

Configuration Microsoft Windows Server 2019



Installation manual for system providers

4/19/2022

Product line Neo, version 7.x

The described functions can be used with the following ASC products:

EVOIP^{neo}

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at <http://www.asctechnologies.com>.

Copyright © 2022 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Contents

1	General information	4
2	Introduction	5
3	System requirements.....	6
4	Installation requirements	7
4.1	Hard disk partitions	7
4.2	Virus protection	7
5	Configuration Microsoft Windows Server 2019	9
5.1	Network cards	9
5.1.1	Configure network cards	9
5.2	Install .NET framework.....	13
5.3	Install Media Foundation (optional).....	17
5.4	Install SNMP service	20
5.5	Configure services	23
5.5.1	Configure SNMP service.....	24
5.5.1.1	Execute script for notifications	26
5.5.1.2	Configure Windows Defender Firewall for SNMP service.....	32
5.5.1.3	Configure SNMP service in Neo	34
5.5.2	Configure Microsoft Windows Time	34
5.5.3	Configure Microsoft Windows Audio (optional)	35
5.5.4	Configure Microsoft Windows firewall	36
5.6	Enable script hosts.....	38
5.7	Configure maximum password age.....	38
5.8	Deactivate write cache for hard disk	40
6	Quick guide.....	43
6.1	General requirements	43
6.2	Observe the following after the installation of Microsoft Windows Server 2019.....	43
	List of figures	45
	List of tables	47
	Glossary	48

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at <https://www.asctechnologies.com>

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

2 Introduction

This document describes the configuration of Microsoft Windows Server 2019 for the EVOIP_{neo} software.

3 System requirements



The system requirements are described in the installation manual *Installation requirements*.

Update operating system



Updates of the operating system are supported with the exception of complete service packs. The installation of new service packs has to be approved explicitly by ASC.

Deactivate the "Automatic update function" of the operating system to prevent the server from starting up inadvertently. Install necessary updates manually if required.



The service *Windows Firewall* has to be started **before** the installation of the Neo software to guarantee the correct operation of the recording system, see [chapter "Configure services", p. 23](#). ASC only supports the Microsoft Windows Firewall.



The time zone of the Microsoft Windows Server must be set **before** the installation of the Neo software.



File Access Auditing/File Access Log must have been deactivated.

4 Installation requirements

4.1 Hard disk partitions



For the partitions, the following variants are supported:

- 1 hard disk with 3 partitions
- 3 hard disks with 1 partition each

1. System partition

The system partition should have a minimum of 60 GB.

- 40 GB operating system
- 20 GB Neo software

2. Database partition

NOTICE! The database partition is required if you install the PostgreSQL database on this server.

- The size of the database depends on the number of recordings and on the retention period of recordings.



Information about how to calculate the size of the database partition can be found on the Manual Package in the file *Postgres_Callpool_Sizing* in folder *1_Sizing calculator*.

3. Data partition

NOTICE! The data partition is required if you save the callpool on this server.

- The size of the data partition depends on the recording requirements.
A minimum of 150 GB is mandatory.



Information about how to calculate the size of the callpool can be found on the Manual Package in the file *Postgres_Callpool_Sizing* in folder *1_Sizing calculator*.

4.2 Virus protection

The installation of an antivirus software on a Neo recording system lies within the responsibility of the customer.

The installation of an antivirus software does affect neither warranty nor maintenance contracts; however ASC does not assume any liability for consequential damages that may occur due to the use of the antivirus software.

Running an antivirus software may slow down the execution of the Neo software during periods of high system utilization. Running an antivirus software has an impact on the execution of functions, too, which involve increased data exchange at the I/O interfaces (e. g. creating diagnostic data, statistics or updating configuration data) and may thus cause functional impairment.

For this reason, ASC recommends defining time intervals for scanning the entire system for viruses when system utilization and data transfer rates are low.

Antivirus programs tested by ASC and supported:

- Windows Defender (virus protection integrated into Windows operating systems)

Required settings of an antivirus software:

- On-access scanning must have been activated.
- The following directories are mandatory to be excluded from the virus scan:
 - All directories on the database partition (ASCDB, replication, ...)

- Directory *ASCDATA*
- Directory *ASC Product Suite*
- The following file is mandatory to be excluded from the virus scan:
 - File *C:\Program Files\PostgreSQL\9.5\bin\postgres.exe* or *C:\Program Files\PostgreSQL\12\bin\postgres.exe* (the path depends on the deployed PostgreSQL version.)



When installing and/or updating the Neo software, on-access scanning must have been disabled.

Troubleshooting

If the antivirus software should cause errors in the Neo software, proceed as follows:

1. Uninstall or deactivate the antivirus software to restore the flawless operation of the Neo software.
2. Contact your local ASC support or the ASC support by calling +49 700 27278776 to coordinate the further course of action.

5

Configuration Microsoft Windows Server 2019

The following images refer to the display mode *View by Category* preset by default.

Configure the EVOIP_{neo} software as follows to guarantee smooth operation:

- Configure Internet Explorer
- Deactivate Internet Explorer Enhanced Security Configuration (IE ESC)
- [chapter "Network cards", p. 9](#)
- [chapter "Configure services", p. 23](#)

5.1

Network cards

Changing the IP address



The IP address should have been configured before the installation of the Neo software.

Changing the IP address once the recorder application has been installed affects the certificates. For further information refer to the installation manual *Installation of the recording software of ASC*.



If you use a [sniffer card](#), you have to enter an unambiguous IP address and a protocol version for this card, too.

5.1.1

Configure network cards

1. Press the Windows icon key.
2. Open the window *Network and Sharing Center* (network connection) by clicking on *Control Panel > Network and Internet > Network and Sharing Center*.
3. Click on *Change adapter settings* on the left side.

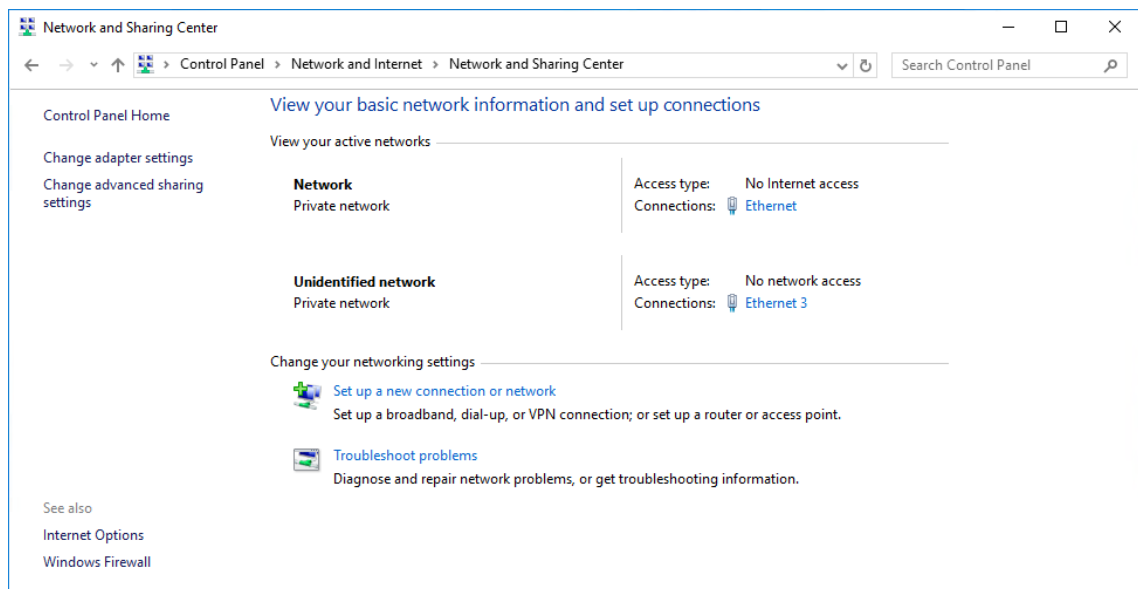


Fig. 1: Network and Sharing Center

4. Click on the inserted card.
5. Open the context menu with a right-click.
6. Select the menu item *Properties*.

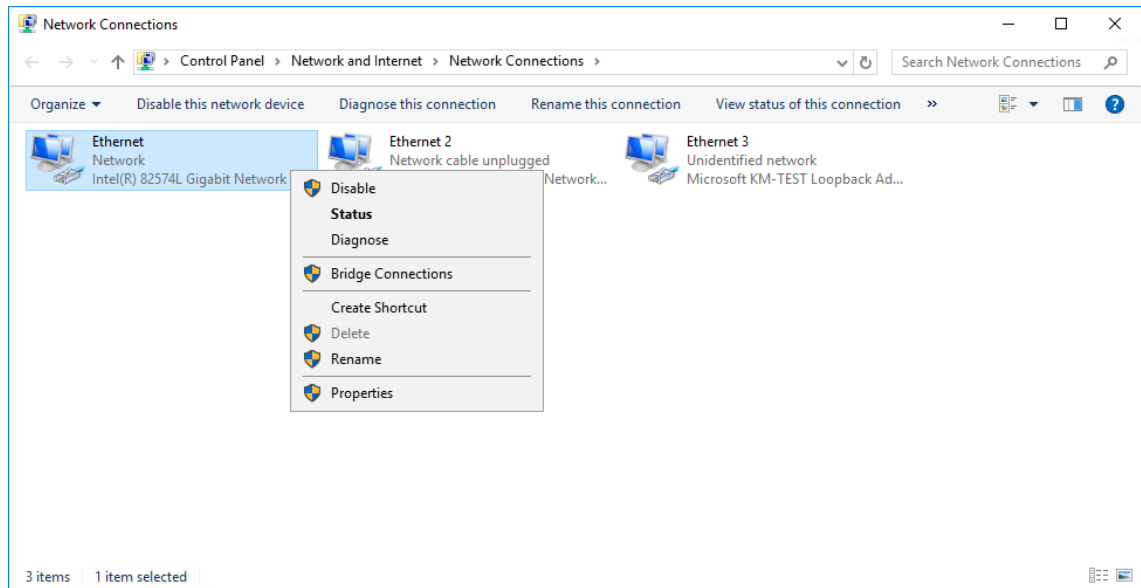


Fig. 2: Network Connections

7. Make sure that the option *File and Printer Sharing for Microsoft Networks* has been activated.
8. Click on *Internet Protocol, Version 4 (TCP/IPv4)*.

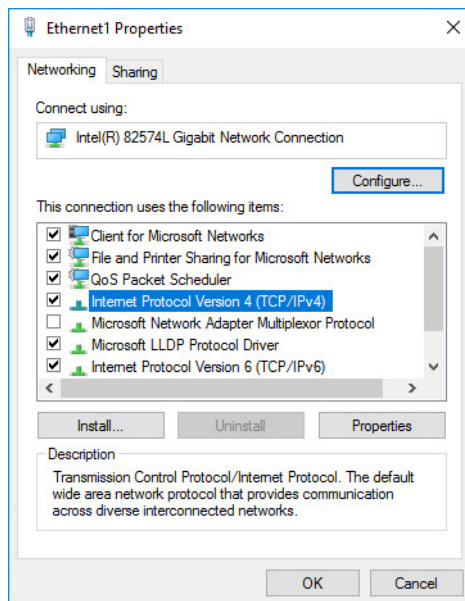


Fig. 3: Network connection properties

9. Click on the button *Properties*.
10. You have to assign a static IP address for the Neo software. Select the option *Use the following IP address*.

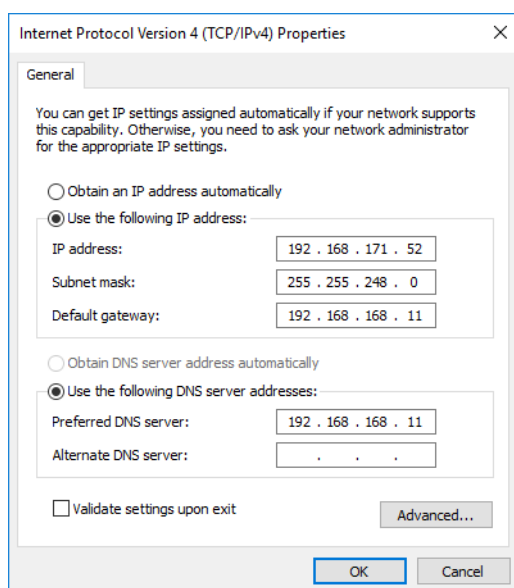


Fig. 4: Internet Protocol Version 4 (TCP/IPv4) Properties (example)

11. Enter the IP address, the subnet mask, and the default gateway.
12. Click on the button *OK* to save the settings and to close the window.
13. Click on the button *Configure*.

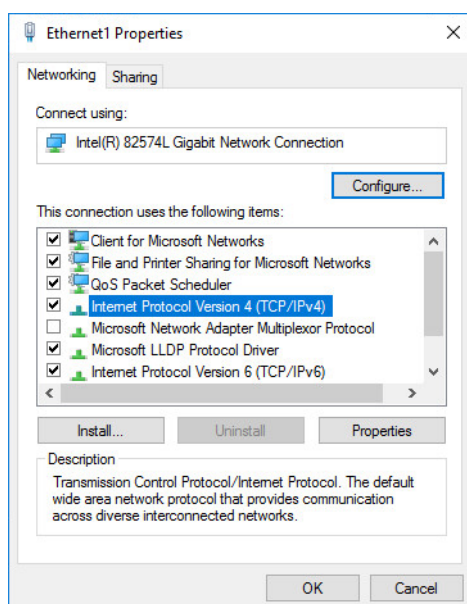


Fig. 5: Network connection properties

14. Click on the tab *Power Management*.

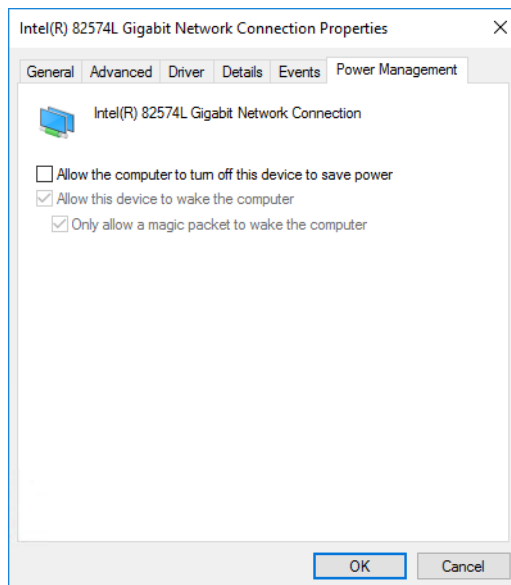


Fig. 6: Network connection power management

15. Deactivate the check box *Allow the computer to turn off this device to save power*.
16. If you do not want to configure a [sniffer card](#) for the passive recording, click on the button **OK**. The settings are saved and the window is closed.
If you would like to configure a [sniffer card](#) for the passive recording, proceed as follows:
17. Click on the tab *Advanced*.

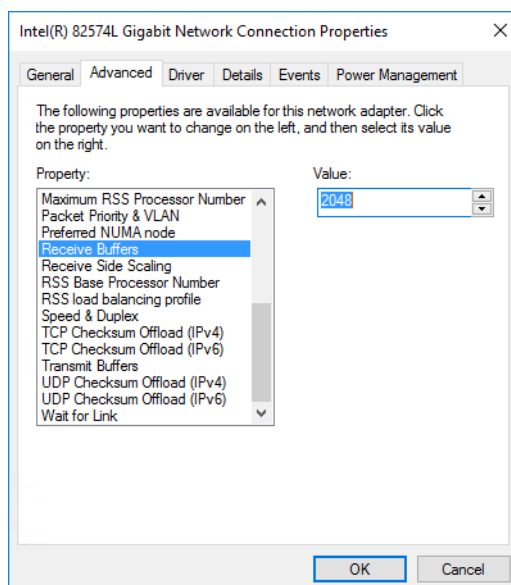


Fig. 7: Network connection advanced properties (example)



Depending on the network card, the following setting dialog may differ.

18. Select the option *Receive Buffers* or *Receive Descriptors* in the list.
19. Enter the maximum value in the field *Value*. Click on one of the arrows to increase or decrease the value.



Depending on the inserted card the maximum value lies between 1024 and 2048.

20. Click on the button **OK** to save the settings and to close the window.

5.2 Install .NET framework

.NET Framework can either be installed as administrator by means of the command *cmd* for systems with internet access or alternatively by means of the Server Manager.

Cmd command

✓ Internet access

1. Open *cmd* as administrator.
 2. Enter the following command:
`dism.exe /online /enable-feature /featurename:NetFX3 /all`
 3. Press the key enter *Enter*.
- ⇒ .NET Framework is installed automatically.

