SoftControl

DLP Client 4.3.10

Installation guide

Dear user!

SAFE 'N SEC Corporation thanks you for choosing SoftControl DLP Client. Specialists of the company do their best to make our software both meets the highest requirements in a field of information protection and be handy in use. We hope that SoftControl DLP Client will be helpful for you.

SAFE 'N SEC Corporation, 2017

Postal address:

127106 Russia, Moscow

Altufyevskoe shosse, 5/2

SAFE 'N SEC Corporation

Tel:

+7 (495) 967-14-51

Fax:

+ 7 (495) 967-14-52

E-mails:

Customer service: sns@safensoft.com

Sales team: sales@safensoft.com

Website: http://www.safensoft.com

Contents

1. Introduction

1.1. Purpose

SoftControl DLP Client is designed to control the actions of the corporate network users and to provide company's information security by means of protection against insider incidents. SoftControl DLP Client collects data about users' activity, which allows the security service to monitor how staff accesses the information that represents the trade secret and other confidential data. The obtained reports can be used to perform backward analysis of the data leaks protection, to monitor the efficiency of the working time, etc.

1.2. Main features

SoftControl DLP Client provides the following key features of data collection:

- **Observation** over file system resources, system registry resources, and network activity:
  - logging all operations (read, create, rename, change, and delete) with file system and system registry objects;
  - logging data in HTTP traffic;
  - creating shadow copies of objects under observation;
  - capturing screenshots when events under observation occur.
- **Monitoring the operating time in applications**:
  - logging the start time and the end time of working with the application.
- **Monitoring the peripherals**:
  - checklist of the system's peripherals;
  - logging when devices are added to or removed from system.
- **Recording text that the user enters with the keyboard**:
  - logging the record time and the text that the user enters with the keyboard, in any application.
- **Tracing files that are sent to print**:
  - logging the path to the file, printing time and description of the print source.
- **Tracing files that are sent by e-mail**:
  - logging user name, the time when the file was sent and the path to the file attachment when working with the Microsoft® Outlook® 2003 mail client.

1.3. Notational conventions and terms

1.3.1. Notational conventions

Table 1 lists notational conventions used in this document.

Table 1. Notational conventions

Notation example	Description
	An important information, a note.
Condition	An execution condition, a note, or an example.
Update	– headers and acronyms; – names of buttons, links, menu items, and other program interface elements.
Control policy	– terms (definitions); – names of files and other objects; – messages displayed to user.
`C:\Program Files\SoftControl`	Paths to directories, files, or registry keys.
`%windir%\system32\msiexec.exe /i`	Source code, command and configuration file fragments.
<SoftControl SysWatchinstallation directory>	Fields with specific names to be replaced with actual values.
Appendix 5	Links to internal resources (document sections) with a specific page number, or links to external resources (URL).

1.3.2. List of acronyms

This documents uses the following acronyms:

- **CPU** – central processing unit;
- **HDD** – hard disk drive;
- **OS** – operating system;
- **RAM** – random access memory.

1.3.3. Glossary

Table 2. Glossary

Term	Description
Host	A computer device (workstation / server / self-service terminal) that is connected to the local area network or wide area network.

2. Hardware and software requirements

2.1. SoftControl DLP Client system requirements

Table 3. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
▪ Microsoft® Windows® XP (SP3) x86 (32-bit) ▪ Microsoft® Windows® Server 2003 (SP2) x86/x64 (32-bit/64-bit)	800MHz	512MB	20MB
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10	1GHz	1024MB	

3. Installing and setting up SoftControl DLP Client

SoftControl DLP Client can be installed onto client hosts both locally [7] and one of the remote centralized [10] ways. Choice of appropriate installation way depends on the specific conditions of employment and defined on basis of such criteria as a number of the endpoints, organization of the network, security policy and other features of the deployment environment.

This section also describes how to register SoftControl DLP Client on the server [24] of SoftControl Service Center.

3.1. Local installation

This way means local installation of application copies to the each client host.

You can install SoftControl DLP Client locally in the following ways:

- standard mode (via GUI) [7];
- silent mode [10].

3.1.1. Installing the component in standard mode

1) Run the *DLP_Client.msi* installation package.
2) Click **Next** in the **SoftControl DLP Client Setup** window (fig. Running the installer [7]).

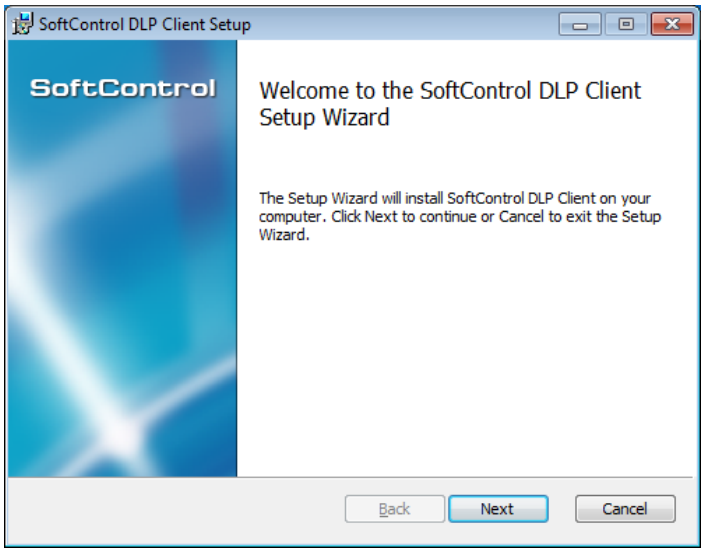

Figure 1. Running the installer

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement [7]).

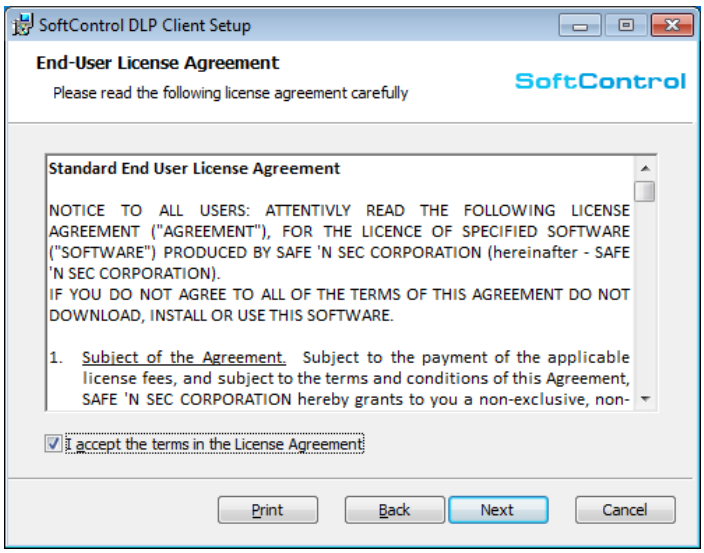

Figure 2. License agreement

4) Select a directory to install SoftControl DLP Client to (with the help of the **Change** button) and click **Next** (fig. Installation path 8).

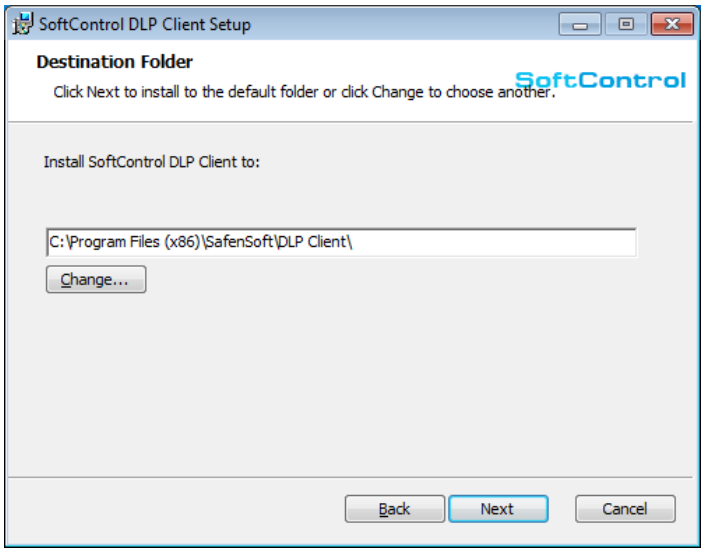

Figure 3. Installation path

5) Click **Install** (fig. Ready to install 8).

