upKeeper Manager 5.0

Installation prerequisites

Revision 1.0
2022-04-11

Table of contents

Summary

This document describes the system requirements for upKeeper on both the server- and client side. The necessary changes to the network environment are also described.

A basic upKeeper installation consists of the following modules:

- upKeeper Database
- upKeeper Administration Website
- upKeeper Admin API
- upKeeper Client API
- upKeeper Application Server
- upKeeper Client

In addition to the above, the following optional modules can also be installed if they are needed:

- upKeeper Files Website
    - Enables distribution of application installation media over HTTP/HTTPS

This document also describes the configuration of optional but recommended services:

- Windows Deployment Services (WDS)
    - Installation of service operating systems across the network
- Windows Server Update Services (WSUS)
    - Automatic client updates
- Wake On Lan (WOL)

Customer Responsibility

Prior the implementation of upKeeper the customer must check that the requirements in the following sections are met:

- System Requirements – Server
- System Requirements – Client (for clients to be managed by upKeeper)
- Network Environment
- Before the installation begins, make sure you contact your supplier or contact upKeeper Solutions to activate the license.

Minimum System Requirements – Server and Client

Server platform

Minimum hardware requirements for upKeeper server platform:

- Windows Server 2016, 8 GB RAM, at least 50 GB HDD free space

Server modules

Requirements for upKeeper server modules:

- upKeeper Database:
  - SQL Server versions 2016 or later, Azure SQL.
  - SQL Server should be installed in Mixed Mode to follow documented installation instructions.

- upKeeper Administration Website:
  - IIS versions 10 or later

- upKeeper Admin API:
  - IIS versions 10 or later
  - ASP.NET Core Runtime 6.0.x (Hosting Bundle)

- upKeeper Application Server:
  - .NET Desktop Runtime 6.0.x

- upKeeper Client API
  - IIS versions 10 or later
  - ASP.NET Core Runtime 6.0.x (Hosting Bundle)

- upKeeper Files Website
  - IIS 7.0 – 10
  - .NET Framework 3.5
  - .NET Framework versions 4.0 – 4.8

- Distribution Points
  - The network share for distribution of operating systems and applications should be located on a server or a NAS with the necessary capacity and performance

Client

Client require .Net Desktop Runtime 6.0.x.

Minimum requirements for clients that are going to be deployed with upKeeper:

NOTE! Computers that does not meet the minimum requirements can still be managed by upKeeper, however, not for deployment of the operating system

- 4 GB RAM
- at least 30 GB HDD free space
- .Net Framework 4.8

NOTE! Install Microsoft SQL Server 2014 Report Builder or later if you are going to administer or build your own SQL reports

Network Environment

The network environment requires several settings for the implementation of the server modules. These settings are described in this section and can be summarized in the following paragraphs.

- DNS
  - Create aliases for the machine that hosts the upKeeper Application Server.
- Rights - User Accounts
  - Create specific upKeeper user accounts and assign rights.
- File Share
  - Create a file share at appropriate server
- Remote Assistance
  - Define a policy for remote assistance
- Windows Firewall
  - Settings for Windows Firewall if it is to be activated

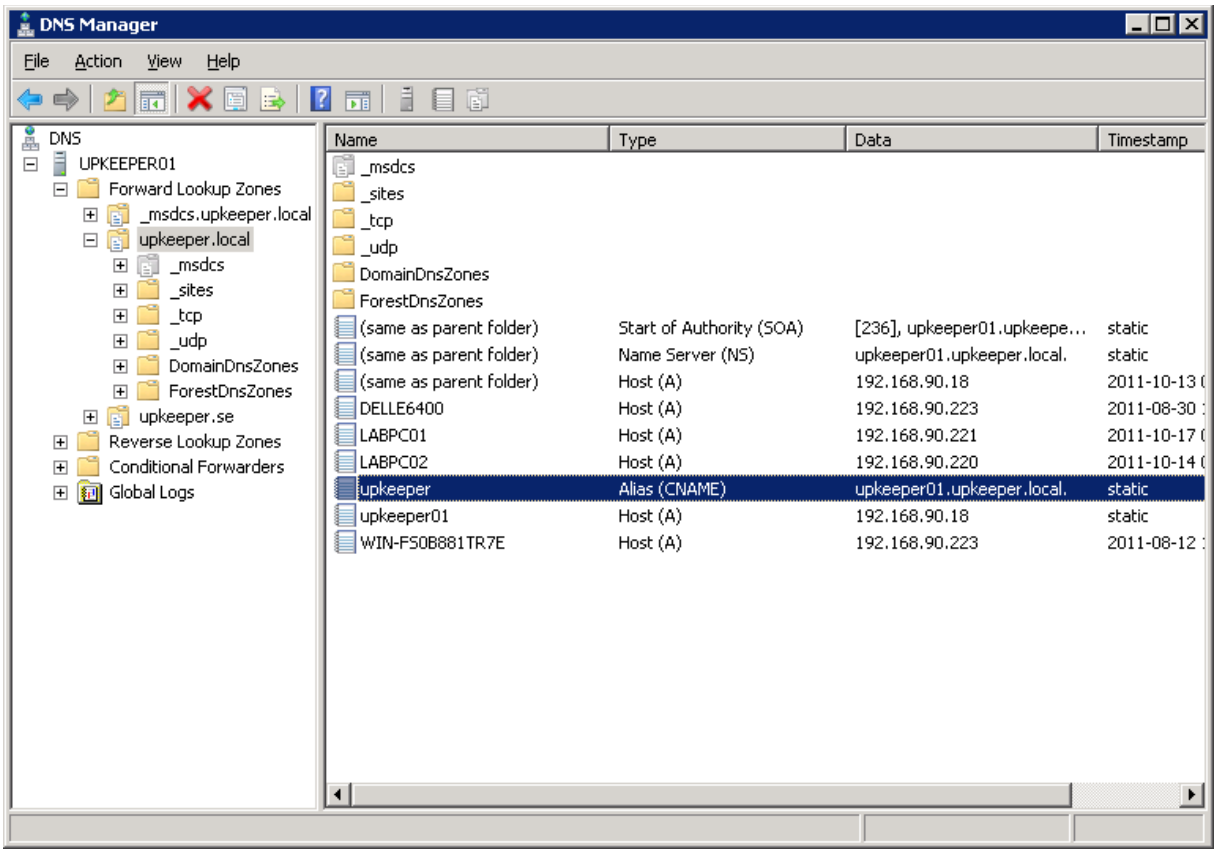
It **must** be possible to perform these settings at the date of implementation of the server modules

Go through the instructions in this document to verify that these changes are feasible (e.g. people with sufficient administrative rights are in place when the server modules will be implemented).

The customers can implement these settings (as described below) to facilitate a smooth implementation of the server modules.

