

SafeDNS AD Agent environment configuration

The manual below describes the whole process of the preparation, configuration, and installation of the Agent under the Active Directory environment. The user operating system used is Windows 11 while the server version OS: Windows Server 2019 Standard.

Prerequisites: fresh installed Windows Server 2019 Standard, fresh installed Windows 11

Important Notice:

I: If the Active Directory is already installed and configured, while the Group Policy Management is not configured, please proceed with the installation of the Group Policy Management.

II: If the Active Directory and Group Policy Management are already installed and configured, please proceed to step 3 - Creating Users/Groups.

III: If the Active Directory and Group Policy Management are already installed and configured and Users/Groups exist, please proceed to step 4 - MSI File Preparation on the Server

Installing Agent in the AD environment without AD functionality

If you need to set up the Agent in the AD environment without using the AD functionality (e.g. adding AD users to SafeDNS Dashboard), you need the special build of the .msi file.

To get the special .msi build, please follow these steps:

1. Send the request for the .msi file to the Support (support@safedns.com) or your SafeDNS Manager.

The request should contain username, password and PIN code.

PIN code is required to enter the Agent GUI. If PIN is not provided, it will be generated randomly.

2. Wait until the .msi file is created and sent to you.

3. Upload the .msi file to the server and hosted in the folder that is available on the network to the end-user computer - we recommend setting the access level to Everyone.
4. Add the .msi file to the following path using the Group Policy Management console:
Computer Configuration > Policies > Software Settings > Software Installation

The .msi file installation will start after the end-user computer restart.

The installation can be forced by running the following command on the end-user computer:
gpupdate /force

This process for the NOAD agent installation follows exactly the same steps as described below. The only difference is that the NOAD agent uses credentials instead of an AD key and has the AD module disabled using the /noad key.

1. Server installation Part. Installation of the Roles and Features.

Start the Server Manager and initiate the installation of the Roles:

🏠 Dashboard

- 🖨️ Local Server
- 🖨️ All Servers
- 🖨️ File and Storage Services ▸



WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1

Configure this local server

2

Add roles and features

3

Add other servers to manage

4

Create a server group

5

Connect this server to cloud services

Hide

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

🖨️ File and Storage Services

1

📈

Manageability

Events

Performance

BPA results

🖨️ Local Server

1

📈

Manageability

Events

5

Services

Performance

BPA results

4/9/2024 12:13 AM

Before you begin

DESTINATION SERVER
SAFEDNS-2k19-test-AD

Before You Begin

[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:

[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

< Previous

Next >

Install

Cancel

Selecting Role-based or feature-based installation:

Select installation type

DESTINATION SERVER
SAFEDNS-2k19-test-AD

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

Selecting the local server from the Server Pool:

Add Roles and Features Wizard

DESTINATION SERVER
SAFEDNS-2k19-test-AD

Select destination server

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool

☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
SAFEDNS-2k19-test-AD	192.168.10.104	Microsoft Windows Server 2019 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

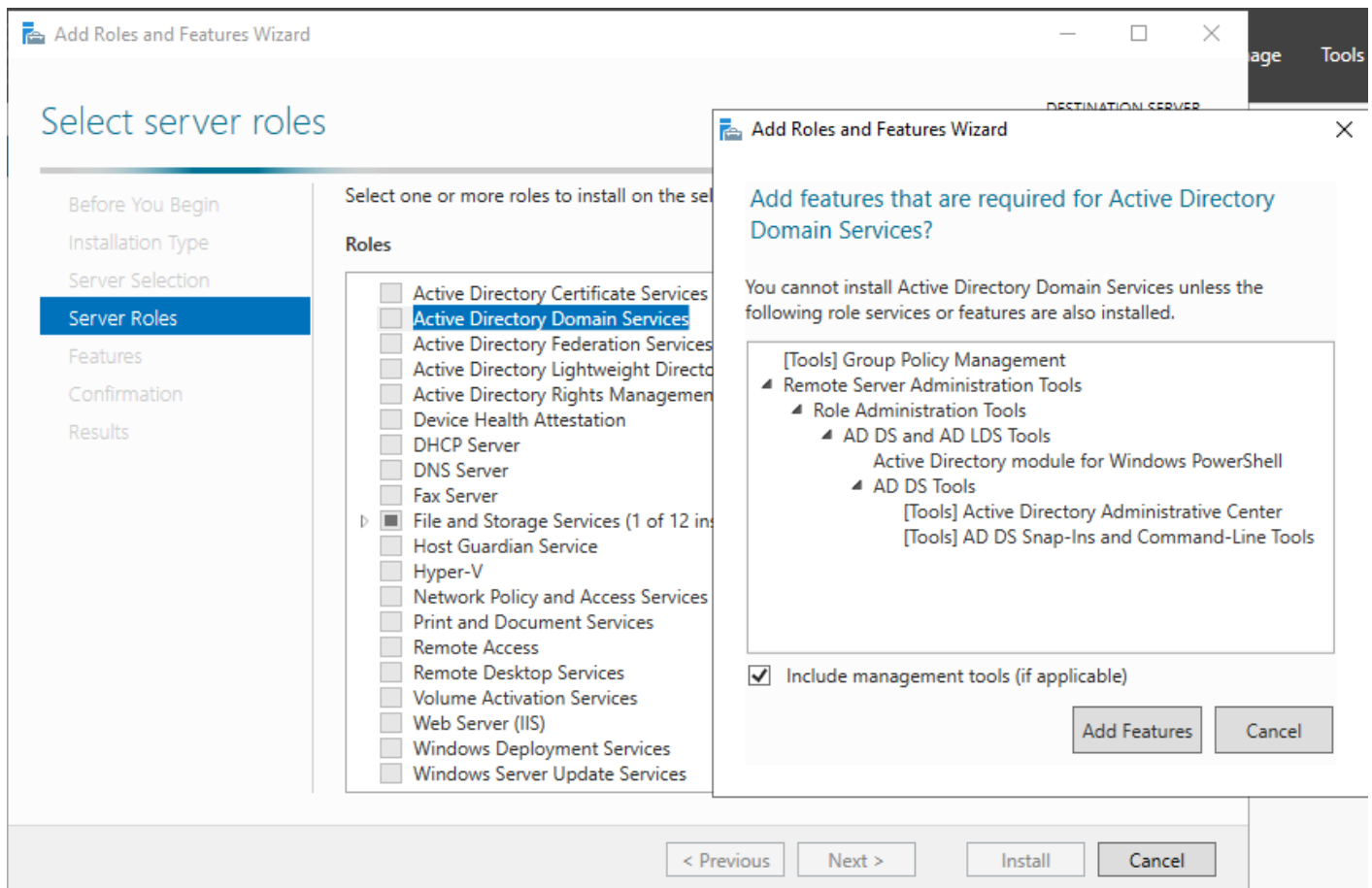
< Previous

Next >

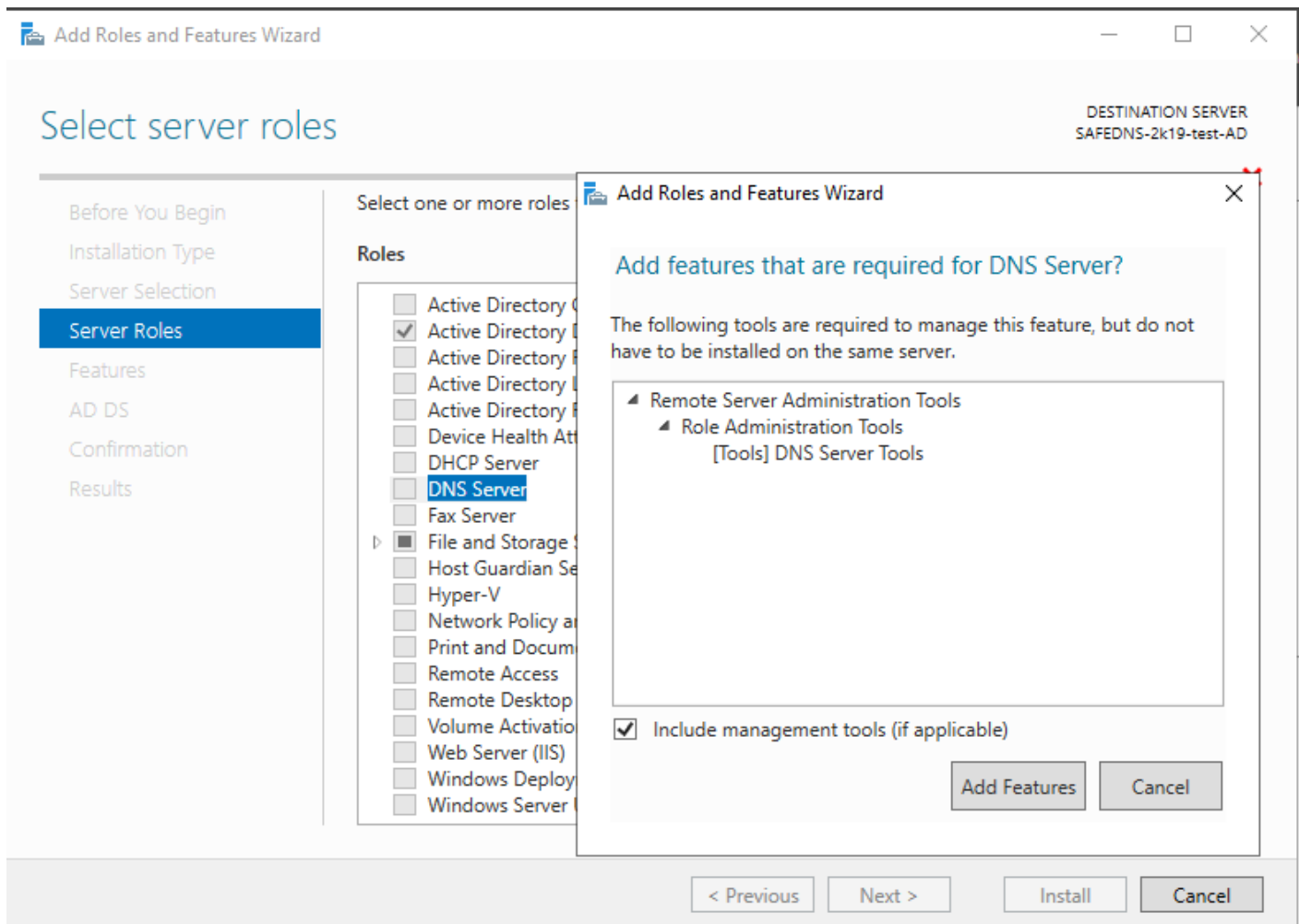
Install

Cancel

Selecting the Active Directory Domain Services role and in the small window taping the Add Features button:



The next step is to select the Role of the DNS Server, accepting the proposed Features list:



Accept the selected before Roles and tap the Next button:

Select server roles

DESTINATION SERVER
SAFEDNS-2k19-test-AD

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☒ DNS Server
- ☐ Fax Server
- ▷ ☒ File and Storage Services (1 of 12 installed)
 - ☐ Host Guardian Service
 - ☐ Hyper-V
 - ☐ Network Policy and Access Services
 - ☐ Print and Document Services
 - ☐ Remote Access
 - ☐ Remote Desktop Services
 - ☐ Volume Activation Services
 - ☐ Web Server (IIS)
 - ☐ Windows Deployment Services
 - ☐ Windows Server Update Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

Next >

Install

Cancel

Select the Group Policy Management feature:

Add Roles and Features Wizard

Select features

DESTINATION SERVER
SAFE DNS-2k19-test-AD

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results

Select one or more features to install on the selected server.

Features	Description
☐ .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
☒ .NET Framework 4.7 Features (2 of 7 installed)	
☐ Background Intelligent Transfer Service (BITS)	
☐ BitLocker Drive Encryption	
☐ BitLocker Network Unlock	
☐ BranchCache	
☐ Client for NFS	
☐ Containers	
☐ Data Center Bridging	
☐ Direct Play	
☐ Enhanced Storage	
☐ Failover Clustering	
☒ Group Policy Management	
☐ Host Guardian Hyper-V Support	
☐ I/O Quality of Service	
☐ IIS Hostable Web Core	
☐ Internet Printing Client	
☐ IP Address Management (IPAM) Server	
☐ iSNS Server service	

< Previous

Next >

Install

Cancel

Brief information about Azure Active Directory Domain Services(promo):

 Add Roles and Features Wizard

DESTINATION SERVER
SAFEDNS-2k19-test-AD

Active Directory Domain Services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