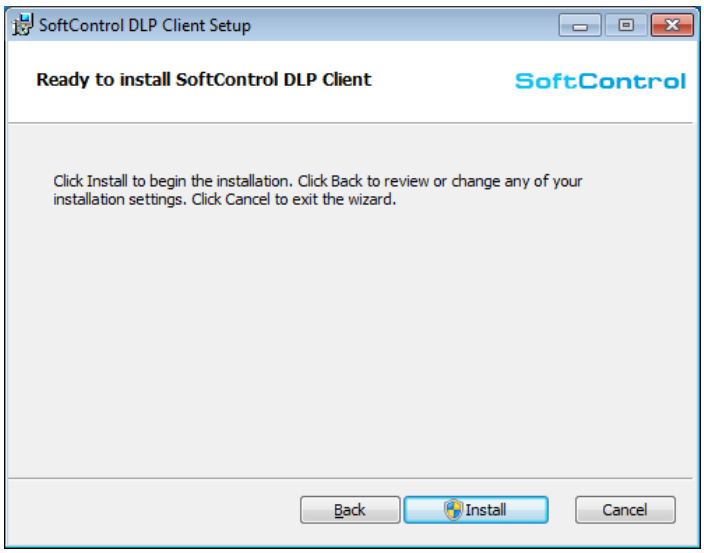

Figure 4. Ready to install

6) Wait until installation completes (fig. Installation progress 9).

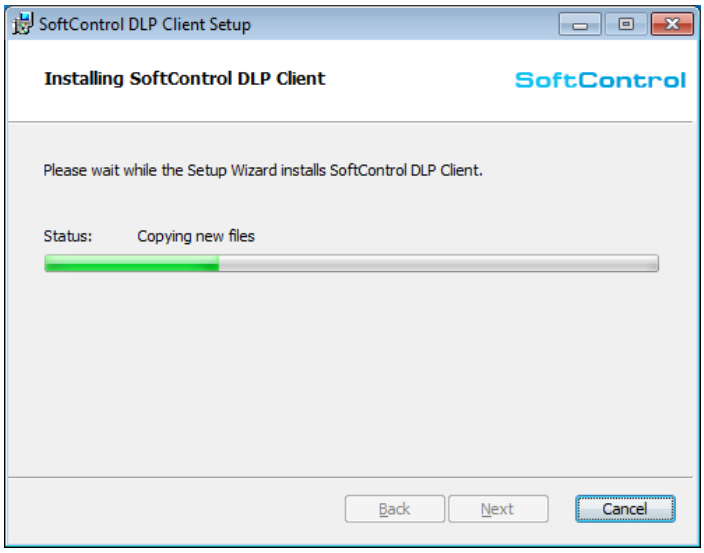

Figure 5. Installation progress

7) After the **Completed the SoftControl DLP Client Setup Wizard** message is displayed, click **Finish** (fig. Installation completes 9).

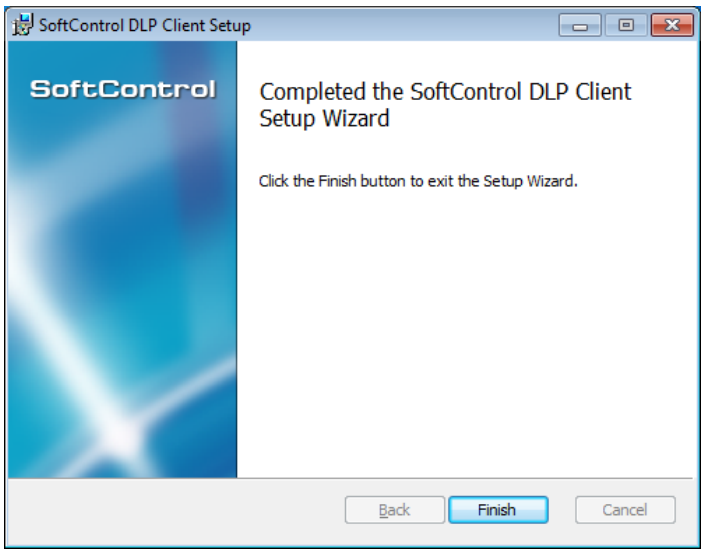

Figure 6. Installation completes

8) Select **Yes** in the dialog box with system restart suggestion. The system restarts to complete the installation (fig. Requesting system reboot 10).

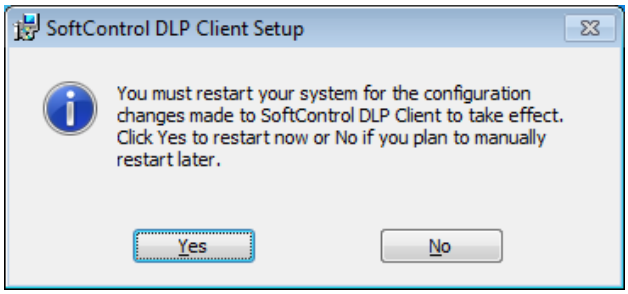

Figure 7. Requesting system reboot

3.1.2. Installing the component in silent mode

Important: all steps require administrator privileges.

1) Copy the *DLP_Client.msi* installation package to the `C:\Temp` directory of a client host.