DNS-settings

Add the following aliases.



upkeeperclientapi – Must point to the location where the upKeeper Client API is planned to be installed. (for internal use or in test environment) In production environment, this record should be replaced with an address reachable from any location so that client can be managed from outside the LAN. (Example: **upkeeperclientapi.yourdomain.com**)

upkeeperadminapi – Must point to the location where the upKeeper Admin API is planned to be installed. (for internal use or in test environment) In production environment, this record should be replaced with an address reachable from any location so that the system can be managed from outside the LAN. (Example: **upkeeperadminapi.yourdomain.com**)

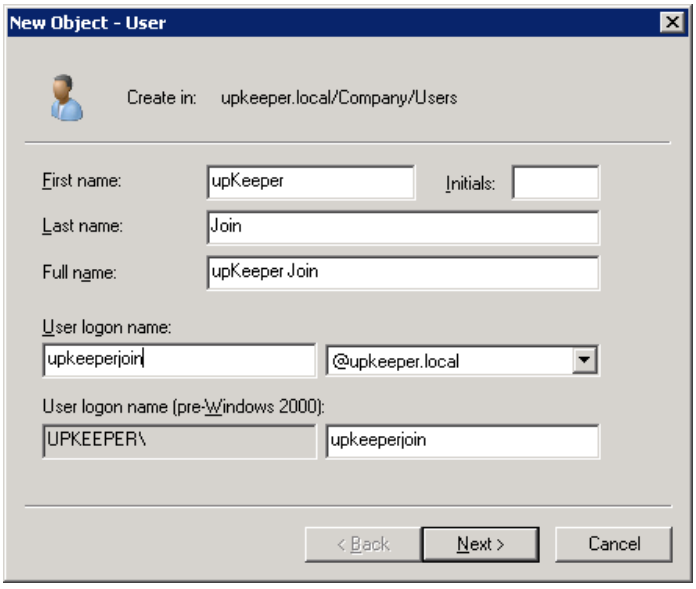
upkeeperweb – Must point to the location where the upKeeper Web is planned to be installed. (for internal use or in test environment) In production environment, this record should be replaced with an address reachable from any location so that the system can be managed from outside the LAN. (Example: **upkeeperweb.yourdomain.com**)

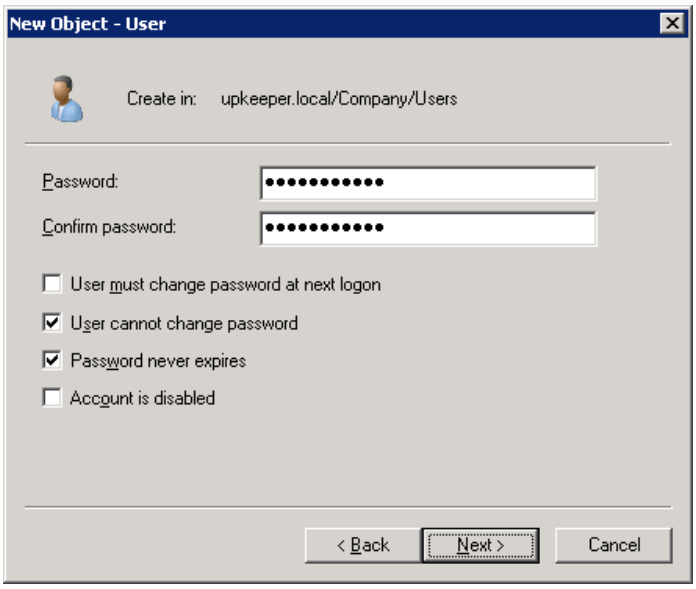
Active Directory – Users

Depending on the features, it is not necessary to create all the accounts as described below. An example is that you do not need to create the account **upKeeper Join** if the managed computers (clients) should not join a domain at installation or reinstallation of the operating system.

upKeeper Join

The user **upKeeper Join** (**note that the user logon name is written together**) is created with the benefit to be used to create computer accounts in the domain and also to join the domain during the setup phase of the client operating system.

