



# **SoftControl**

## **DLP Client 6.1.398**

Installation guide

Dear user!

ARUDIT SECURITY, LLC thanks you for choosing SoftControl DLP Client. Specialists of the company do their best to make sure our software both meets the highest requirements in a field of information protection and is easy use. We hope you find SoftControl DLP Client helpful.

#### COPYRIGHT

This document is a property of the ARUDIT SECURITY, LLC and can be used only for personal purposes. It is prohibited to reproduce parts of the document, make changes, share on network resources, distribute (including in translation) in hard- and soft-copy form, via communication channels and mass media or by any other means without prior written permission from the company and a reference to the source.

All the names used throughout this document are trademarks of its respective owners.

#### LIABILITY LIMIT

Contents of the document may change without notice. ARUDIT SECURITY, LLC doesn't bear responsibility for inaccuracies and/or errors in this document, and possible damage associated with it.

#### **ARUDIT SECURITY, LLC, 2024**

Postal address:

127106 Russia, Moscow

Novoladykinsky passage, house 8, building 3

ARUDIT SECURITY, LLC

Tel:

+7 499 201-55-12

Fax:

+7 499 201-55-12

E-mails:

Customer service: [support@safensoft.com](mailto:support@safensoft.com)

Sales team: [sales@safensoft.com](mailto:sales@safensoft.com)

Website: [safensoft.com](http://safensoft.com)

## Contents

1. Introduction	4
1.1 Purpose	4
1.2 Main features	4
1.3 Notational conventions and terms	5
1.3.1 Notational conventions	5
1.3.2 List of acronyms	5
1.3.3 Glossary	5
2. Hardware and software requirements	6
2.1 SoftControl DLP Client system requirements	6
3. Installing and setting up SoftControl DLP Client	8
3.1 Local installation	8
3.1.1 Installing the component in standard mode	8
3.1.2 Installing the component in silent mode	11
3.2 Remote installation	11
3.2.1 Installing via domain group policy	12
3.2.2 Installing via the remote installation utility	22
3.2.3 Installing via third party administrative tools	25
3.3 Registration on the server	25
4. Updating SoftControl DLP Client	26
4.1 Local update	26
4.1.1 Updating the component in standard mode	26
4.1.2 Updating the component in silent mode	29
4.2 Remote update	29
5. Removing SoftControl DLP Client	30
5.1 Local uninstallation	30
5.1.1 Uninstalling the component in standard mode	30
5.1.2 Uninstalling the component in silent mode	30
5.2 Remote uninstallation	31
5.2.1 Uninstalling via domain group policy	31
5.2.2 Uninstalling via third party administrative tools	33
6. Customer support	34
7. Supplemental information	35
7.1 Sources	35
7.2 Updating SoftControl SysWatch and antivirus bases on Windows XP	35

# 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
<b>i</b>	Important information.
<u>Condition</u>	An execution condition, a note, or an example.
<b>Update</b>	<ul style="list-style-type: none"> <li>– headers and acronyms;</li> <li>– names of buttons, links, menu items, and other program interface elements.</li> </ul>
<i>Control policy</i>	<ul style="list-style-type: none"> <li>– terms (definitions);</li> <li>– names of files and other objects;</li> <li>– messages displayed to user.</li> </ul>
C:\Program Files\SoftControl	Paths to directories, files, or registry keys.
%windir%\system32\msiexec.exe /i	Source code, command and configuration file fragments.
<SoftControl DLP Client installation directory>	Fields with specific names to be replaced with actual values.
<a href="#">Appendix</a> <sup>(5)</sup>	Links to internal resources (document sections) with the page numbers, 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
Client host	A computer (a workstation, a server, a self-service terminal) with the installed SoftControl DLP Client.

## 2. Hardware and software requirements

### 2.1 SoftControl DLP Client system requirements

**Table 3. Minimal system requirements**

OS	CPU frequency <sup>1</sup>	RAM size	HDD free space	
<b>Client operating systems:</b>				
Microsoft® Windows® XP (SP2) 64-bit <sup>2</sup>	800MHz	512MB	20MB	
Microsoft® Windows® XP (SP3) 32-bit <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® XP Embedded (SP3) <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® Embedded for Point of Service 1.0 <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® 7 (SP1) 32-bit <sup>3</sup>	1GHz	1GB		
Microsoft® Windows® 7 (SP1) 64-bit <sup>3</sup>	1GHz	2GB		
Microsoft® Windows® 8 32-bit	1GHz	1GB		
Microsoft® Windows® 8 64-bit	1GHz	2GB		
Microsoft® Windows® 8.1 32-bit	1GHz	1GB		
Microsoft® Windows® 8.1 64-bit	1GHz	2GB		
Microsoft® Windows® 10 32-bit	1GHz	1GB		
Microsoft® Windows® 10 64-bit	1GHz	2GB		
Microsoft® Windows® 10 IoT Enterprise 32-bit	1GHz	1GB		
Microsoft® Windows® 10 IoT Enterprise 64-bit	1GHz	2GB		
<b>Server operating systems:</b>				
Microsoft® Windows® Server 2003 (SP2) 32-bit <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® Server 2003 (SP2) 64-bit <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® Server 2003 (SP2) 32-bit <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® Server 2003 (SP2) 64-bit <sup>2</sup>	800MHz	512MB		
Microsoft® Windows® Server 2008 R2 64-bit <sup>3,4</sup>	1.4GHz	512MB		
Microsoft® Windows® Server 2012 64-bit <sup>4</sup>	1.4GHz	512MB		
Microsoft® Windows® Server 2012 R2 64-bit <sup>4</sup>	1.4GHz	512MB		
Microsoft® Windows® Server 2016 64-bit <sup>4</sup>	1.4GHz	2GB		
Microsoft® Windows® Server 2019 64-bit <sup>4</sup>	1.4GHz	2GB		