Server Manager

- ✓ The Microsoft Windows 2019 DVD has been inserted or mounted.
1. Open the *Server Manager* in the taskbar.
- ⇒ The following window appears:

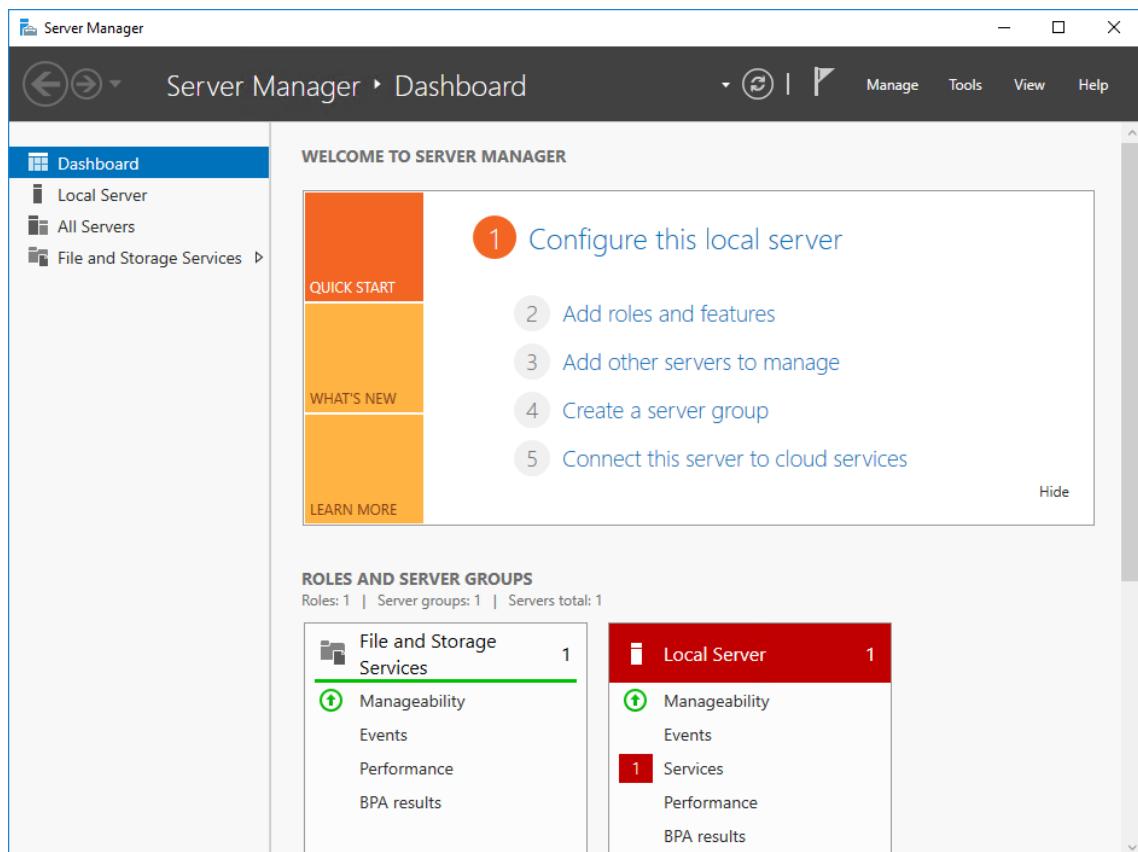


Fig. 8: Server Manager

2. Click on *Add roles and features*.
- ⇒ The following window appears:

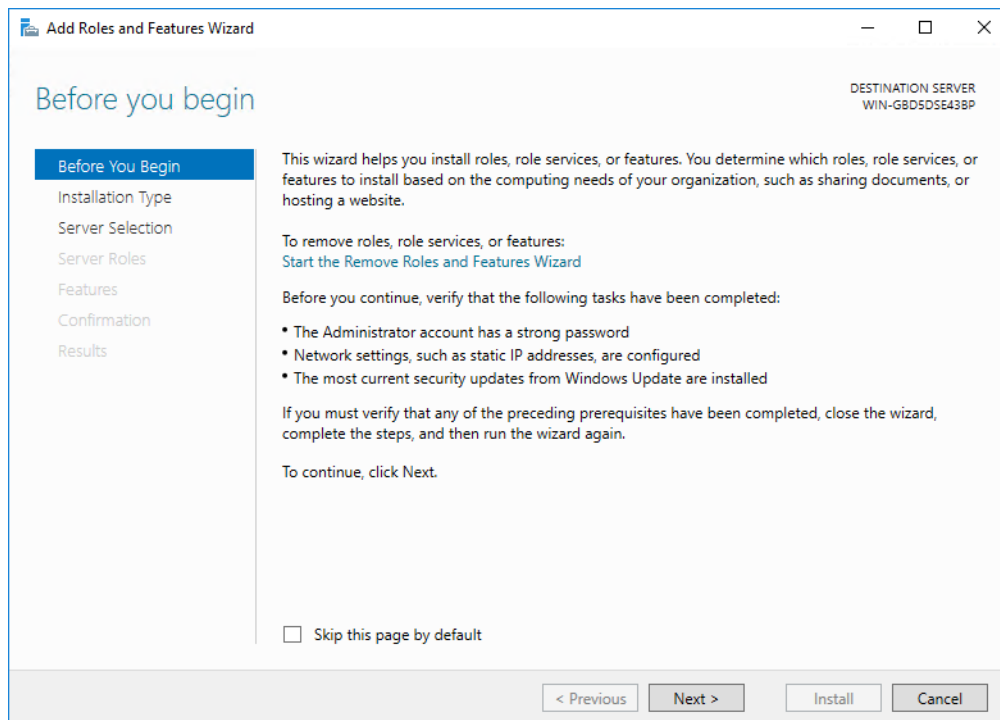


Fig. 9: Add Roles and Features Wizard

3. In the menu item *Installation Type*, click on the button *Next*.
4. In the menu item *Server Selection*, click on the button *Next*.
5. In the menu item *Server Roles*, click on the button *Next*.
6. In the menu item *Features*, click on the button *Next*.
7. Activate the check box *.NET Framework 3.5 Features*.
8. Click on the button *Next*.

⇒ The following window appears:

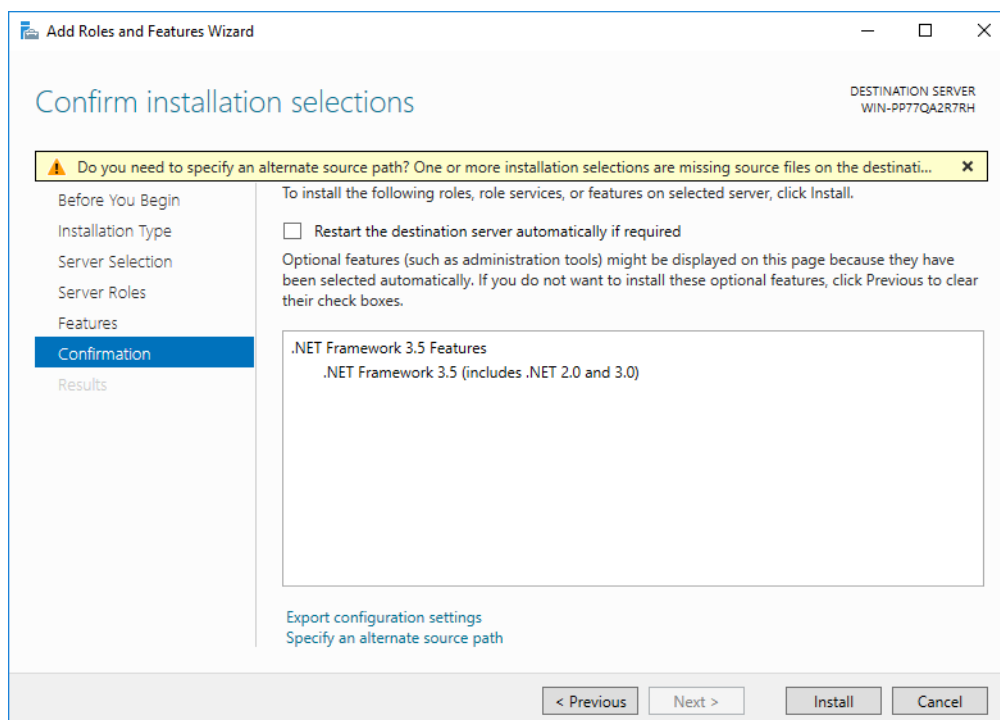


Fig. 10: Add Roles and Features Wizard

9. Open the *Microsoft Windows Explorer* in the taskbar.

10. Click on the button *This PC*.
11. Right-click on the DVD drive.
 - ⇒ A context menu appears.
12. Click on *Open* in the context menu.

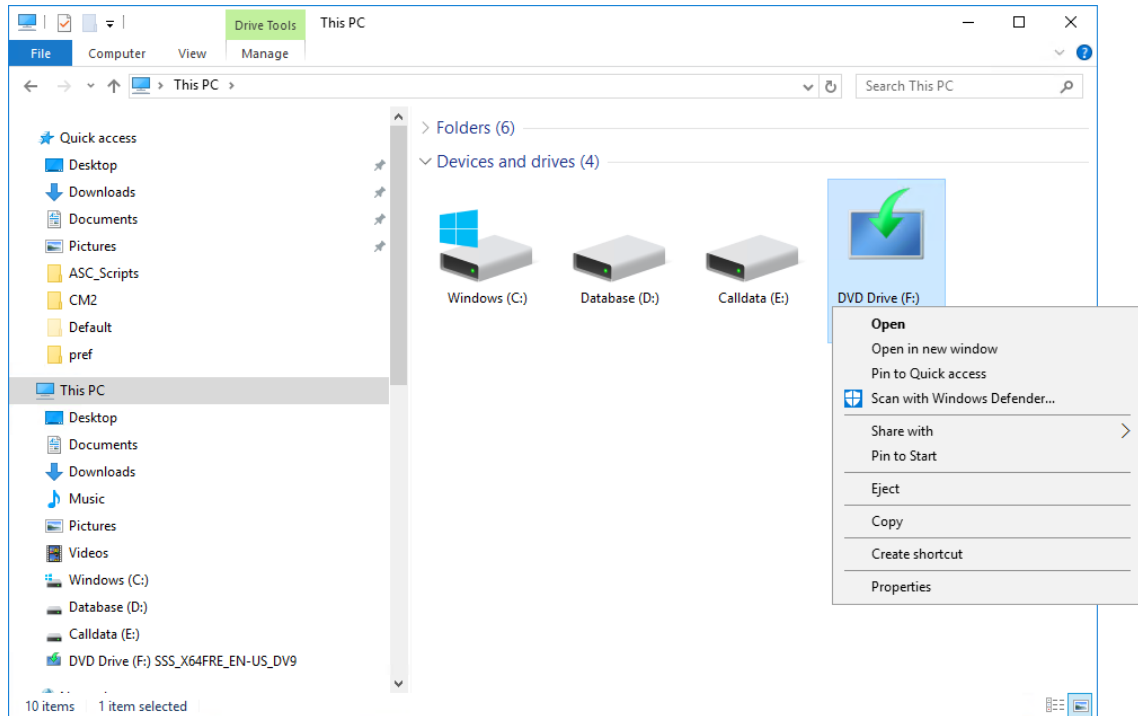


Fig. 11: Computer

13. Double-click on the folder *sources* in the structure view.
14. Click on the folder *sxs* in the structure view.
15. Left-click into the address bar at the top.
 - ⇒ The folder path is selected.
16. Right-click into the address bar at the top.
 - ⇒ A context menu appears.
17. Click on *Copy* in the context menu.

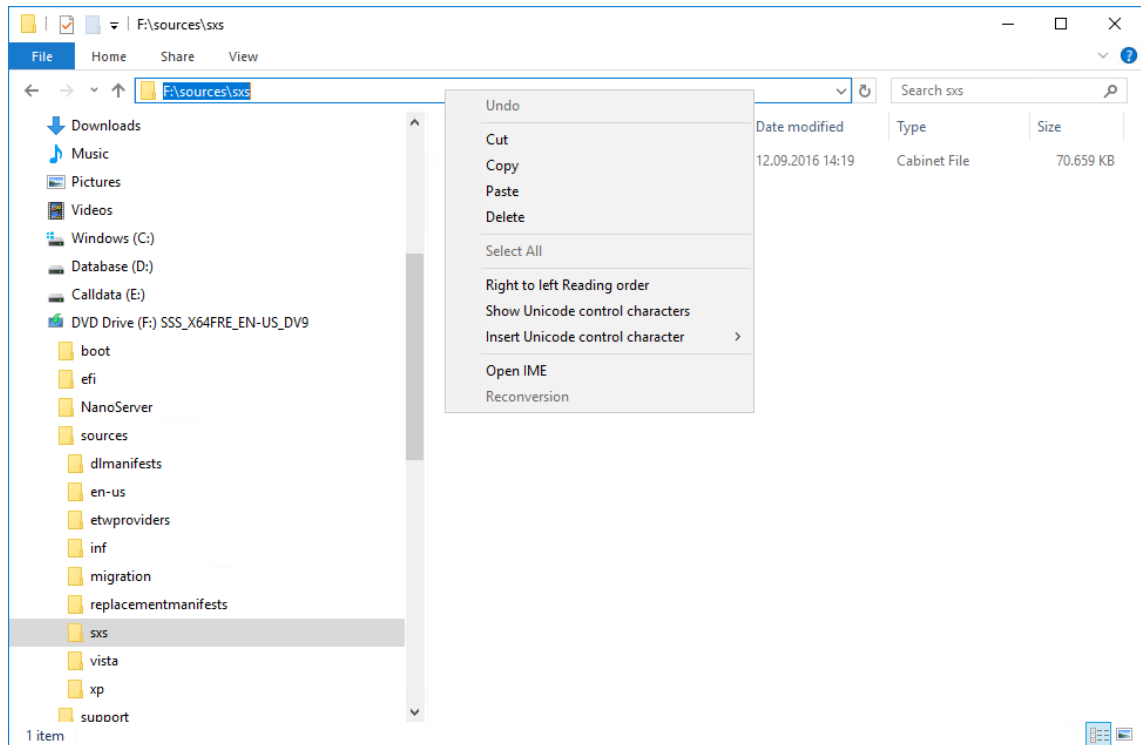


Fig. 12: Copy source path for configuration settings

18. Change to the window *Add Roles and Features Wizard*.

19. Click on *Specify an alternate source path*.

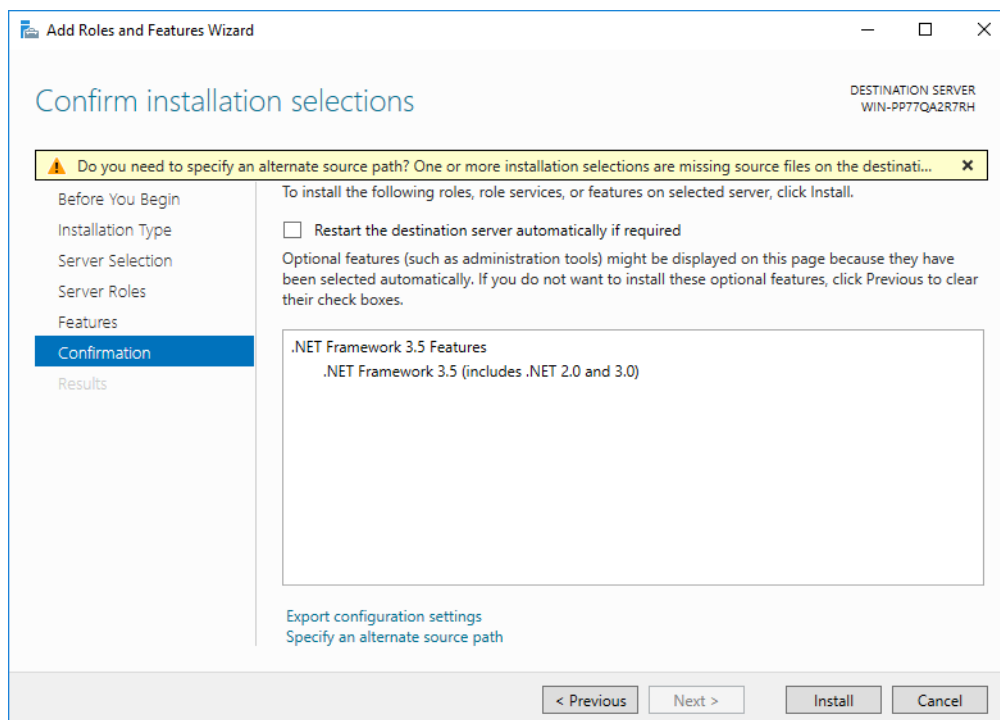


Fig. 13: Add Roles and Features Wizard

20. Right-click in the entry field *Path*.

⇒ A context menu appears.

