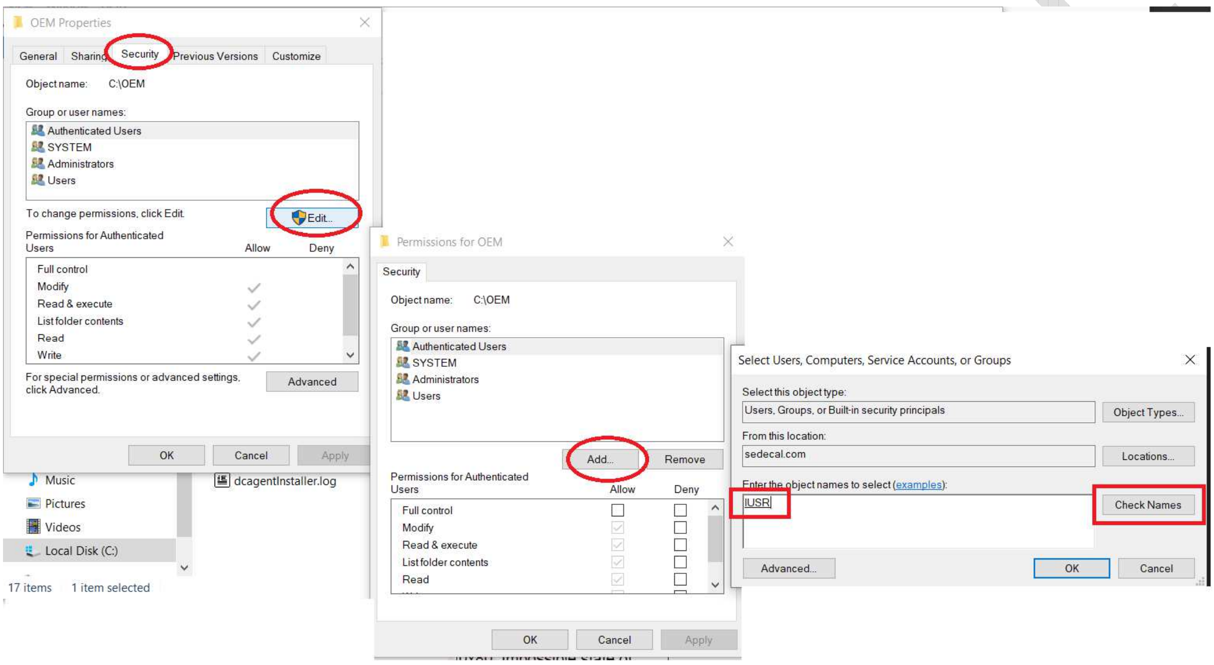
6. Windows settings

8.1. Configure date and time in Windows. Set local date and time correctly.

8.2. Configure “OEM” folder user permissions for IUSR and IIS_ IUSRS users.

8.2.1. Allow modify permissions in folder: “C:\OEM\” to web users: **IUSR.**

- Open File explorer. Right click on C:\OEM folder.
- Click “Properties”
- Click “Security”.
- Click “Edit” → “Add” → write user name “IUSR” and click “Check names”
- When user name is underlined, click “OK”



OEM Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\OEM

Group or user names:
Authenticated Users
SYSTEM
Administrators
Users

To change permissions, click Edit. Edit...

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK | Cancel | Apply

Music
Pictures
Videos
Local Disk (C:)
17 items 1 item selected
dcagentInstaller.log

Permissions for OEM

Security

Object name: C:\OEM

Group or user names:
Authenticated Users
SYSTEM
Administrators
Users

Add... | Remove

Permissions for Authenticated Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

OK | Cancel | Apply

Select Users, Computers, Service Accounts, or Groups

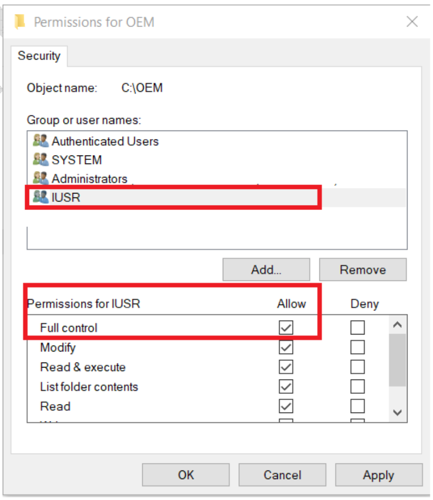
Select this object type:
Users, Groups, or Built-in security principals | Object Types...

From this location:
sedecal.com | Locations...

Enter the object names to select (examples):
IUSR | Check Names

Advanced... | OK | Cancel

- Select “IUSR” user and enable full control by checking “Allow”.