#### Notes:

1. Support of the SSE2 instruction set is required for CPU. This instruction set is supported by most CPUs released since 2000. A popular CPU that does not support the SSE2 instruction set is Intel Pentium III (released in 1999, stopped being produced in 2003).
2. Additional operations may be required for Windows XP and Windows Server 2003 (see [Updating SoftControl SysWatch and antivirus bases on Windows XP](#)<sup>(35)</sup>).
3. Update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature

verification).

4. Only desktop installation options are supported.

## 3. Installing and setting up SoftControl DLP Client

SoftControl DLP Client can be installed onto client hosts both [locally](#)<sup>(8)</sup> and one of the [remote centralized](#)<sup>(11)</sup> 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](#)<sup>(25)</sup> 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 \(via GUI\)](#)<sup>(8)</sup>;
- [silent mode](#)<sup>(11)</sup>.

#### 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](#)<sup>(8)</sup>).



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](#)<sup>(8)</sup>).

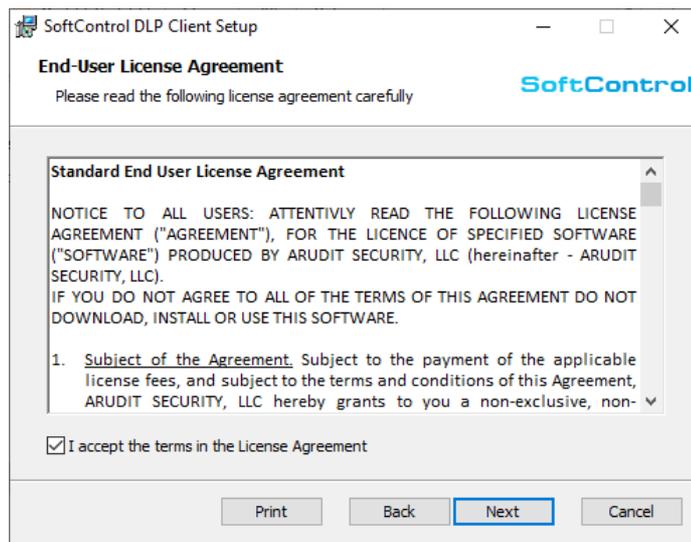


Figure 2. License agreement

4) Select a directory to install SoftControl DLP Client to (with the help of the **Change** button) and click **Next** (fig. [Installation path](#)<sup>9</sup>).

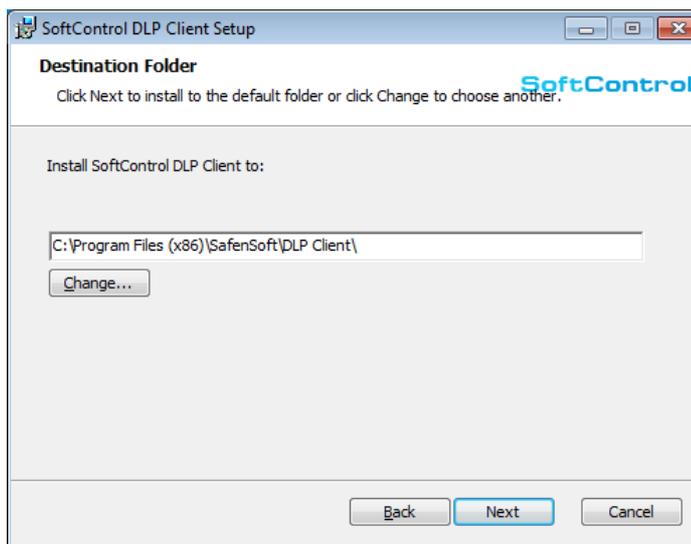


Figure 3. Installation path

5) Click **Install** (fig. [Ready to install](#)<sup>9</sup>).