2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /i "C:\Temp\DLP_Client.msi" /quiet
```

After the installation completes, system restarts automatically.

3.2. Remote installation

Remote SoftControl DLP Client installation implies centrally managed installation of client applications on the group of hosts that are integrated into a network. Choosing the installation method depends on the structure of network with the endpoints where client applications are to be

deployed (a workgroup or a domain), and the administrative tools in use.

You can install SoftControl DLP Client remotely in the following ways.

- via domain group policy [11];
- via the remote installation utility [21];
- via third party administrative tools [24].

3.2.1. Installing via domain group policy

Note: The example below uses Microsoft® Windows® Server 2008 R2.

1) Open the **Server Manager** snap-in from the **Administrative Tools** section of the **Start** menu in the OS of the domain controller.
2) Go to the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section, invoke its context menu and select **New Organizational Unit** (fig. Creating new domain organizational unit [11]).
3) Enter **Name** of the unit in the **New Organizational Unit** dialog box and click **OK** (fig. Specifying the name of the organizational unit [12]).
4) Invoke context menu of the created organizational unit in the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section and select **Create a GPO in this domain, and Link it here** (fig. Creating a new object of the group policy [12]).

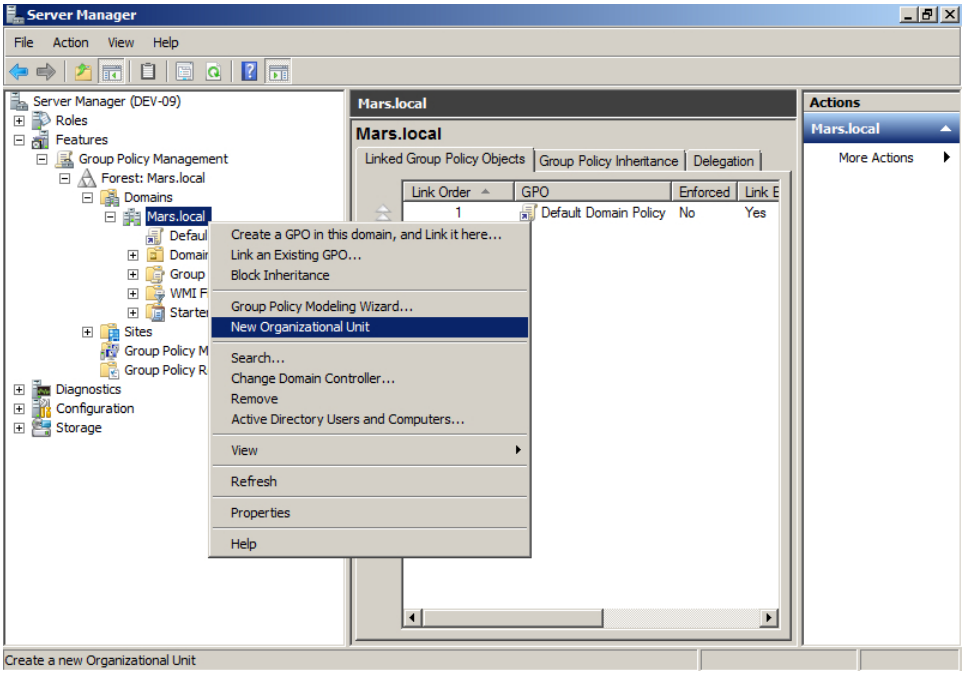

Figure 8. Creating new domain organizational unit

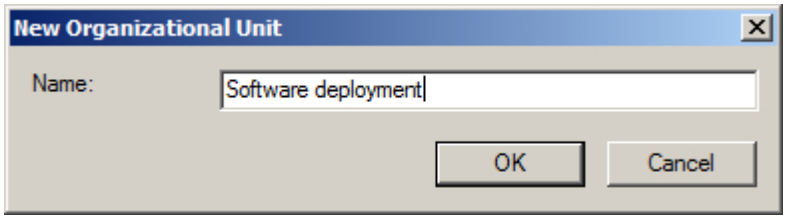

Figure 9. Specifying the name of the organizational unit

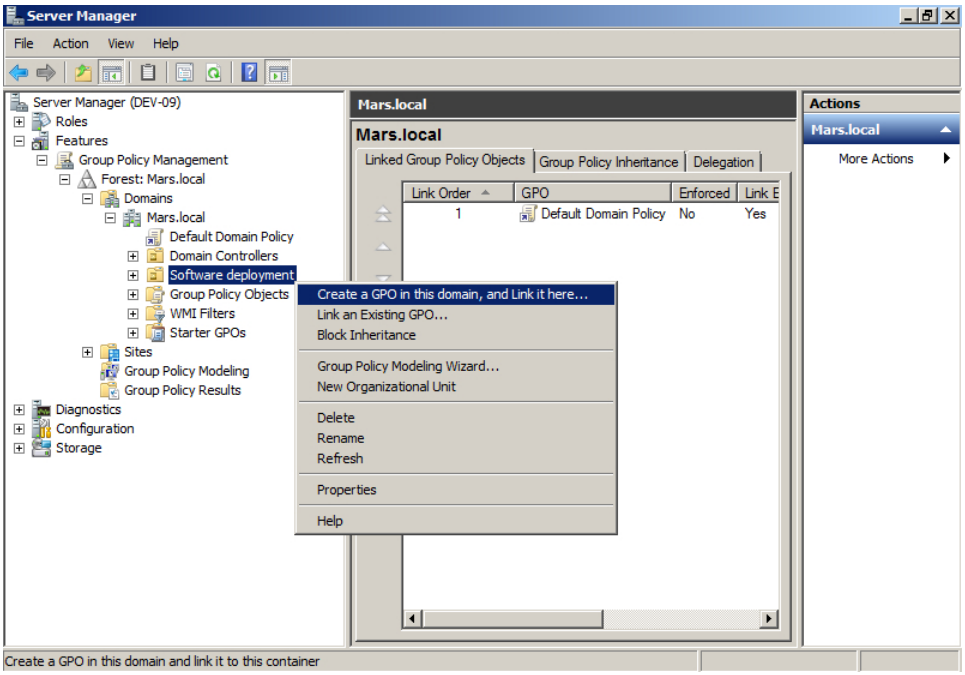

Figure 10. Creating a new object of the group policy

5) Enter **Name** of the new object in the **New GPO** dialog box and specify **Source Starter GPO**, if

the new object should inherit properties from the pattern group policy, and then click **OK** (fig. Specifying the name and source starter GPO of new group policy 13).

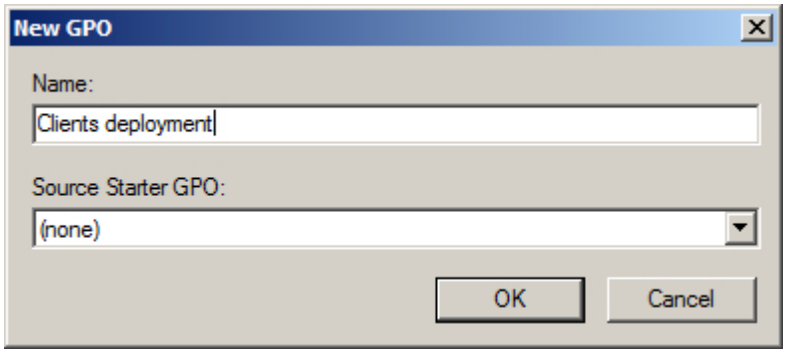

Figure 11. Specifying the name and source starter GPO of new group policy

6) Expand the created organizational unit, invoke the context menu of the created group policy object and select **Edit** (fig. Modifying group policy object 13).
7) Go to the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the displayed **Group Policy Management Editor** snap-in window, invoke the context menu of the section and select **New** → **Package** (fig. Adding new installation package 13).
8) Select the *DLP_Client.msi* installation package which is in the network source available to the client hosts you need to install the products to, and click **Open** (fig. Selecting the installation package 14).

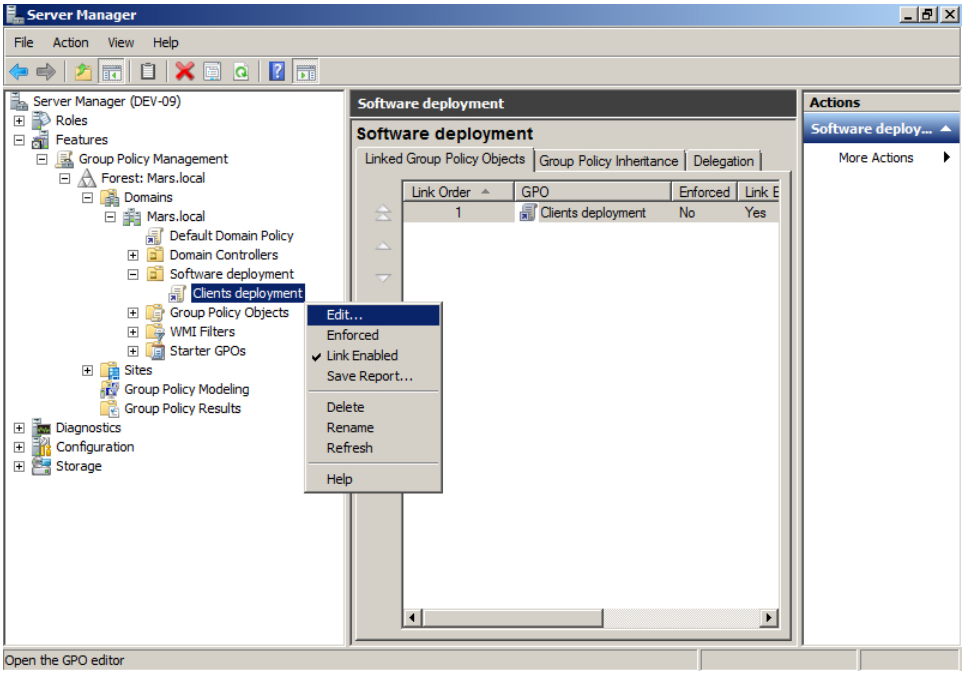

Figure 12. Modifying group policy object

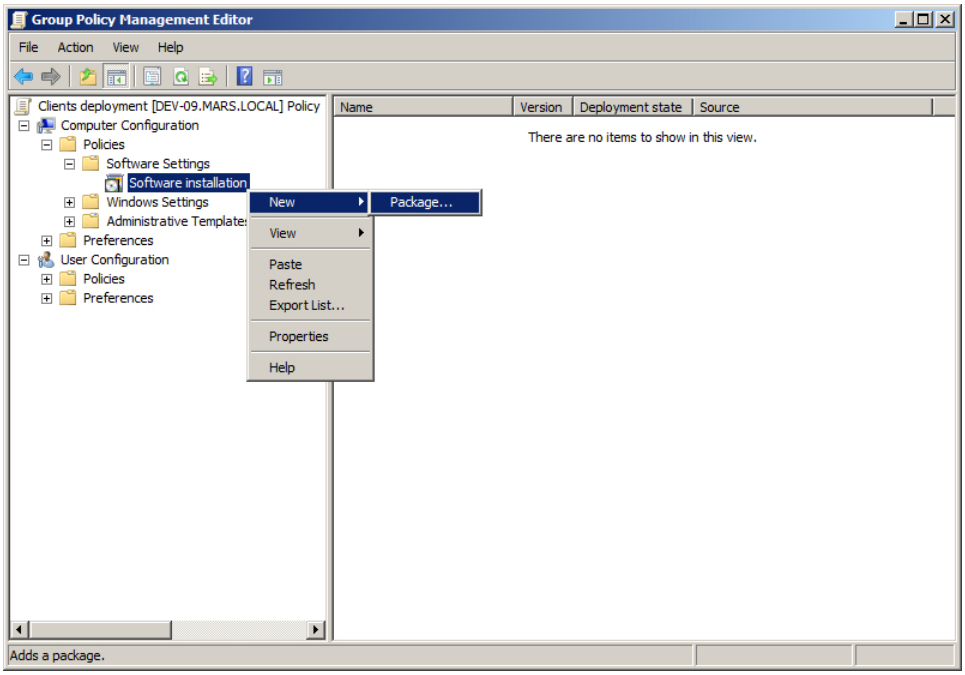

Figure 13. Adding new installation package

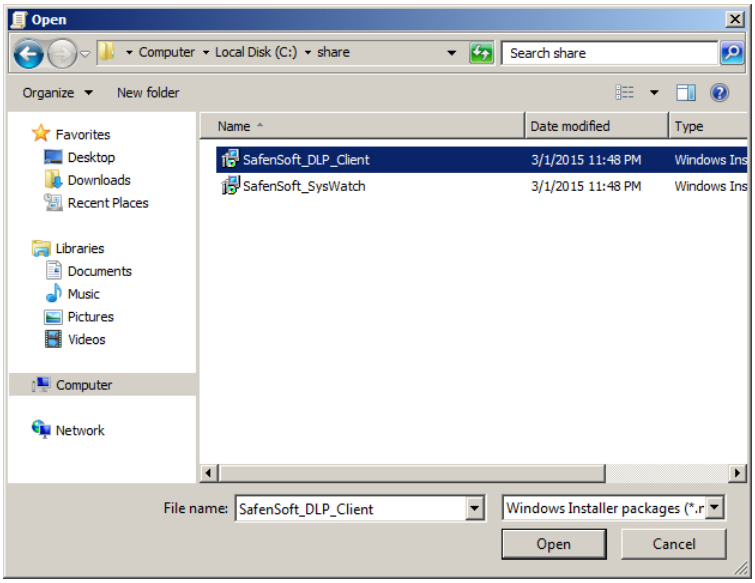

Figure 14. Selecting the installation package

9) If an alert is displayed, make sure that the selected installation package is available for the remote client hosts via network, and click **Yes** (fig. Alert when selecting the location of the installation package 14).

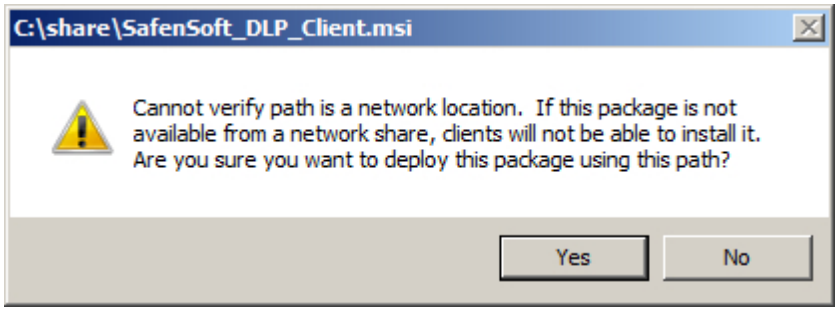

Figure 15. Alert when selecting the location of the installation package

10) Select the **Assigned** deployment method in the **Deploy Software** dialog box and click **OK** (fig. Selecting deployment method 15).

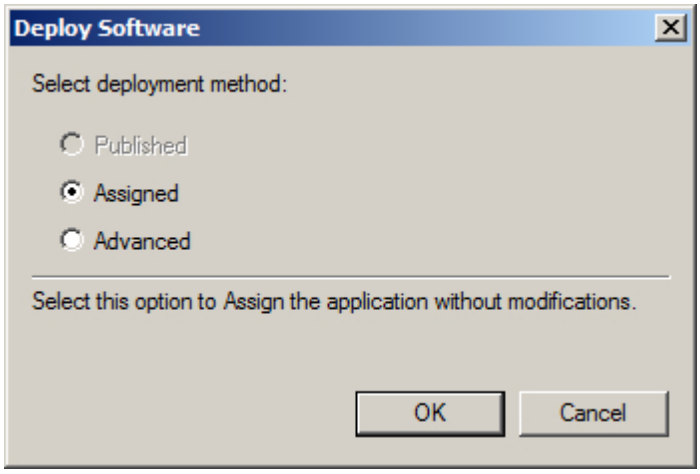