Permissions for OEM

Security

Object name: C:\OEM

Group or user names:
Authenticated Users
SYSTEM
Administrators
IUSR

Add... | Remove

Permissions for IUSR	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

OK | Cancel | Apply

8.2.2. Allow modify permissions in folder: “C:\OEM\” to web user: **IIS_IUSRS.**

- Open File explorer. Right click on C:\OEM folder.
- Click “Properties”
- Click “Security”.

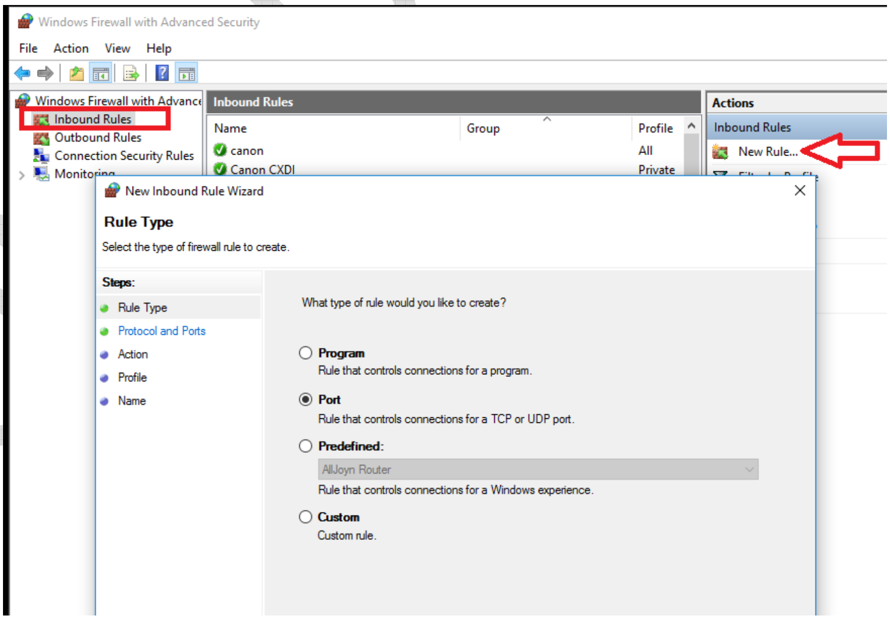
- Click “Edit” → “Add” → write user name “IIS_IUSRS” and click “Check names”
- When user name is underlined, click “OK”
- Select “IIS_IUSRS” user and enable full control by checking “Allow”.

7. Windows firewall

Go to Control Panel →Windows Firewall. Turn on Windows Firewall if it is not already enabled.
Sedecal installers create their own rules to allow application communications.

NOTE: If Windows Firewall is not properly configured, it could be the reason of node connection failures.
It is necessary to create a custom exception rule for SNTP Server
Click on “Inbound rules” → “new rule” and configure it as follows:

- Inbound rule
- Type: Port
- Protocol: UDP
- Specific local port: 123
- Action: allow connection
- Profiles: all



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

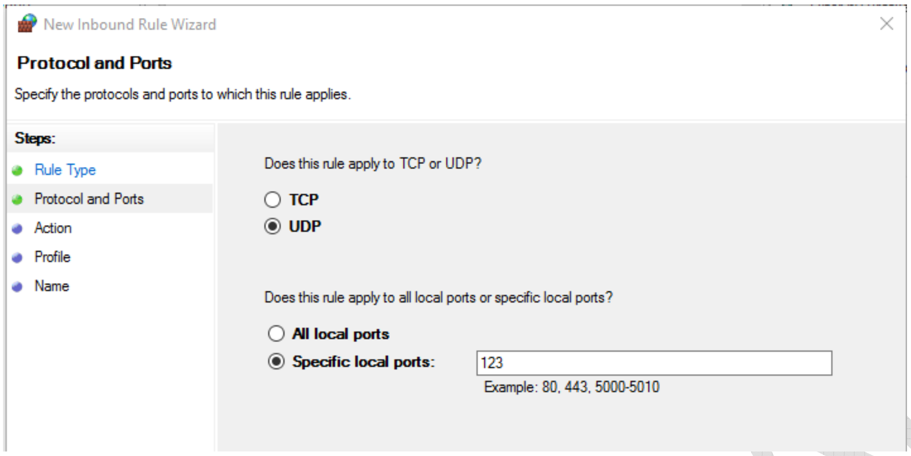
What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