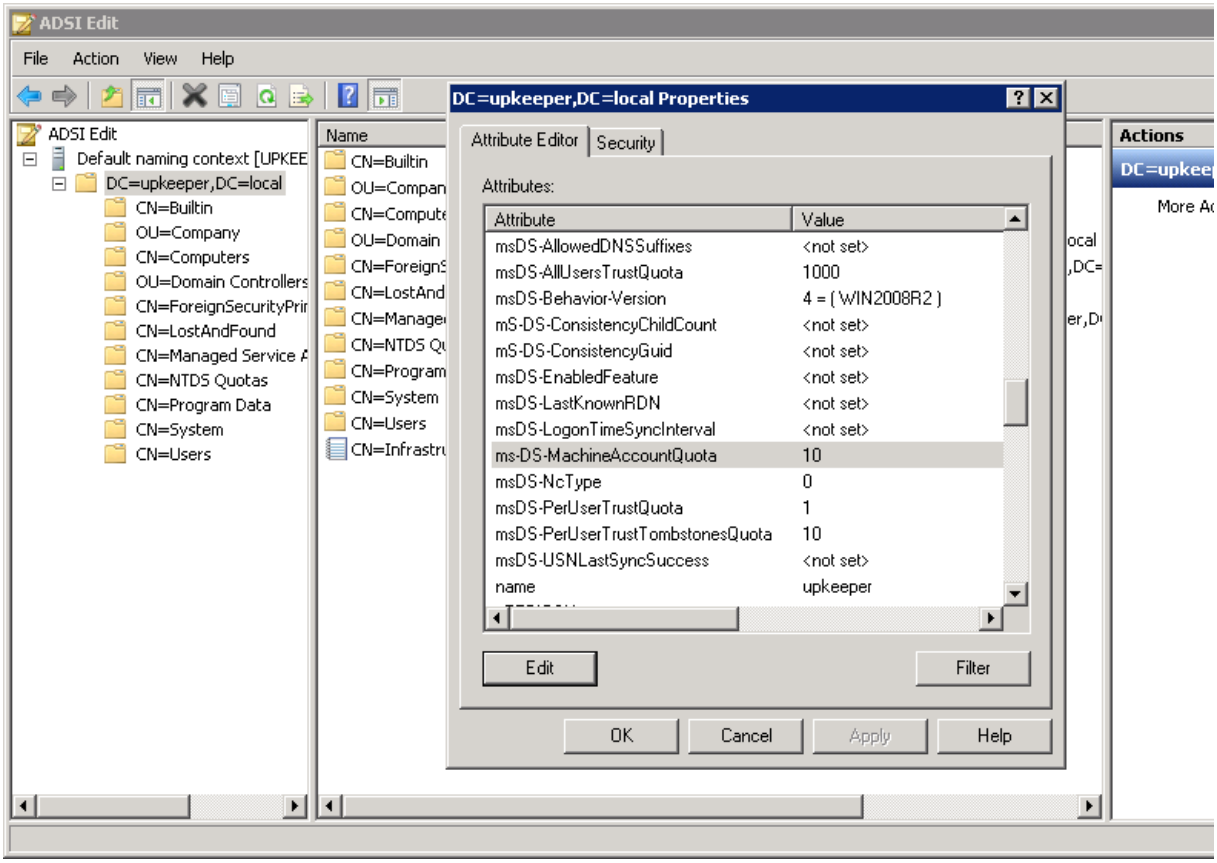




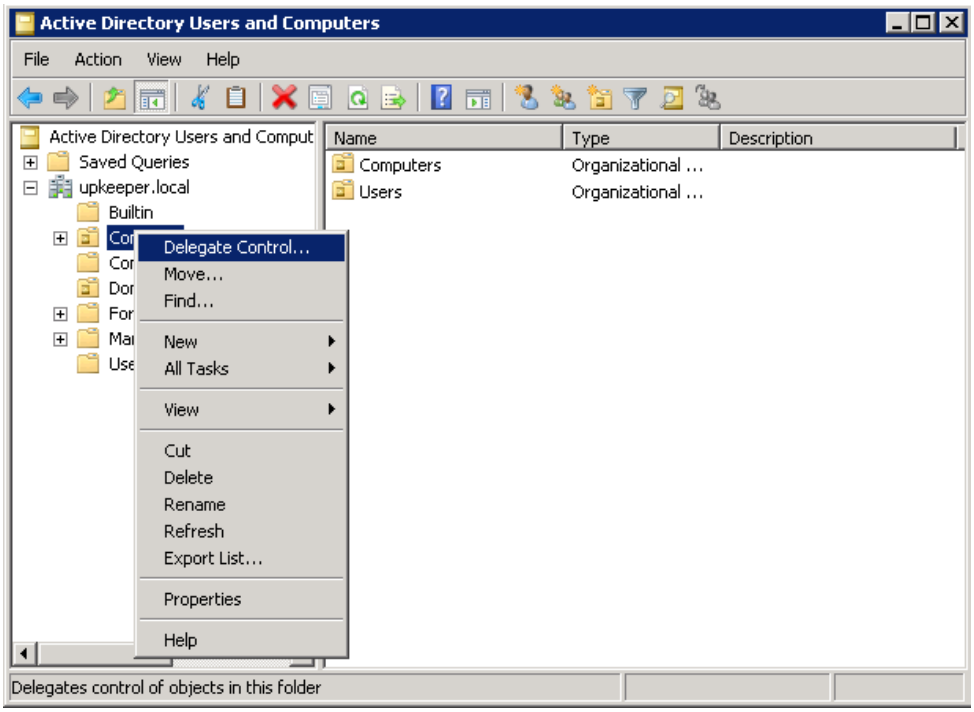
The user should have low rights in the domain. The initial setting of membership in the **Domain Users** group is sufficient. Write down the password entered.

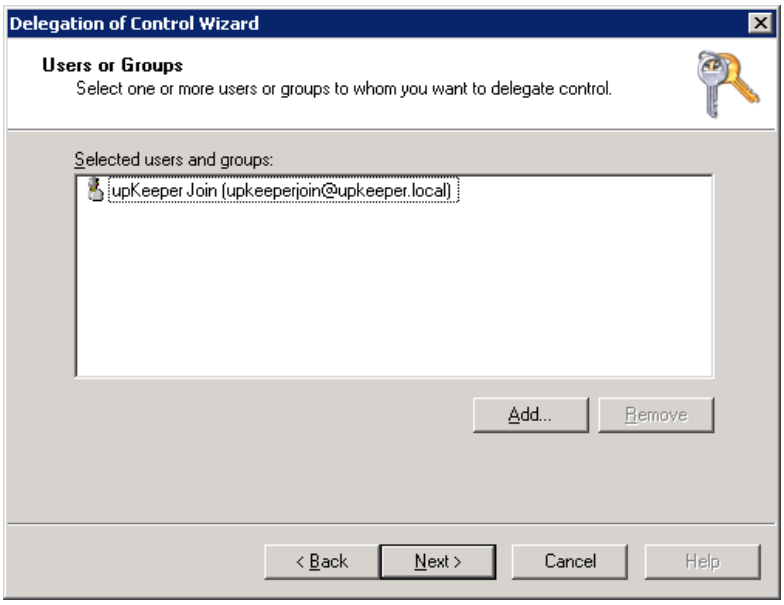
An attribute in the domain schema must be modified in order for the user to include computers in the domain. To do this, adsiedit.msc must be available. ADSIedit is part of the Active Directory Domain Controller Tools feature.

- Start ADSI Edit (start/run/adsiedit.msc)
- Expand the domain node, right click and select properties
- Scroll down to the attribute ms-DS-MachineAccountQuota
- Click on Edit, reset the value by clicking the Clear button, then OK.

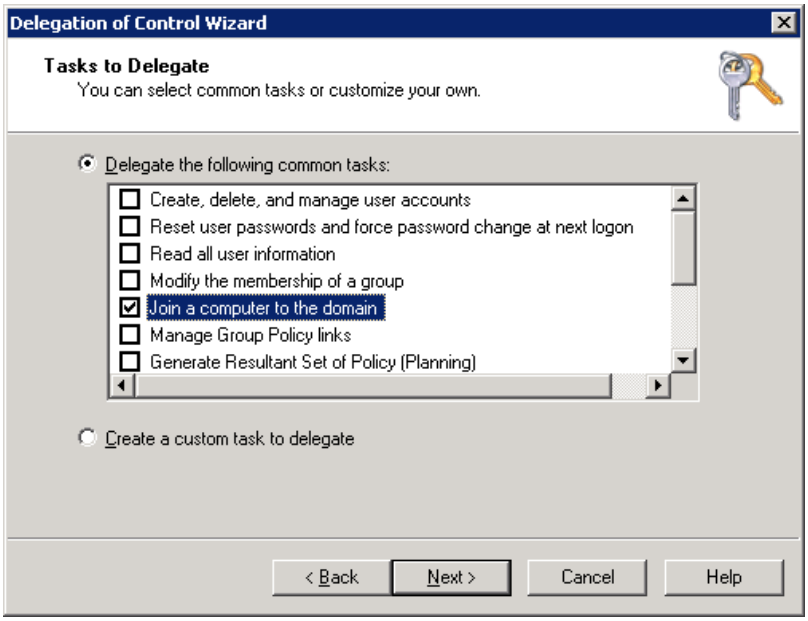


Start the application **Active Directory Users and Computers**, right-click the OU containing your computer objects and select **Delegate Control**. Select the user **upKeeper Join**.



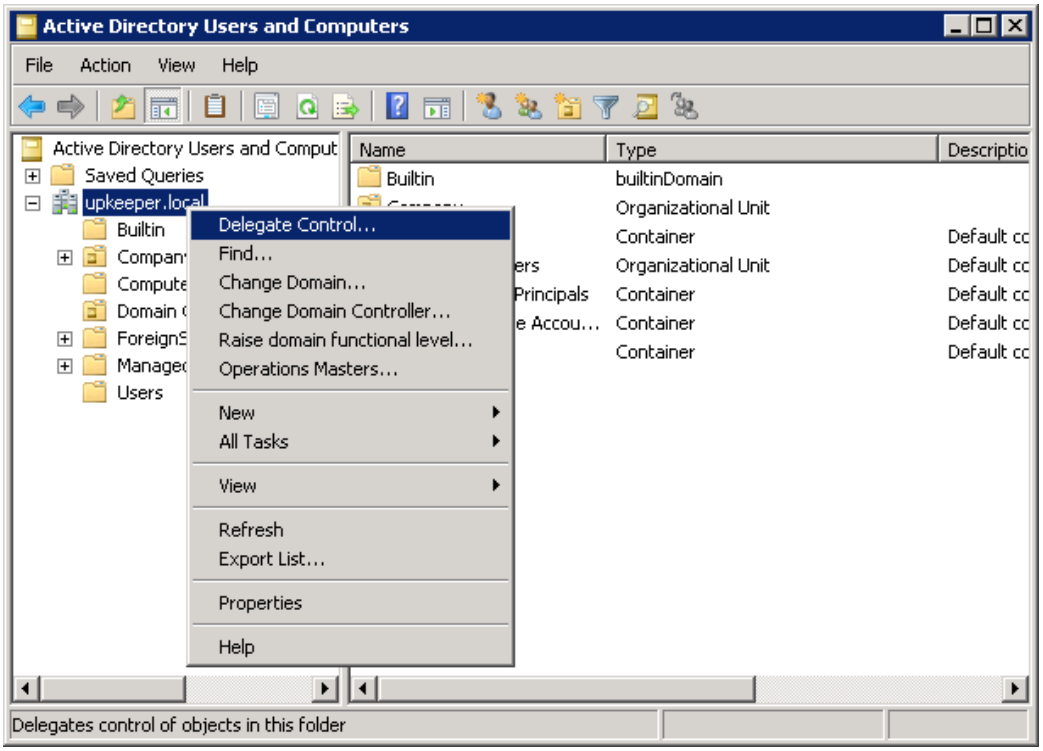


Delegate the task **Join a computer to the domain** and exit the **Delegation of Control Wizard**.