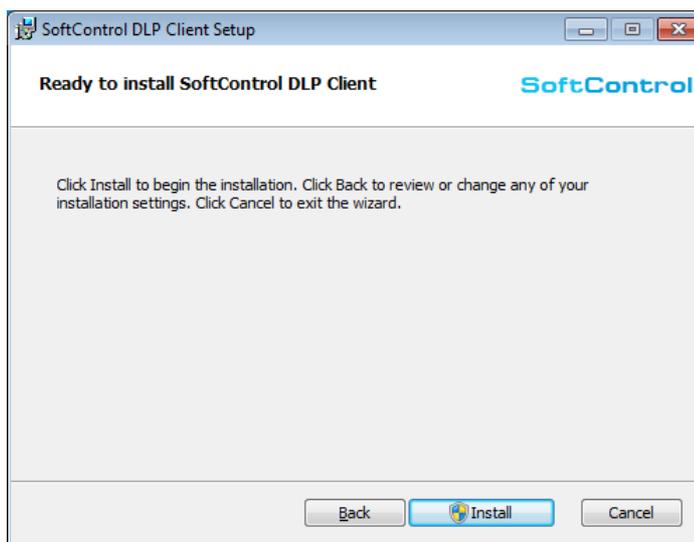


Figure 4. Ready to install

6) Wait until installation completes (fig. [Installation progress](#)<sup>(10)</sup>).

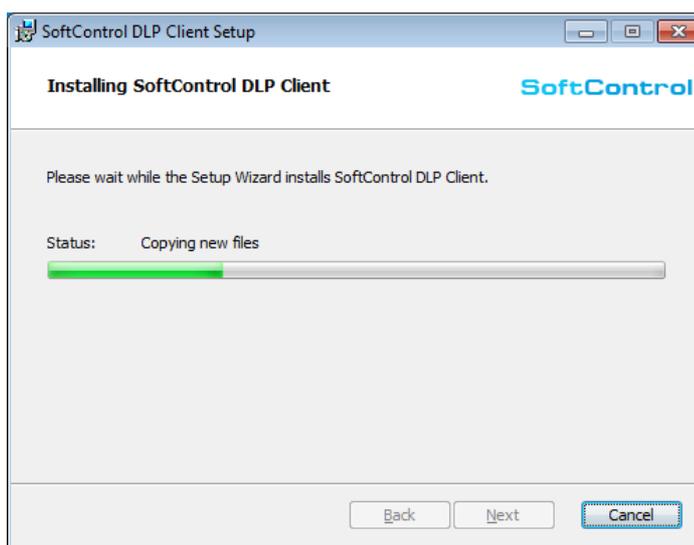


Figure 5. Installation progress

7) After the **Completed the SoftControl DLP Client Setup Wizard** message is displayed, click **Finish** (fig. [Installation completes](#)<sup>(10)</sup>).

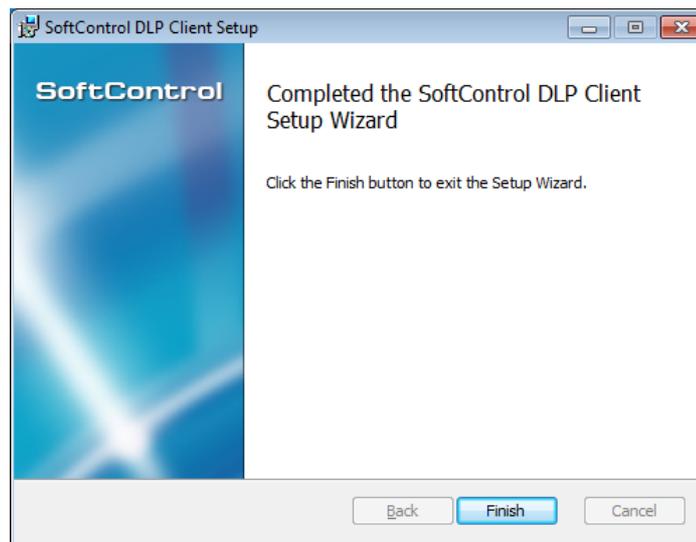


Figure 6. Installation completes

8) Select **Yes** in the dialog box with system restart suggestion. The system restarts to complete the installation (fig. [Requesting system reboot](#)<sup>(11)</sup>).

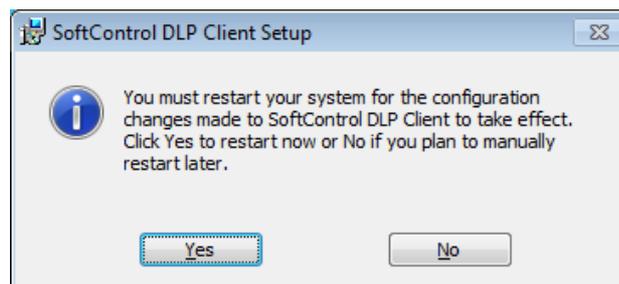


Figure 7. Requesting system reboot

### 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](#)<sup>(12)</sup>;
- [via the remote installation utility](#)<sup>(22)</sup>;
- [via third party administrative tools](#)<sup>(25)</sup>.

### 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](#)<sup>(12)</sup>).
- 3) Enter **Name** of the unit in the **New Organizational Unit** dialog box and click **OK** (fig. [Specifying the name of the organizational unit](#)<sup>(13)</sup>).
- 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](#)<sup>(13)</sup>).