Figure 16. Selecting deployment method

11) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the **Group Policy Management Editor** snap-in window, invoke the context menu of the section and select **Properties** (fig. Modifying properties of software deployment 15).

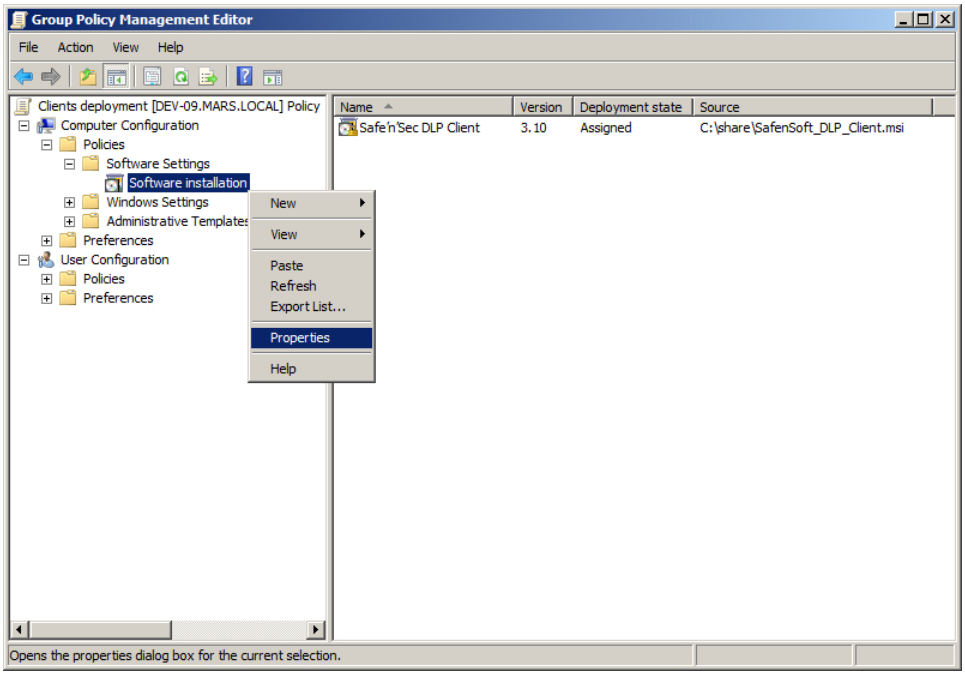

Figure 17. Modifying properties of software deployment

12) Switch to the **Advanced** tab of the **Software installation Properties** settings window, tick off **Uninstall the applications when they fall out of the scope of the management** if you need to remove applications when the specified group policy regarding the client hosts expires, and tick off **Make 32-bit X86 Windows Installer applications available to Win64 machines**, if you plan to install onto the client hosts with 64-bit OS (fig. Properties of software deployment 16). To apply changes, click **OK**.

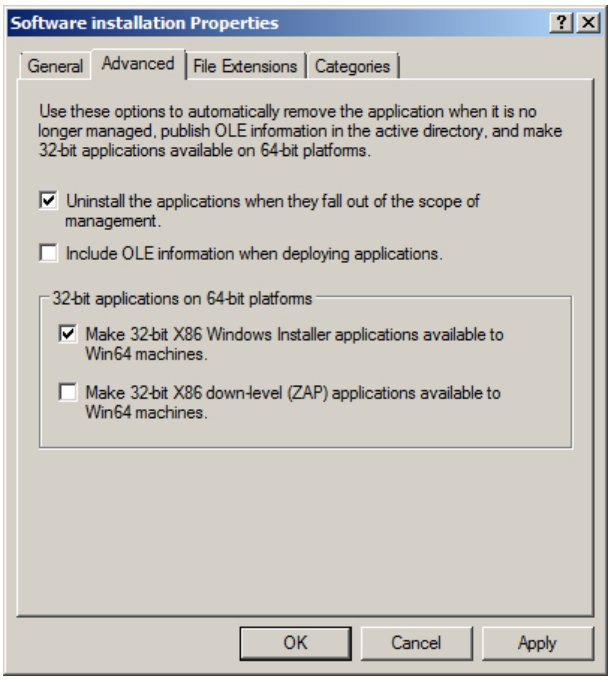

Figure 18. Properties of software deployment

13) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the **Group Policy Management Editor** snap-in window, select the required application from the list on the right, invoke its context menu and select **Properties** (fig. Modifying the properties of the application deployment 17).

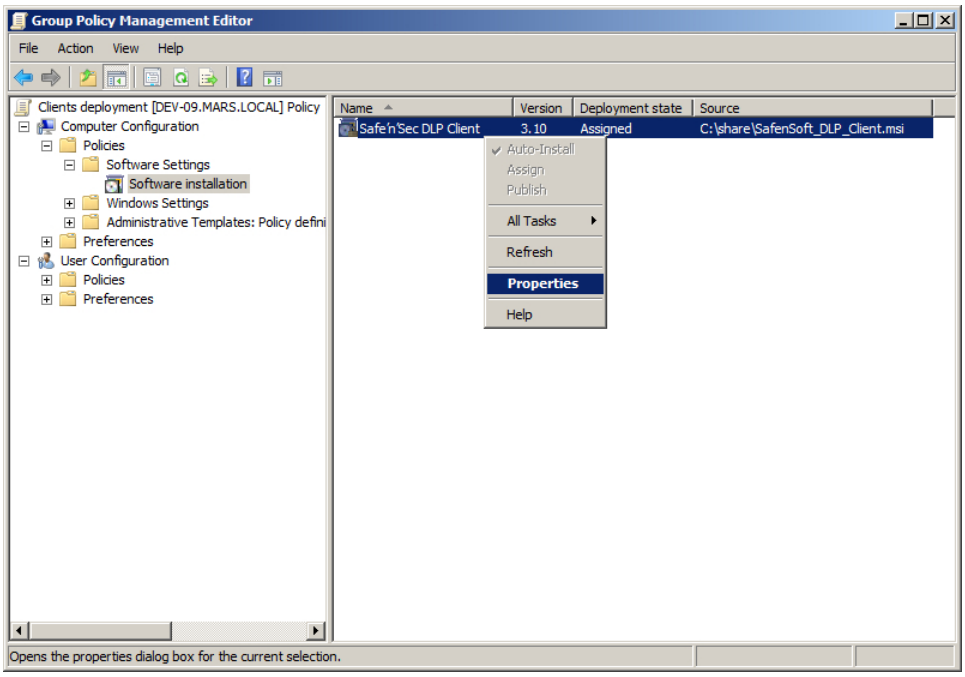

Figure 19. Modifying the properties of the application deployment

14) Switch to the **Deployment** tab of the displayed settings window and tick off **Uninstall this application when it falls out of the scope of the management** if you need to remove the application when the specified group policy regarding the client hosts expires (fig. Properties of the specific application deployment 17).

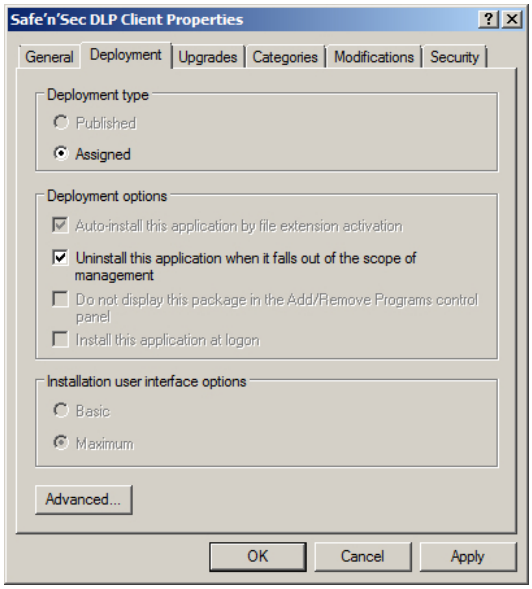

Figure 20. Properties of the specific application deployment

Click **Advanced** and tick off **Make this 32-bit X86 application available to Win64 machines** in the **Advanced deployment options** window, if you plan to install onto the client hosts with 64-bit OS (fig. Additional properties [18]). To apply changes, click **OK** in both settings window.

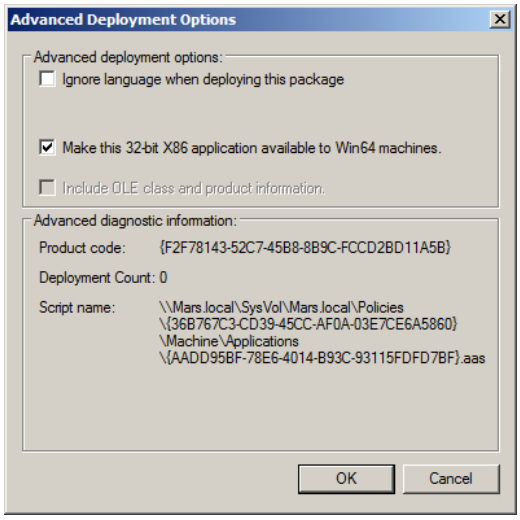

Figure 21. Additional properties

15) Close the **Group Policy Management Editor** and **Server Manager** snap-in windows and open the **Active Directory Users and Computers** snap-in from the **Administrative Tools** section of the **Start** menu.

16) Expand the **<domain name>** section and select the **Computers** section (fig. List of the domain hosts [18]).

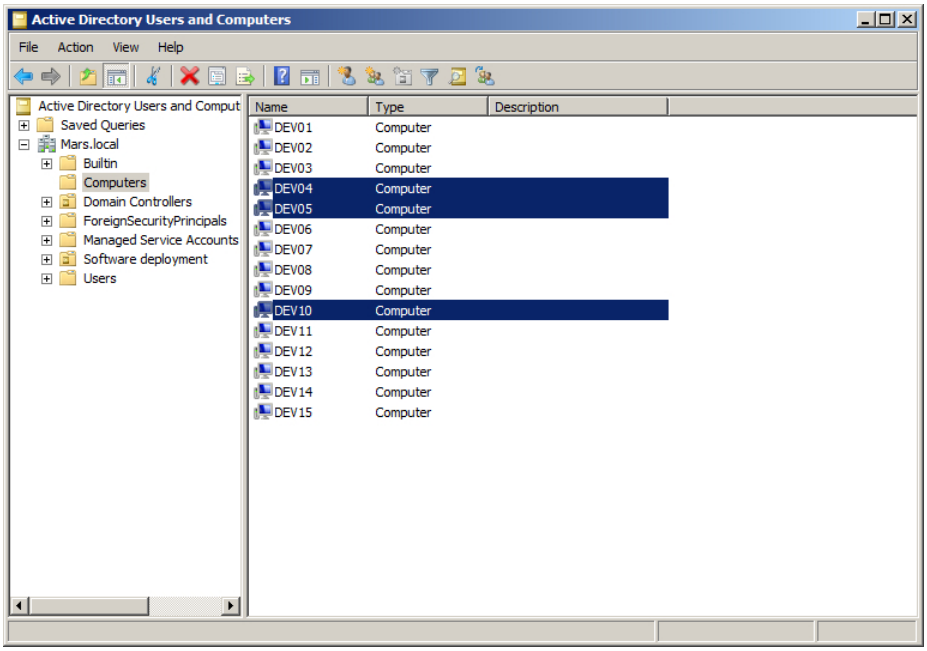

Figure 22. List of the domain hosts

17) Select the hosts that the client applications should be installed to and move them to the **Software deployment** section. Click **Yes** in the displayed alert window (fig. Alert when moving the hosts to another organizational unit 19).

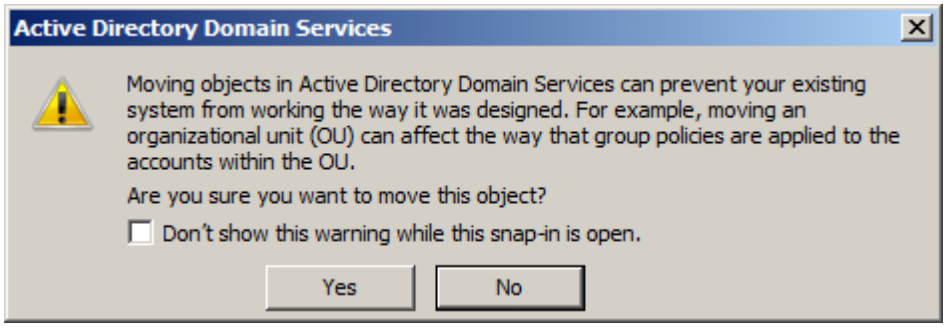

Figure 23. Alert when moving the hosts to another organizational unit

18) Open the **Software deployment** section and make sure that the required client hosts are in the list of the computers of the organizational unit (fig. List of the organizational unit hosts 19).

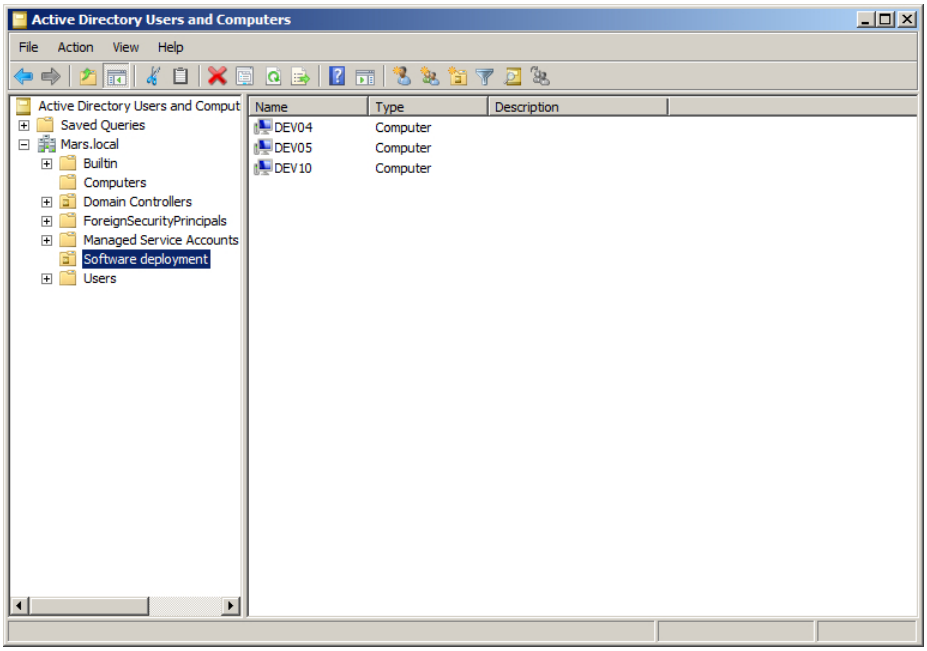

Figure 24. List of the organizational unit hosts

19) After the period of the group policy update update expires (the period depends on the Active Directory settings), the created policy is applied to the client hosts. Installation of the selected applications is performed after the next reboot of the client hosts. To apply the created group policy immediately, run Windows command prompt with the administrator privileges on a client host and enter the following command:

```
gpupdate /force
```

After the command executes, confirm system reboot by the *Y* command to apply the updated group policy (fig. Updating the group policy manually 20).

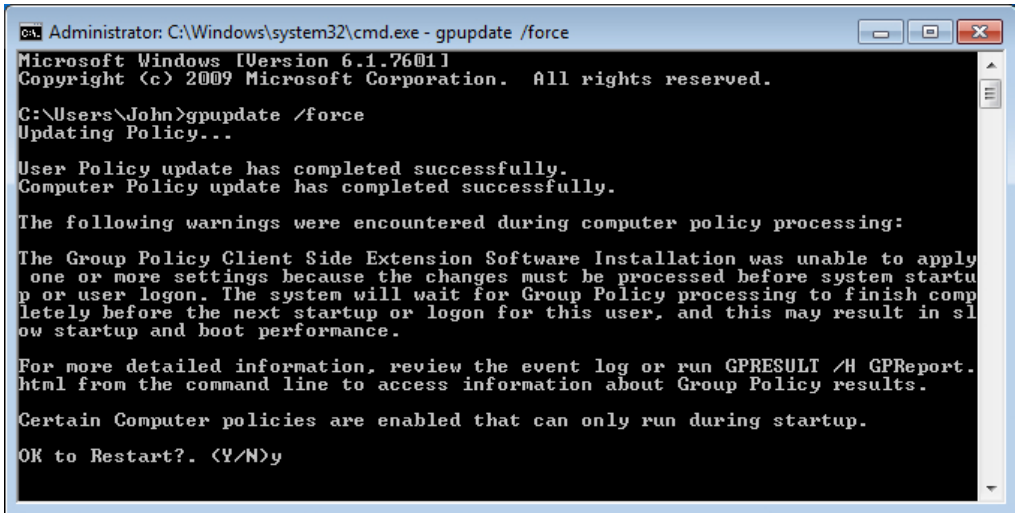

Figure 25. Updating the group policy manually

3.2.2. Installing via the remote installation utility

This installation method is designed for cases when installation via domain group policy is impossible, for example, if a network of protected endpoints is organized into a workgroup.

The *srvrimp.exe* command prompt utility is supplied along with SoftControl Service Center and is intended for remote installation of the SAFE 'N SEC Corporation client components. The utility is in the SoftControl Server component installation directory.

To install successfully, the remote hosts should meet the following conditions.

Installation conditions

- User account with administrator privileges from the **Administrators** group exists on the server and remote endpoints. Login and password of such account should be the same on all the hosts.
- The following system services are running:
  1) *Remote Registry*;
  2) *Remote Procedure Call (RPC)*;
  3) *Remote Procedure Call (RPC) Locator*;
  4) *Windows Management Instrumentation*.
- The *Windows Installer* system service isn't disabled and isn't blocked.
- Shared resources *\\host\C$* and *\\host\ADMIN$* are open for Read, Write and Delete access.

  Microsoft® Windows® XP, Microsoft® Windows® Server 2003:
  1) Open the **Folder options** tool of the Windows Control panel.
  2) Switch to the **View** tab.
  3) Disable the **Use Simple File Sharing** option.

  Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:
  1) Open the **Folder options** tool of the Windows Control panel.
  2) Switch to the **View** tab.
  3) Disable the **Use Sharing Wizard** option.
  4) Open the **User Account Control Settings** tool of the Windows Control panel.

5) Disable user account control by moving the slider with the notification level to **Never notify**.
6) Open the following system registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
7) Invoke the context menu of the above-mentioned key, select the **New** → **DWORD Value** command and enter the **LocalAccountTokenFilterPolicy** name for the created value.
8) Invoke the context menu of the created value, select the **Modify** command and enter **1** in the **Value data** field of the displayed window; then click **OK**.
9) Reboot the system to apply the changes.

- Common access is enabled with the following parameters.

Microsoft® Windows® 7, Microsoft® Windows® Server 2008:

1) Open **Network and Sharing Center** of the Windows Control panel.
2) Make sure that the host has the following network location: **Home network** or **Work network** for a workgroup, or **Domain network** for a domain. To change network type, click the link with name of the current network location.
3) Click **Change advanced sharing settings** and expand the profile of the current network location.
4) Select the **Turn on file and printer sharing** option in the **File and printer sharing** section.
5) Select the **Use user accounts and passwords to connect to other computers** option in the **HomeGroup Connections** section.
6) Click **Save changes**.

Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

1) Double-click the network icon in the notification area.
2) Right-click the network name in the displayed list on the right and select **Turn sharing on or off**.
3) Select **Yes, turn on sharing and connect to devices**.
4) Open **Network and Sharing Center** of the Windows Control panel.
5) Click **Change advanced sharing settings** and expand the **Private** network profile.
6) Select the **Turn on file and printer sharing** option in the **File and printer**

sharing section.

7) Select the **Use user accounts and passwords to connect to other computers** option in the **HomeGroup Connections** section.

8) Click **Save changes**.

- Connection to the **File and Printer Sharing** service is enabled when Windows firewall is on.

  Microsoft® Windows® XP, Microsoft® Windows® Server 2003:

  1) Open Windows firewall.
  2) Switch to the **Exceptions** tab.
  3) Add to exceptions (tick off a checkbox at the rule) **File and Printer Sharing**.

  Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

  1) Open Windows firewall.
  2) Open **Advanced settings**.
  3) Select **Inbound Rules**.
  4) Enable the **File and Printer Sharing (SMB-In)** rule for the profile of the network the host is located in.

- The following parameters are selected in the **Administrative Tools** → **Local Security Policy** tool of the Windows Control panel: **Local Policies** → **Security Options** → **Network access: Sharing and security model for local accounts** → **Classic - local users authenticate as themselves**.

Utility startup options

Command line options for the remote installation utility are described in table 4.

Table 4. Srvrimp options

Option	Description
-h	Brief information about the utility options.
-i	Switch to the installation mode. Mandatory keys and their values should be specified as described below..
--login=<login>	Login of the user that have administrator privileges on the remote host.
--password=<password>	Password of the user that have administrator privileges on

Option	Description
	the remote host.
--client="<path to installer>"	Path to the SoftControl DLP Client installation package. If the file is in the utility execution folder, you can specify only the file name (without the quotes).
--config="<path to configuration file>"	Path to the configuration file with the settings of connection to the remote server. It is necessary to send automatic request for registration [24] to the SoftControl Server after the installation completes. If the file is in the utility execution folder, you can specify only the file name (without the quotes).
--hostnames=<name 1> <name 2>...<name N>	List of NetBIOS names of the remote hosts (separated with spaces) which the installation should be performed on.

You can also run the utility without specifying the key names, by placing the values in the following order:

```
srvrimp -i <login> <password> "<path to installer>" "<path to configuration file>" <name 1> <name 2>...<name N>
```

If you need to install the client component on the server as well, run Windows command prompt with the administrator privileges and run the utility from it.

If installation is successful, the following message is displayed: *Installation successfully completed on host <name>*.

3.2.3. Installing via third party administrative tools

To install SoftControl DLP Client remotely, you can use third-party IT infrastructure management systems, for example, Microsoft® System Center Configuration Manager (hereafter referred to as MS SCCM). In this case, the installation method depends on the system in question and on the way in which the installation packages are distributed in this system.

3.3. Registration on the server

SoftControl DLP Client is a client component, and can operate only in conjunction with SoftControl Service Center. To connect SoftControl DLP Client to SoftControl Service Center, you need to register SoftControl DLP Client on SoftControl Server. To do so, take the following steps.

1) Copy the *ClientSettings.xmlc* encrypted configuration file with the server connection settings (see 'SoftControl Service Center administrator's guide') to the SoftControl DLP Client installation directory on a client host.
2) Reboot the system to apply the configuration file. Make sure that the settings have

applied: the full name of the file should change to *ClientSettings.xmlc_used*.

3) Confirm registration in SoftControl Admin Console on the **Client statuses** tab (see 'SoftControl Service Center administrator's guide).

4. Updating SoftControl DLP Client

You can update SoftControl DLP Client on the client hosts both locally[26] and remotely via SoftControl Service Center[29].

4.1. Local update

This method implies updating the application locally on each client host.

You can update SoftControl DLP Client locally in the following ways.

- standard mode (via GUI)[26];
- silent mode[29].

4.1.1. Updating the component in standard mode

1) Run the *DLP_Client.msi* installation package of the version you want to update to.
2) Click **Next** in the **SoftControl DLP Client Setup** window (fig. Running the update[26]).

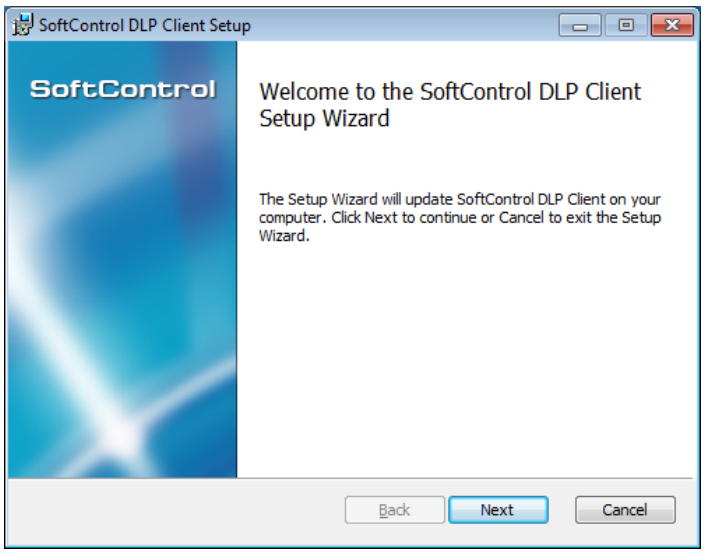

Figure 26. Running the update

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement[26]).

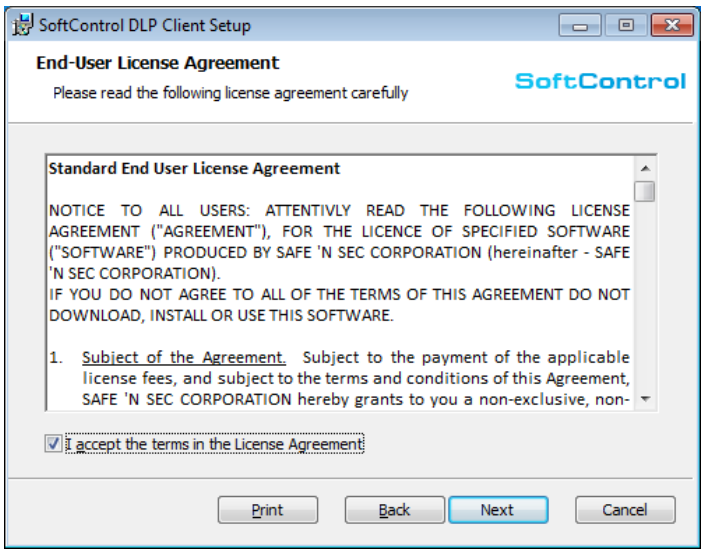

Figure 27. License agreement

4) Click **Update** (fig. Ready to update 27).

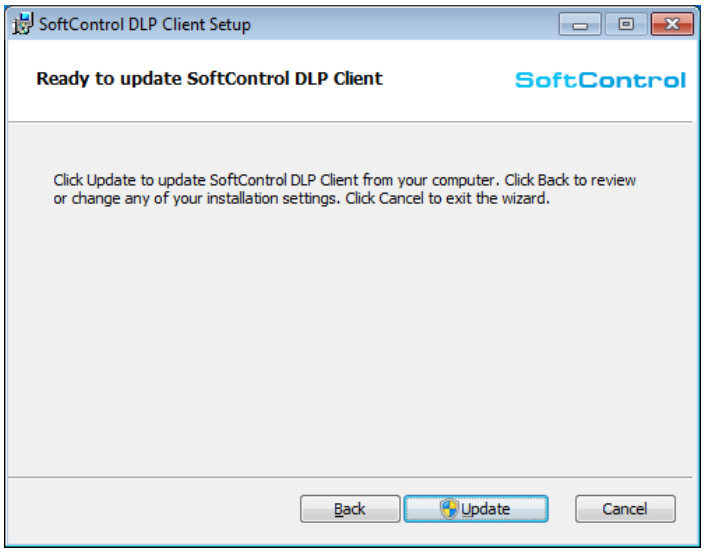

Figure 28. Ready to update

5) Wait until the update completes (fig. Updating progress 27).

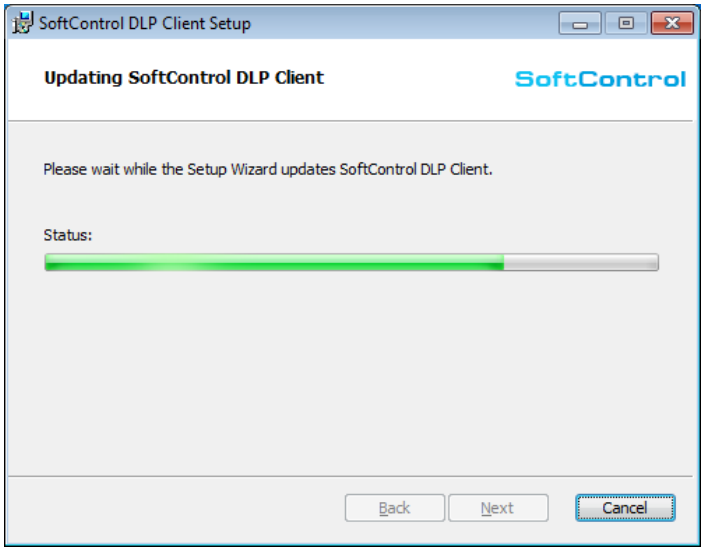

Figure 29. Update progress

6) After the **Completed the SoftControl DLP Client Setup Wizard** message is displayed, click **Finish** (fig. Update completes 28).

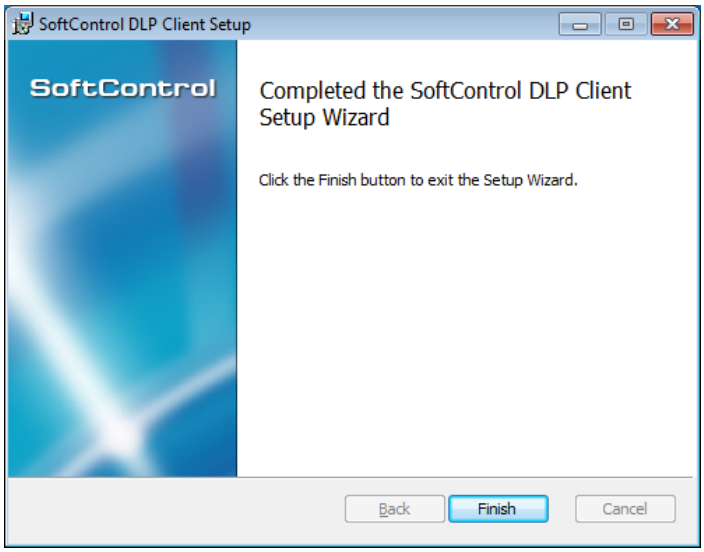

Figure 30. Update completes

7) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete the updates (fig. Requesting system restart 28).

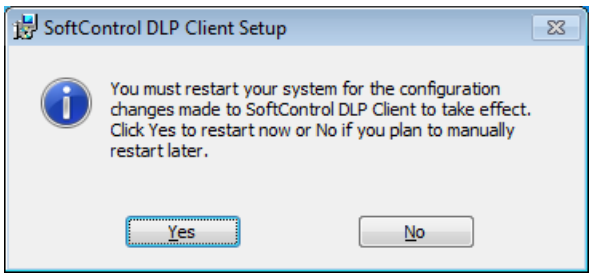

Figure 31. Requesting system reboot

4.1.2. Updating the component in silent mode

Important: all steps require administrator privileges.

1) Copy the *DLP_Client.msi* installation package of the version you want to update to, to the `C:\Temp` directory of the client host.
2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /i "C:\Temp\DLP_Client.msi" /quiet
```