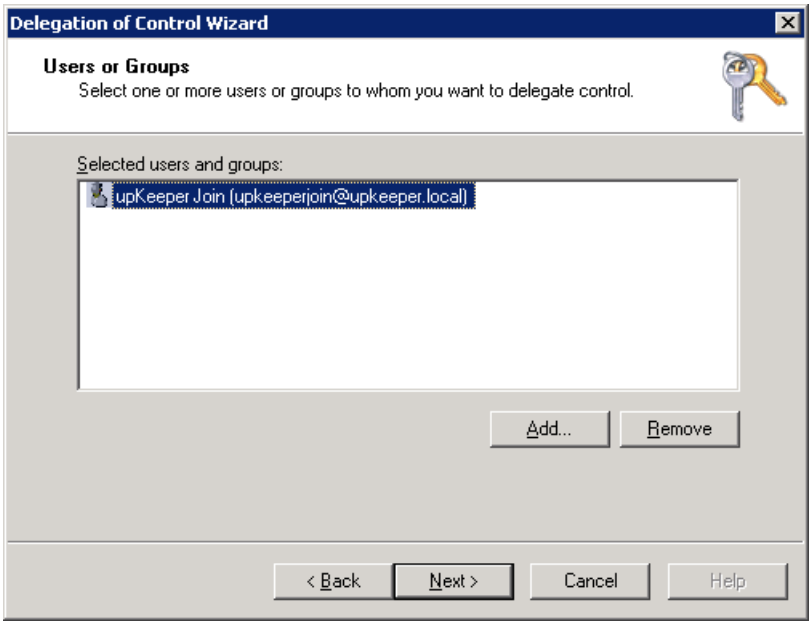


Note! If the task **Join a computer to the domain** does not exist, then try this:

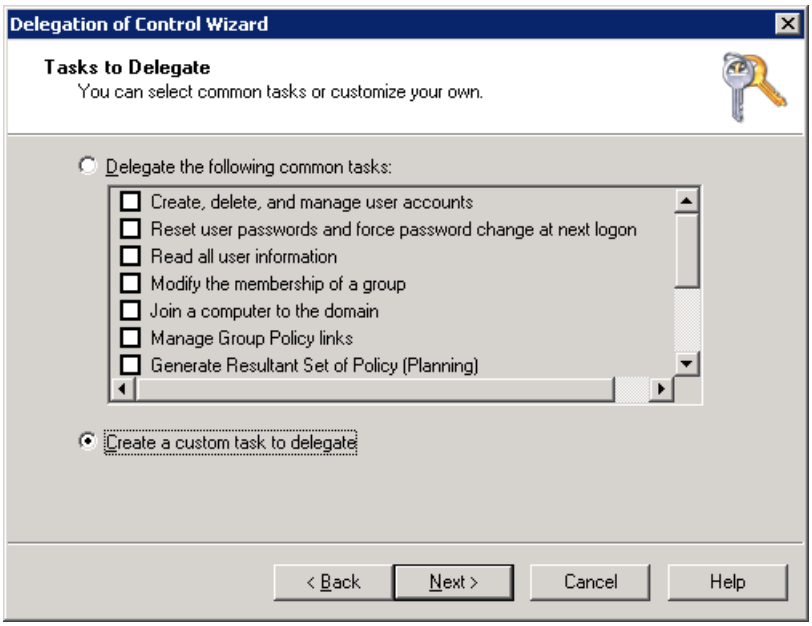
Right-click the OU containing your computer objects and select **Delegate Control**.



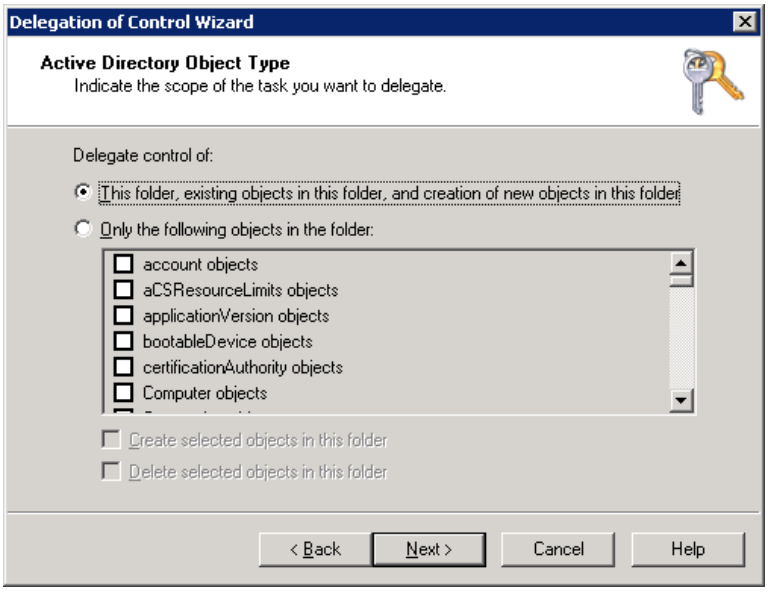
Select **upKeeper Join**.



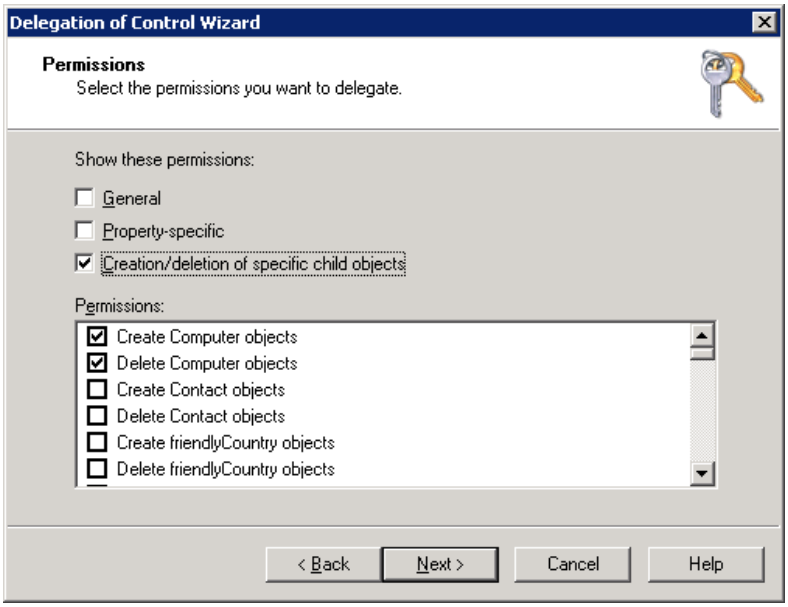
Select **Create a custom task to delegate**.