21. Click on *Paste* in the context menu.

⇒ The path is pasted.

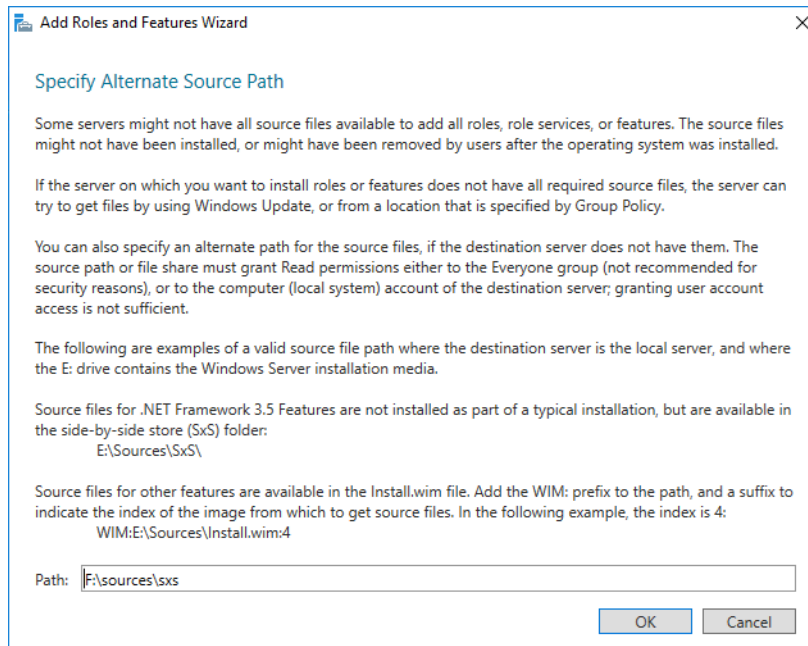


Fig. 14: Source path for configuration settings was pasted.

22. Click on the button *OK* to save the settings and to close the window.
23. Click on the button *Install* to install the service.
24. Click on the button *Close* to close the window.

5.3 Install Media Foundation (optional)

To allow local replay on the server, the Microsoft Windows Media Foundation Service must have been installed. Proceed as follows:

1. Press the Windows icon key.
2. Open the Microsoft Windows options by clicking on *Control Panel > Programs and Features*.
3. Click on the option *Turn Windows features on or off*.

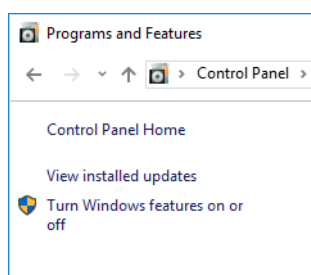


Fig. 15: Microsoft Windows options

4. The following window appears:

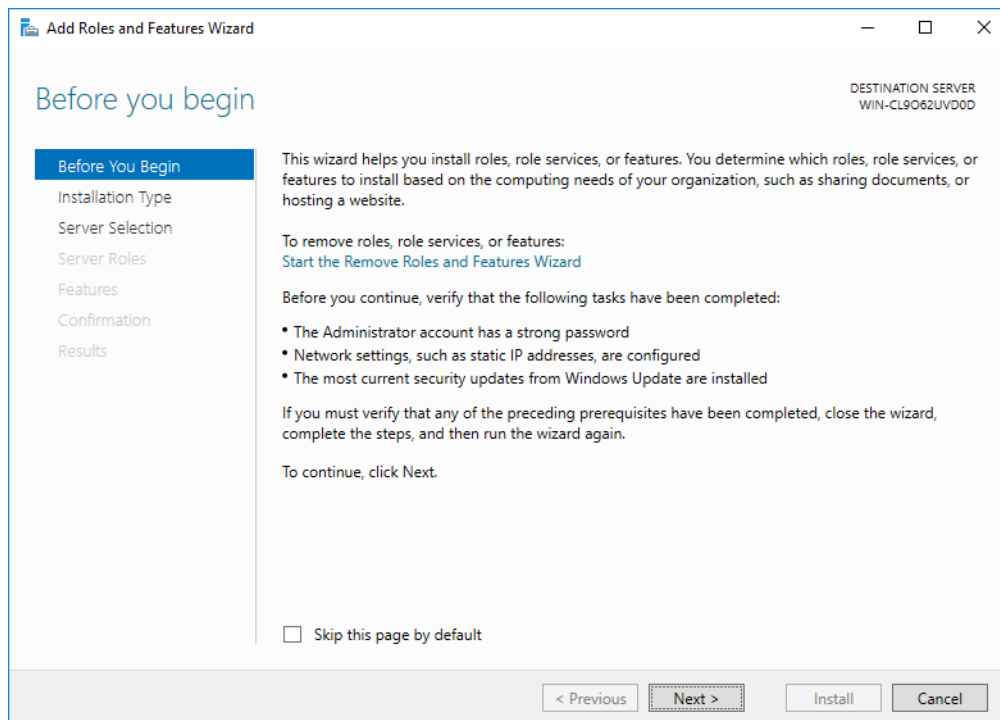


Fig. 16: Add Roles and Features Wizard

5. Click on the button *Next*.
6. Under *Installation Type*, activate the option *Role-based or feature-based installation*.

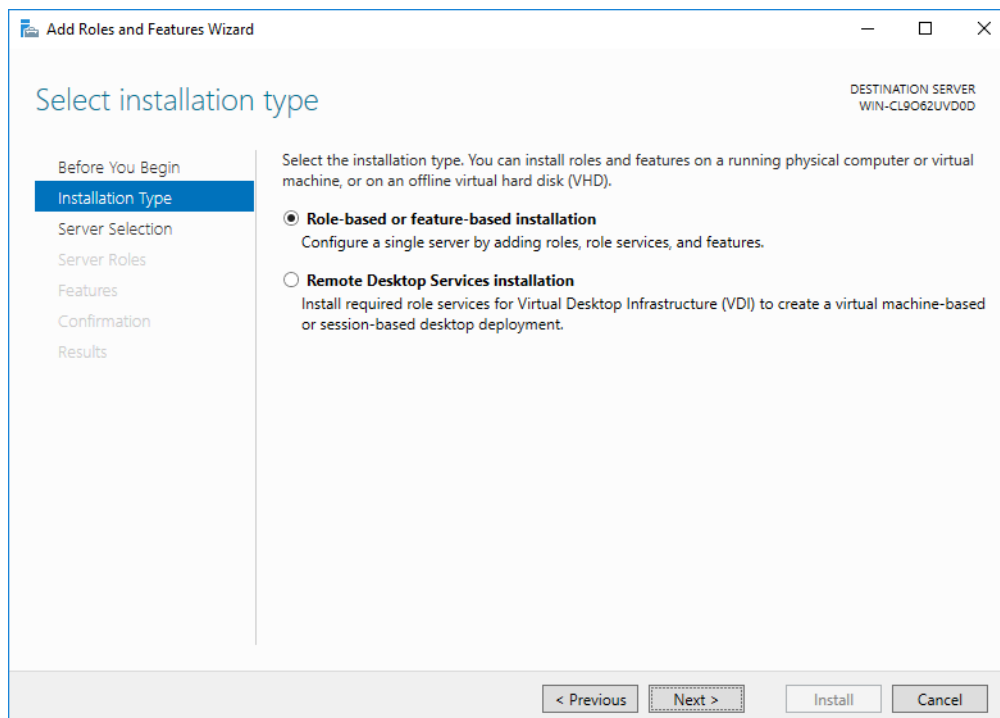


Fig. 17: Installation type

7. Click on the button *Next*.
⇒ The following window appears:

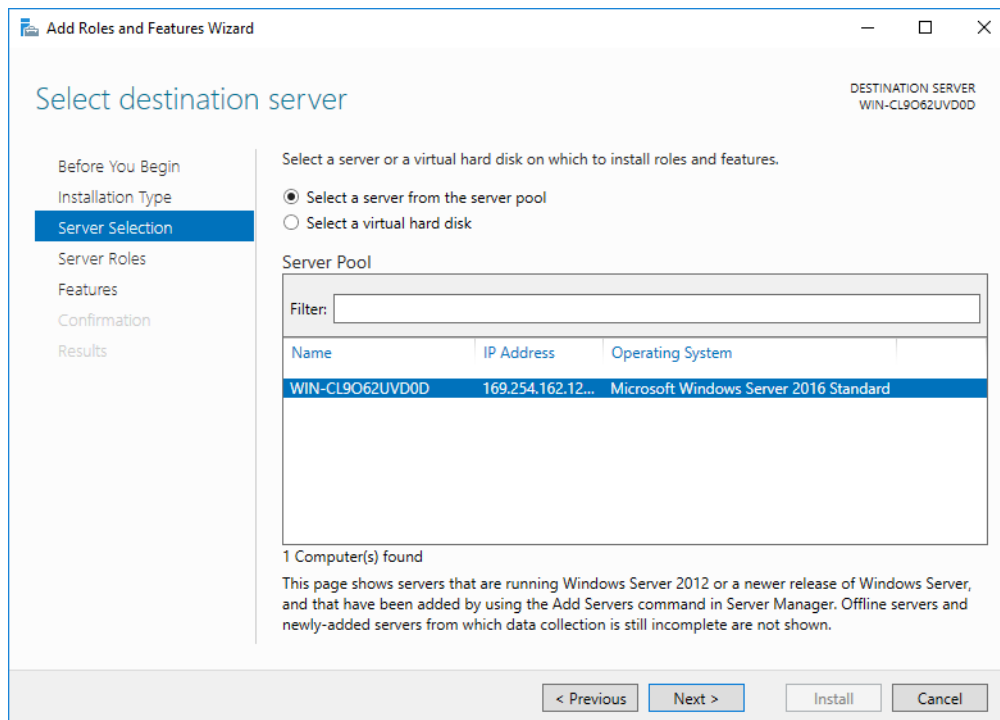


Fig. 18: Server selection

8. Under *Server Selection*, activate the option *Select a server from the server pool*.
 9. Select your server from the pool of servers.
 10. Click on the button *Next*.
- ⇒ The following window appears:

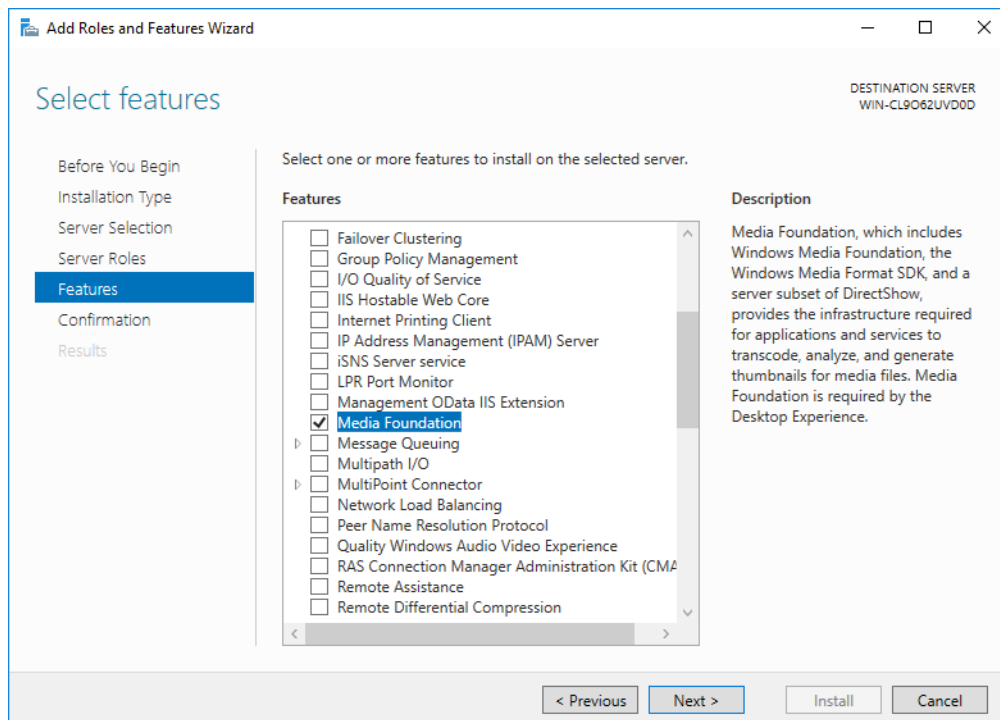


Fig. 19: Features

11. Under *Features*, activate the option *Media Foundation*.
12. Click on the button *Install* to install the service.
13. Restart the computer after the installation to apply the settings.

5.4 Install SNMP service



The recording system uses a native **SNMP** service for SNMPget requests. The **SNMP** service of the operating system is **not** used.

Use a different network port for the Neo **SNMP** agent than the default **SNMP** port of the operating system or deactivate the **SNMP** service of the operating system if you do not need it for other applications.

You must install the **SNMP** service by means of the Microsoft Windows options.

1. Press the Windows icon key.
2. Open the Microsoft Windows options by clicking on *Control Panel > Programs and Features*.
3. Click on the option *Turn Windows features on or off*.

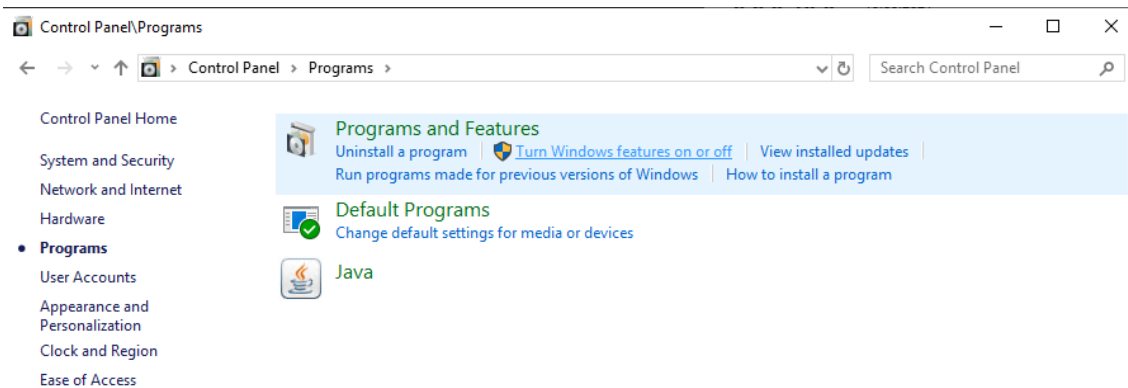


Fig. 20: System control - Turn Windows features on

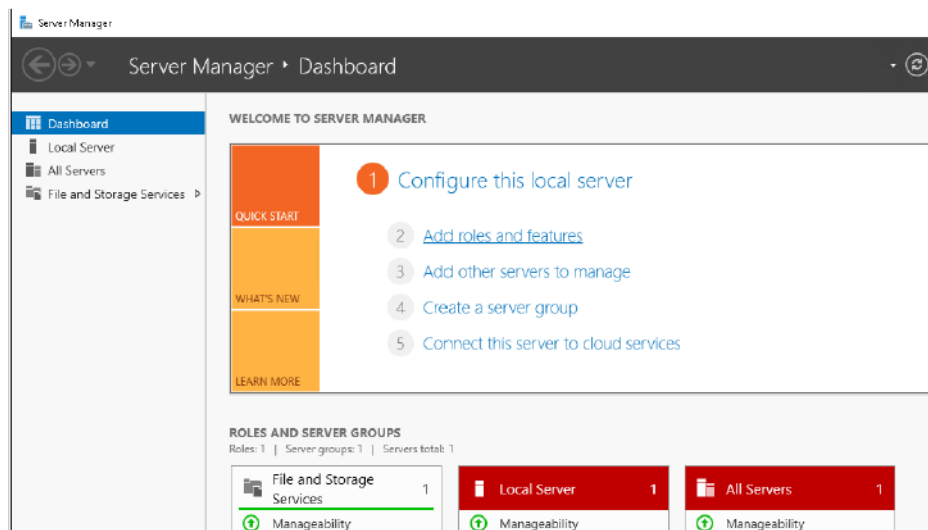


Fig. 21: Add roles and features

4. Select the menu item *Add roles and features*.
⇒ The installation wizard appears.

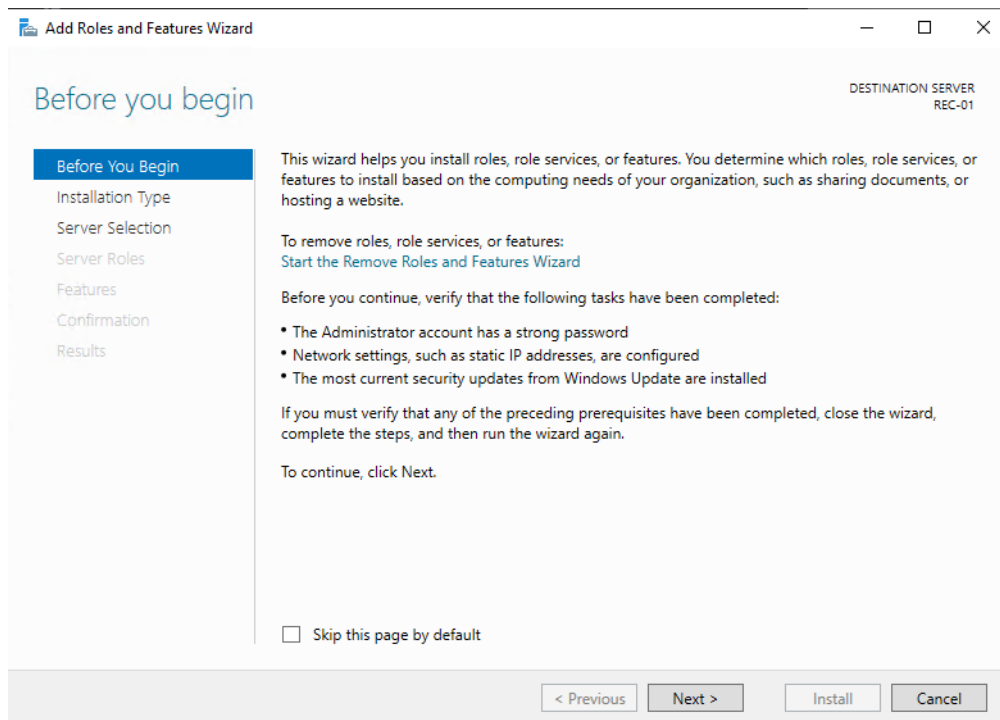


Fig. 22: Add Roles and Features Wizard

5. Click on the button *Next*.
6. Under *Installation Type*, activate the option *Role-based or feature-based installation*.