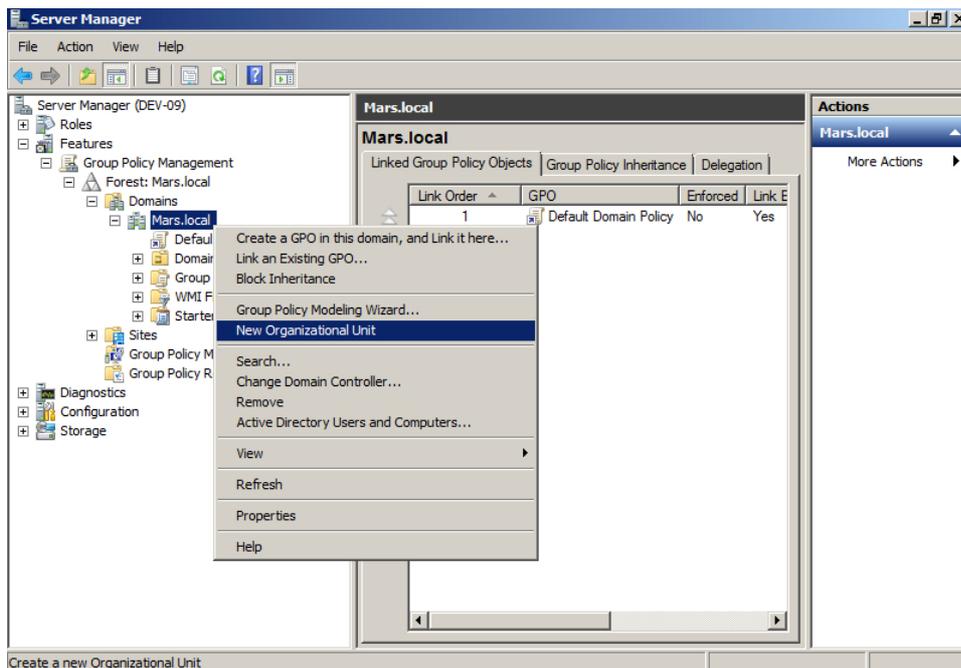


Figure 8. Creating new domain organizational unit

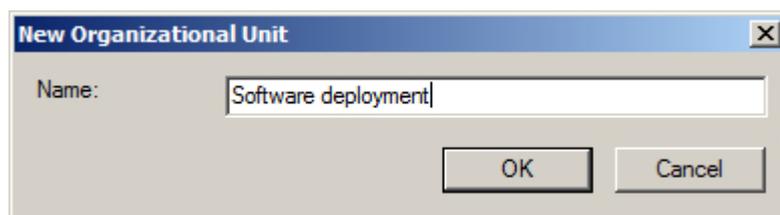


Figure 9. Specifying the name of the organizational unit

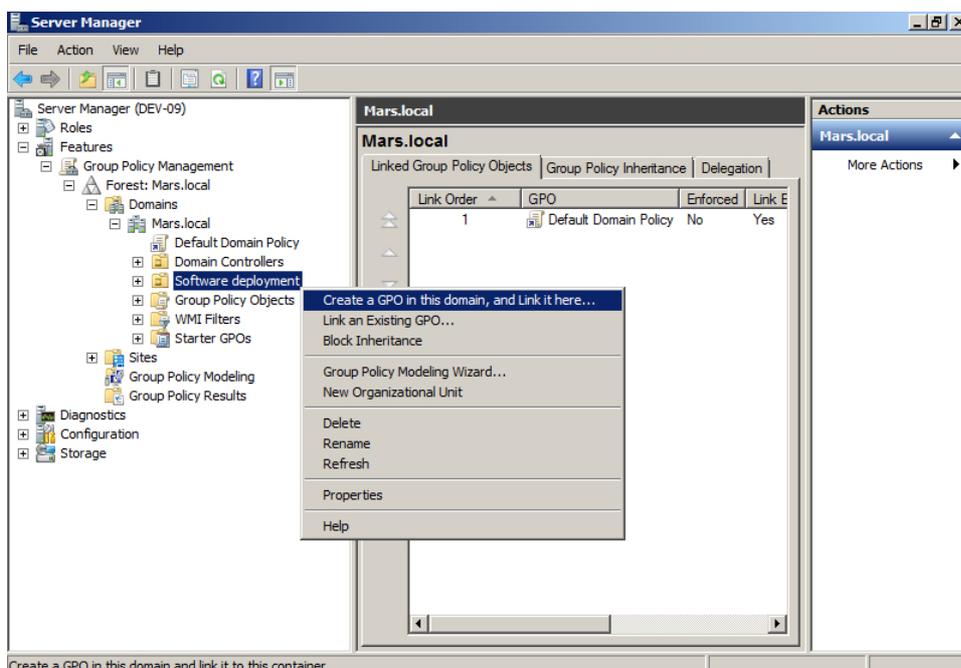


Figure 10. Creating a new object of the group policy

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](#)<sup>(14)</sup>).