Perform the settings below and continue.



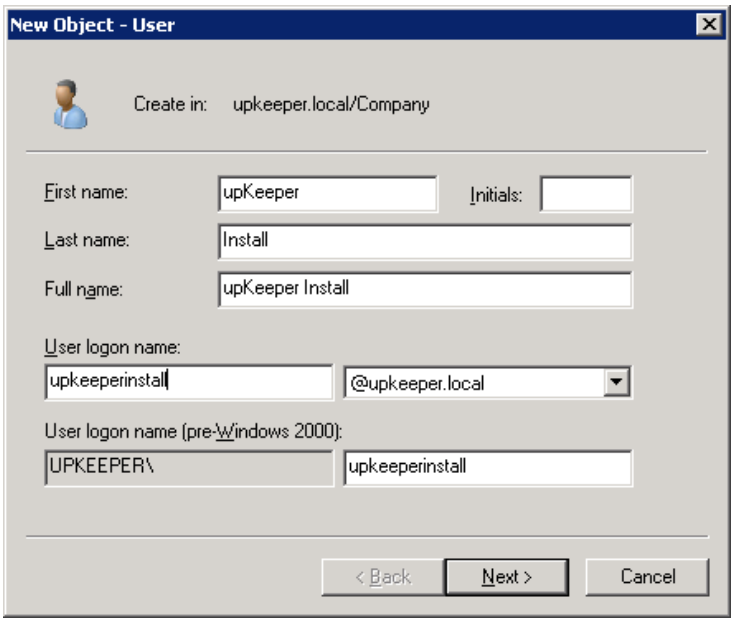
Perform the settings as shown below and continue. The delegation is finished.

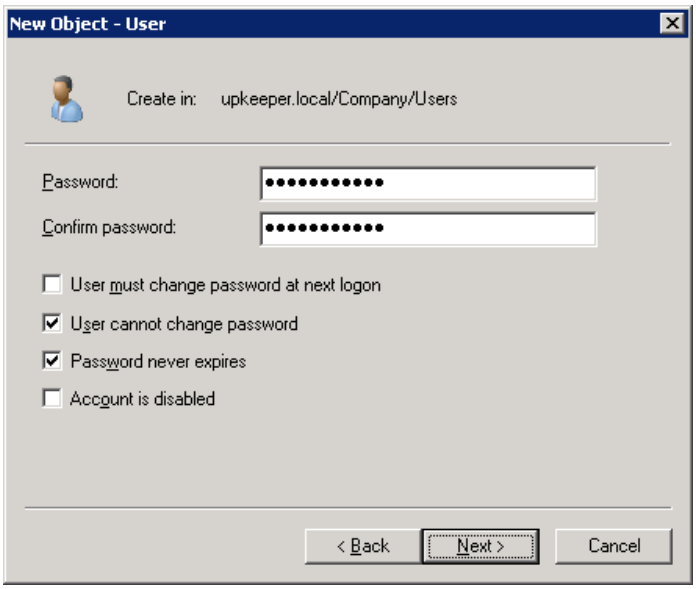


The procedure can of course be repeated on several containers if the structure is not strictly hierarchical.
It can also be applied to the domain object if the delegation must run in the entire domain.

upKeeper Install

Create the user **upKeeper Install** (**note that the user logon name is written together**). The user's purpose is to have access to file sharing, containing OS, applications, drivers, scripts, etc.
This could also be a local account on the distribution point.



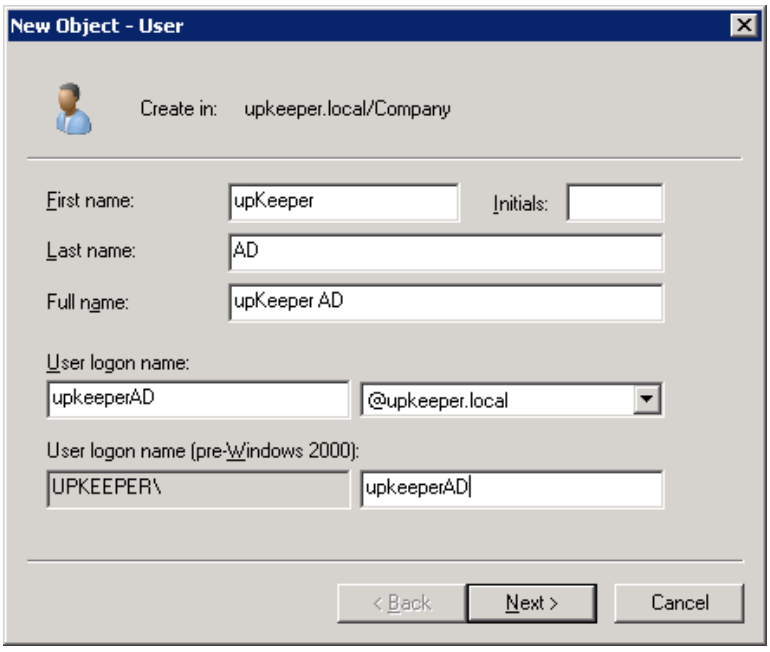


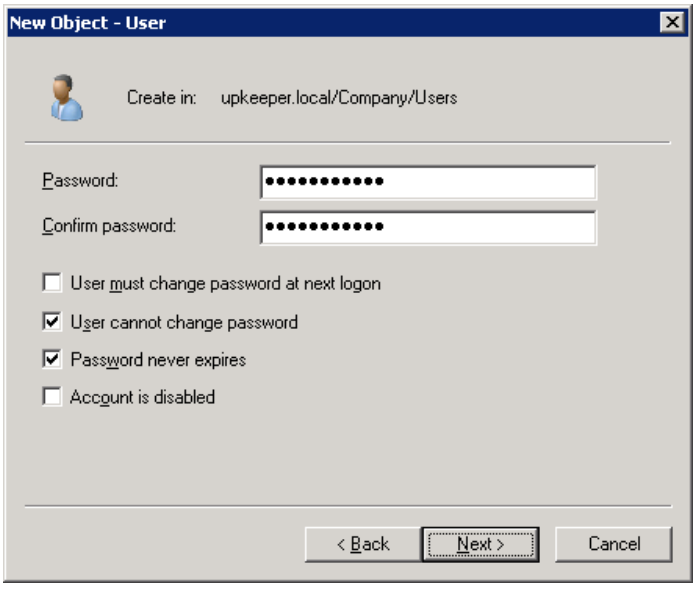
The user must have low rights in the domain.
The initial setting of membership write in the **Domain Users** group is sufficient.
Make a note of the password entered.

upKeeper AD

This account is used by upKeeper to retrieve information from AD.
If groups from AD are going to be synchronized to upKeeper,
then this account shall be created. If not, you can ignore this.

Create user **upKeeper AD** (**note that the username is written together**).





The user must have low rights in the domain.
The initial setting of membership in the **Domain Users** group is sufficient.
Make a note of the password entered.