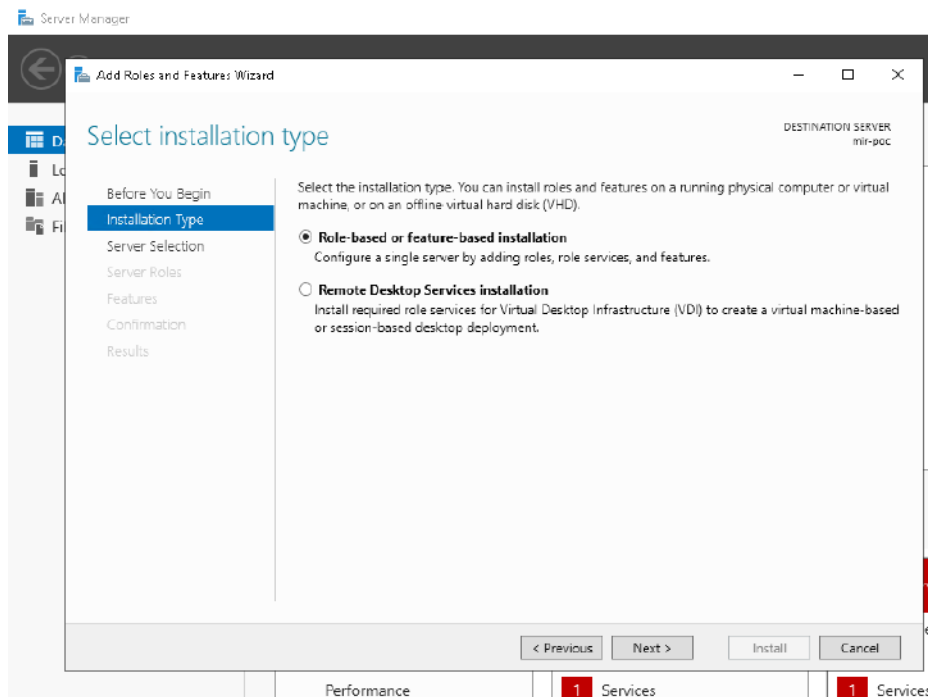


Fig. 23: Select installation type

7. Click on the button *Next*.
⇒ The window to select the server appears.

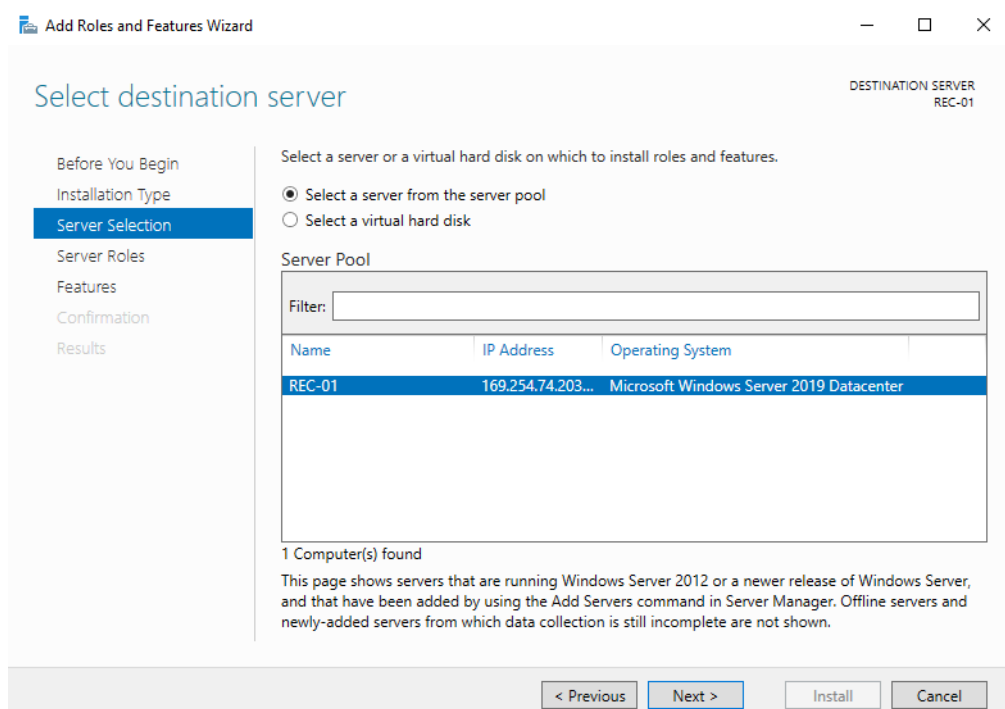


Fig. 24: Server Selection

8. Under *Server Selection*, activate the option *Select a server from the server pool*.
9. Select your server from the pool of servers.
10. Click on the button *Next*.
⇒ The list of features appears.

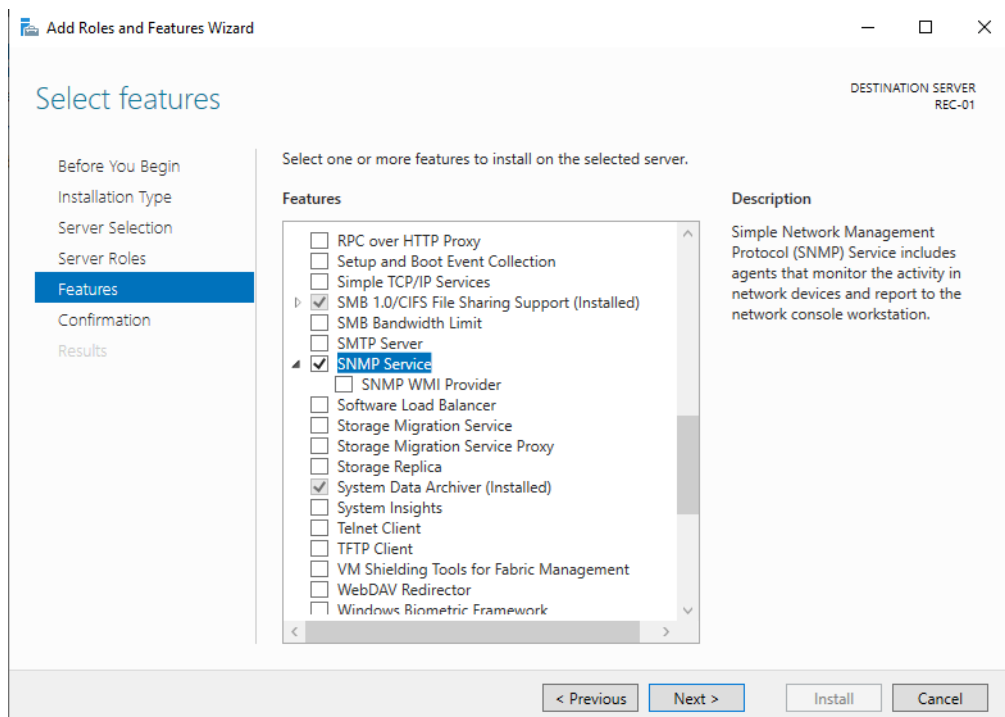


Fig. 25: Features - Activate SNMP service

11. Activate the option *SNMP Service*.
⇒ The window to select the tools opens.

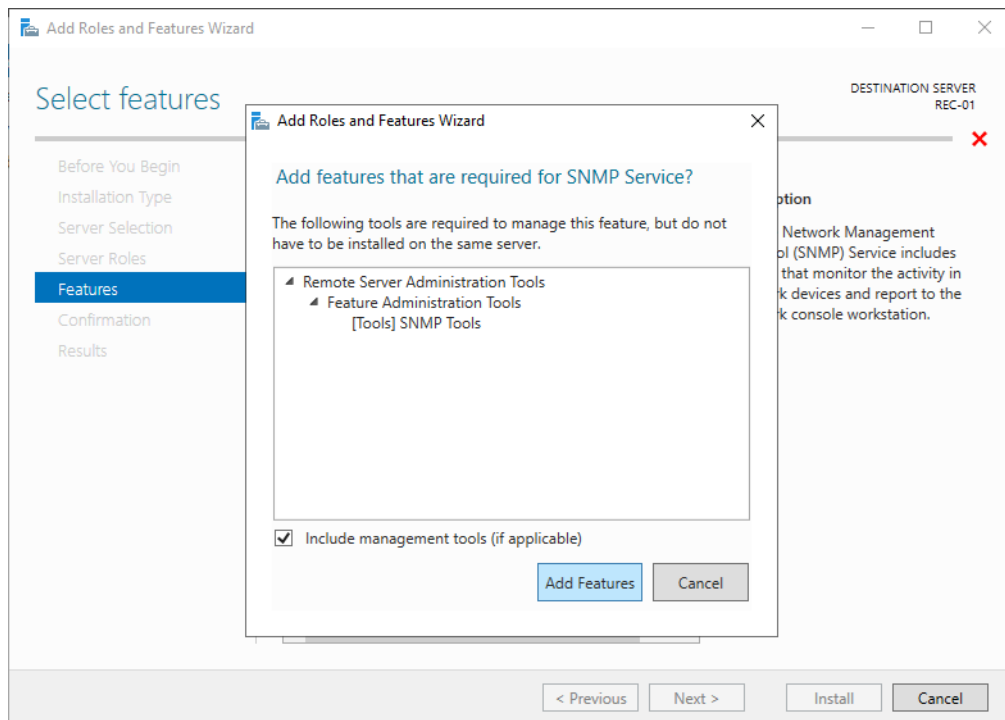


Fig. 26: **SNMP** service - Add remote server administration tools

12. Click on the button *Add Features* to add the administration tools.

⇒ The confirmation window appears.

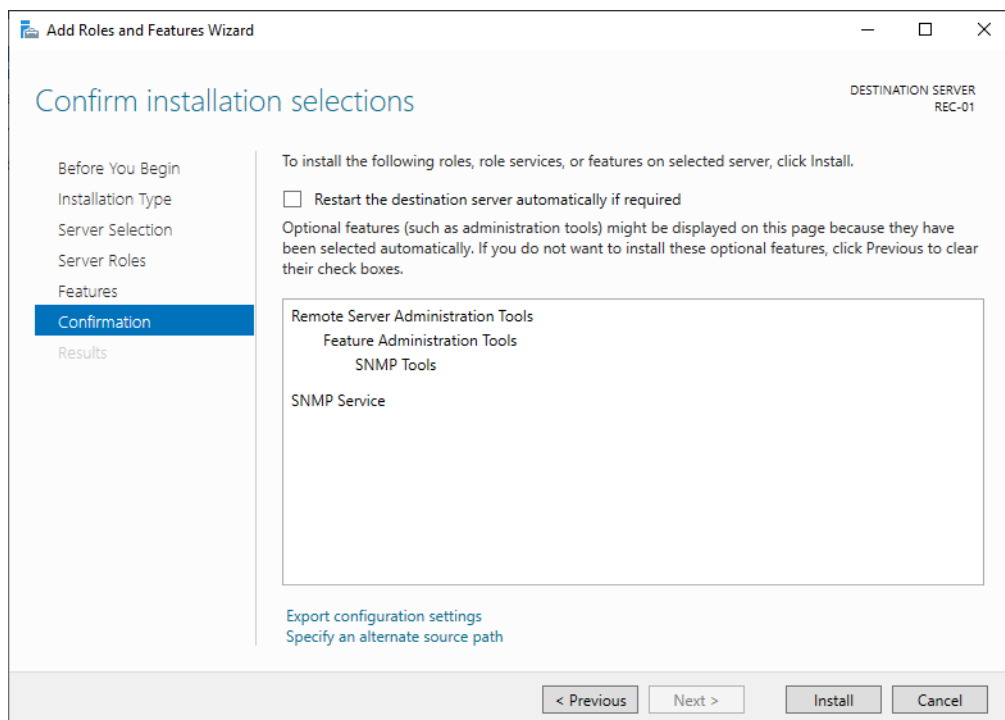


Fig. 27: Install **SNMP** service

13. Activate the option *Restart the destination server automatically if required*.

14. Click on the button *Install* to install the service.

⇒ The server is restarted after the installation.

5.5 Configure services

1. Open the *Server Manager* in the taskbar.

- Click on the menu item *Tools > Services*.

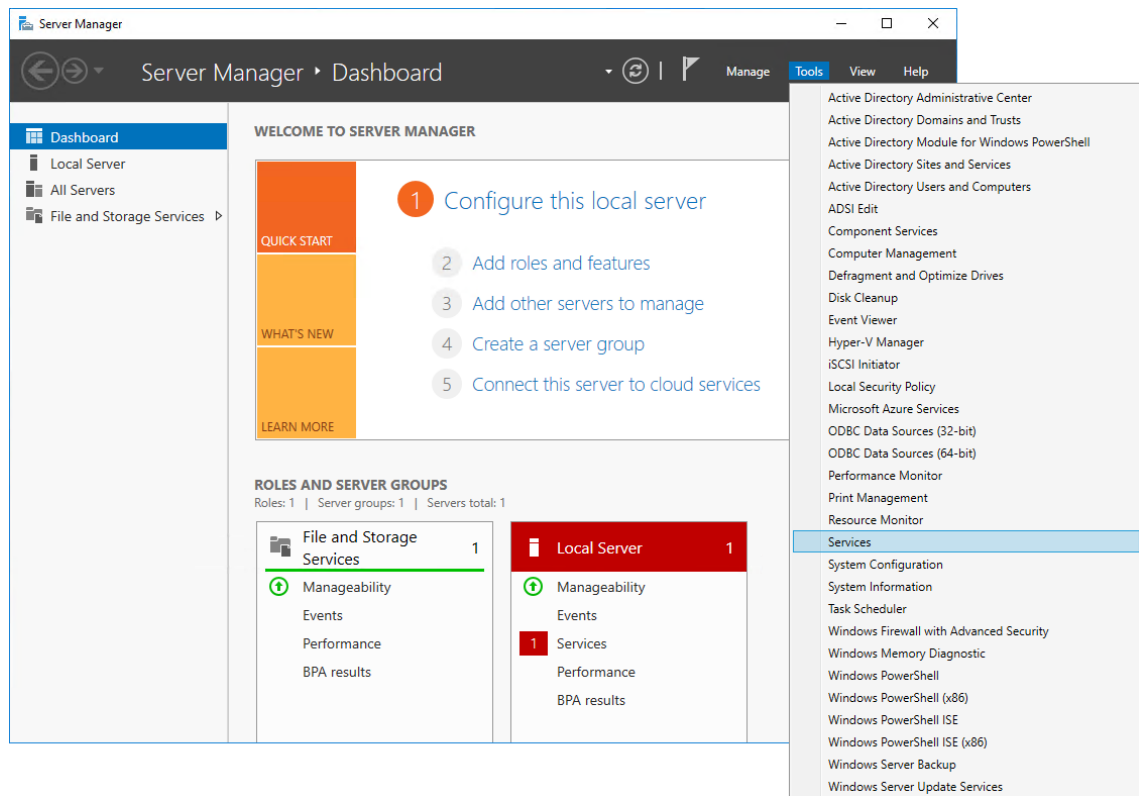


Fig. 28: Select services

5.5.1 Configure SNMP service

- Select the menu item *Properties* in the context menu of the **SNMP** service.
- In the tab *General*, select the *Startup type Automatic* from the drop-down list.