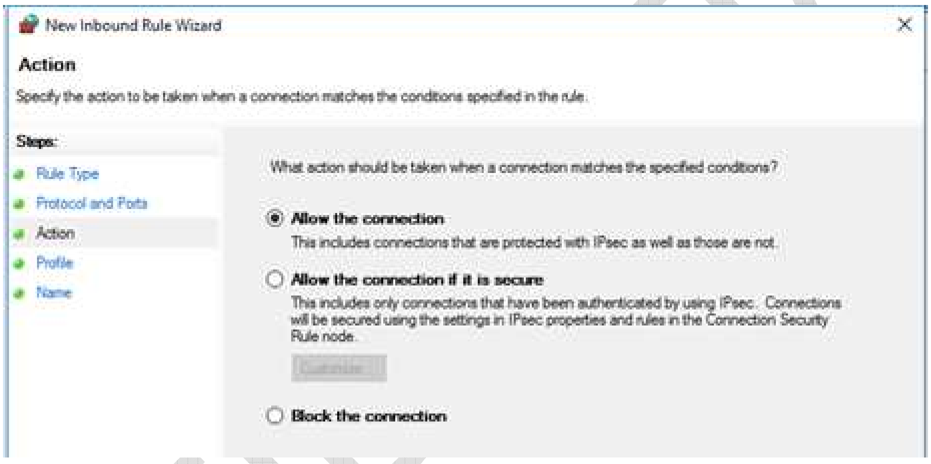
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

○ TCP
● UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 123
Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

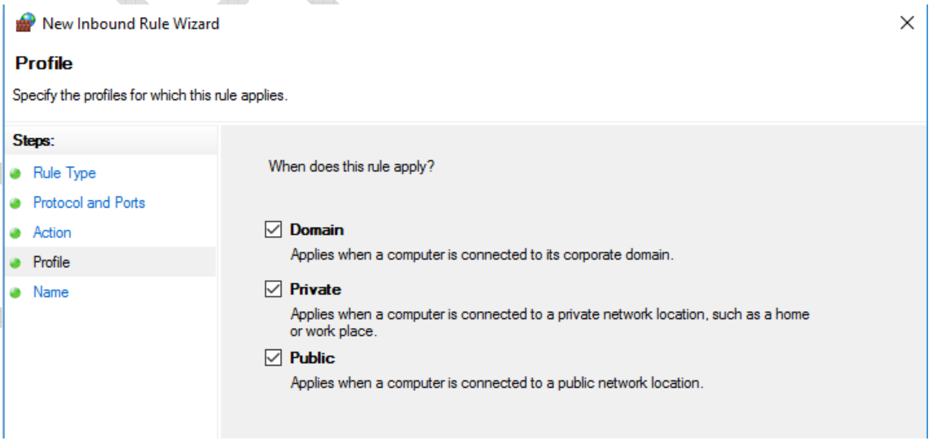
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

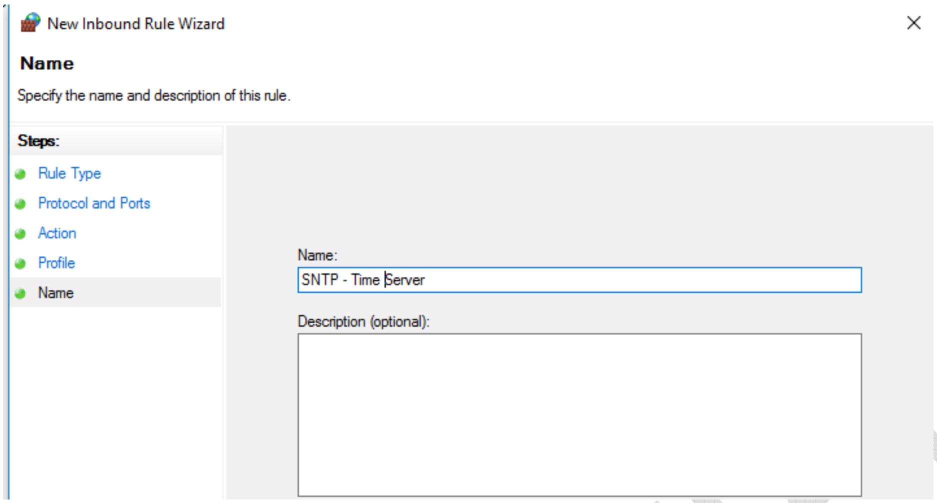
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ Domain
Applies when a computer is connected to its corporate domain.

☑ Private
Applies when a computer is connected to a private network location, such as a home or work place.

☑ Public
Applies when a computer is connected to a public network location.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
SNTP - Time Server

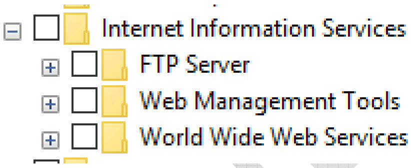
Description (optional):

8. Appendix

8.1 Disable Internet Information Service (IIS)

Currently configuration is incompatible with IIS previous configuration. If PC has IIS enabled, disable this feature:

- Go to Control Panel → Programs and Features → Turn Windows features on or off
- Disable all IIS options



□ Internet Information Services
□ FTP Server
□ Web Management Tools
□ World Wide Web Services

- Reboot PC to ensure changes