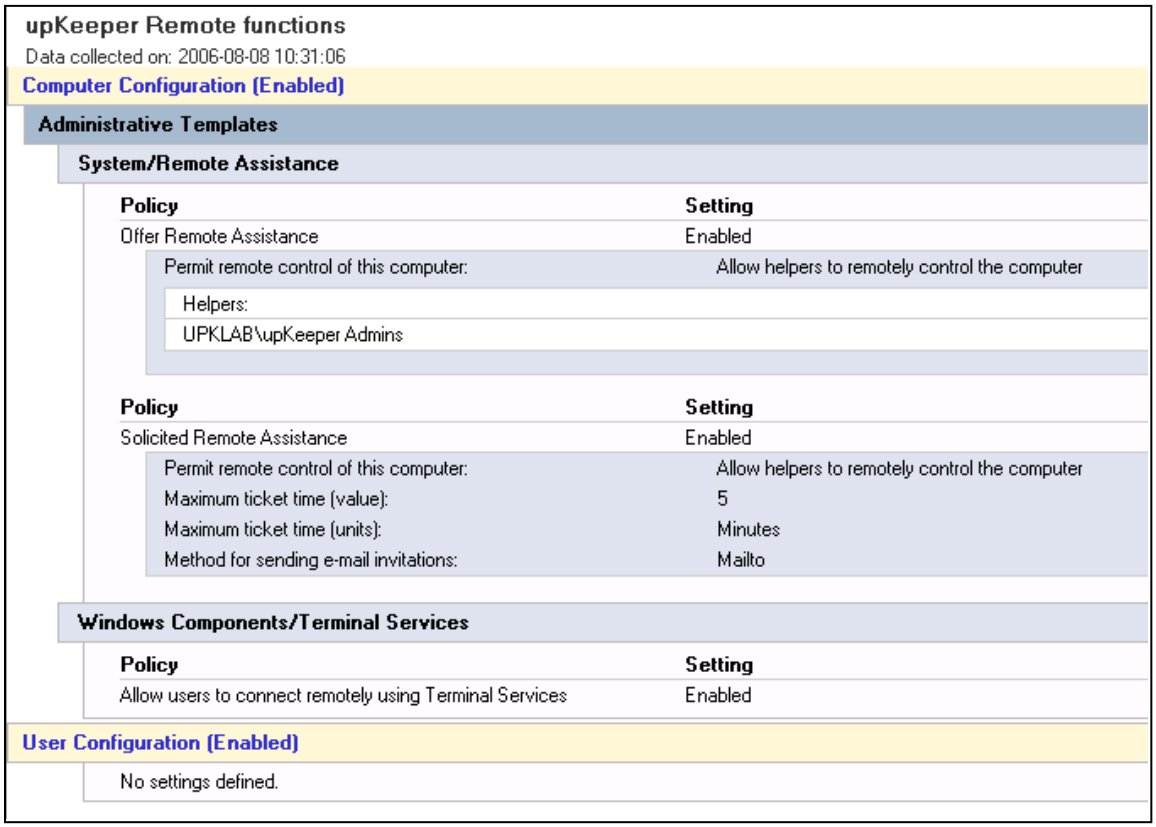
Fileshare

Create a Windows-file share with the NTFS file system on an appropriate server. The file share will house images for operative systems and all of the packaged applications in the environment and should therefore be of generous size.

- Correct the permissions on the file level
  - Remove the rights of ordinary users, such as **Authenticated Users**
  - Provide upKeeper Install the authority to create and remove objects.

Remote Assistance

To be able to use the Remote Assistance you must define that policy.



upKeeper Remote functions

Data collected on: 2006-08-08 10:31:06

Computer Configuration (Enabled)

Administrative Templates

System/Remote Assistance

Policy	Setting
Offer Remote Assistance	Enabled
Permit remote control of this computer:	Allow helpers to remotely control the computer
Helpers:	
UPKLAB\upKeeper Admins	

Policy	Setting
Solicited Remote Assistance	Enabled
Permit remote control of this computer:	Allow helpers to remotely control the computer
Maximum ticket time (value):	5
Maximum ticket time (units):	Minutes
Method for sending e-mail invitations:	Mailto

Windows Components/Terminal Services

Policy	Setting
Allow users to connect remotely using Terminal Services	Enabled

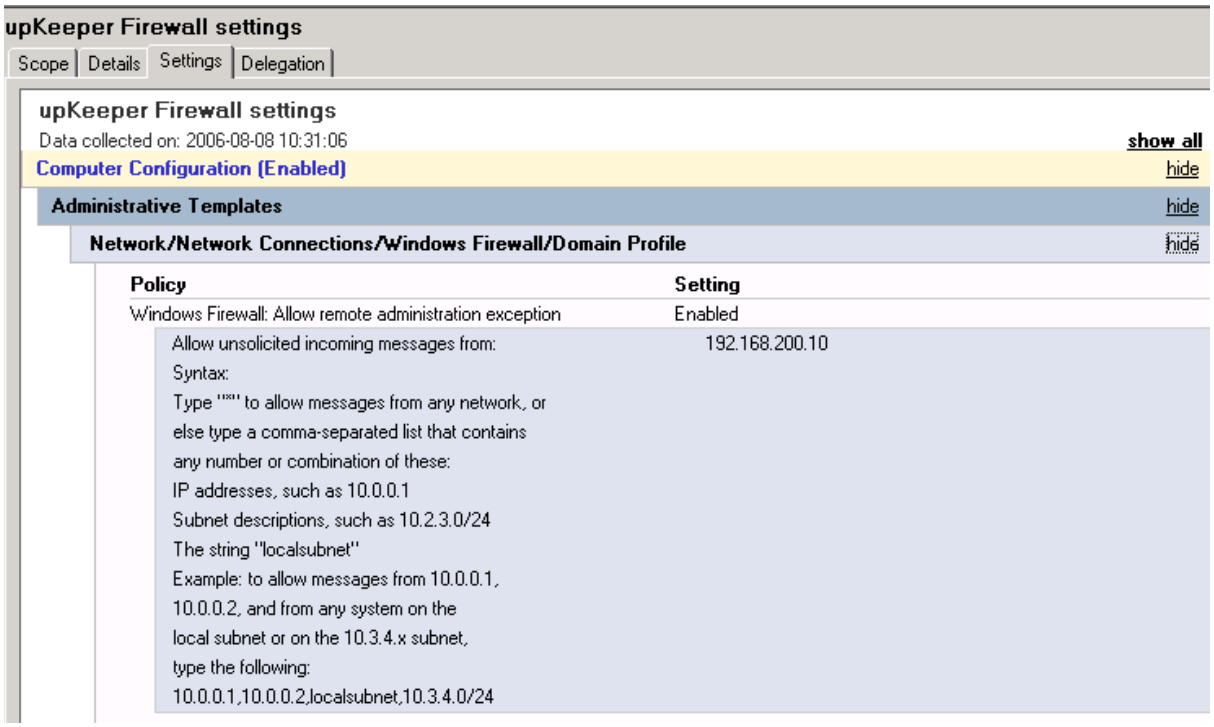
User Configuration (Enabled)

No settings defined.