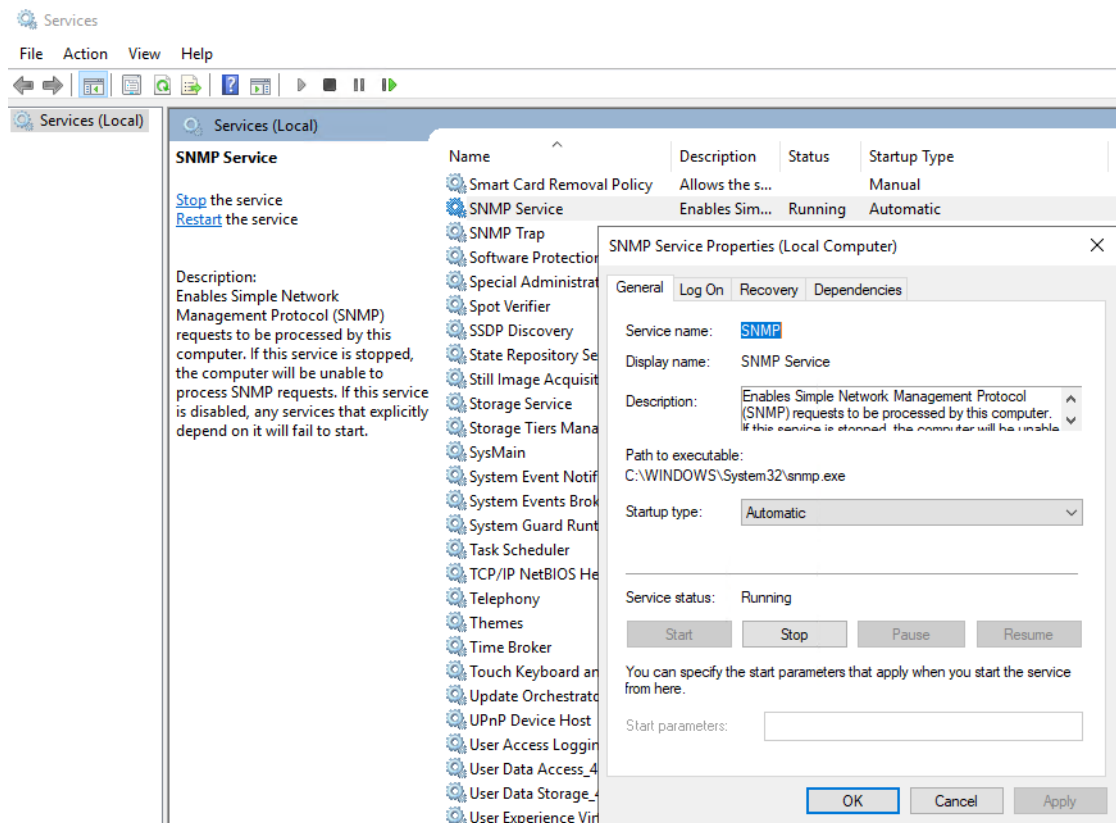


Fig. 29: Configure **SNMP** service - tab General

3. Click on the tab *Agent* to enter the contact data and the location.
4. Activate the check boxes in front of the services that you would like to monitor.

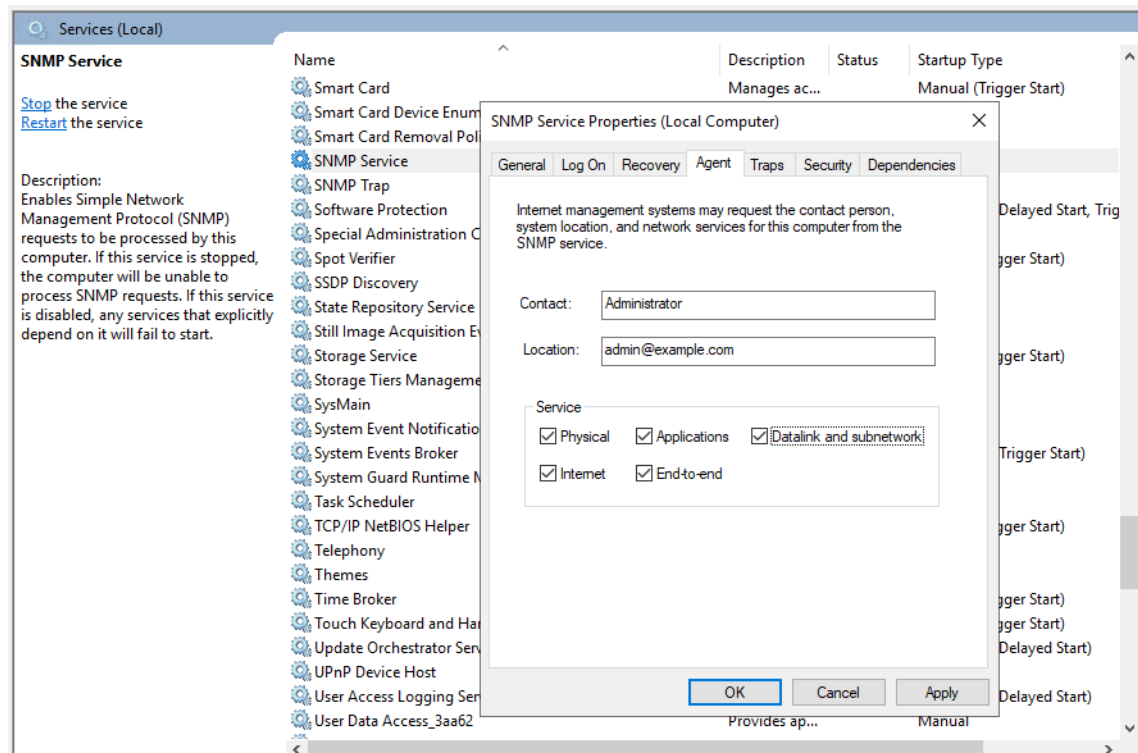


Fig. 30: Configure **SNMP** service - tab Agent

5. Click on the tab *Security* to grant the community read rights.

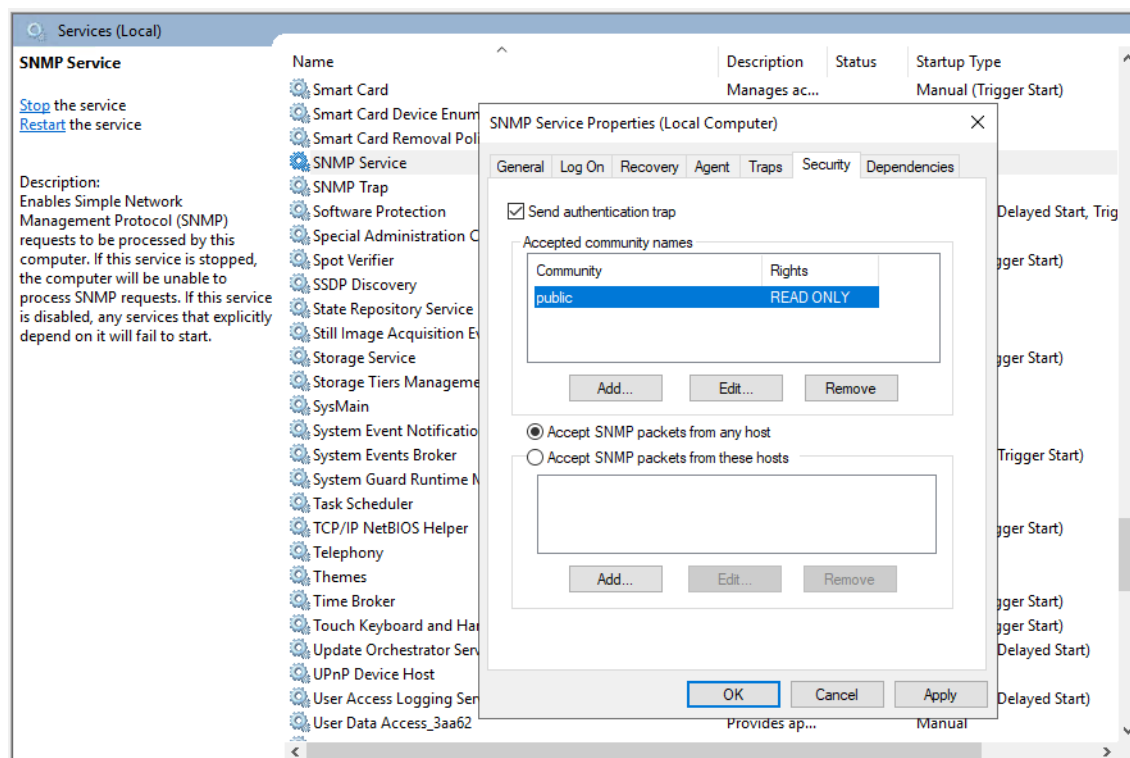


Fig. 31: Configure **SNMP** service - tab Security

6. Click on the button *Add*.
7. Enter the name of the community and click on the button *Add*.
8. Activate the option *Accept SNMP packages from any host*.
9. Eventually, click on the button *OK* to save the settings and to close the window.
10. Restart the **SNMP** service to apply the settings.

5.5.1.1 Execute script for notifications

ASC provides a script for setting the IP address of the **SNMP** recipient automatically.

The file `SQLInserter_Notif_SNMP.ex_` can be found in folder
`C:\Program Files (x86)\ASC\ASC Product Suite\scripts`.

1. Change the file extension `SQLInserter_Notif_SNMP.ex_` to `.exe`.
2. Execute the script on the server where the Enterprise Core with the database connection has been configured.
 - ⇒ The entry dialog with the IP address of the **SNMP** recipient opens.

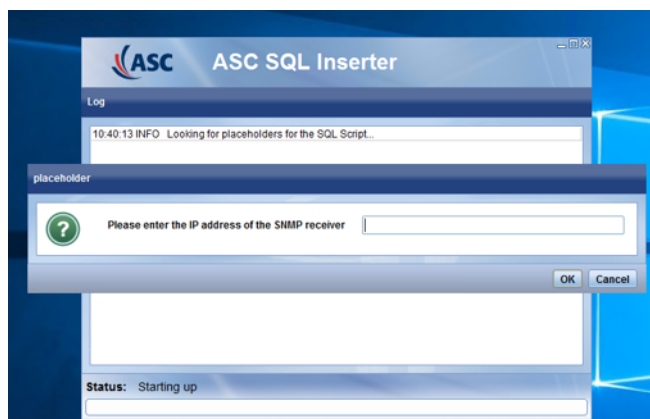


Fig. 32: SQL Inserter - IP address of the **SNMP** recipient

3. Enter the IP address of the **SNMP** recipient.
NOTICE! For Mitel, this must be a **MPA** Probe Address.
4. Click on the button **OK**.
 - ⇒ The script scans the ASC environment by means of the environment variable saved in the system and reads out all required information such as database type, user, and password.
- ⇒ A security prompt appears.



Fig. 33: SQL Inserter - Confirm security prompt

5. Confirm the security prompt to execute the script.
 - ⇒ Once the script has been executed, a security prompt appears.

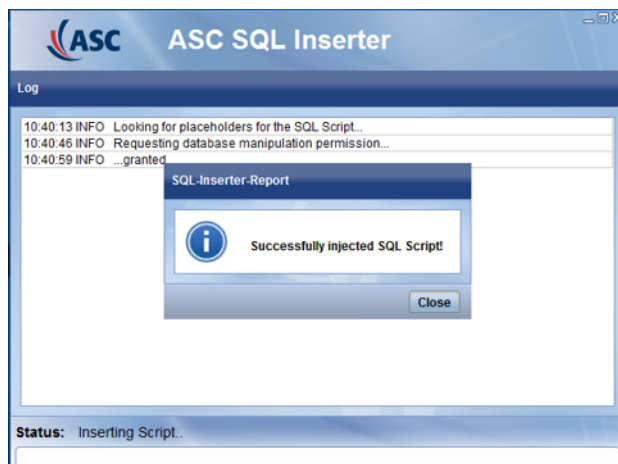










Fig. 34: SQL Inserter - Close success notification













6. Confirm the success notification.
 - ⇒ The **SNMP** traps for the following notifications are sent exclusively to the IP address of the **SNMP** recipient.

5.5.1.1.1 Notifications

Subject	Status	Description	Measures	Priority
CONFIGURATION_STATUS	!	The configuration is not correct. Please check the configuration parameters.	Check the configuration parameters.	↑ (High)
CONNECTION_STATUS	!	The service <i>name</i> on server <i>IP address</i> or <i>server name</i> is not available.	Reboot the affected server.	↑↑ (Very high)
CONVERSATION_STREAM_MISSING		One or several streams are missing in the conversation <i>conversation ID</i> (recording issue).	Contact ASC support at +49 700 27278776.	↑ (High)
CORE_AVAILABILITY_STATUS	!	The server is not available.	Check the server.	↑↑ (Very high)
CTICONNECT_MODULE_STATE	!	The module Neo <i>application</i> for the PBX <i>name</i> is not ready for operation.	Reboot the affected server.	↑↑ (Very high)
CTICONNECT_MONITOR_POINTS_STATE	!	Monitoring in module Neo <i>application</i> has failed for <i>extension</i> .	Contact ASC support at +49 700 27278776.	↑ (High)
CTICONNECT_PBX_CONNECTION_STATE	!	The module Neo <i>application</i> is not connected with <i>name</i> .	Check the connection to the PBX .	↑↑ (Very high)
CTICONNECT_RC_CONNECTION_STATE	!	Recording Control is not connected.	Reboot the affected server.	↑↑ (Very high)
CTICONNECT_RECORDING_EXTENSIONS_STATE	!	Activating the recorder extensions in module Neo <i>application</i> has failed for <i>extension</i> .	Contact the PBX manufacturer and/or ASC support at +49 700 27278776.	↑ (High)
CTICONNECT_STREAM_REQUEST_FAILED		<p>* An error with code <i>error code</i> for <i>CTI-ID</i> in conversation <i>conversation ID</i> has occurred.</p> <p>NOTICE! This notification is an INFO notification for the feature <i>Recording Content Validation</i>. The feature <i>Recording Content Validation</i> allows checking recordings for functionality.</p>	Contact the PBX manufacturer and/or ASC support at +49 700 27278776.	↑ (High)
DATABASE_BACKUP_STATE	!	An error occurred while backing up the database.	Check whether there is enough storage space for a database backup.	↑↑ (Very high)
DATABASE_CONNECTION_ERROR		The primary database has failed.	Check the database.	↑↑ (Very high)

Subject	Status	Description	Measures	Priority
DB_DRIVE_SPACE		* The size of the database currently is <i>storage space</i> GB. In addition, there is external data on the partition with <i>used storage space</i> GB. As a result, the free storage space of the database partition currently is <i>free storage space</i> GB.	Make more storage capacity available to the database partition.	 (Very high)
DB_DRIVE_SPACE		* The size of the database currently is <i>storage space</i> GB. In addition, there is external data on the partition with <i>used storage space</i> GB. As a result, the free storage space of the database partition currently is <i>free storage space</i> GB.	Make more storage capacity available to the database partition.	 (High)
DRIVE_SPACE		* Drive <i>name</i> has reached the storage capacity of <i>free storage</i> GB. The deletion process now starts to delete not archived/expanded/transferred calls.	To provide more storage capacity, <ul style="list-style-type: none"> • assign the tenant more storage capacity, or • archive the data, or • transfer data to a storage expansion. 	 (High)
DRIVE_SPACE		* On drive <i>name</i> only <i>free storage</i> GB remains. On drive <i>name</i> only <i>free storage</i> GB remains. Attention! When the capacity reaches the error level, calls which have not been archived/not been moved to an expansion/not been transferred are deleted.	The error level will be reached soon. If the drive is the callpool, archiving or copying to a <i>storage expansion</i> can be configured to avoid loss of data. If it is a different drive other than the callpool, <ul style="list-style-type: none"> • increase the drive capacity, or • manually delete data to make sufficient capacity available. NOTICE! The following capacity values are recommended when configuring the drive: <ul style="list-style-type: none"> • Capacity level: 15 % of drive capacity • Warn level: 10 % of drive capacity • Error level: 5 % of drive capacity 	 (High)