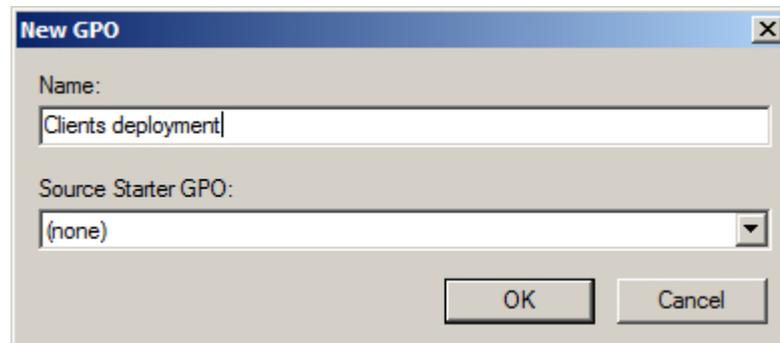


Figure 11. Specifying the name and source starter GPO of new group policy

- 6) Expand the created organizational unit, invoke the context menu of the created group policy object and select **Edit** (fig. [Modifying group policy object](#)<sup>(14)</sup>).
- 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](#)<sup>(14)</sup>).
- 8) Select the *DLP\_Client.msi* installation package which is in the network source available to the client hosts you need to install the applications to, and click **Open** (fig. [Selecting the installation package](#)<sup>(15)</sup>).