After the update completes, the system restarts automatically.

4.2. Remote update

The administrator performs the update on demand or on schedule from the SoftControl Admin Console management console. For detailed description of the remote update on demand and the update scheduling, see 'SoftControl Service Center administrator's guide'.

5. Removing SoftControl DLP Client

You can uninstall SoftControl DLP Client from the client hosts either locally[30] or in one of the remote centralized[31] methods.

5.1. Local uninstallation

You can remove SoftControl DLP Client locally in the following ways:

- standard mode (via GUI)[30];
- silent mode[30].

5.1.1. Uninstalling the component in standard mode

1) For Microsoft® Windows® XP, Microsoft® Windows® Server 2003: go to Windows Control Panel → **Add or Remove Programs** → **Change or Remove Programs**, select *SoftControl DLP Client* and click **Remove**.

   For Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012: go to Windows Control Panel → **Programs** → **Programs and Features**, select *SoftControl DLP Client* and click **Uninstall**.
2) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete uninstallation (fig. Requesting system restart[30]).

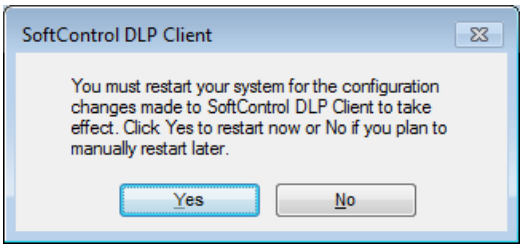

Figure 32. Requesting system restart

5.1.2. Uninstalling the component in silent mode

Important: all steps require administrator privileges.