Subject	Status	Description	Measures	Priority
			For information about the configuration of drives refer to the administration manual for system providers <i>System Configuration - Configuration drives</i> .	
FILEMAN_INVALID_PACKAGE_FOUND		* The package <i>name</i> is invalid.	Contact ASC support at +49 700 27278776.	↑ (High)
JOB_EXECUTION_ERROR		* While executing the job <i>job name</i> of job type <i>job type</i> the following error occurred. The job execution announced: <i>description</i>	Contact ASC support at +49 700 27278776.	↑ (High)
JOB_EXECUTION_UNKNOWN		* While executing the job <i>job name</i> of job type <i>job type</i> an unknown error occurred. The job execution announced: <i>description</i>	Contact ASC support at +49 700 27278776.	↑ (High)
LDAP_CONNECTION	!	* The connection to the LDAP server could not be established. The <i>cause</i> is filled dynamically.	Contact your IT administrator to check which error is affects the LDAP connection.	↑ (High)
LICENSE_FILE_VALIDATION	!	The license file is invalid.	Request a new license file. ATTENTION! A missing license file will cause loss of data after 30 days after having received this notification.	↑ (High)
LICENSING_AUTHENTICATION_SERVER	!	The authentication server is not connected. You need an authentication server for key management or VM support. The system will expire in <i>number with unit</i> . The connection to the authentication server could not be established. Please check the connection data and the configuration of the firewall. The authentication server is not connected. You need an authentication server for key management or VM support.	If a dongle has been configured, check whether the dongle is connected. If licensing has been configured via a direct Internet connection to the LMS (ASC Licensing Management Service), check whether the IP address of the LMS has been configured and whether the Firewall accepts a connection. If the problem continues to exist, restart the service <i>DongleManConnector</i> .	↑ (High)
RECORDING_EXTENSION_STATE	!	* Module <i>name</i> could not register any of the SIP phone numbers on the PBX.	Check the configuration of the SIP registration in the System Configuration and on the PBX.	↑ (High)

Subject	Status	Description	Measures	Priority
RECORDING_EXTENSION_STATE		* Module <i>name</i> could not register the following phone numbers on the PBX: <i>description</i> .	Check the configuration of the SIP registration in the System Configuration and on the PBX.	 (Medium)
RECORDING_FILE_ERROR		* The following error occurred while writing the file <i>name</i> for the module <i>name</i> : <i>error code</i>	Contact ASC support at +49 700 27278776.	 (High)
RECORDING_MODULE_RC_CONNECTION_STATE		The recording module <i>name</i> has lost the connection to Recording Control.	Contact ASC support at +49 700 27278776.	 (High)
RECORDING_MODULE_STATE		The module <i>name</i> is not available. <i>Description</i> .	Reboot the affected server.	 (Very high)
RECORDING_STREAM_DATA_MISSING		* The data for stream <i>stream ID</i> in conversation <i>conversation ID</i> is missing. NOTICE! This notification is an INFO notification for the feature <i>Recording Content Validation</i> . The feature <i>Recording Content Validation</i> allows checking recordings for functionality.	Contact ASC support at +49 700 27278776.	 (High)
RECORDING_STREAM_OPEN_FAILED		* Opening stream <i>stream ID</i> in conversation <i>conversation ID</i> has failed. NOTICE! This notification is an INFO notification for the feature <i>Recording Content Validation</i> . The feature <i>Recording Content Validation</i> allows checking recordings for functionality.	Contact ASC support at +49 700 27278776.	 (High)
TRUNK_STATE		Trunk <i>number</i> is not connected.	Check the cabling between recording card, PBX, and, if required, primary multiplex connection.	 (High)
UNCAUGHT_EXCEPTION		An unexpected error has occurred: <i>description</i>	Contact ASC support at +49 700 27278776.	 (High)

* A tenant-specific configuration is possible for this notification (option)

5.5.1.2 Configure Windows Defender Firewall for SNMP service

If you have installed and activated several [SNMP](#) services, you must configure different ports for them. The default port UDP 161 has been reserved for the [SNMP](#) service of the operating system.

Configure a different port for the Neo application in the System Configuration in the Tenants module. In the example *UDP 1161*. You must open this port in the Windows firewall.

1. Open the Windows firewall settings by clicking on *Control Panel > System and Security > Windows Defender Firewall*.

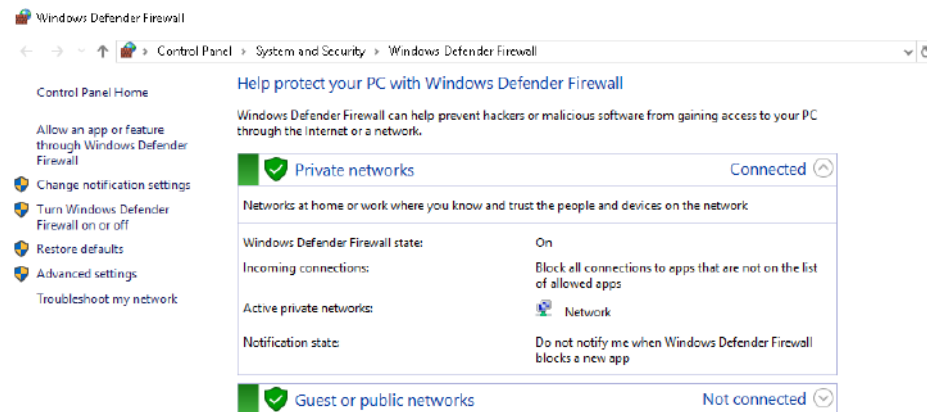


Fig. 35: Configure Windows Defender Firewall - Advanced settings

2. In the navigation bar, select the menu item *Advanced settings*.
3. In the navigation bar, select the menu item *Inbound Rules*.

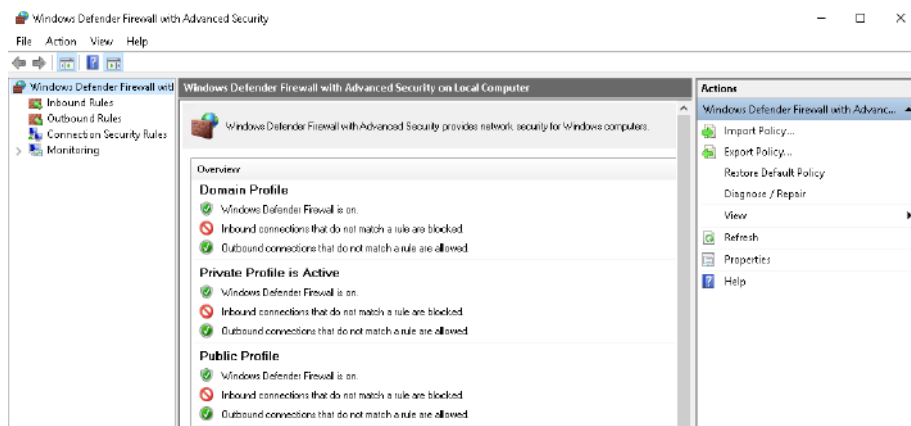


Fig. 36: Configure Windows Defender Firewall - Inbound Rules

4. From the list of rules, select the rule *ASC_SNMP-GET*.
5. Select the entry *Properties* from the context menu.
6. Select the tab *Protocols and Ports* to enter the settings.

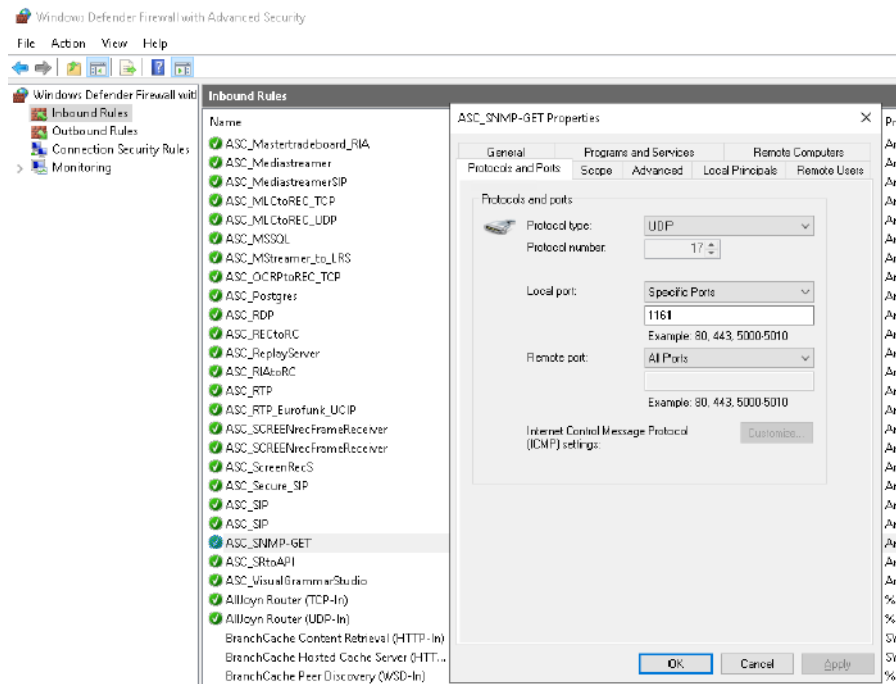


Fig. 37: Configure Windows Defender Firewall - Configure protocols and ports

7. From the drop-down list *Protocol type*, select the entry *UDP*.
8. From the drop-down list *Local port*, select the entry *Specific Ports* and enter the port, e.g. *1161*.
9. From the drop-down list *Remote port*, select the entry *Specific Ports* and enter the port, e.g. *1161*.
10. Click on the button *OK* to apply the settings.
11. From the list of services, select the entry *SNMP Service (UDP In)* with the profile *Private, Public*.
12. Select the entry *Properties* from the context menu.
13. Click on the tab *Advanced*.

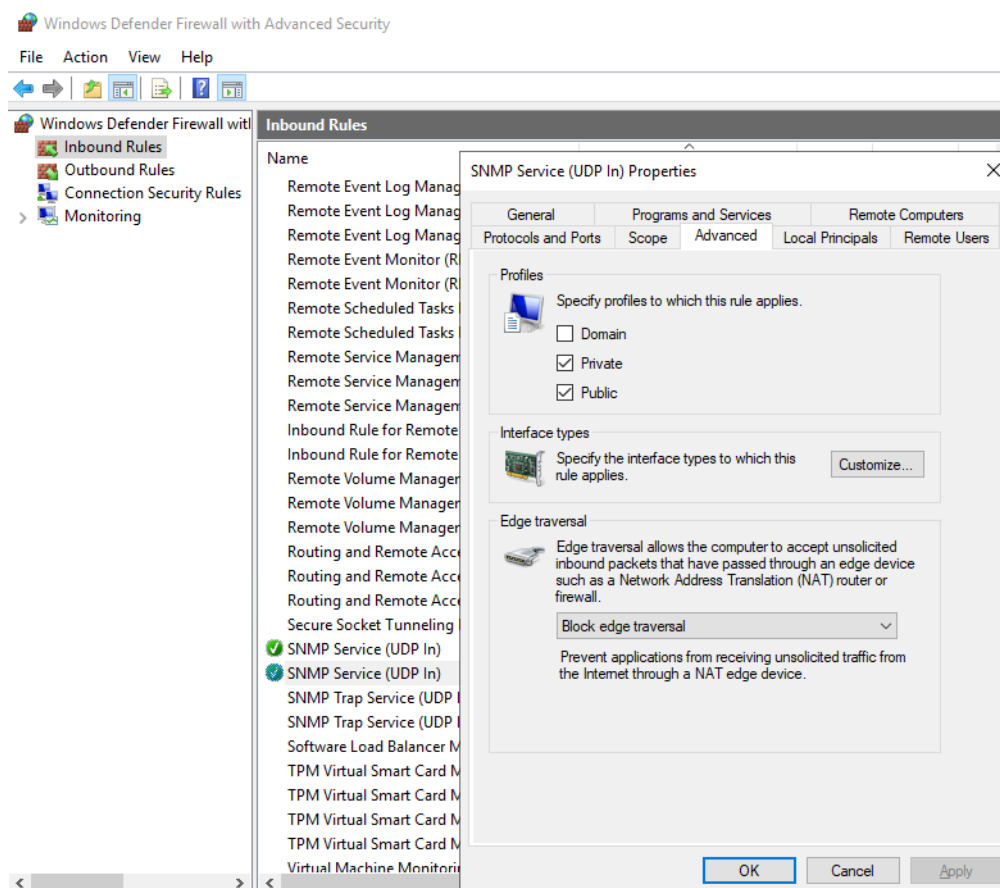


Fig. 38: Configure Windows Defender Firewall - Check SNMP service (UDP In)

14. Confirm that the rule has been activated for the following profiles:

- *Private*
- *Public*

15. Click on the button *OK* to close the window.

5.5.1.3 Configure SNMP service in Neo

Configuration in the Neo application

You must configure and assign the [SNMP](#) service to the tenant as system administrator in the System Configuration in the Tenants module.



For information about the configuration refer to the administration manual *System Configuration - User management for system providers*.

5.5.2 Configure Microsoft Windows Time

Since ASC uses a time emitter system based on [NTP](#), the Windows time emitter service has to be deactivated. Proceed as follows:

1. Right-click on the entry *Windows Time*.
⇒ A context menu appears.
2. Click on *Properties* in the context menu.

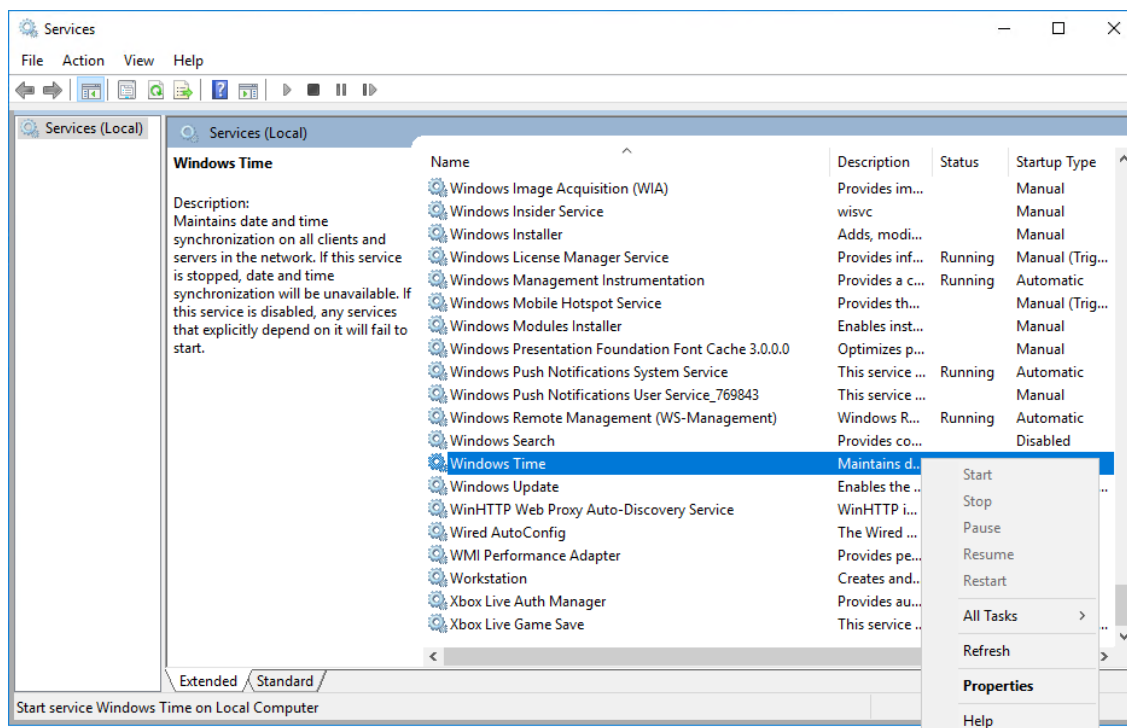


Fig. 39: Open window “Windows Time Properties”

3. Click on the tab *General*.
4. In the window *Windows Time Properties* under *Startup type*, select the option *Disabled*.
5. Check whether the *Service status* has been set to the mode *Stopped*. If this is not the case, stop the service by clicking on the button *Stop*.