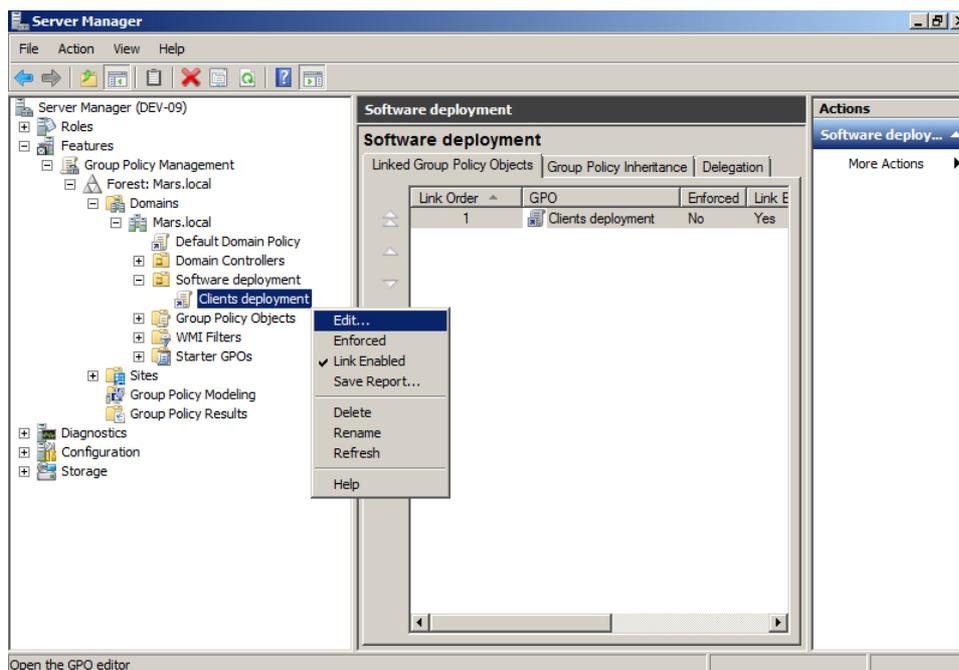


Figure 12. Modifying group policy object

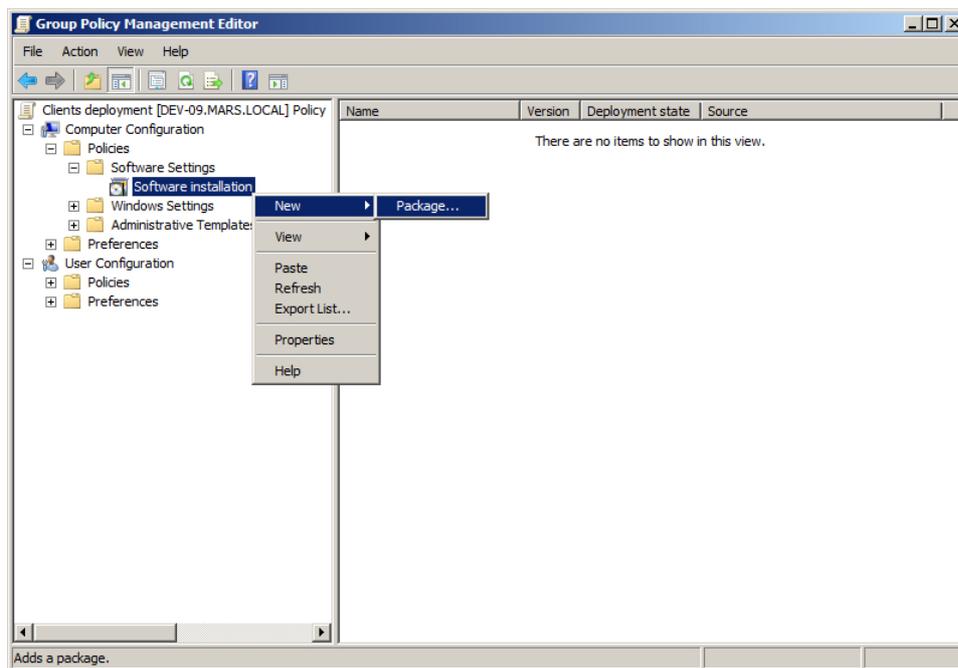


Figure 13. Adding new installation package

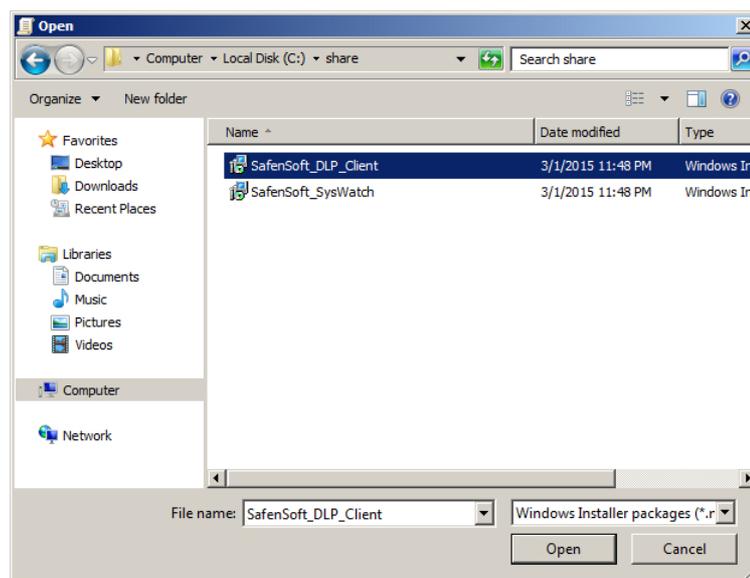


Figure 14. Selecting the installation package

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](#) <sup>(15)</sup>).

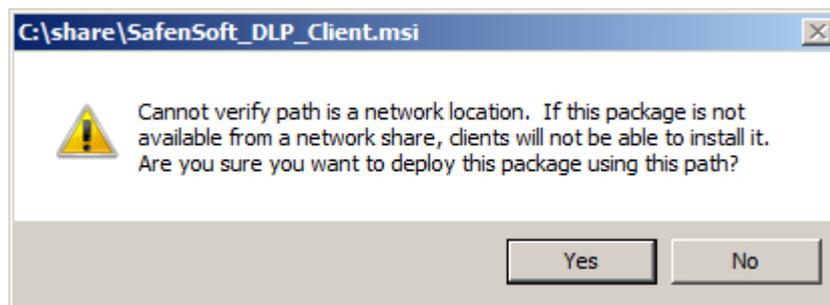


Figure 15. Alert when selecting the location of the installation package

- 10) Select the **Assigned** deployment method in the **Deploy Software** dialog box and click **OK** (fig. [Selecting deployment method](#)<sup>16</sup>).

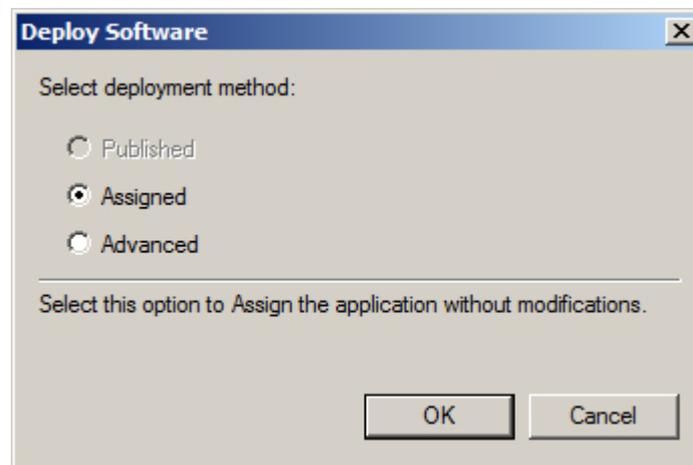


Figure 16. Selecting deployment method

- 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](#)<sup>16</sup>).