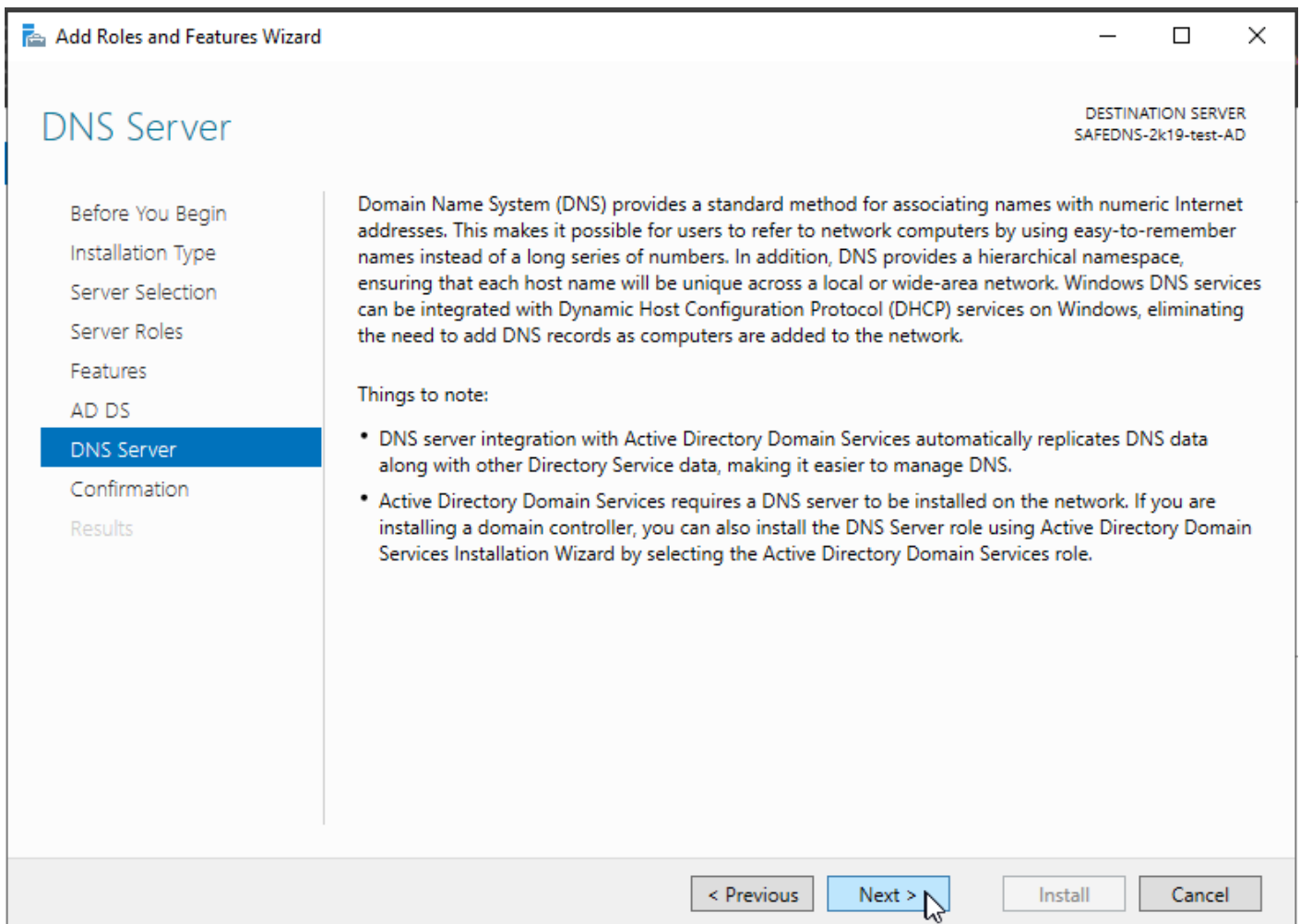
< Previous

Next >

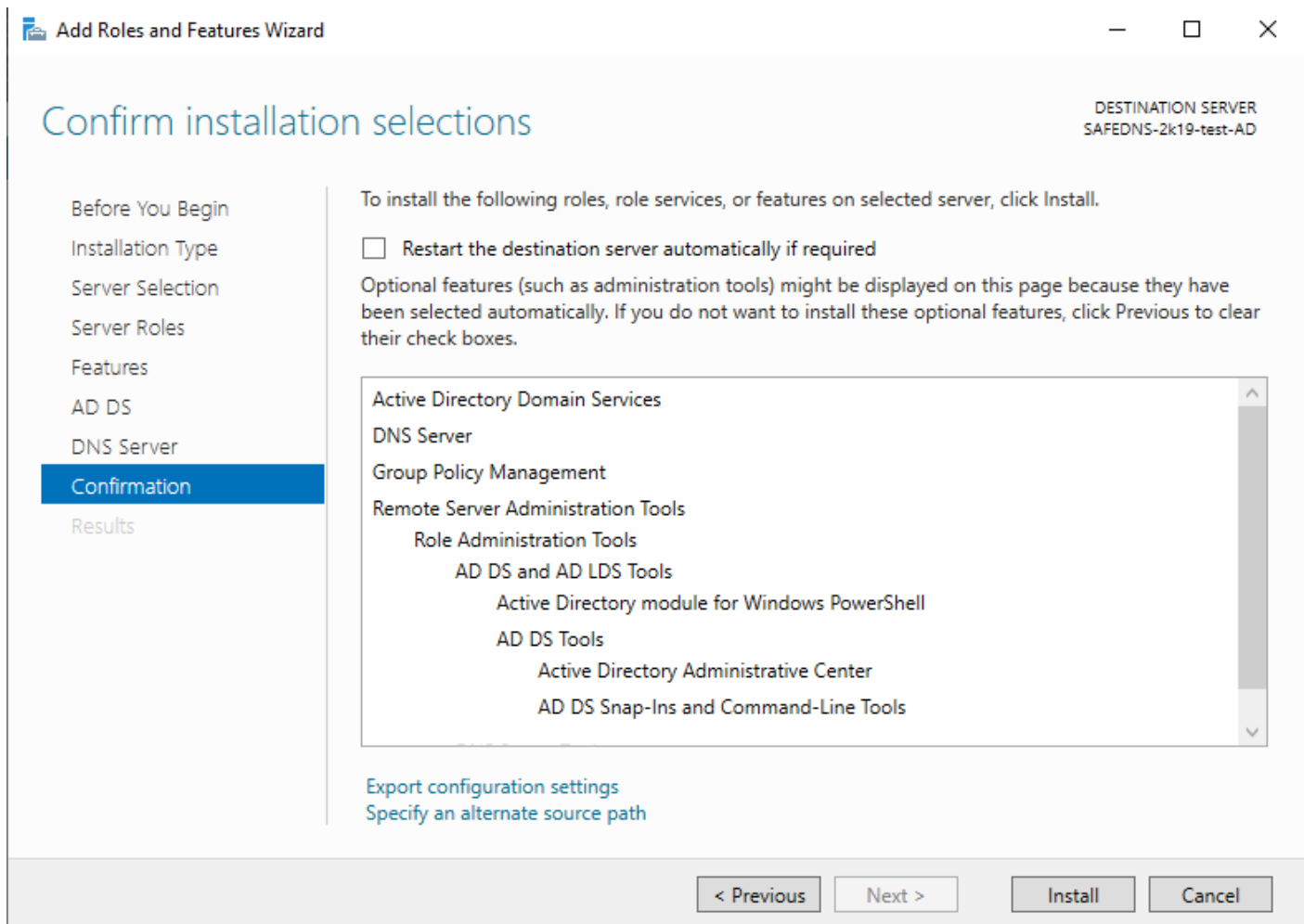
Install

Cancel

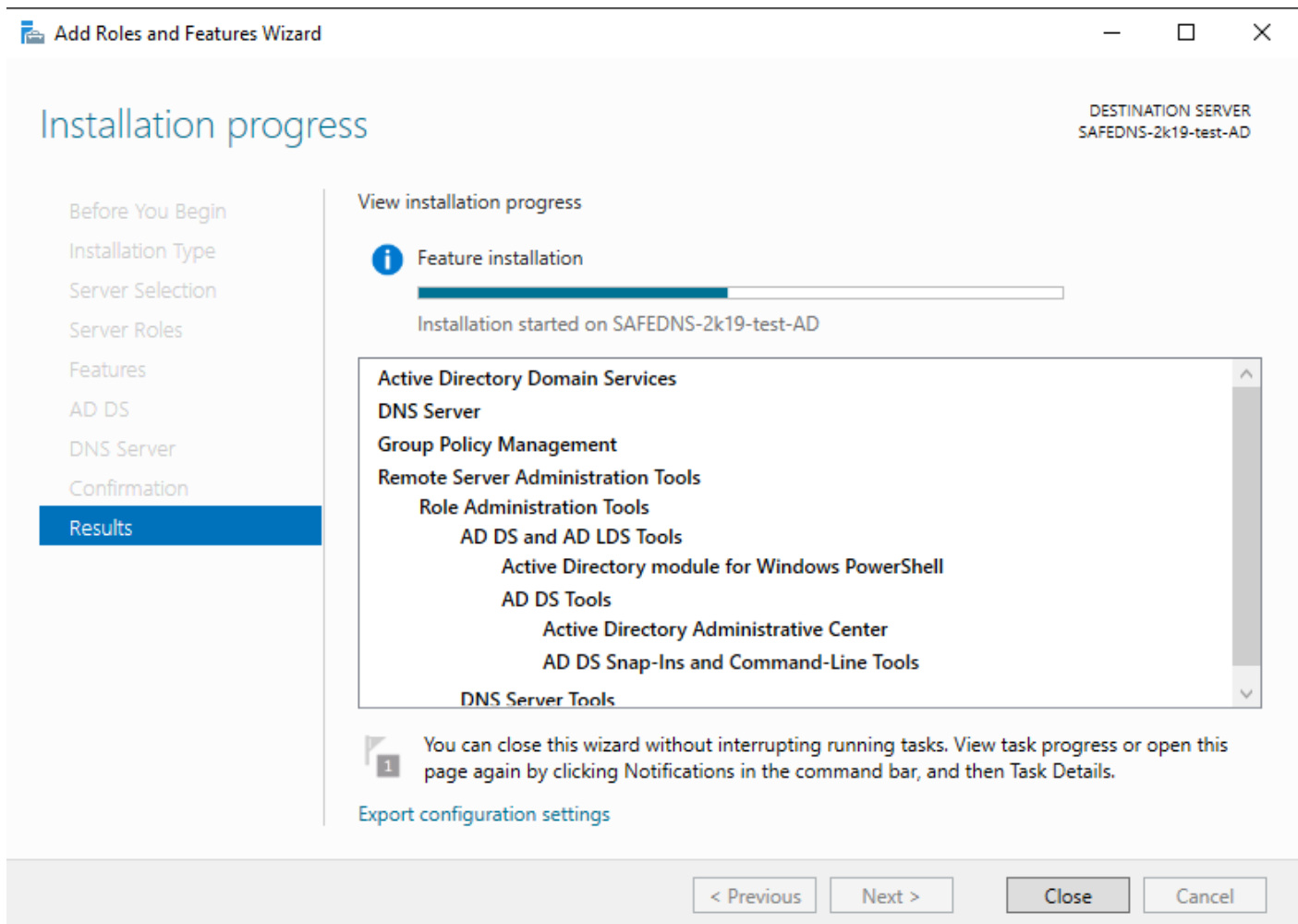
Brief information about installing DNS server:



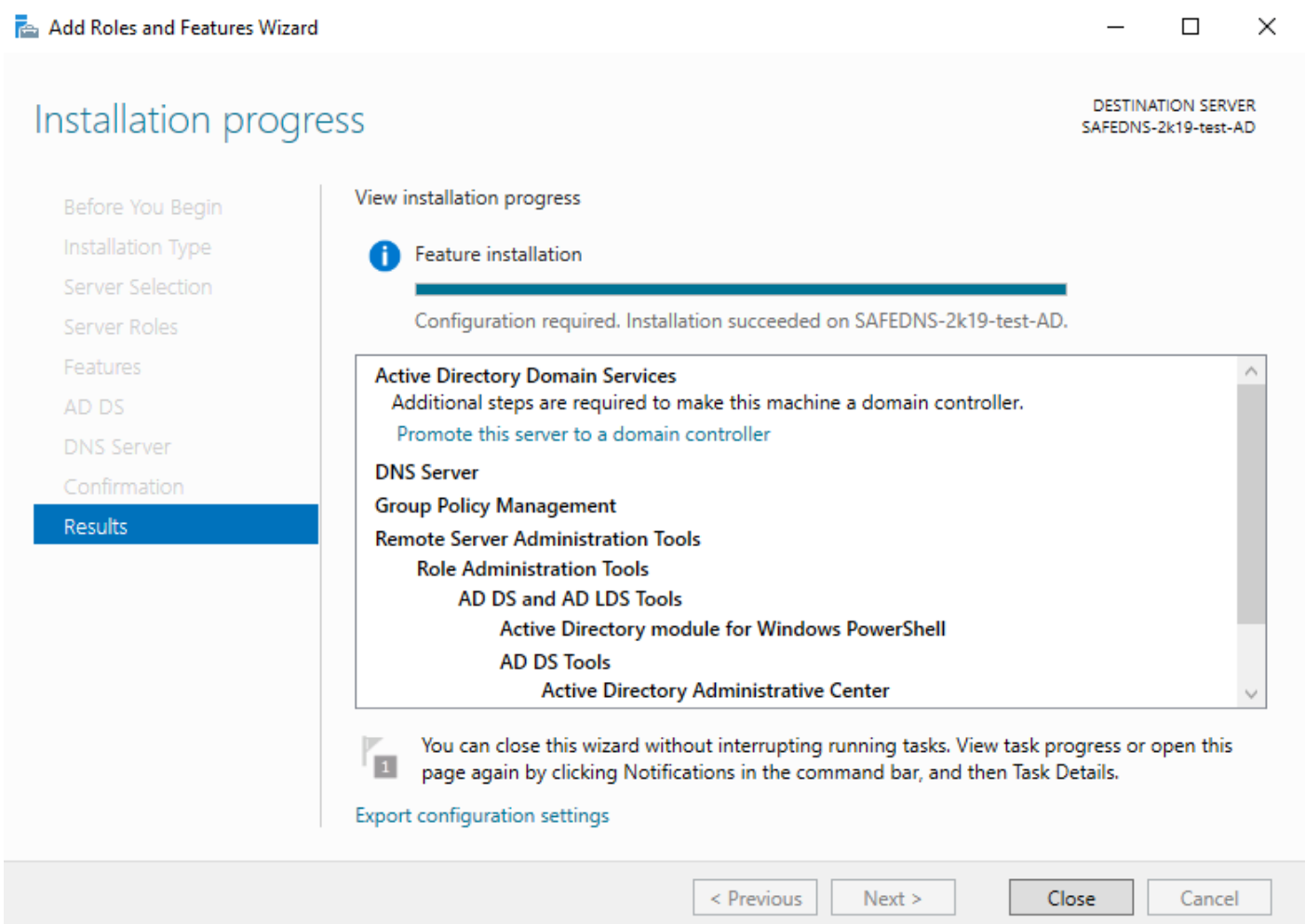
The summary with the list of installing Roles and Features:



The installation process begins:



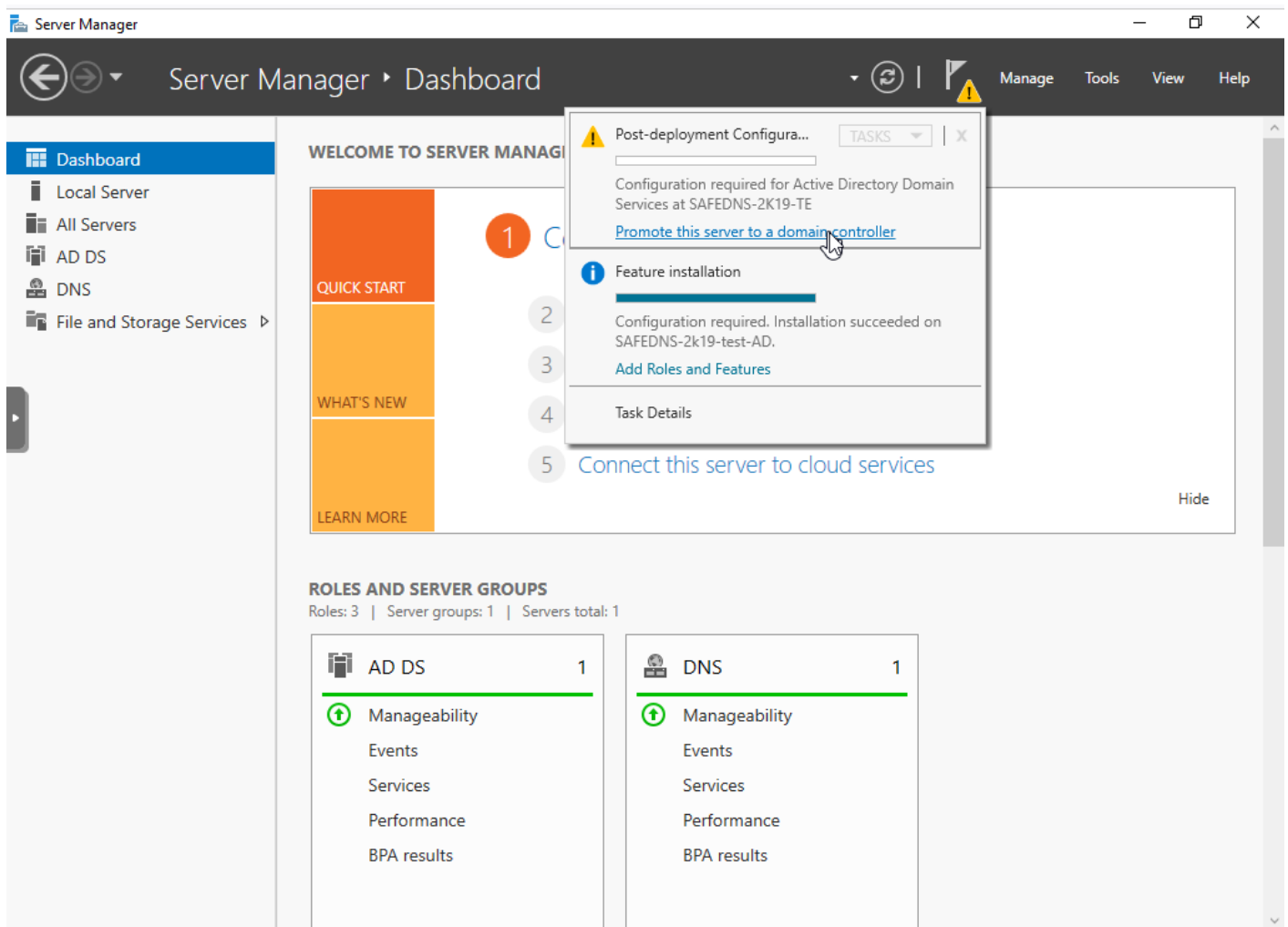
Once installed, the wizard shows the results of the installation:



We are set with the installation of the Roles & Features. Please close the window.