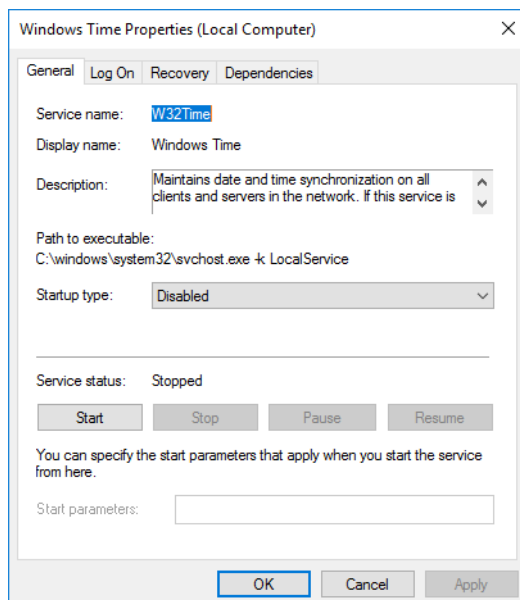


Fig. 40: Windows Time Properties

6. Click on the button *OK* to save the settings and to close the window.

5.5.3 Configure Microsoft Windows Audio (optional)

To allow a local replay on the server, the Microsoft Windows Audio Service has to be enabled. Proceed as follows:

1. Right-click on the entry *Windows Audio*.
⇒ A context menu appears.

2. Click on *Properties* in the context menu.

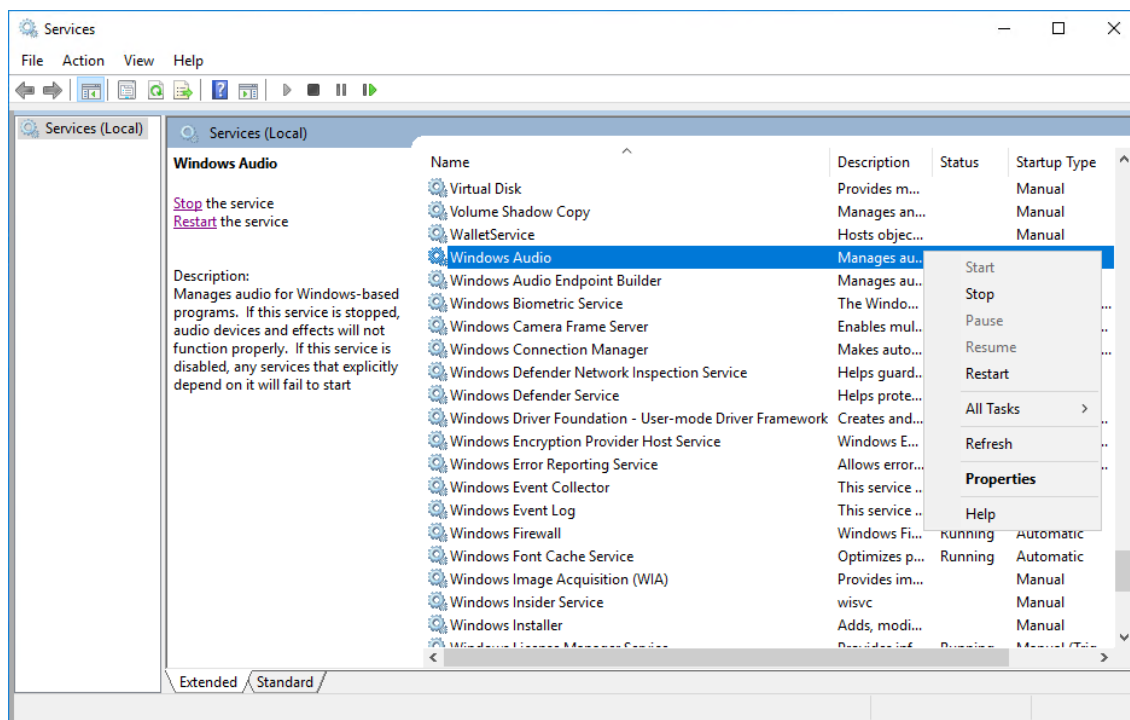


Fig. 41: Open the window "Windows Audio Properties"

3. Click on the tab *General*.
4. In the drop-down list *Startup type*, select the option *Automatic*.

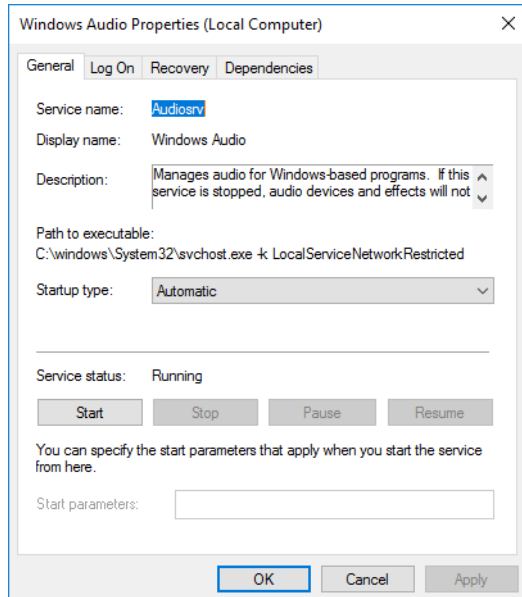


Fig. 42: Windows Audio Properties

5. Click on the button *OK* to save the settings and to close the window.

5.5.4 Configure Microsoft Windows firewall

During the Neo setup, the necessary port to be opened will be entered automatically if the firewall has been activated.



For information about the communication matrix (port configuration) see installation manual *Installation requirements*.

To start the service *Windows Firewall*, proceed as follows:

1. Right-click on the entry *Windows Firewall*.
⇒ A context menu appears.
2. Click on *Properties* in the context menu.

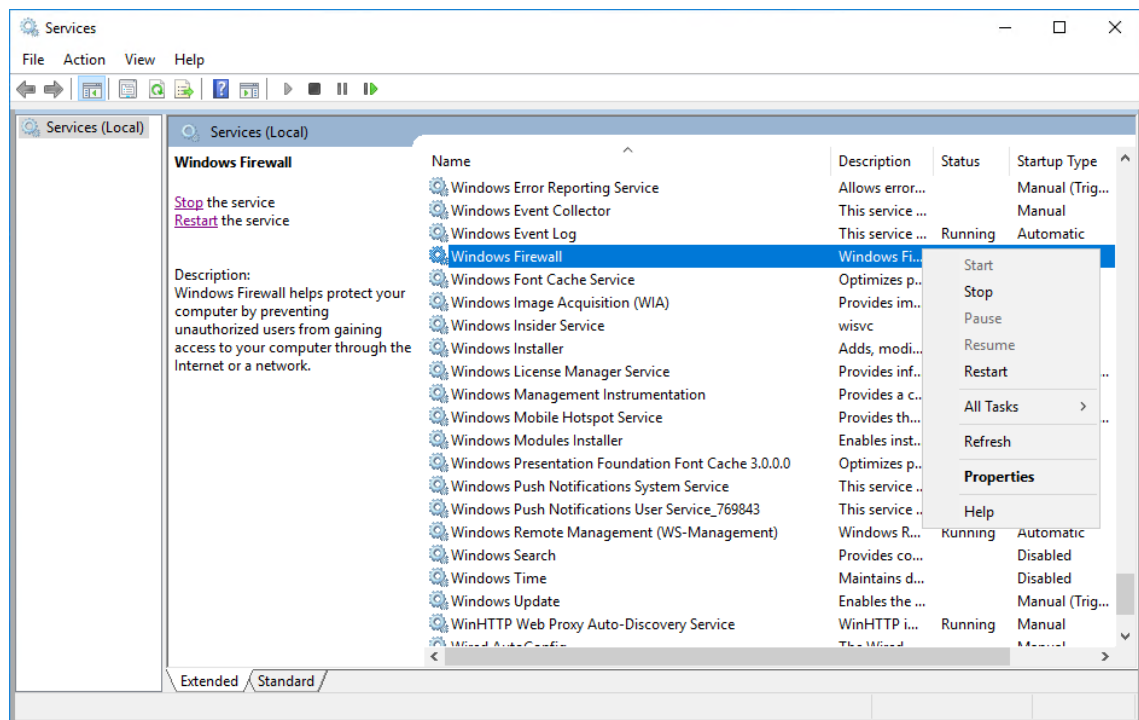


Fig. 43: Open window “Windows Firewall Properties”

3. Click on the tab *General*.
4. Click on the button *Start*.

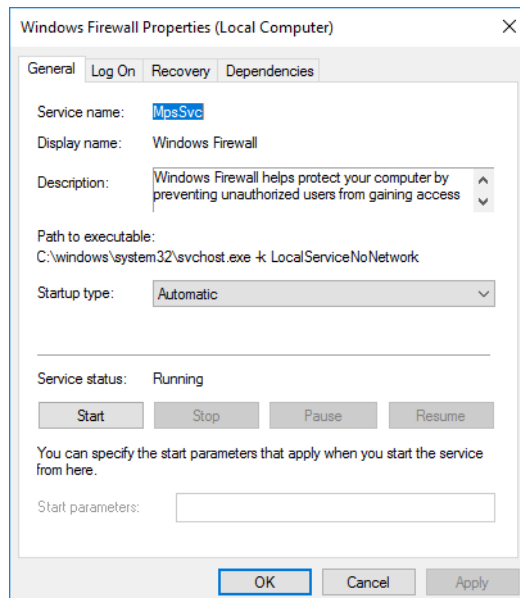


Fig. 44: Windows Firewall Properties

5. In the drop-down list *Startup type*, select the option *Automatic* if the service *Windows Firewall* is supposed to be started automatically upon starting Microsoft Windows.
6. Click on the button *OK* to save the settings and to close the window.

5.6 Enable script hosts

To check whether script hosts have been enabled and to configure scrip hosts if required, proceed as follows:

1. Press the Windows icon key.
2. Enter *regedit.exe*.
3. In the list of search results above, right-click on *regedit.exe*.
⇒ A context menu appears.
4. In the context menu, click on the menu item *Execute as administrator*.
5. Change to the path *HKEY_LOCAL_MACHINE > Software > Microsoft > Windows Script Host > Settings*.
6. If the entry *Enabled* is not displayed in the main view, you do not have to continue the configuration of the script hosts.
If the entry *Enabled* is displayed in the main view, proceed as follows:
7. Double-click on the entry *Enabled*.
8. In the entry field *Value Data*, enter the value *1*.

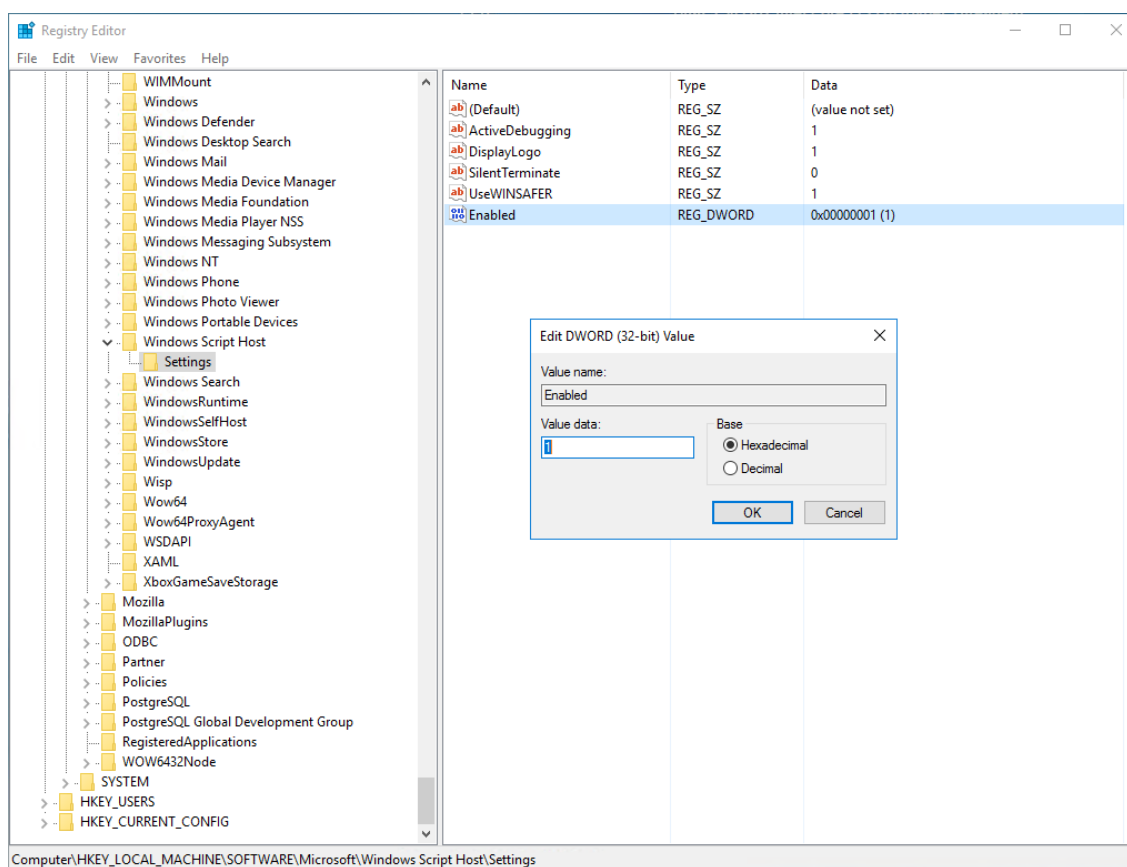


Fig. 45: Enable script hosts

9. Click on the button *OK* to save the entries and close the window.

5.7 Configure maximum password age

1. Press the Windows icon key.
2. Enter *gpedit.msc*.
3. In the list of search results above, right-click on *gpedit.msc*.
⇒ A context menu appears.
4. Click on *Run as administrator* in the context menu.

⇒ The window *Local Group Policy Editor* opens.

5. Change to the path *Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy*.

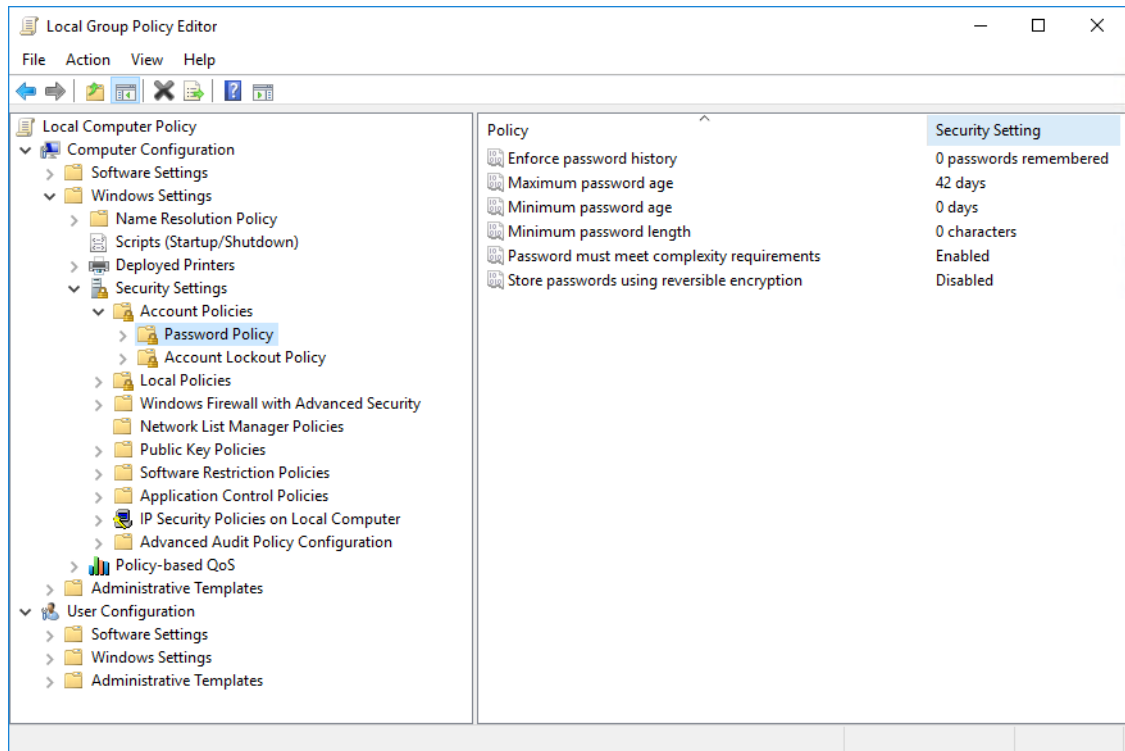


Fig. 46: Local Group Policy Editor

6. In the main view, right-click on *Maximum password age*.

⇒ A context menu appears.

7. Click on *Properties* in the context menu.

8. Under *Password will expire* enter the value *0*.

⇒ The description now says *Password will not expire*.