1) Copy the *DLP_Client.msi* installation package of the current version to the `C:\Temp` directory of the client host.
2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /x "C:\Temp\DLP Client.msi" /quiet
```

After the program is removed, system restarts automatically.

5.2. Remote uninstallation

Remote uninstallation of SoftControl DLP Client implies centrally managed removal of client applications from a group of hosts integrated into a network.

You can uninstall SoftControl DLP Client remotely in the following ways.

- via domain group policy [31];
- via third party administrative tools [33].

5.2.1. Uninstalling via domain group policy

Note: Microsoft® Windows® Server 2008 R2 is used as an example.

1) Open the **Server Manager** snap-in from the **Administrative Tools** section of the **Start** menu in the OS of the domain controller.
2) Go to the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section, expand the **Software deployment** organizational unit, invoke context menu of the previously created [11] group policy object for the client application deployment (**Clients deployment**), and select **Edit** (fig. Modifying a group policy object [31]).
3) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the displayed **Group Policy Management Editor** snap-in window, select the application to remove from the list of applications, invoke its context menu and select **All tasks** → **Remove** (fig. Invoking the application removal task [32]).
4) Select **Immediately uninstall the software from users and computers** in the **Remove Software** dialog box and click **OK** (fig. Selecting the removal method [32]).

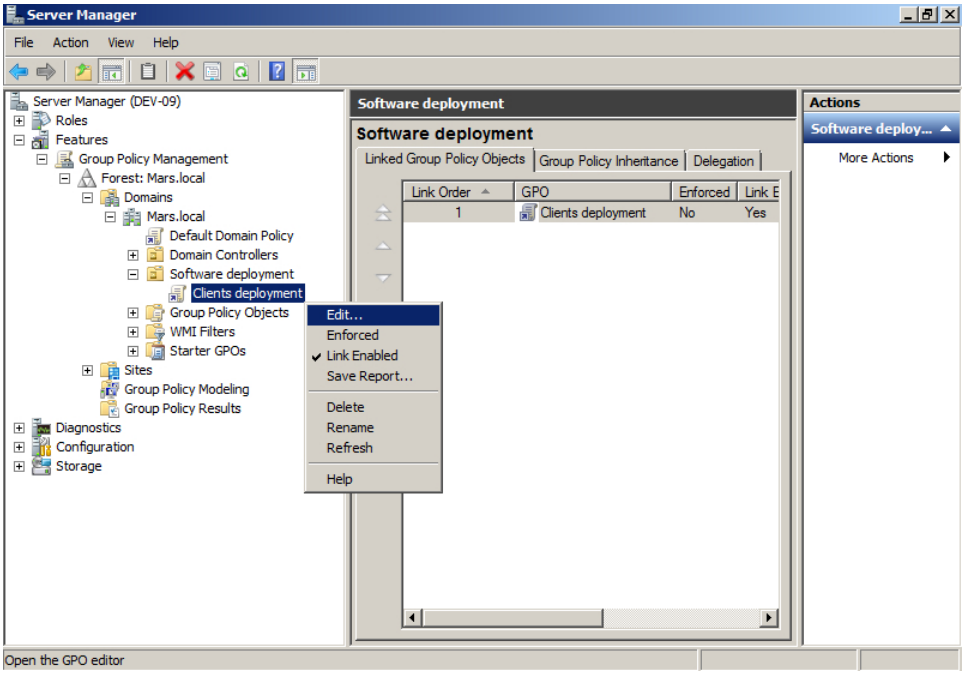

Figure 33. Modifying a group policy object

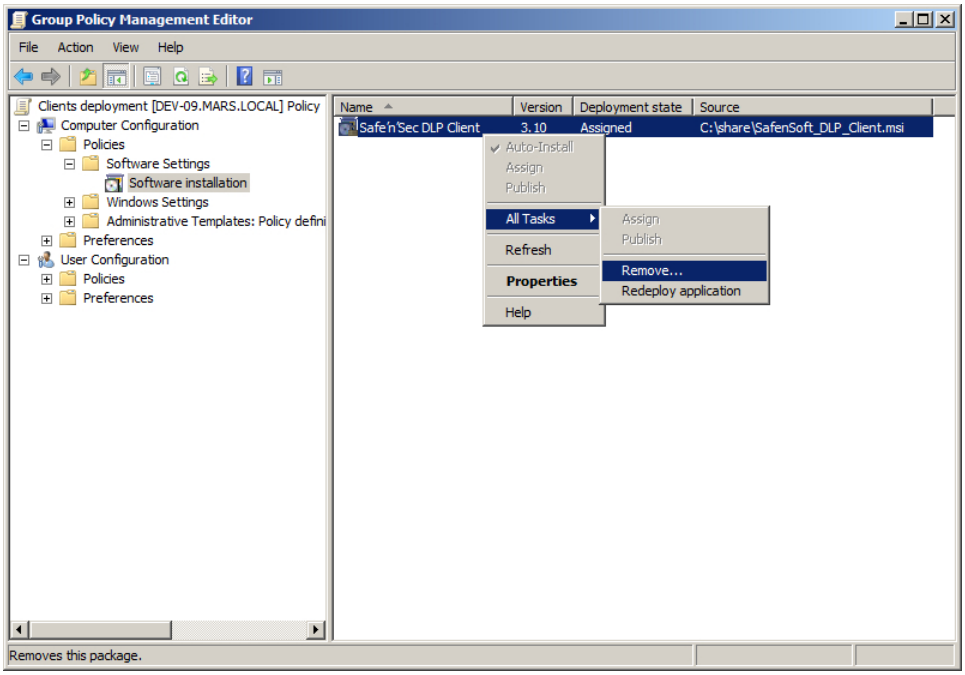

Figure 34. Invoking the application removal task

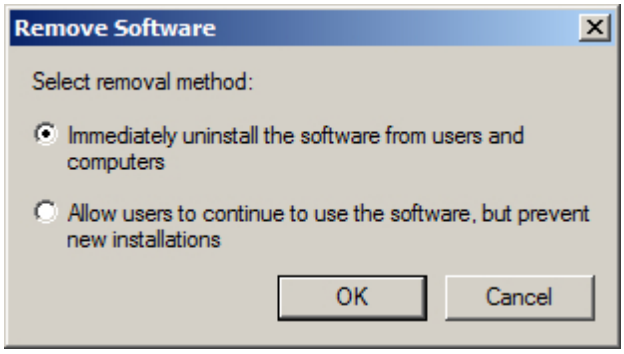

Figure 35. Selecting the removal method

5) After the period of the group policy update expires (the parameter depends on the Active Directory settings), the created policy is applied to the client hosts. The selected applications are removed after the client hosts are rebooted. To apply the created group policy immediately, run Windows command prompt with administrator privileges on a client host and enter the following command:

```
gpupdate /force
```

After the command executes, confirm system reboot by the *Y* command to apply the updated group policy (fig. Updating the group policy parameters manually 33).

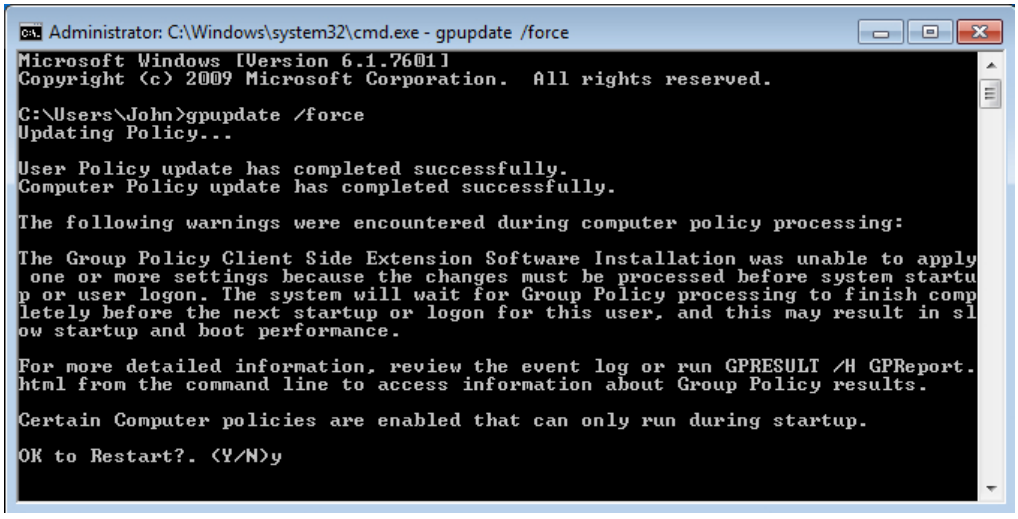

Figure 36. Updating the group policy parameters manually

5.2.2. Uninstalling via third party administrative tools

As with the installation, to to uninstall SoftControl DLP Client remotely you can use third-party IT infrastructure management systems. In this case, the removal method is selected depending on the specific system and the software removal methods that are used in this system.

6. Supplemental information

6.1. Sources

Sources of supplemental information are presented in table 5.

Table 5. Supporting documentation

Name	Description
SoftControl Service Center administrator's guide	Working with the SoftControl Server and SoftControl Admin Console administrative tools.

7. Customer support

If you have any questions concerning the installation, setting up and operation of SoftControl DLP Client, please contact our customer support by e-mail support@safensoft.com.