2. Active Directory Configuration process.

Start the Server Management and promote the server as a domain controller:



Creating a new forest and name it accordingly:

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SAFEDNS-2k19-test-AD

Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous Next > Install Cancel

Leaving the options by default. Please set the DSRM password:

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
SAFEDNS-2k19-test-AD

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server
☒ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Configure the delegation options (if there is a need for that):

Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER
SAFEDNS-2k19-test-AD

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) ✕

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

< Previous **Next >** Install Cancel

Configure the NETBIOS name:

Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
SAFEDNS-2k19-test-AD

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous Next > Install Cancel

Configuring the system folders:

Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER
SAFEDNS-2k19-test-AD

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS ...

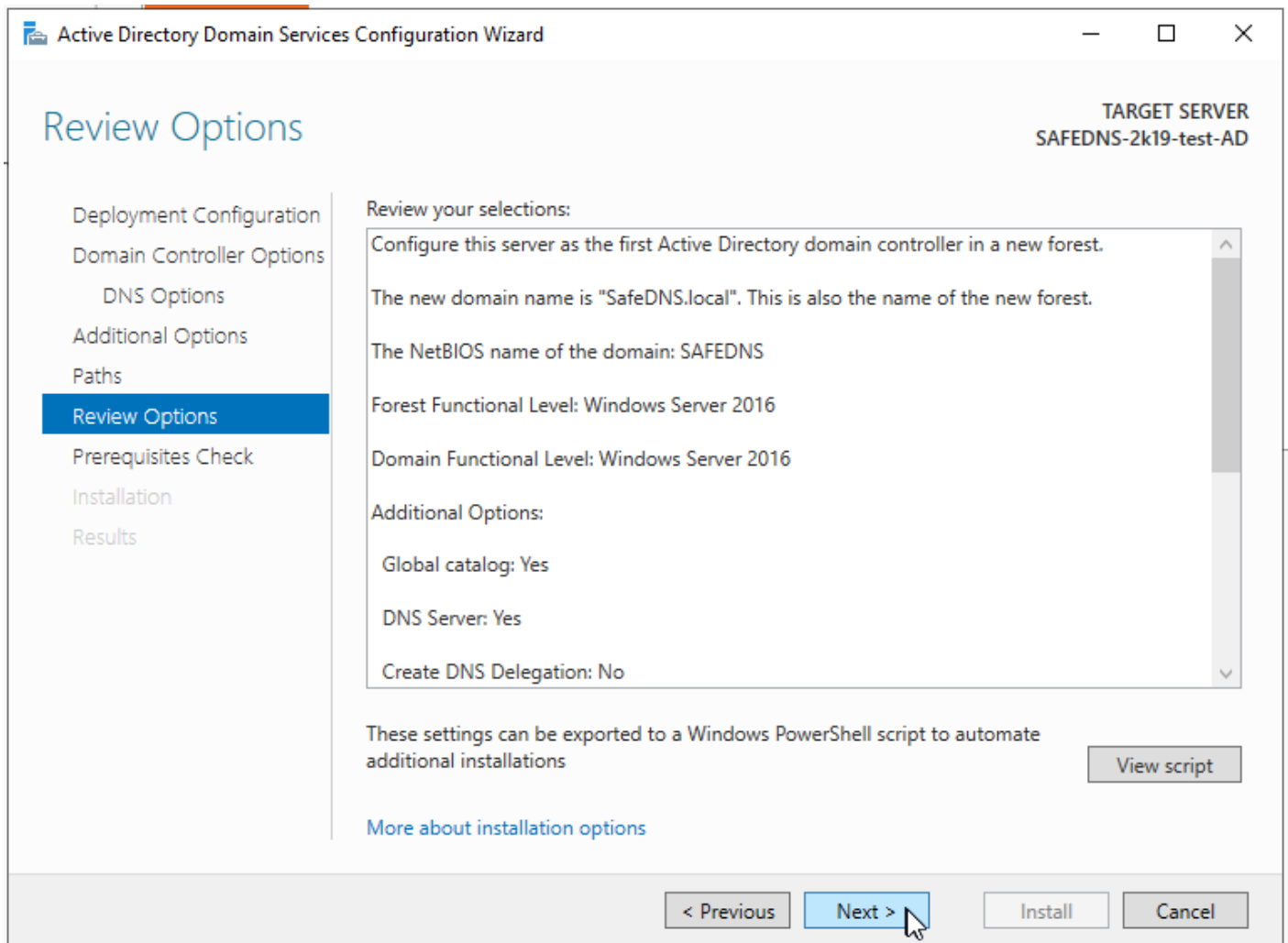
Log files folder: C:\Windows\NTDS ...

SYSVOL folder: C:\Windows\SYSVOL ...

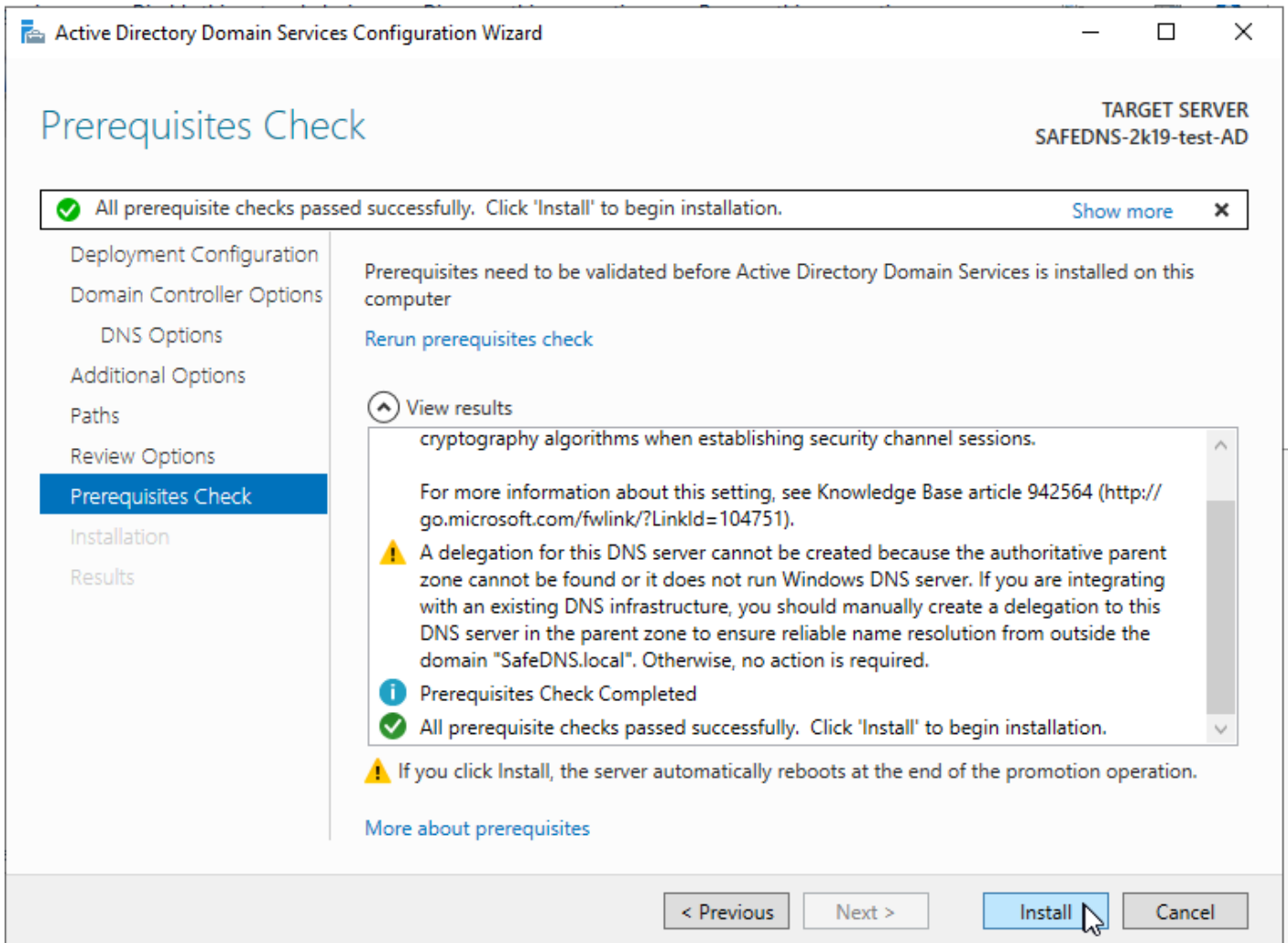
[More about Active Directory paths](#)

< Previous Next > Install Cancel

The preview of the installing options:



Prerequisites check and install:

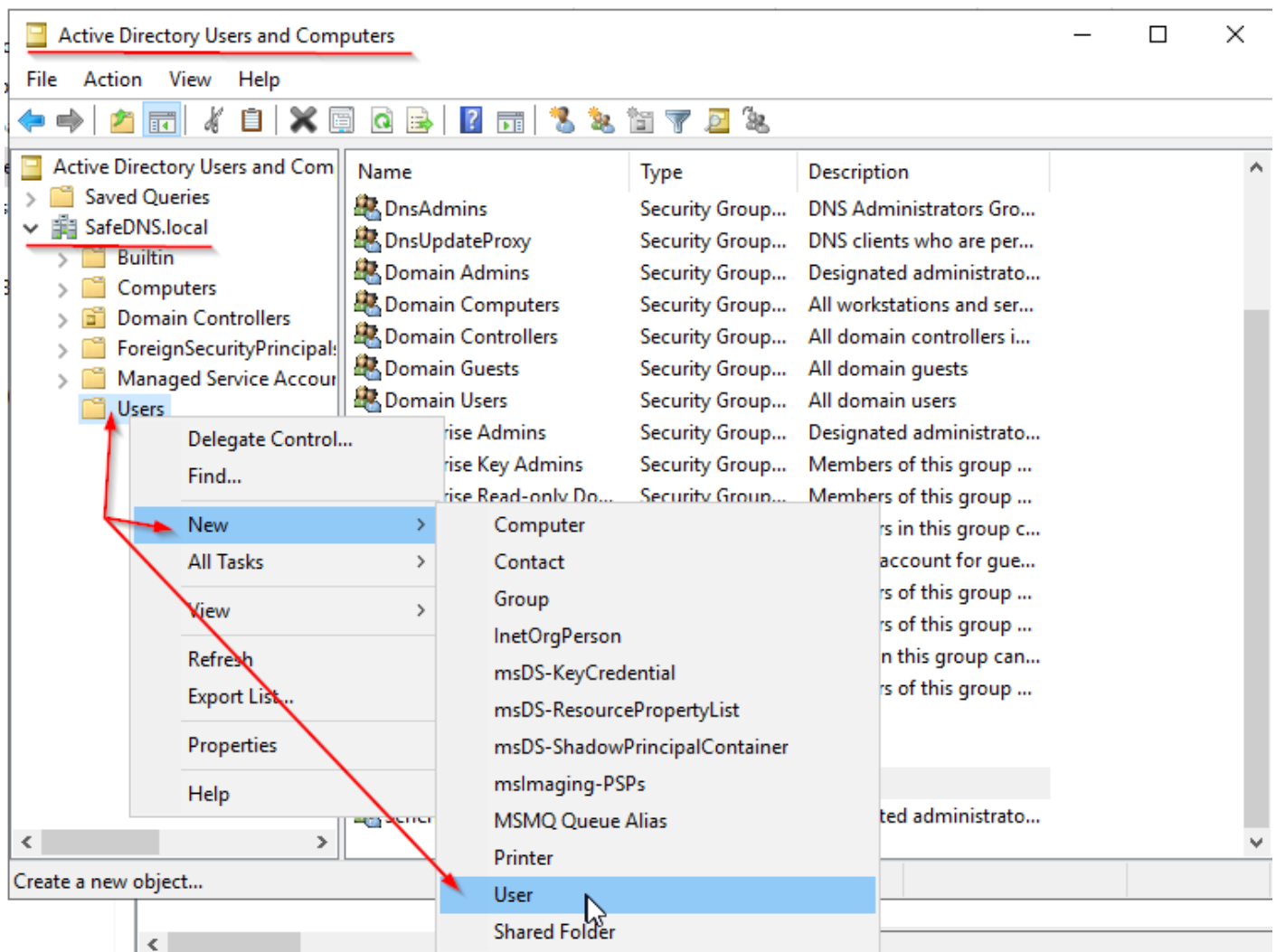


3. Creating User/Groups on the AD.

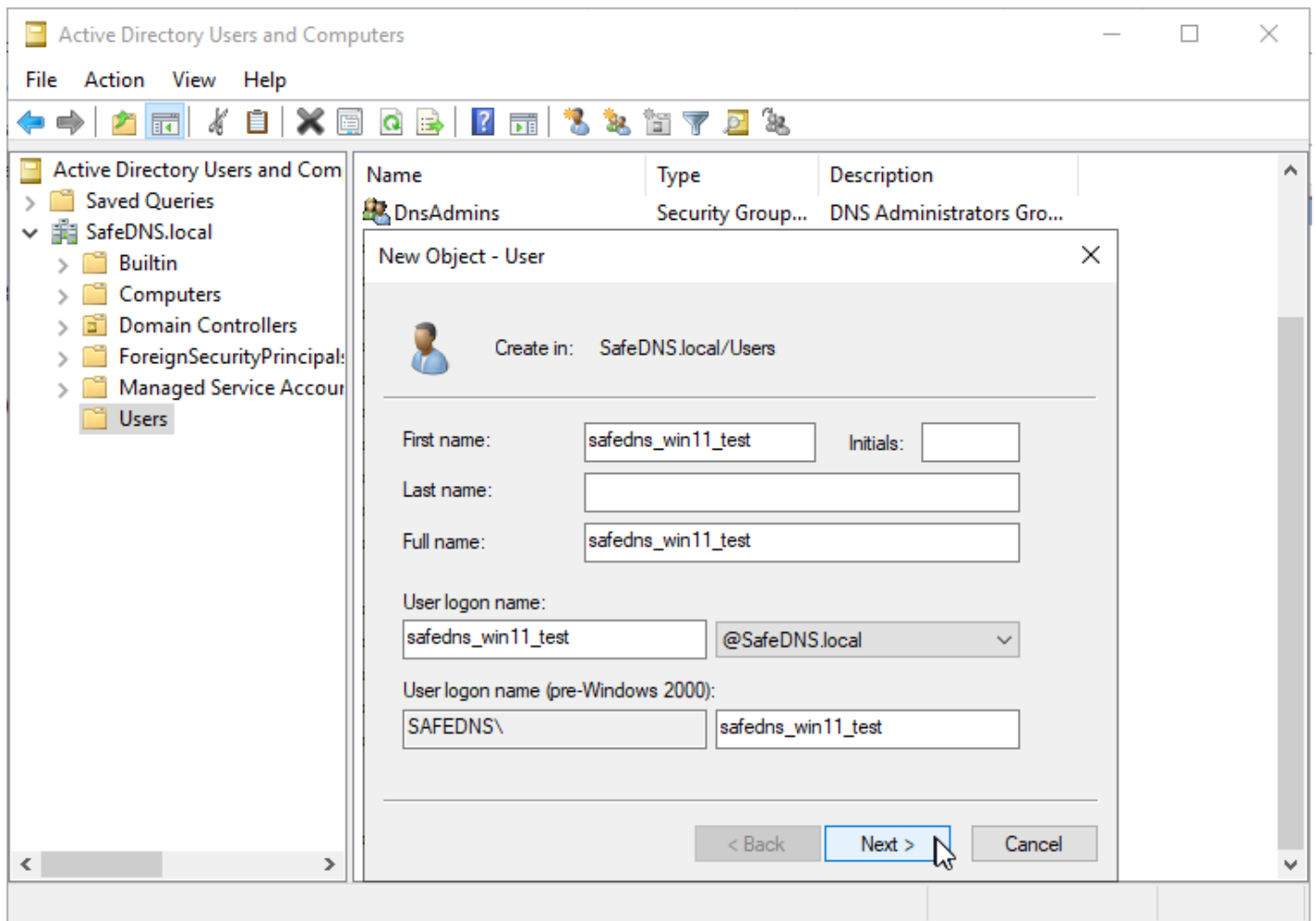
The new group and user should be created for the Agent Software delivery to the end-user computers. The application installation starts immediately after first user logon to the computer.