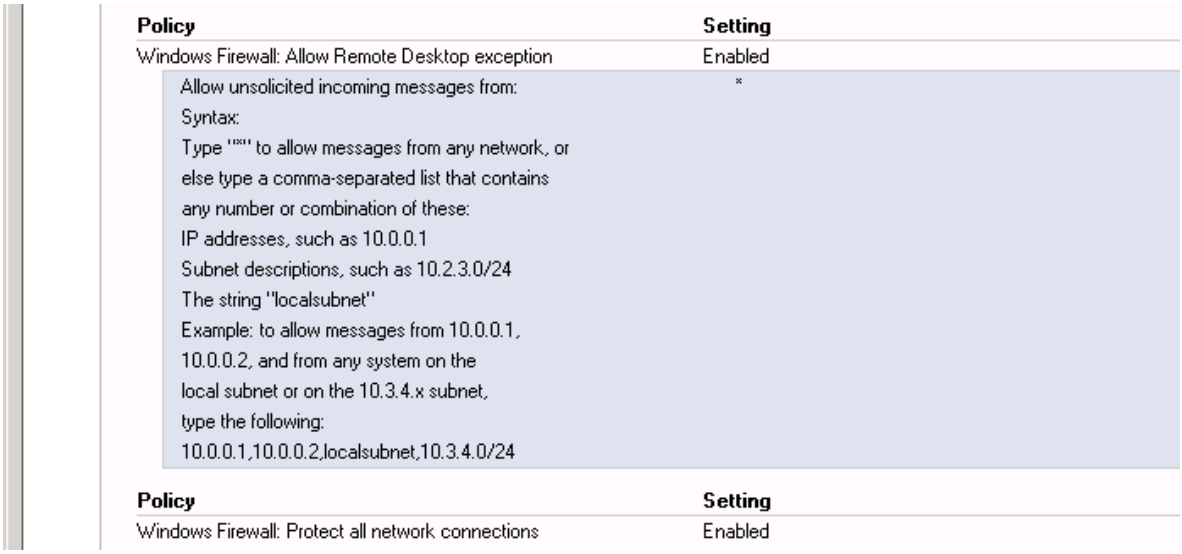
Windows Firewall

Define the following settings if you want the Windows Firewall enabled on the clients.

Replace the IP address below to the address of the server where the upKeeper Application Server has been installed.



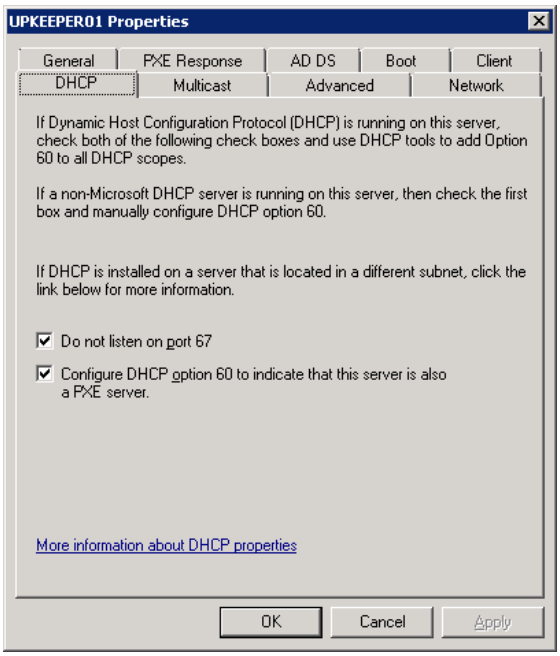
Enter the subnet or IP addresses from which remote desktop connections are allowed to the clients. Enter * to allow all of the subnets.



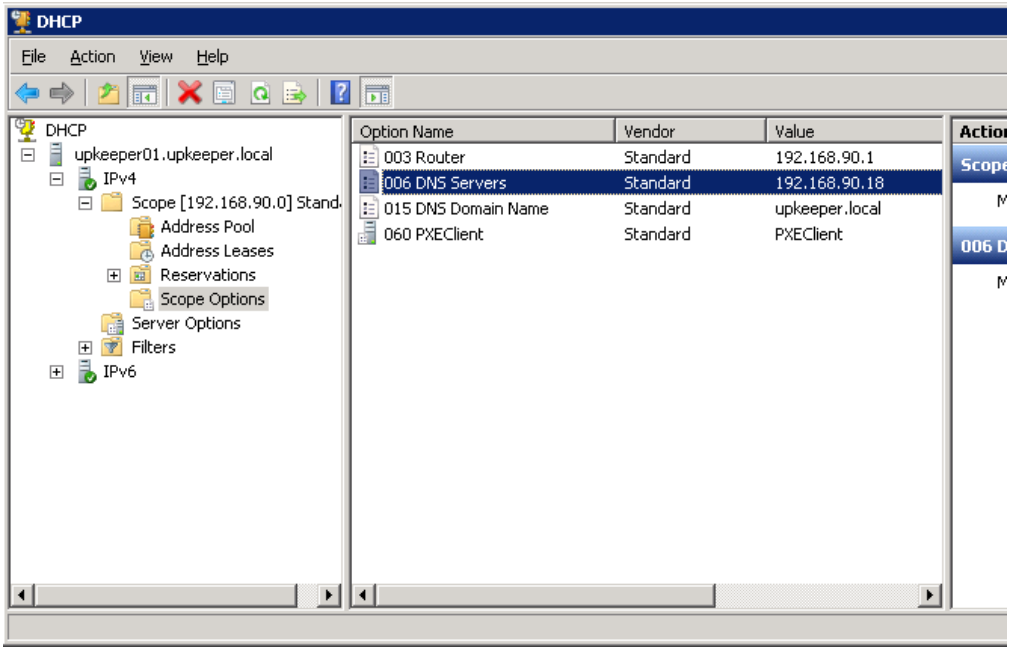
Recommended Services

Windows Deployment Services (WDS)

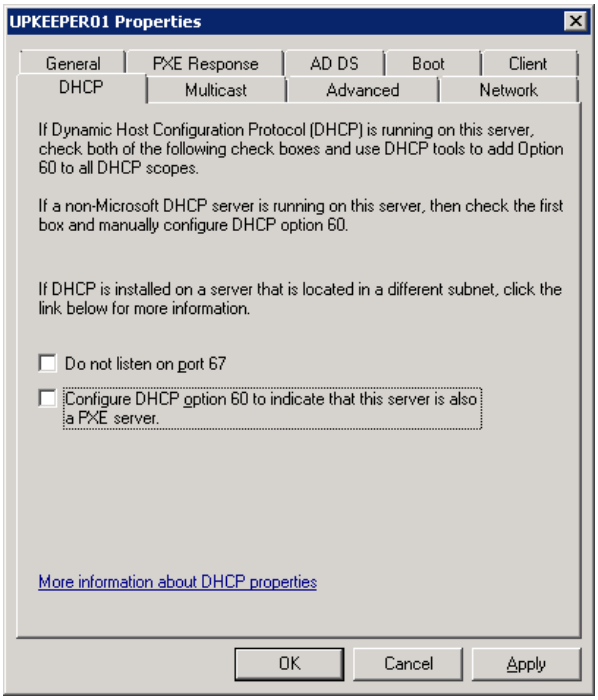
If WDS and DHCP services are running on the same server, ensure that the following settings are enabled in the WDS.