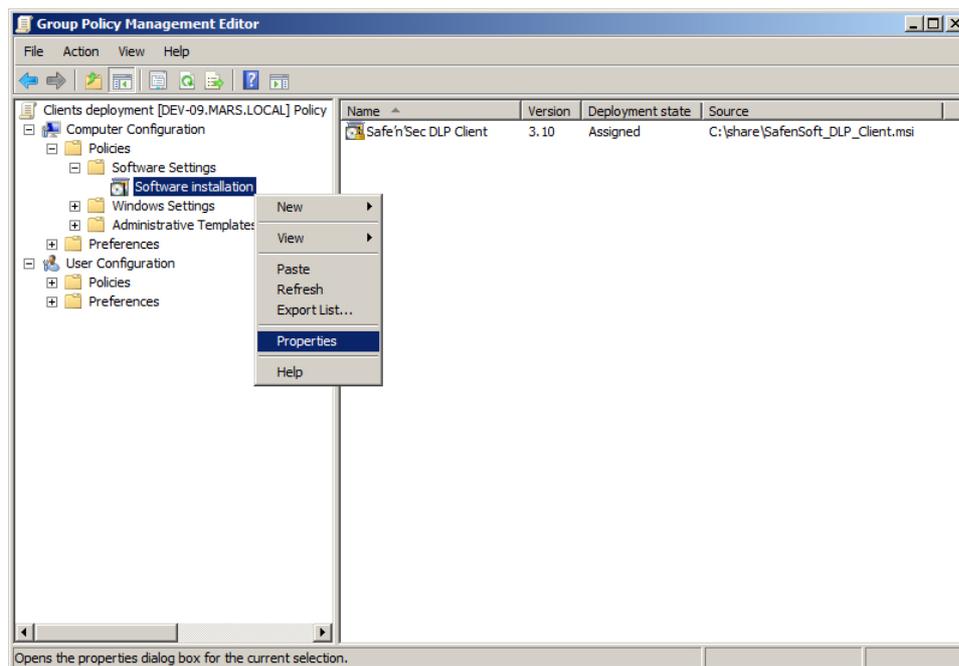


Figure 17. Modifying properties of software deployment

- 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](#)<sup>17</sup>). To apply changes, click **OK**.

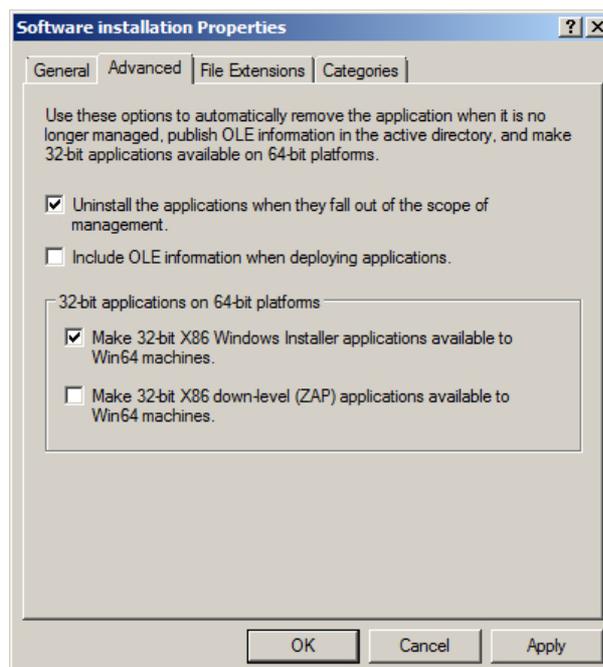


Figure 18. Properties of software deployment

- 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](#)<sup>(18)</sup>).

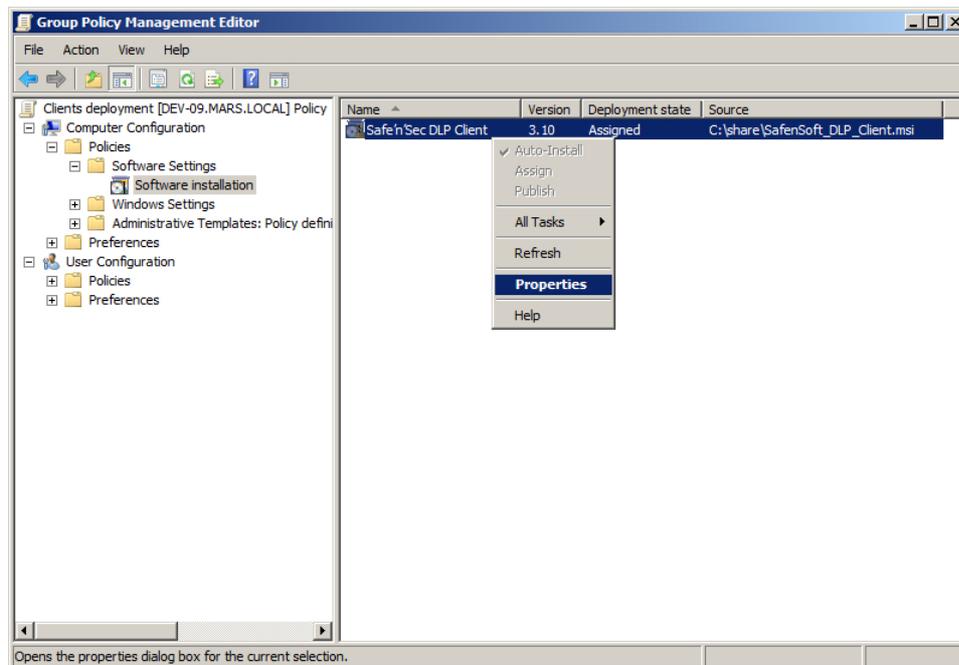


Figure 19. Modifying the properties of the application deployment

- 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](#)<sup>(18)</sup>).