3.1. Creating a new user.

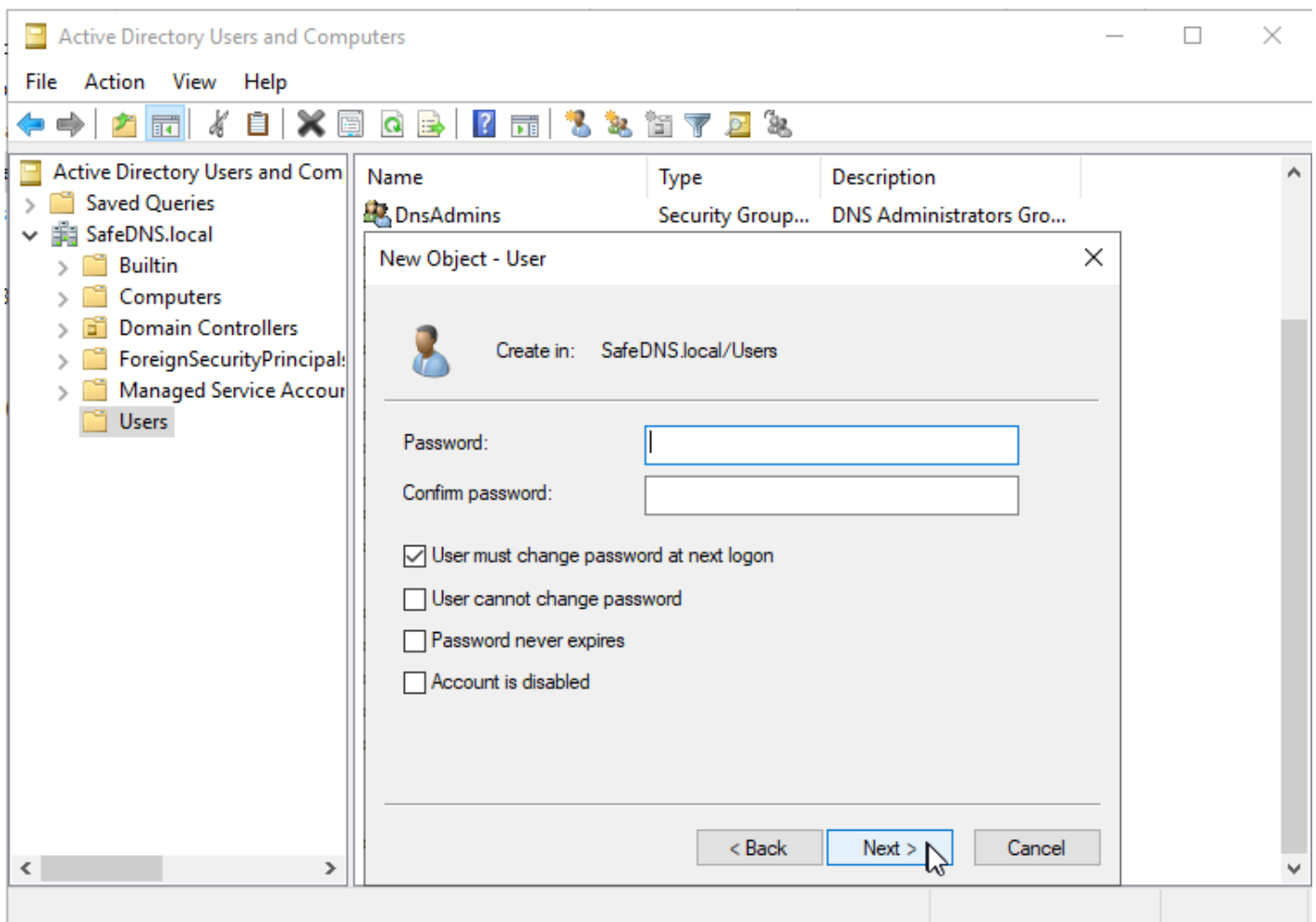
Open the Active Directory Users and Computers, select the recently created domain, then Users => New => User:



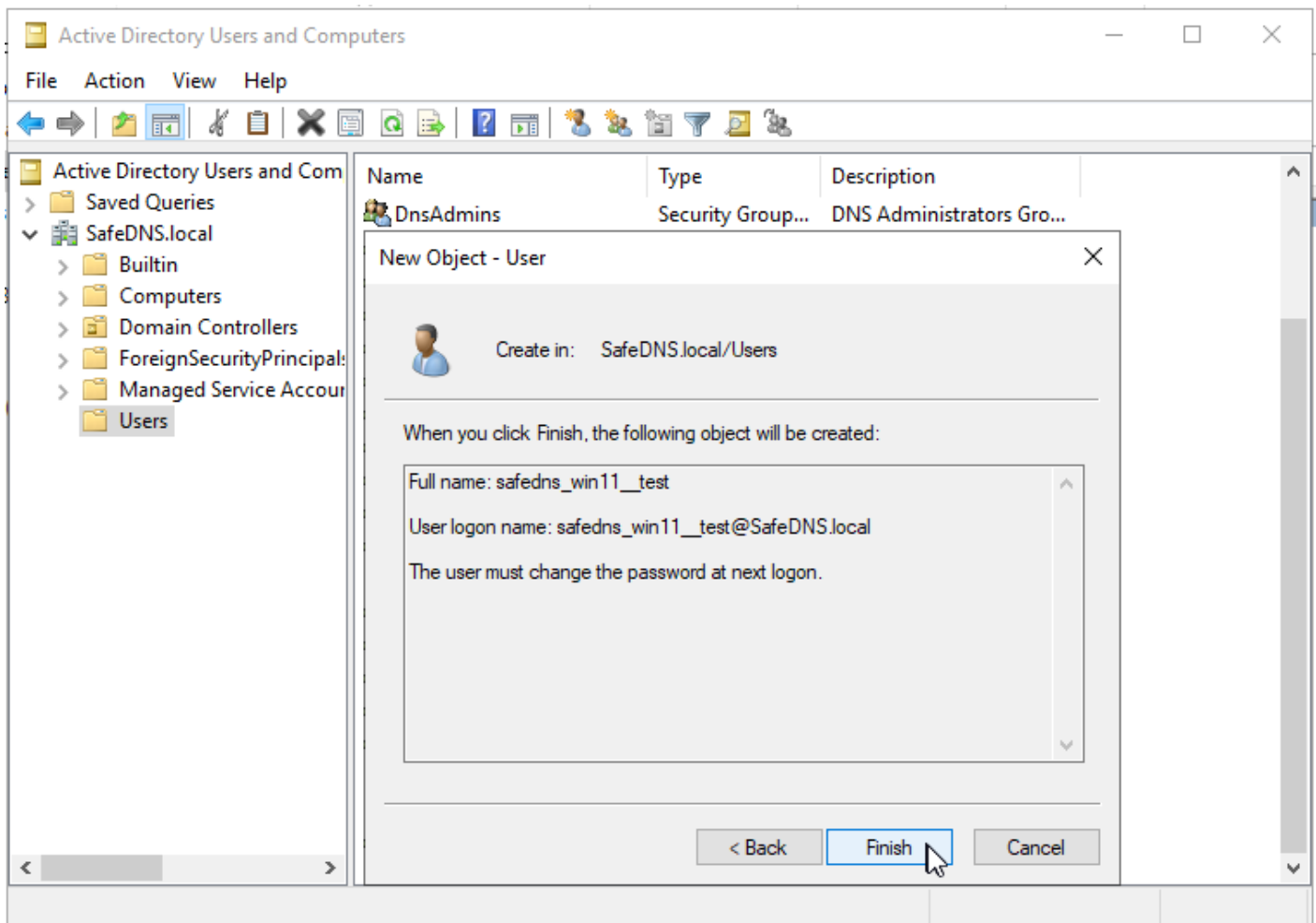
Setting the username:



Password:



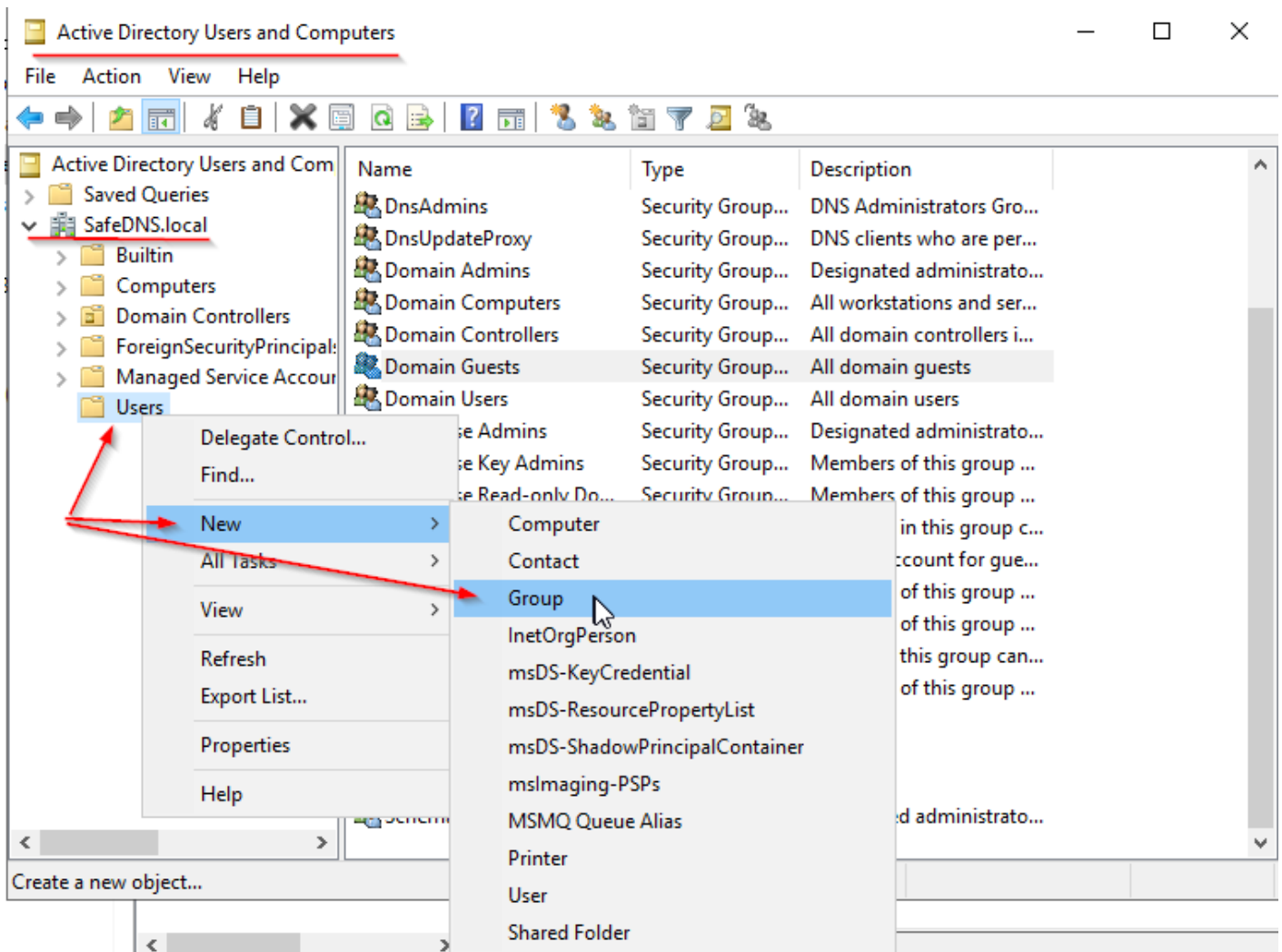
Reviewing the object(User) summary and finishing the process:



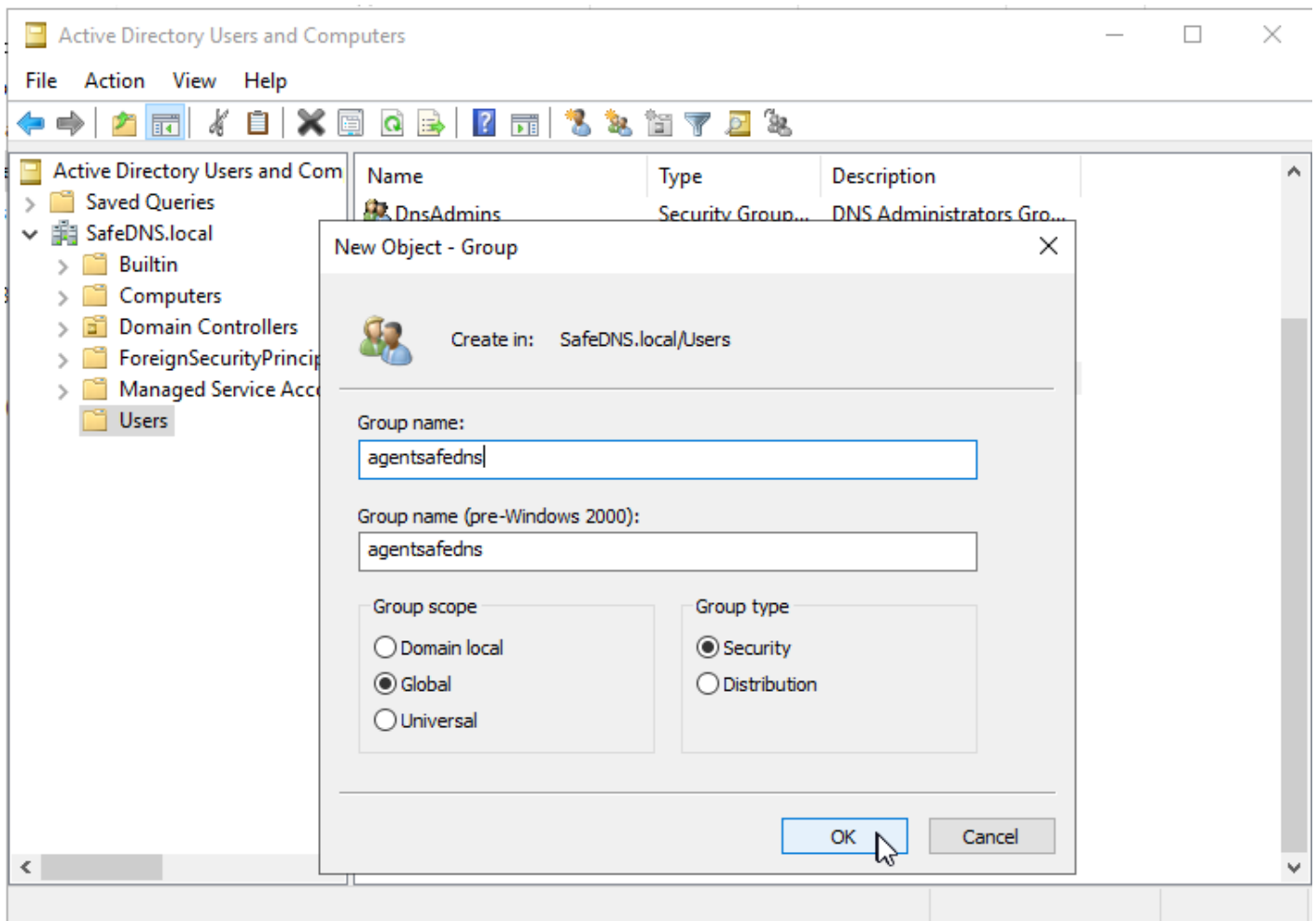
3.2. Creating of the User Group.