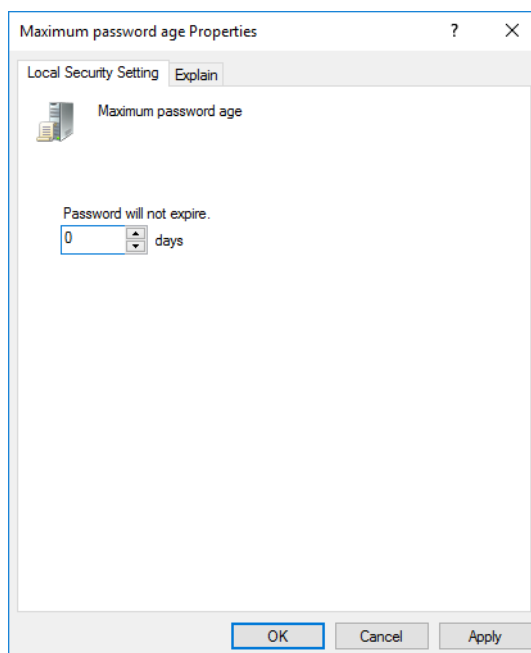


Fig. 47: Maximum password age Properties

9. Click on the button *OK* to save the entries and close the window.

5.8 Deactivate write cache for hard disk

1. Press the Windows icon key.
2. Open the system configuration by clicking on *Control Panel > All Control Panel Items > System*.
3. Click on the shortcut *Device Manager*.

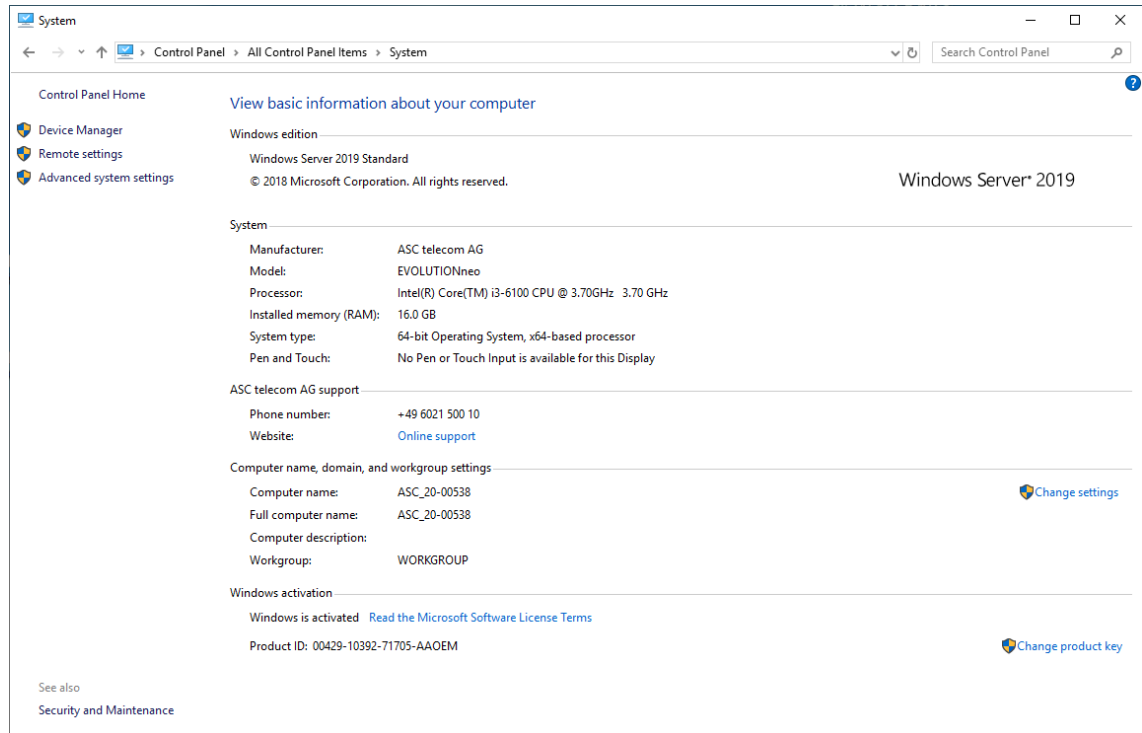


Fig. 48: System

4. Open the menu item *Disk drives* in the structure view.
5. Right-click on the hard disk where the database data has been saved.
⇒ A context menu appears.
6. Click on the menu item *Properties* in the context menu.

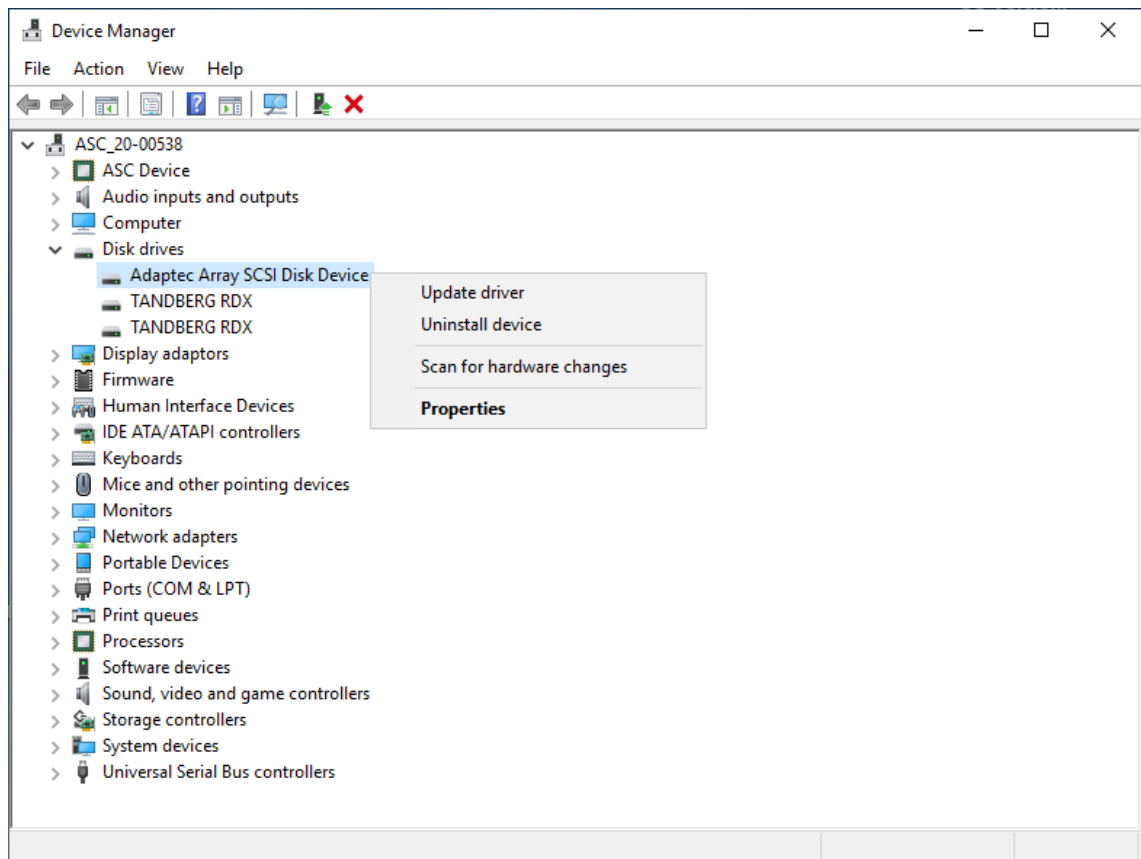


Fig. 49: Device Manager

7. Click on the tab *Policies*.
8. Deactivate the option *Enable write cache on the device*.

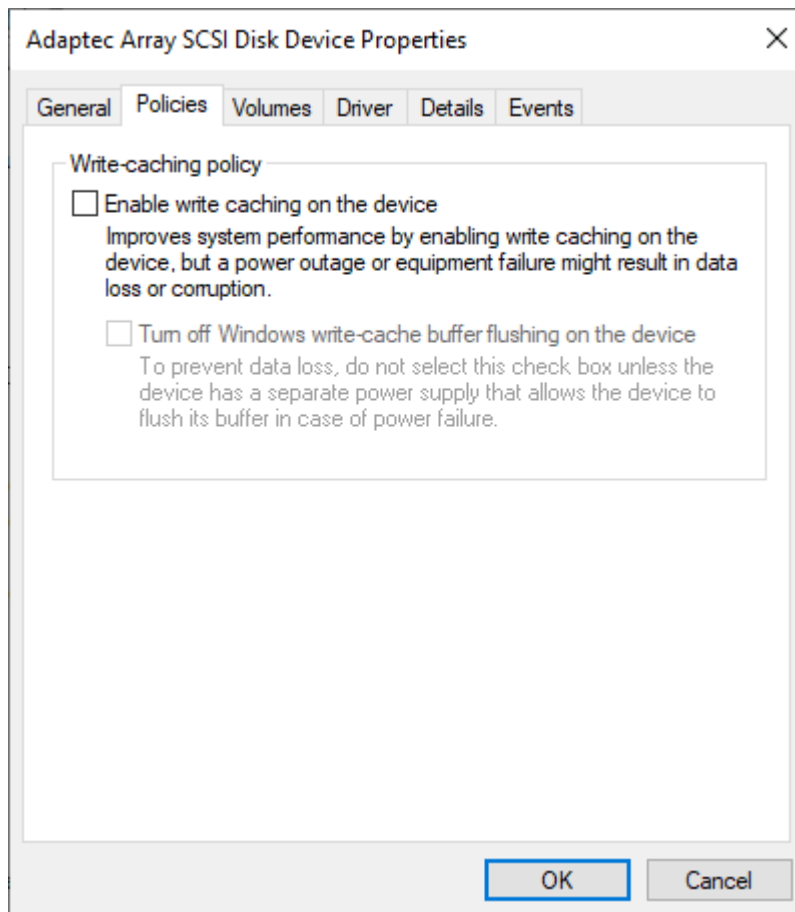


Fig. 50: Properties of hard disk

9. Click on the button **OK**.

6 Quick guide

6.1 General requirements

- 3 partitions:
At least 60 GB for the system partition
At least 40 GB for the database partition
At least 150 GB for the data partition

6.2 Observe the following after the installation of Microsoft Windows Server 2019

- Configure network card:
Windows icon key > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings > NIC > right-click NIC > Properties > Internet Protocol, Version 4 (TCP/IPv4) > Properties > Use the following IP address > enter IP address, subnet mask, default gateway > OK > Configure > Power Management > deactivate Allow the computer to turn off this device to save power
if no **sniffer card** > **OK**.
Configure **sniffer card** for passive recording:
> Advanced > Receive Buffers or Receive Descriptors > Value: enter maximum value: 1024-2048 (depending on the network card) > **OK**.
- . Install .NET framework:
Activate **Server Manager > Add roles and features > Next > Next > Next > Next > NET framework 3.5 Features > Next > Windows Explorer > This PC > right-click to copy folder path DVD > Open > \sources\jsx:** and change to the following window **Add Roles and Features Wizard > Specify an alternate source path > Path:** paste copied folder path > **OK > Install**.
- Install Media Foundation (optional):
Activate **Windows icon key > Control Panel > Programs and Features > Turn Windows features on or off > Next > Roles-based or feature-based installation activate > Next > Select a server from the server pool** and select your server and activate > **Next > Media Foundation > Install >** and reboot computer.
- Install SNMP service:
Activate **Windows icon key > Control Panel > Programs and Features > Turn Windows features on or off > Add roles and features > Next > Role-based or feature-based installation activate > Next > Select a server from the server pool** and select your server and activate > **Next > SNMP Service activate Add features > Restart the destination server automatically if required > Install >** and restart computer.
- Configure services:
Server Manager > Tools > Services >
 - Configure SNMP service:
right-click **SNMP Service > Properties > General > Start type:** Automatic > **Agent > activate services that you would like to monitor > Security > Add > enter name of the community activate > Add> Accept SNMP packages from any host > OK > restart SNMP service.**
 - Configure Windows Defender Firewall for SNMP service:
Select rule **Control Panel > System and Security > Windows Defender Firewall > Advanced settings > Inbound Rules > ASC_SNMP-GET > Properties > Protocols and Ports > Protocol type:** UDP > **Local type:** enter Specific Ports and port > **Re-**

mote port: enter **Specific Ports** and port > **OK** > right-click **SNMP Service (UDP)** > **Properties** > **Advanced** > ensure that profile **Private** and **Public** have been activated > **OK**.

- Configure Windows Time:

right-click **Windows Time** > **Properties** > **General** > **Startup type:** Disabled > **Stop** > **OK**.

- Configure Windows Audio (optional):

right-click **Windows Audio** > **Properties** > **General** > **Startup type:** Automatic > **OK**.

- Configure Windows firewall:

right-click **Windows Firewall** > **Properties** > **General** > **Start** > **Startup type:** Automatic > **OK**.

- Enable script hosts:

Windows icon key > enter **regedit.exe** > right-click on search result **regedit.exe** > **Run as administrator** > select path **HKEY_LOCAL_MACHINE** > **Software** > **Microsoft** > **Windows Script Host** > **Settings** >

If the entry **Enabled** is not displayed in the main view, you do not have to continue the configuration of the script hosts.

If the entry **Enabled** is displayed in the main view, proceed as follows: double-click **Enabled** > **Value Data** enter 1 > **OK**.

- Configure maximum password age:

Windows icon key > enter **gpedit.msc** > right-click on the search result **gpedit.msc** > **Run as administrator** > select path **Computer Configuration** > **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy** > right-click on **Maximum password age** > **Properties** > **Password will expire in:** enter value 0 > **OK**.

- Deactivate write cache for hard disk:

Windows icon key > **Control Panel** > **All Control Panel Items** > **System** open **Device Manager** in the **Disk drives** structure view > right-click on the hard disk where database data has been saved, deactivate > **Properties** > **Policies** > **Enable write caching on the device** > **OK**.

List of figures

Fig. 1	Network and Sharing Center	9
Fig. 2	Network Connections	10
Fig. 3	Network connection properties	10
Fig. 4	Internet Protocol Version 4 (TCP/IPv4) Properties (example)	11
Fig. 5	Network connection properties	11
Fig. 6	Network connection power management	12
Fig. 7	Network connection advanced properties (example)	12
Fig. 8	Server Manager	13
Fig. 9	Add Roles and Features Wizard	14
Fig. 10	Add Roles and Features Wizard	14
Fig. 11	Computer	15
Fig. 12	Copy source path for configuration settings	16
Fig. 13	Add Roles and Features Wizard	16
Fig. 14	Source path for configuration settings was pasted.	17
Fig. 15	Microsoft Windows options	17
Fig. 16	Add Roles and Features Wizard	18
Fig. 17	Installation type	18
Fig. 18	Server selection	19
Fig. 19	Features	19
Fig. 20	System control - Turn Windows features on	20
Fig. 21	Add roles and features	20
Fig. 22	Add Roles and Features Wizard	21
Fig. 23	Select installation type	21
Fig. 24	Server Selection	22
Fig. 25	Features - Activate SNMP service	22
Fig. 26	SNMP service - Add remote server administration tools	23
Fig. 27	Install SNMP service	23
Fig. 28	Select services	24
Fig. 29	Configure SNMP service - tab General	25
Fig. 30	Configure SNMP service - tab Agent	25
Fig. 31	Configure SNMP service - tab Security	26
Fig. 32	SQL Inserter - IP address of the SNMP recipient	26
Fig. 33	SQL Inserter - Confirm security prompt	27
Fig. 34	SQL Inserter - Close success notification	27
Fig. 35	Configure Windows Defender Firewall - Advanced settings	32
Fig. 36	Configure Windows Defender Firewall - Inbound Rules	32
Fig. 37	Configure Windows Defender Firewall - Configure protocols and ports	33
Fig. 38	Configure Windows Defender Firewall - Check SNMP service (UDP In)	34
Fig. 39	Open window "Windows Time Properties"	35
Fig. 40	Windows Time Properties	35
Fig. 41	Open the window "Windows Audio Properties"	36

Fig. 42	Windows Audio Properties	36
Fig. 43	Open window "Windows Firewall Properties".....	37
Fig. 44	Windows Firewall Properties.....	37
Fig. 45	Enable script hosts.....	38
Fig. 46	Local Group Policy Editor.....	39
Fig. 47	Maximum password age Properties.....	39
Fig. 48	System	40
Fig. 49	Device Manager	41
Fig. 50	Properties of hard disk	42

List of tables

Glossary

LDAP

Lightweight Directory Access Protocol

MPA

Mitel Performance Analytics

NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

PBX

Private Branch Exchange

SIP

Session Initiation Protocol

Sniffer card

A sniffer card is a network card approved by ASC for passive VoIP recording.

SNMP

Simple Network Management Protocol is a network protocol and serves to monitor and manage network components. The protocol does not depend on the IP network protocol for the transport. It sends notifications (traps) about the activities on the network components on its own accord.