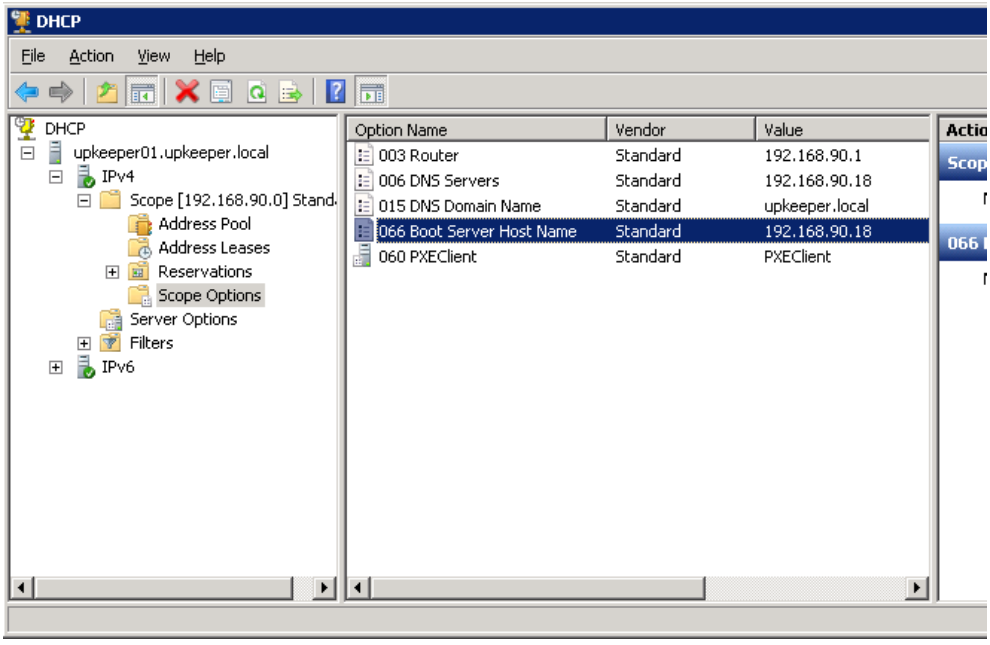
It is recommended that the DHCP options 060 and 066 are configured in a scenario with WDS and DHCP services running on the same server.



The settings below in WDS are applied if the WDS and DHCP services are not running on the same server:



It is also recommended that the DHCP option 066 is configured.

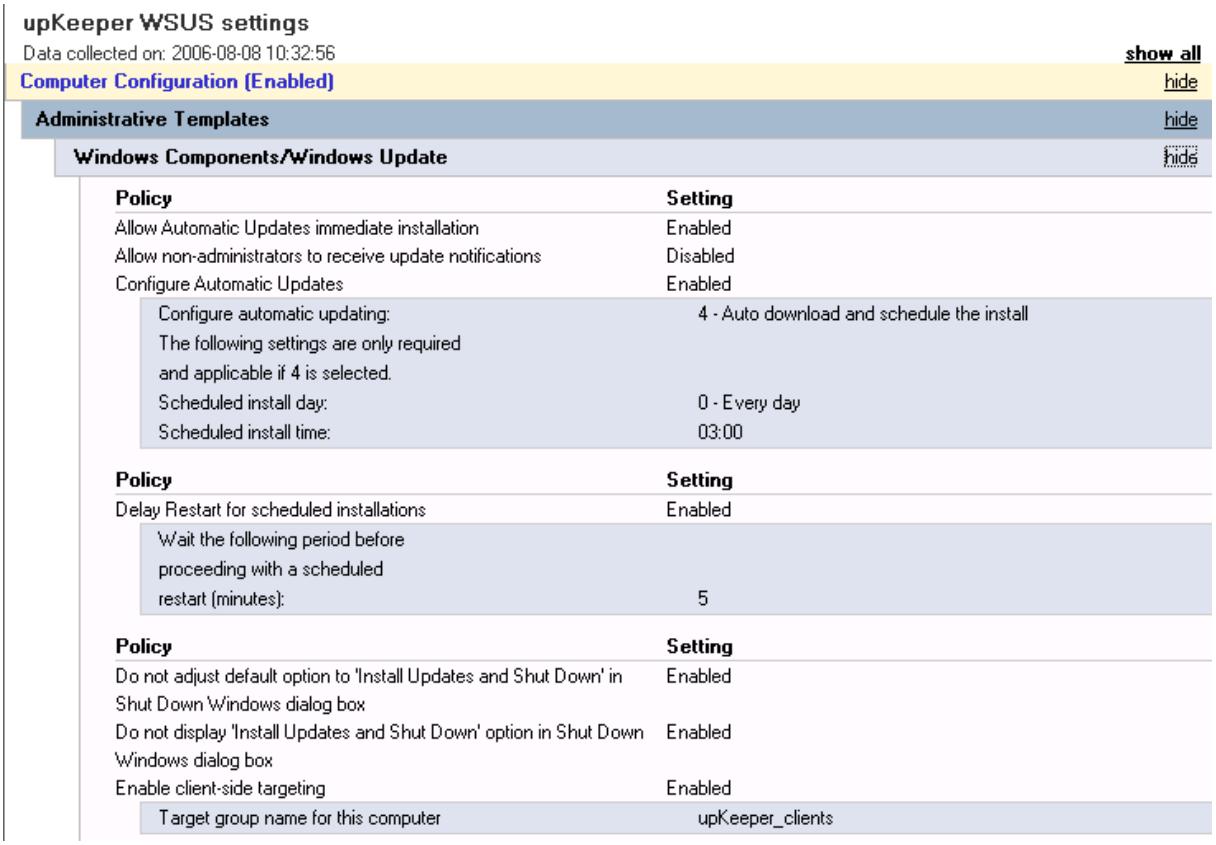


NOTE! IP-helpers are needed if you are going to use WDS in a routed network.

Windows Server Update Services (WSUS)

The settings are only going to be applied if WSUS is used in the organization.

Configure the following policies.



upKeeper WSUS settings

Data collected on: 2006-08-08 10:32:56 — show all

Computer Configuration (Enabled) — hide

Administrative Templates — hide

Windows Components/Windows Update — hide

Policy	Setting
Allow Automatic Updates immediate installation	Enabled
Allow non-administrators to receive update notifications	Disabled
Configure Automatic Updates	Enabled
Configure automatic updating:	4 - Auto download and schedule the install
The following settings are only required and applicable if 4 is selected.	
Scheduled install day:	0 - Every day
Scheduled install time:	03:00

Policy	Setting
Delay Restart for scheduled installations	Enabled
Wait the following period before proceeding with a scheduled restart (minutes):	5

Policy	Setting
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled
Enable client-side targeting	Enabled
Target group name for this computer	upKeeper_clients

Policy	Setting
No auto-restart for scheduled Automatic Updates installations	Enabled
Re-prompt for restart with scheduled installations	Enabled
Wait the following period before prompting again with a scheduled restart (minutes):	10

Policy	Setting
Reschedule Automatic Updates scheduled installations	Enabled
Wait after system startup (minutes):	5

Policy	Setting
Specify intranet Microsoft update service location	Enabled
Set the intranet update service for detecting updates:	http://upkeeper:8530
Set the intranet statistics server: (example: http://IntranetUpd01)	http://upkeeper:8530

Change the setting **Enable client-side targeting** so the **Target group name for this computer** matches the WSUS-group you created in the WSUS-admin interface for computers. Also replace the **Specify intranet Microsoft update service location**" to the current address of the WSUS server.

Wake On Lan

If you are going to use Wake On Lan in a routed network you have to enable sub directed broadcast (Magic packet).