Users can be part of one group within the AD environment. The application can be applied to a group of users optimizing the configuration and management of the Application Rollout.

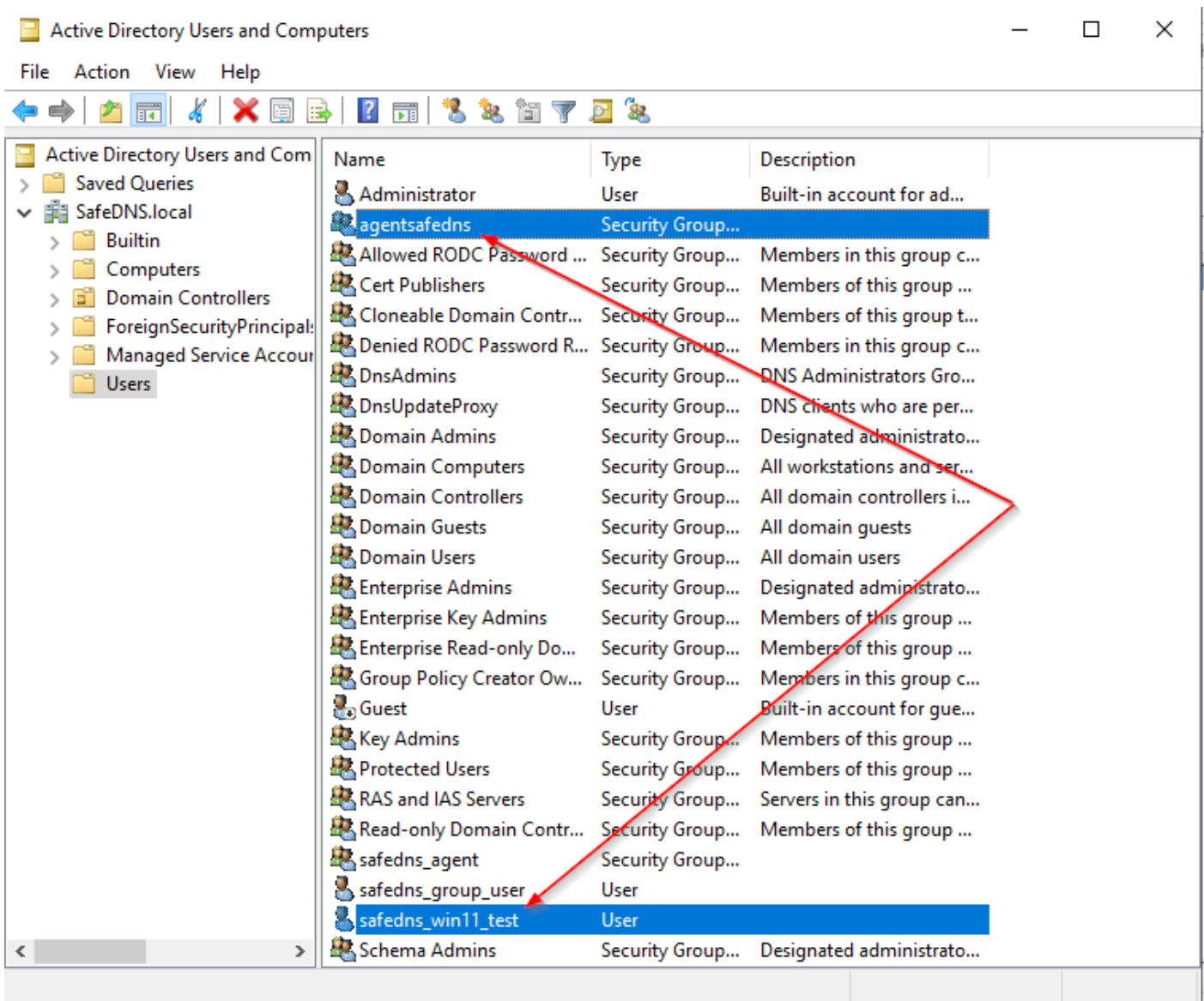
Active Directory Users and Computers, Selecting our domain, and then tap on the Users => New
=> Group:



Entering the data of the Group and tap OK:

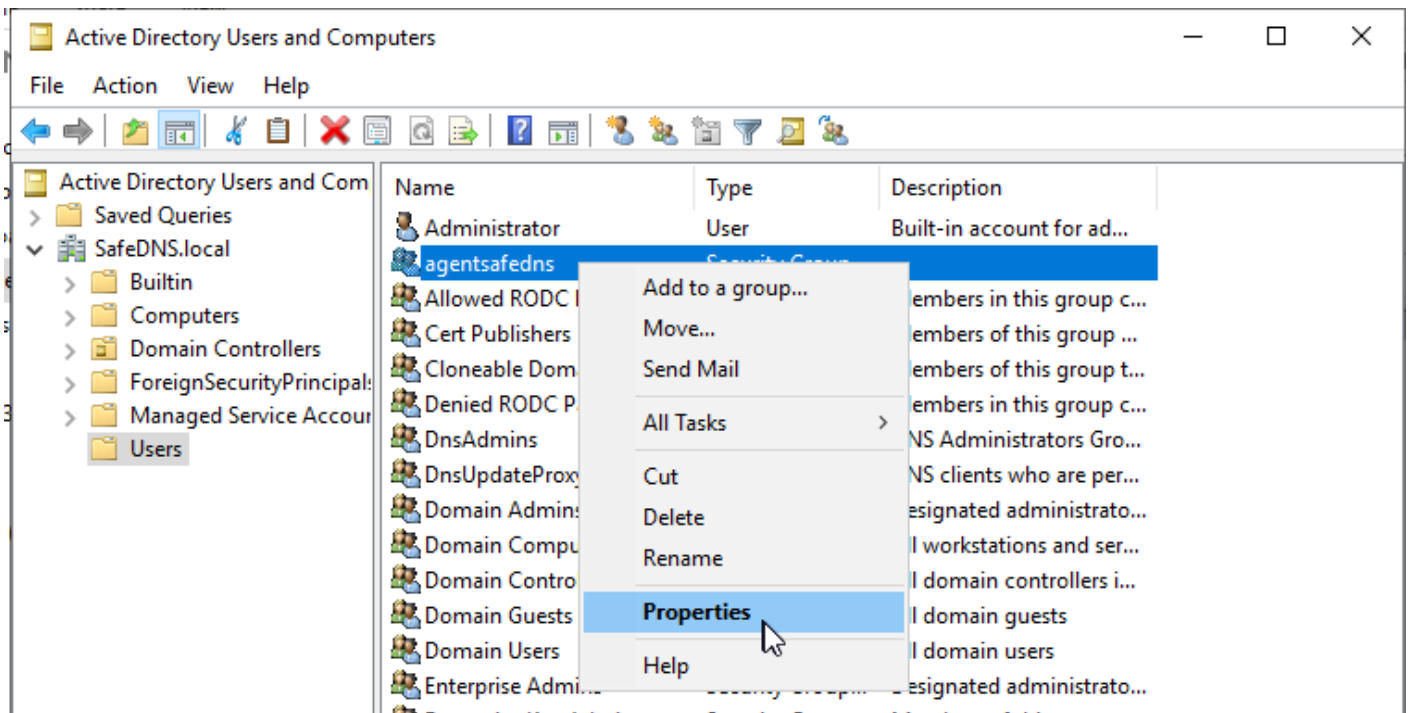


Please check that User and group has been created:

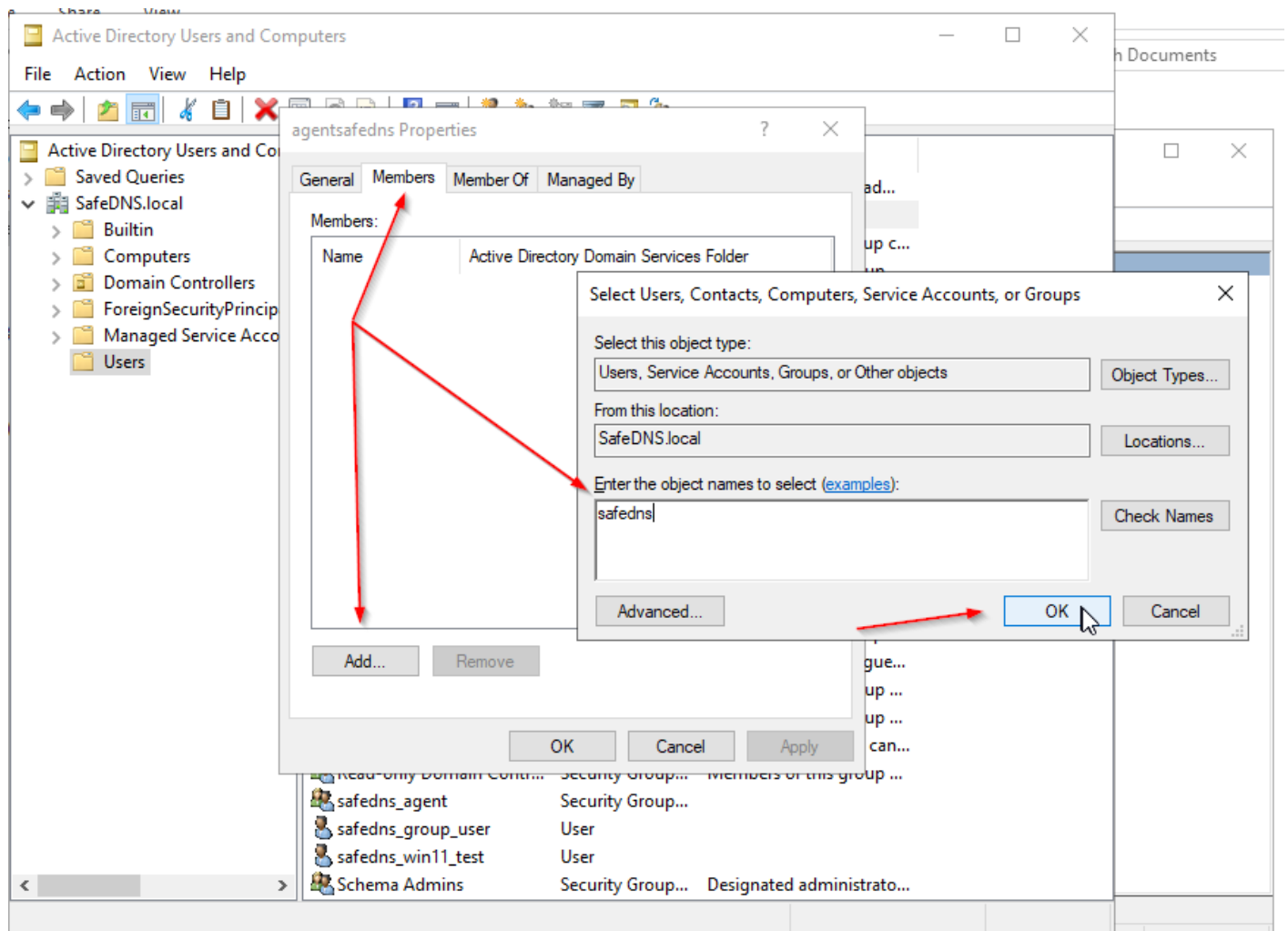


3.3. User added to the group.

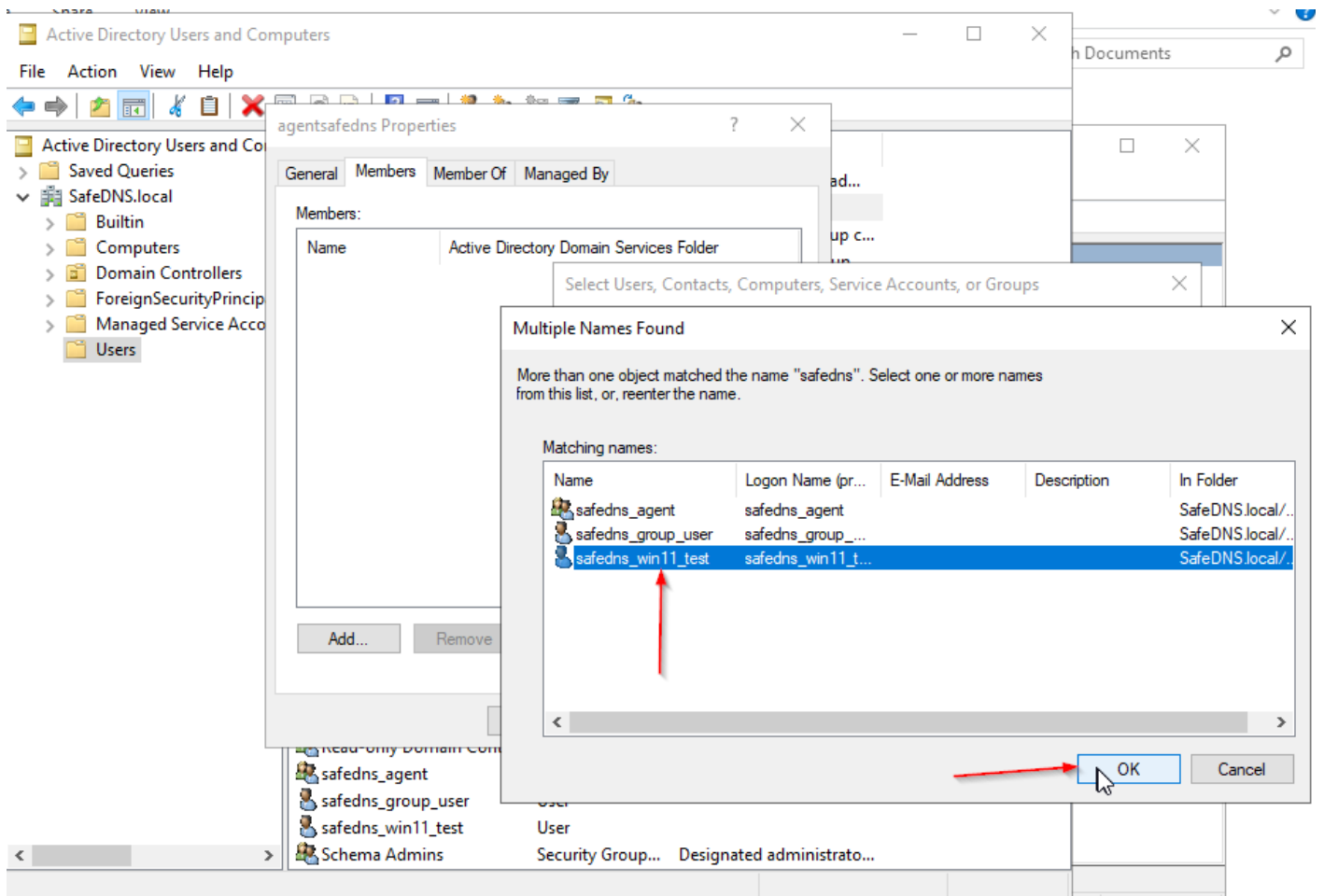
Select the group and in the context menu tap the Properties:



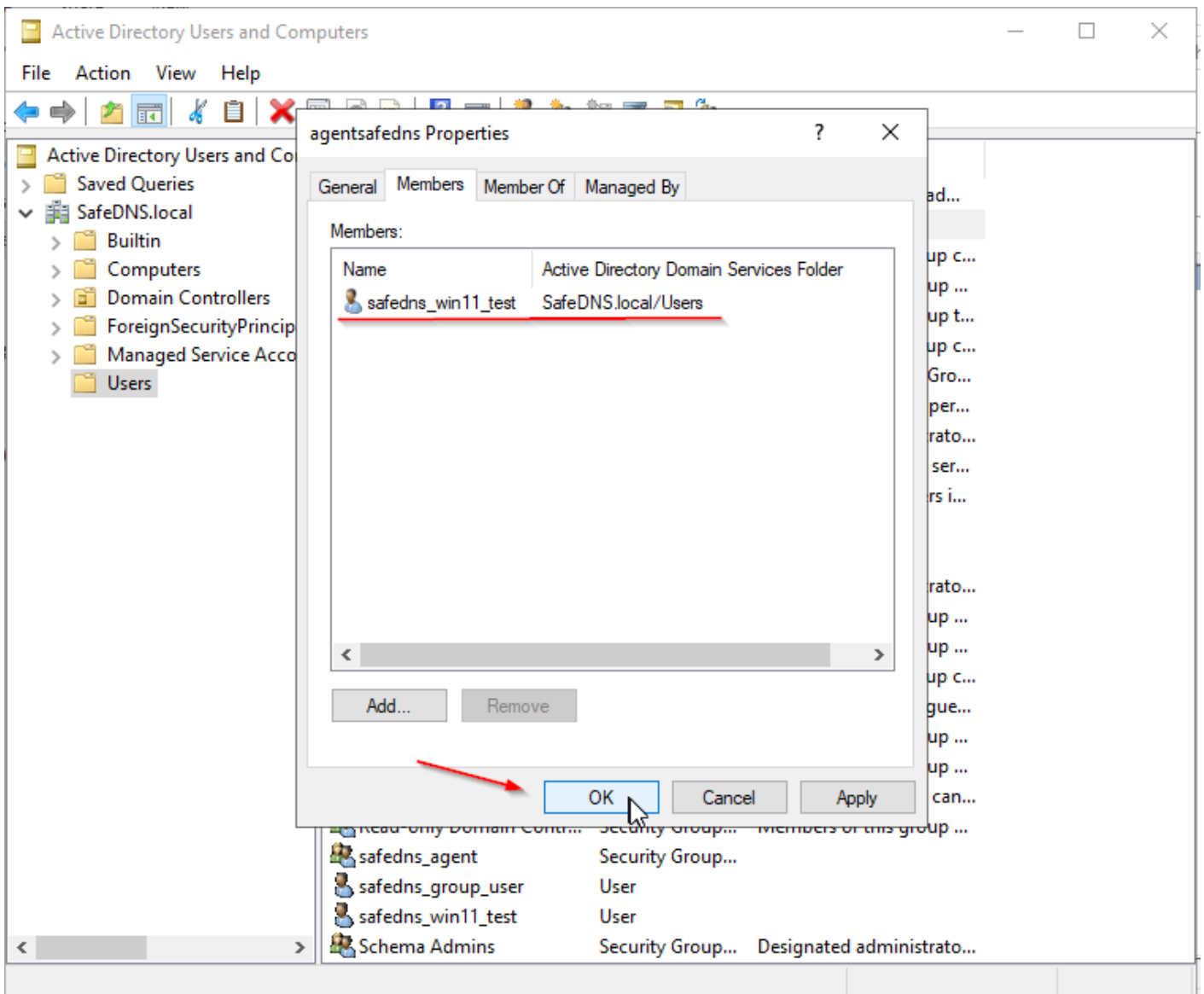
On the appeared window select Members and tap the Add button. Enter the username in the search field and press OK:



Select the user safedns_win11_test and tap OK button:



Check the result and press OK button:



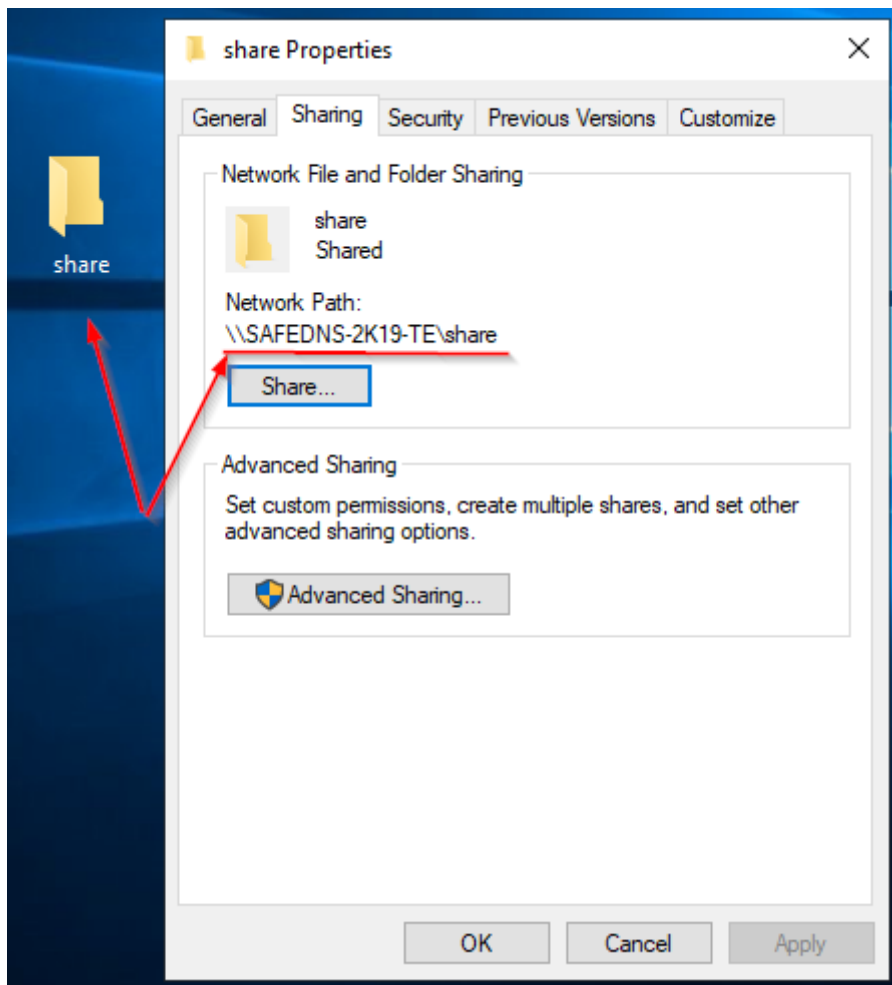
The user creation part is over, now we need to configure GPO.

4. MSI file Preparation on the server.

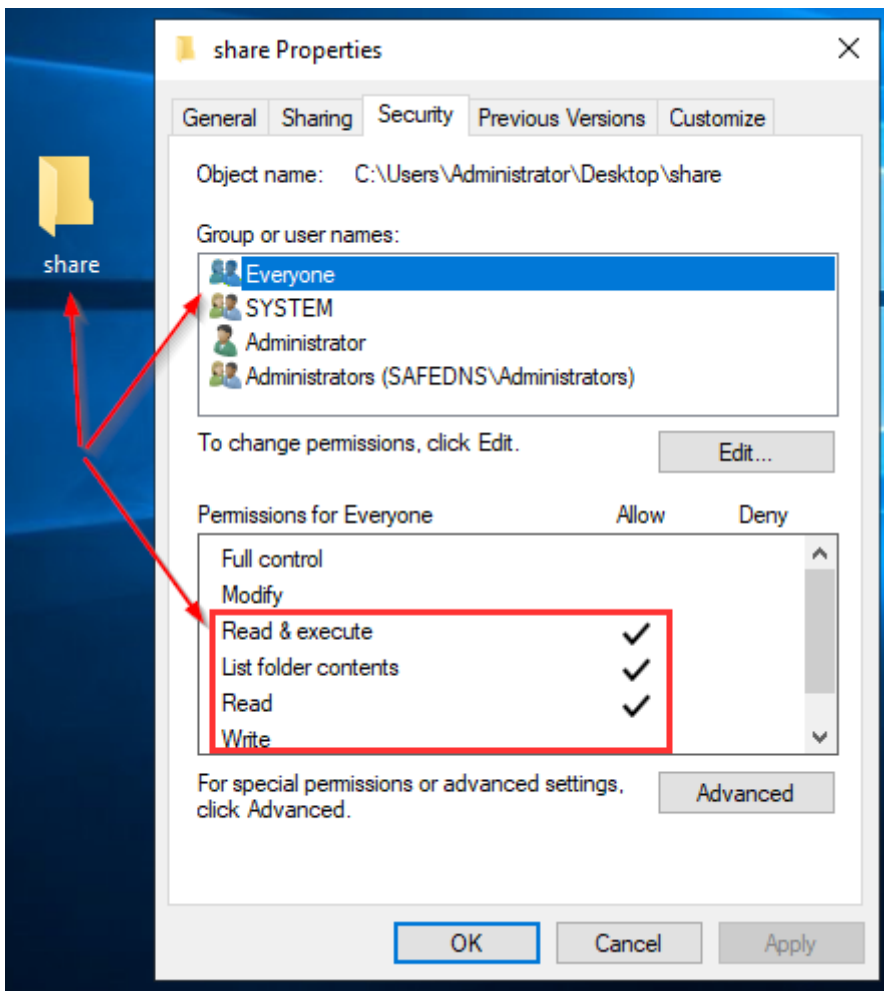
The MSI Agent package should be prepared and copied to the folder on the Active Directory Server.

The MSI Agent package is prepared by SafeDNS. Our technical team generates and inserts your personal identification token into the package.

The folder with the Agent package should be available from the client's computer.



The folder permissions should be the following. User Everyone should have access to the read&execute:

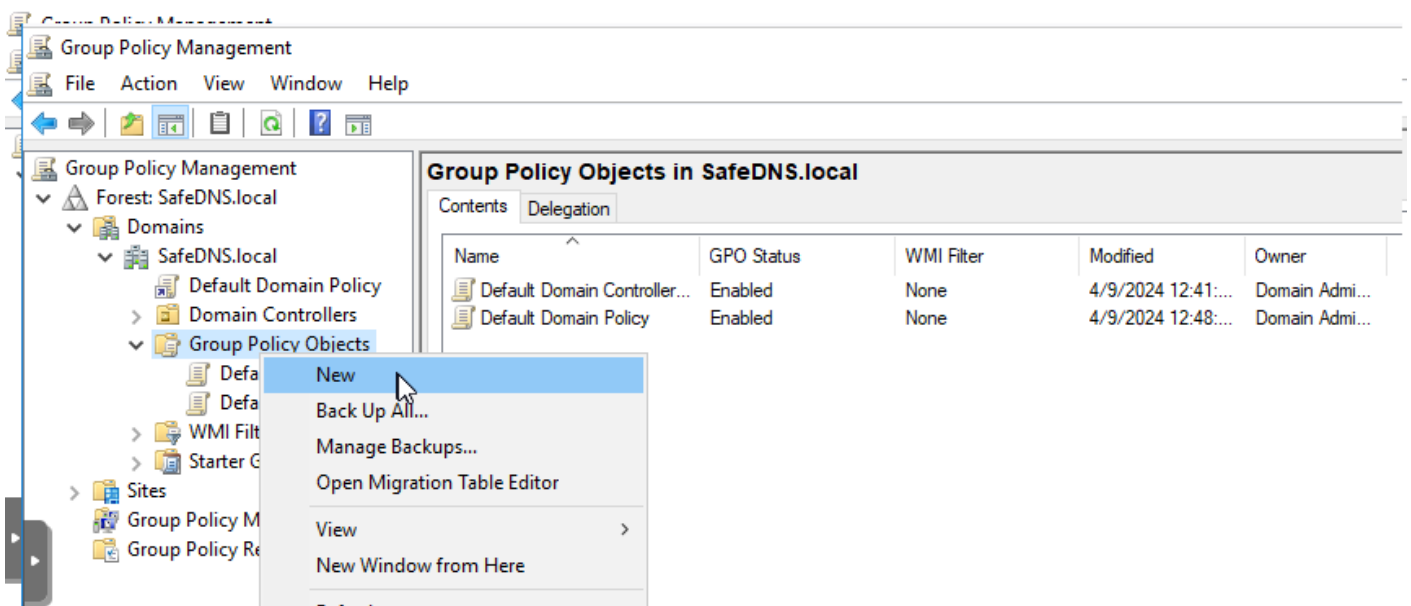


The preparation of the file process is over.

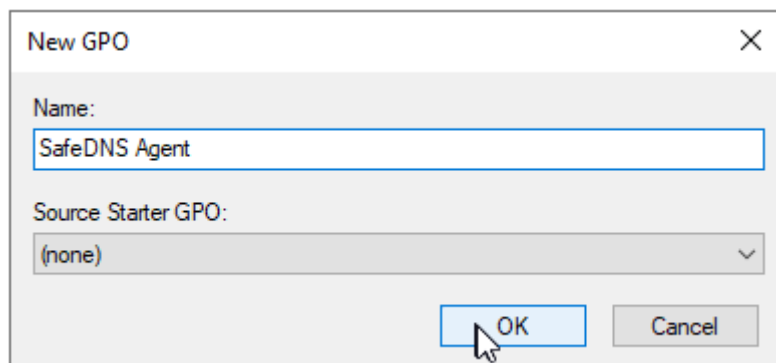
5. Group Policy Configuration.

Open the Group Policy Management console

Select the current domain, then Group Policy Objects and open the context menu => New

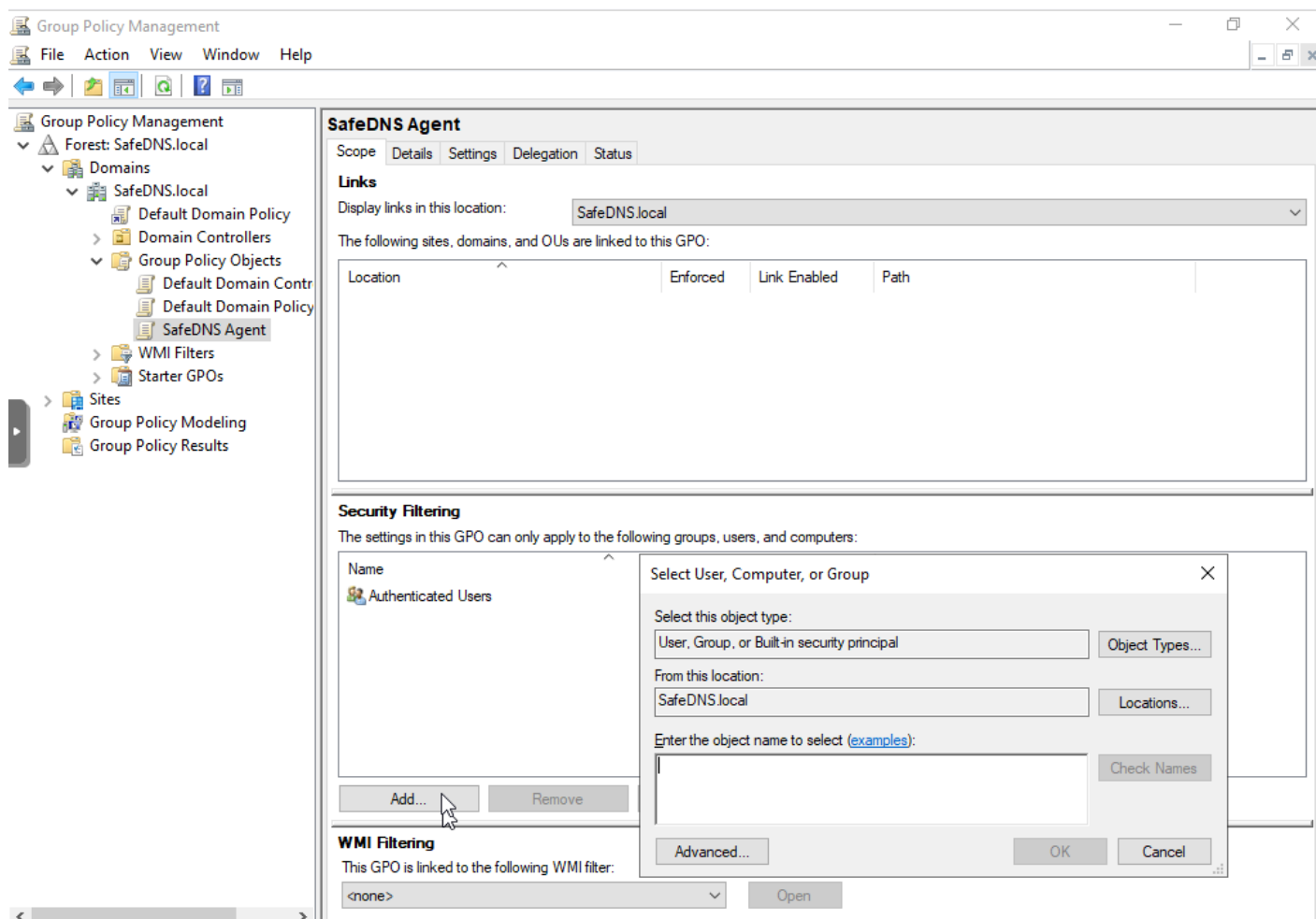


Please name the Group Policy accordingly:



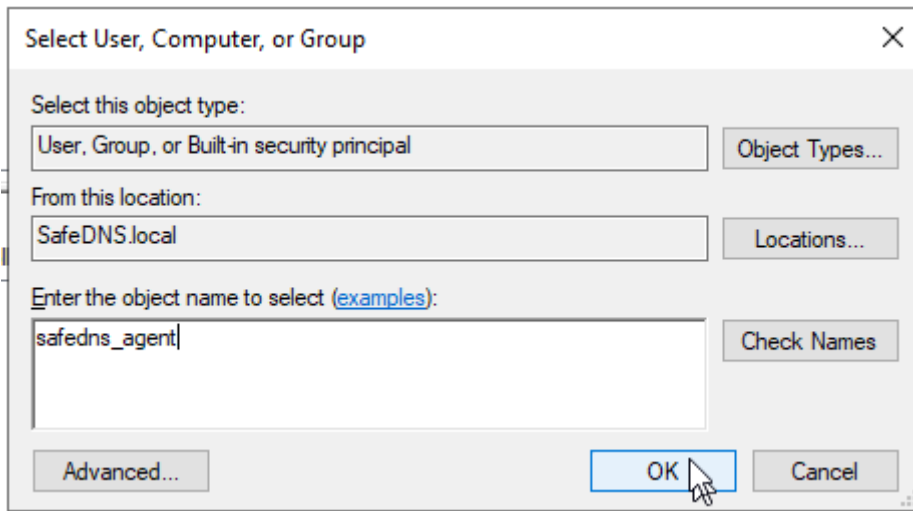
A dialog box titled "New GPO" with a close button (X) in the top right corner. It contains two input fields: "Name:" with the text "SafeDNS Agent" entered, and "Source Starter GPO:" with a dropdown menu showing "(none)". At the bottom right are "OK" and "Cancel" buttons. A mouse cursor is pointing at the "OK" button.

Once the policy is created, please set the User/Group applied the GPO installation:

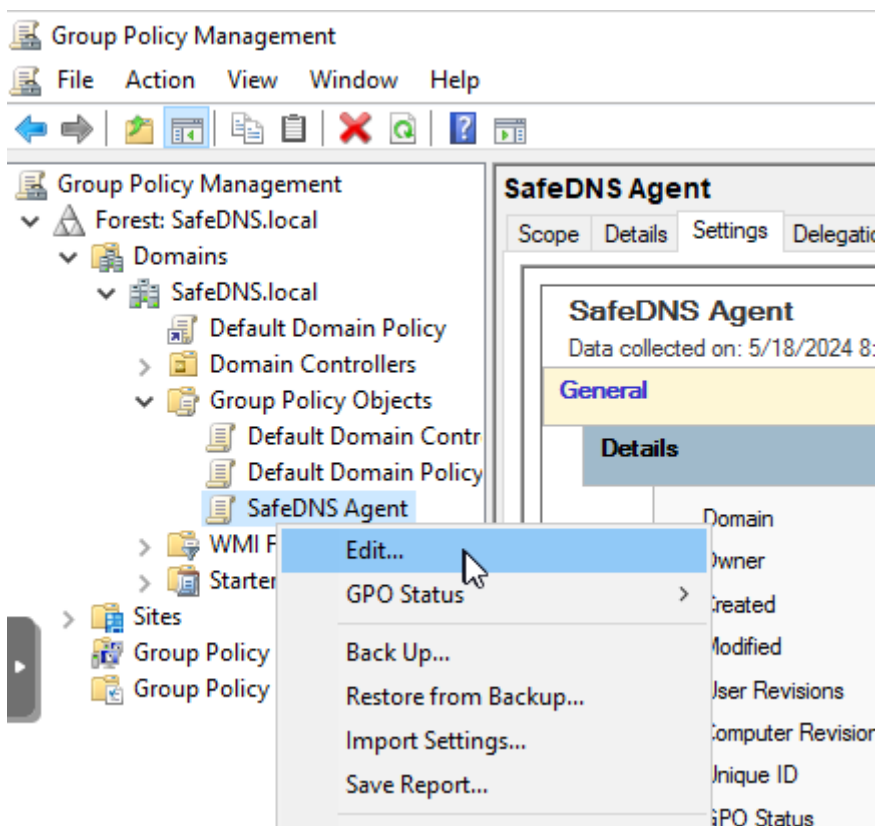


The Group Policy Management console window. The left pane shows the tree structure: Group Policy Management > Forest: SafeDNS.local > Domains > SafeDNS.local > SafeDNS Agent. The right pane shows the "SafeDNS Agent" policy details. The "Links" tab is active, showing "Display links in this location:" set to "SafeDNS.local". Below it, a table lists linked sites, domains, and OUs. The "Security Filtering" section shows a list of groups with "Authenticated Users" selected. An "Add..." button is highlighted. A "Select User, Computer, or Group" dialog box is open, showing "Select this object type:" set to "User, Group, or Built-in security principal", "From this location:" set to "SafeDNS.local", and an empty "Enter the object name to select" field. The "WMI Filtering" section shows "<none>" selected.

In the appeared window select the Group safedns_agent - with the user safedns_win11_test:

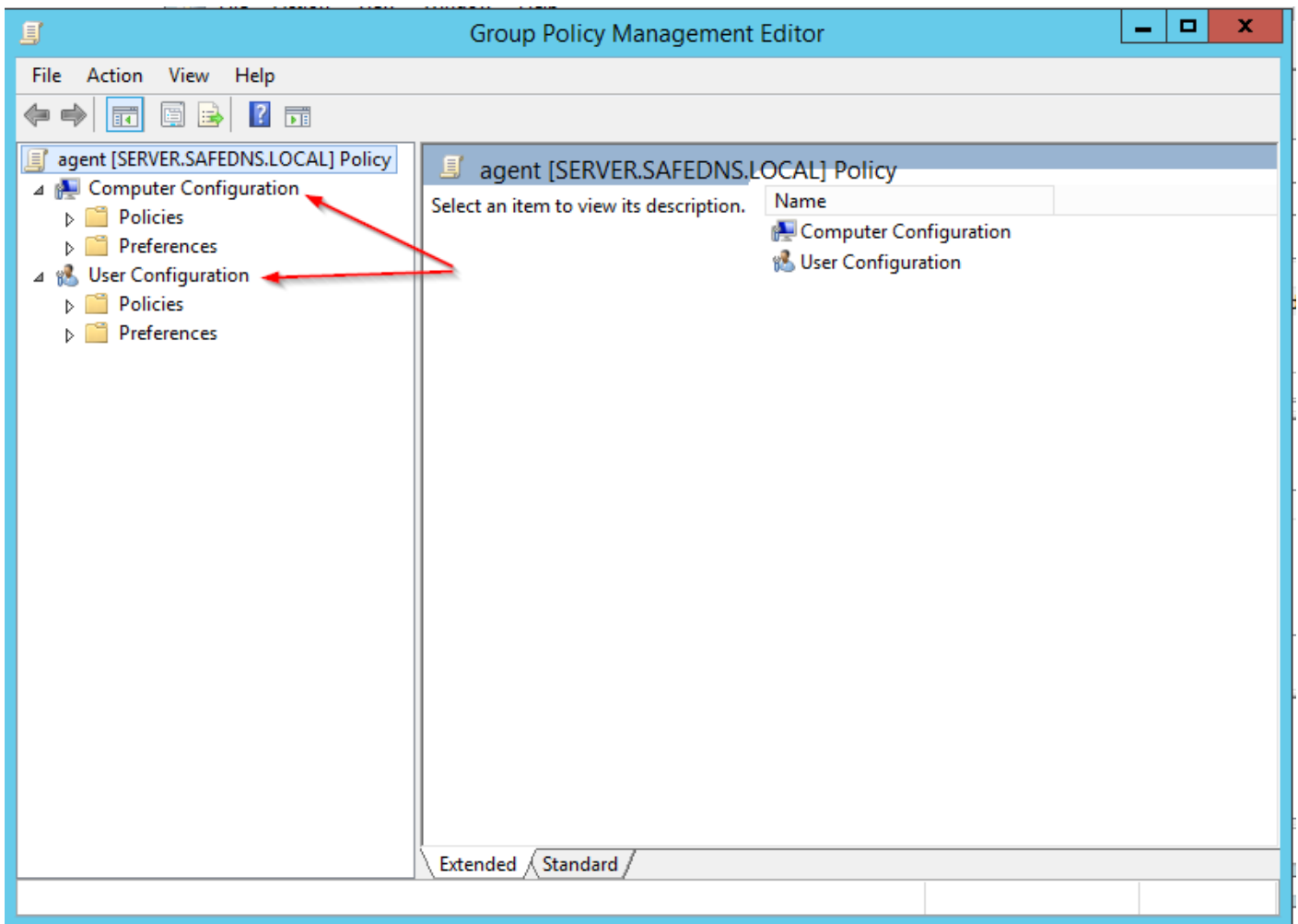


Once the GPO is created, tap the context menu of the object and click on Edit button:



Important notice: There are 2 possible ways of the MSI package installation:

1. Installation Policy applied to the computer - Computer Configuration
2. Installation Policy applied to the user - User configuration

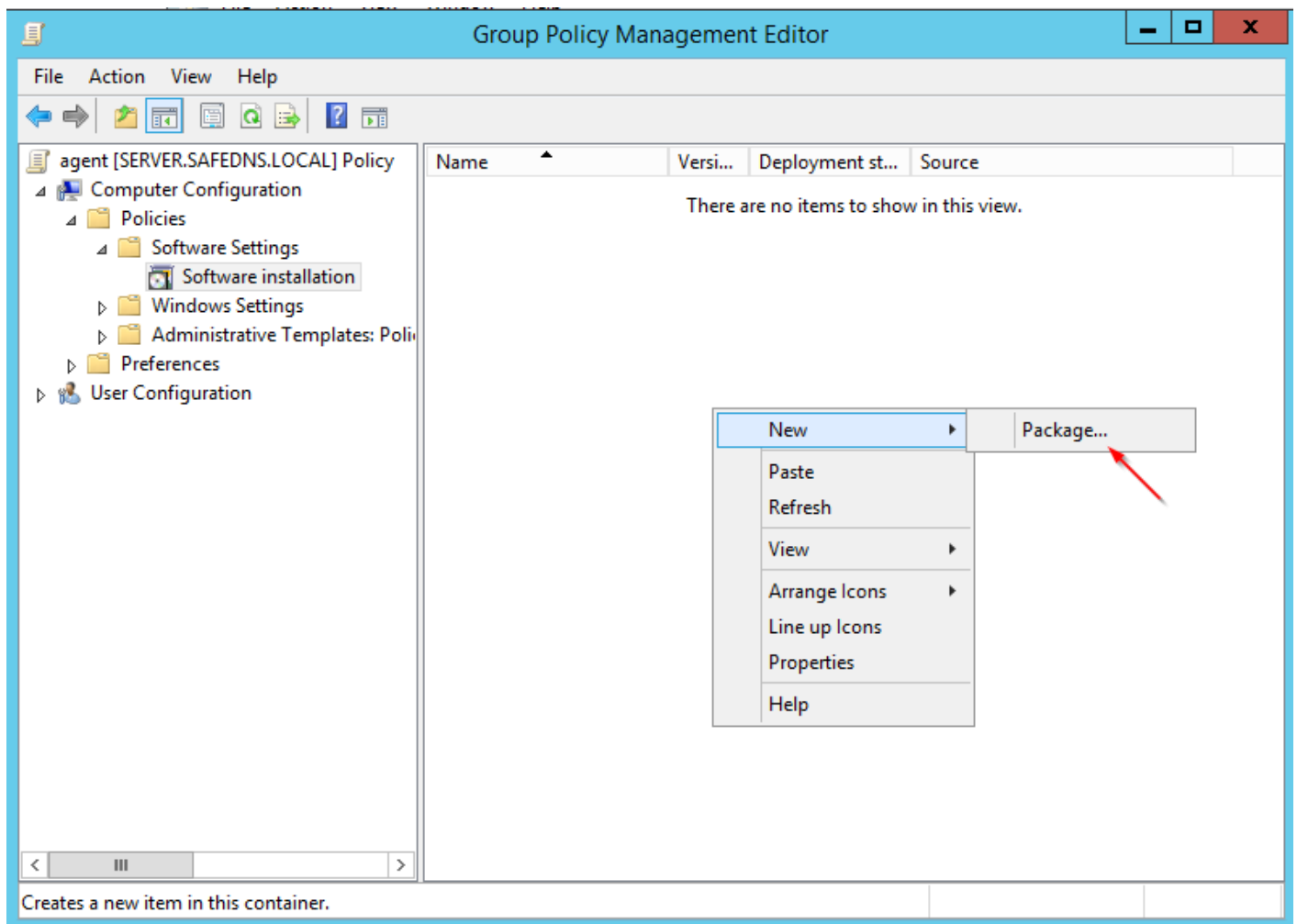


It is recommended to use Computer Configuration - the software installation will start without user interaction and the user can not stop/close installation.

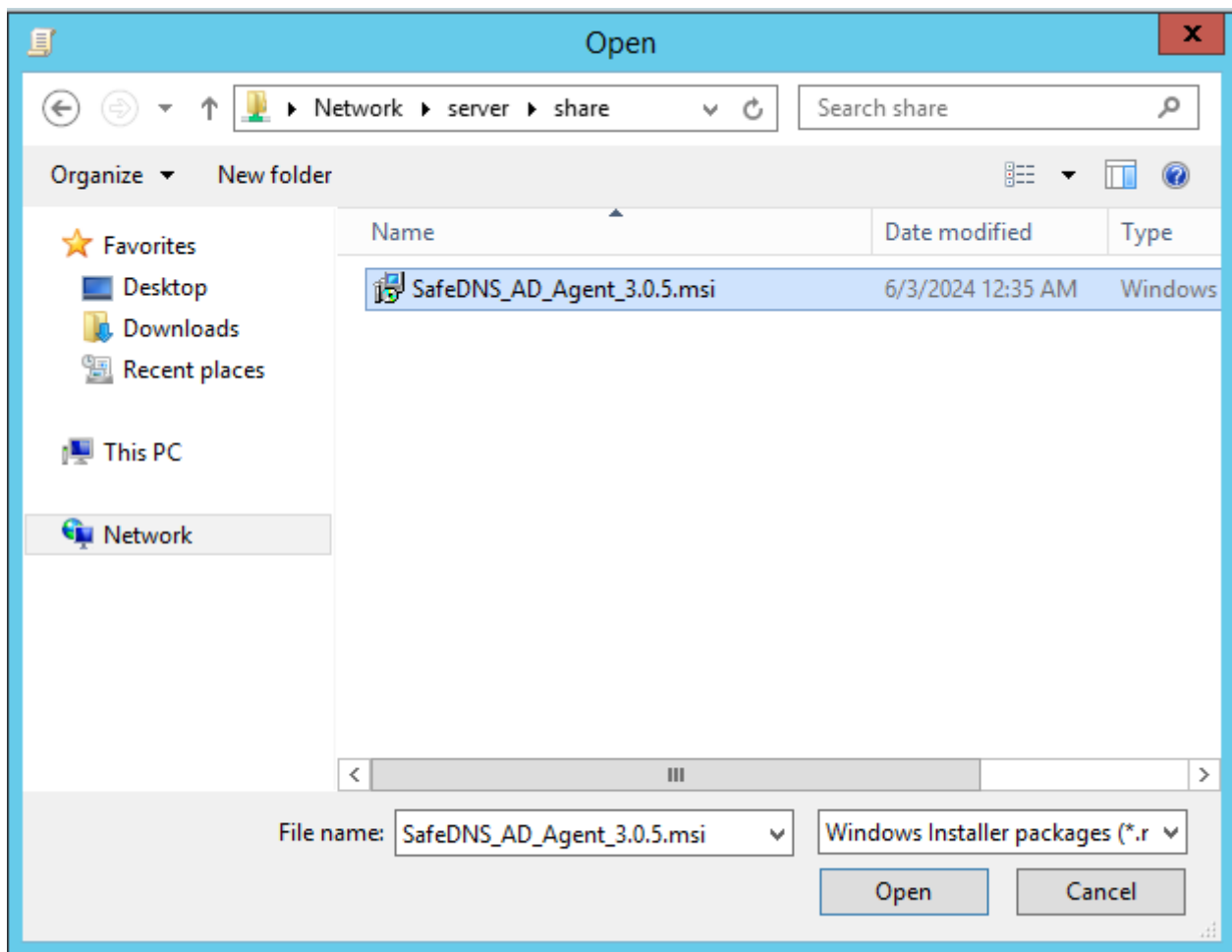
The second option - User Configuration requires user actions on the computer to start the package installation and will require Administrator credentials.

In the Group Policy Management Editor select Computer Configuration then Policies => Software Settings => Software Installation.

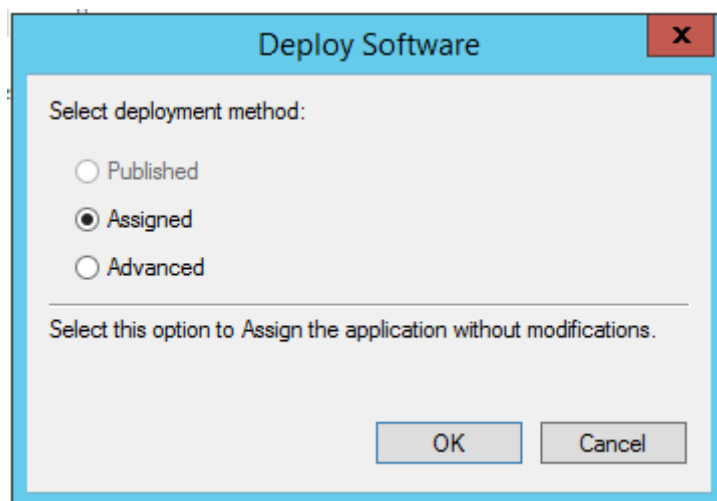
Tap the context menu button and select New=>Package:



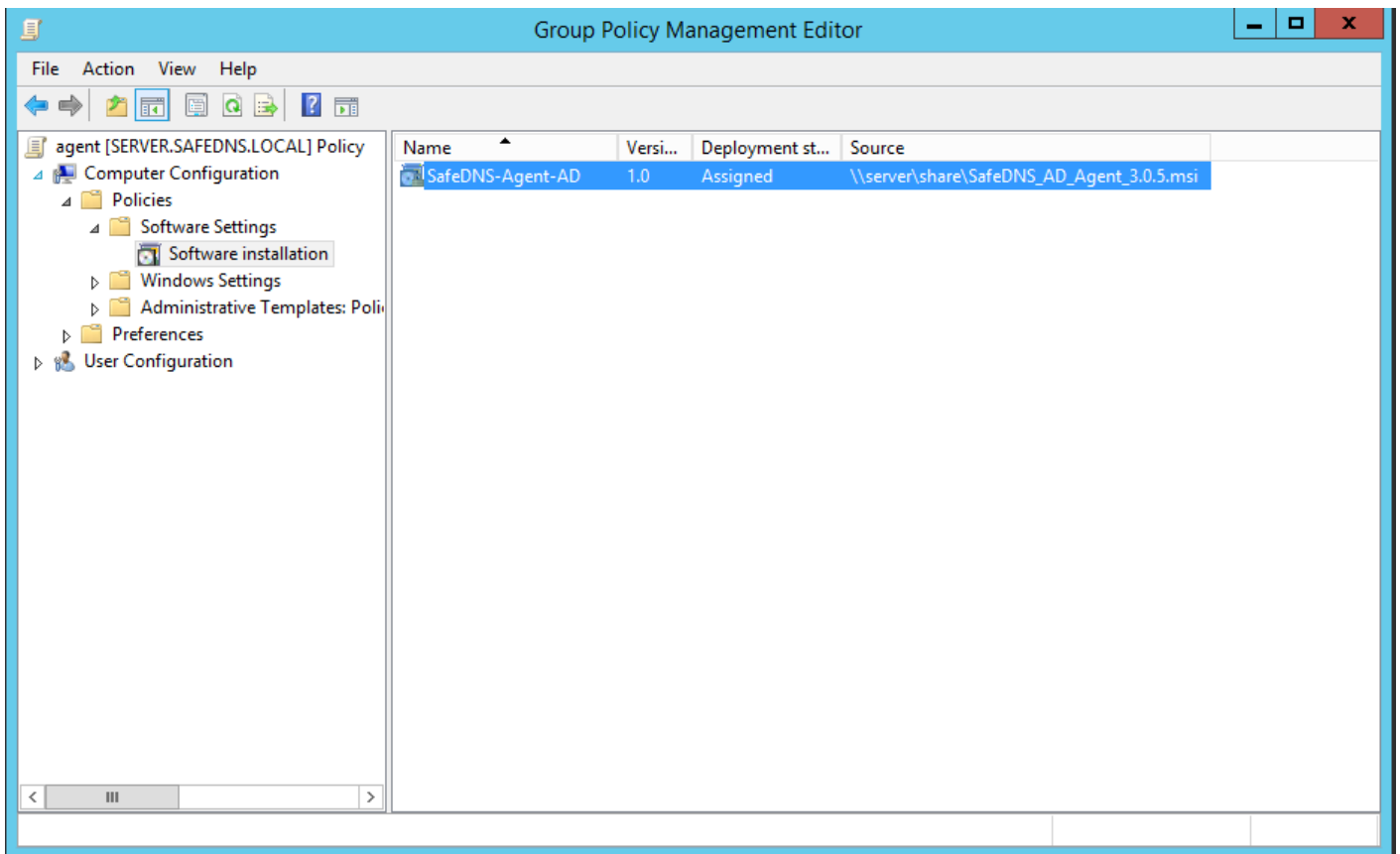
Select the SafeDNS Agent installation package. The path should be the following:
\\server\share\SafeDNS_AD_Agent_3.0.5.msi



Select the Assigned deploy method:



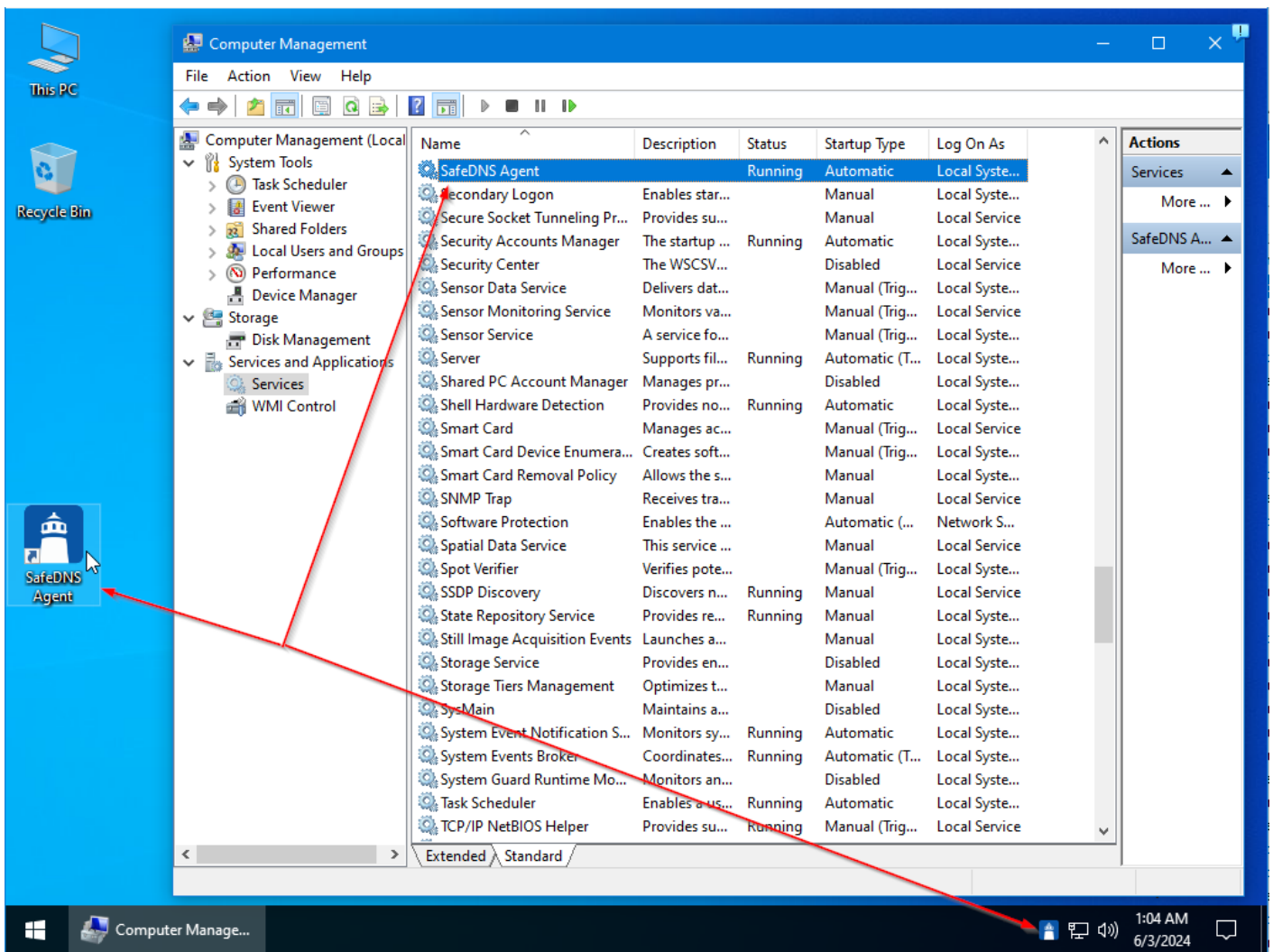
Once the Application package is added, the new record should appear in the list:



The installation is finished, the Agent should be installed after the next login to the computer.

Depending on the MSI package settings, after the installation the following objects should appear:

1. SafeDNS Agen icon on the Desktop
2. SafeDNS Agent service
3. SafeDNS icon on the system tray



If there is a need to start the MSI package installation before restarting/new login please start the CMD command line and run the following command:

gpupdate /force

This command will initiate the installation process:

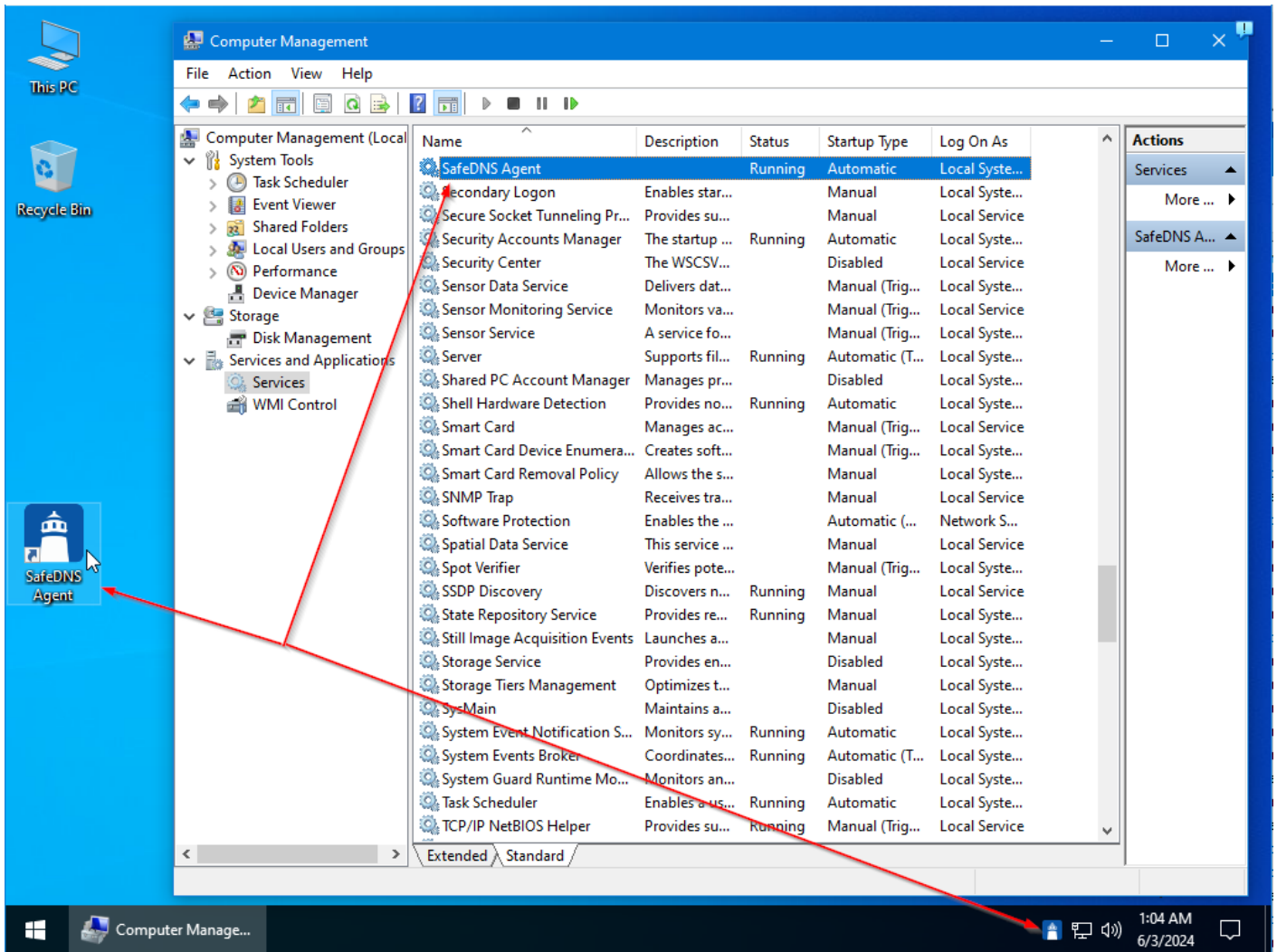
```
C:\Windows\system32\cmd.exe - gpupdate /force
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\supertest>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

Certain Computer policies are enabled that can only run during startup.
OK to restart? (Y/N)
```

Once the computer restarted, the applicaation will appear on the Desktop, the service created and the icon appeared in the system tray:



Revision #8

Created 1 July 2024 22:19:47 by Mark Woodman

Updated 27 September 2024 07:39:22 by Mickaël Gauthier