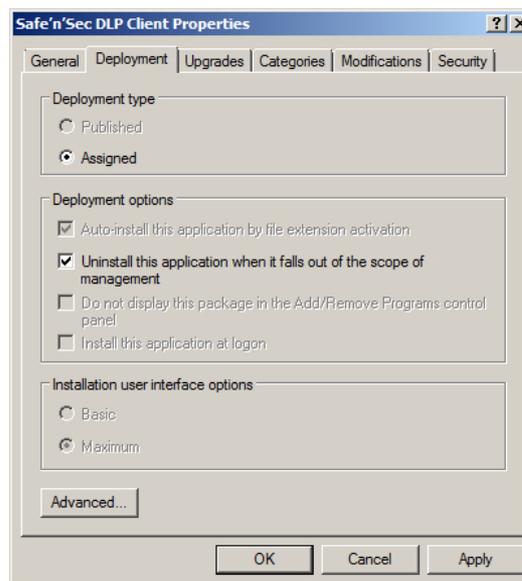


Figure 20. Properties of the specific application deployment

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](#)<sup>(19)</sup>). To apply changes, click **OK** in both settings window.

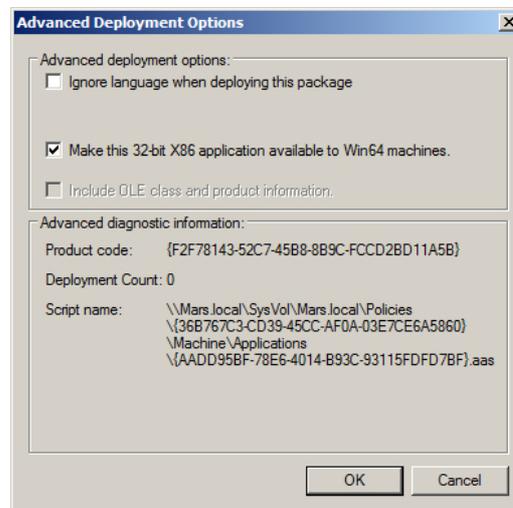


Figure 21. Additional properties

- 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](#)<sup>(19)</sup>).

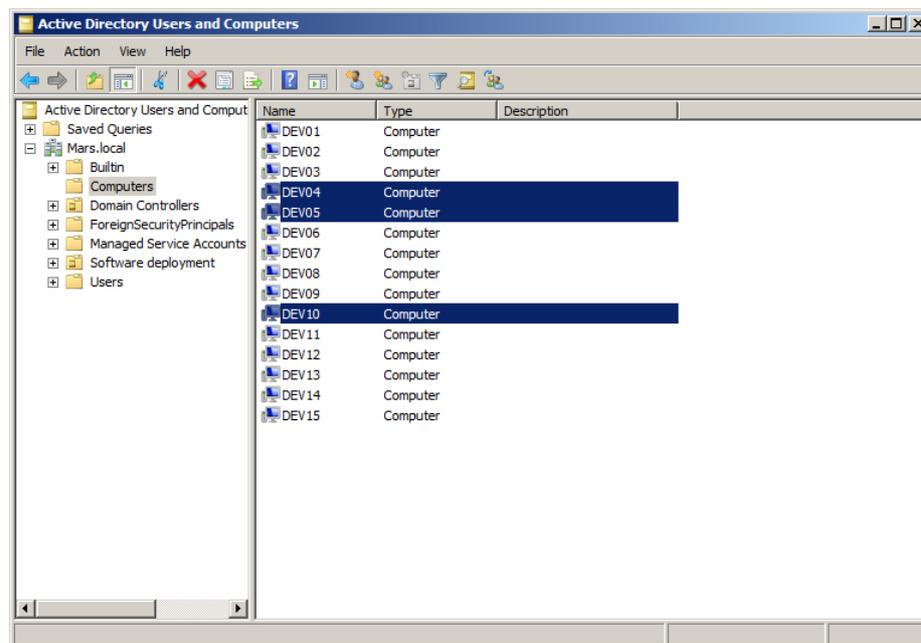


Figure 22. List of the domain hosts

- 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](#)<sup>(20)</sup>).

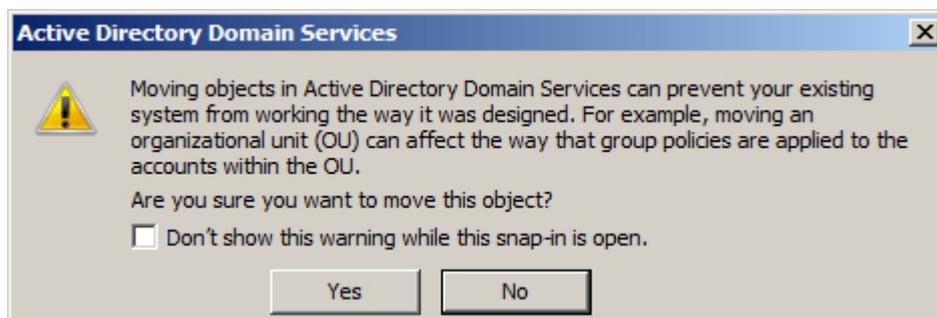


Figure 23. Alert when moving the hosts to another organizational unit

- 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](#)<sup>(20)</sup>).

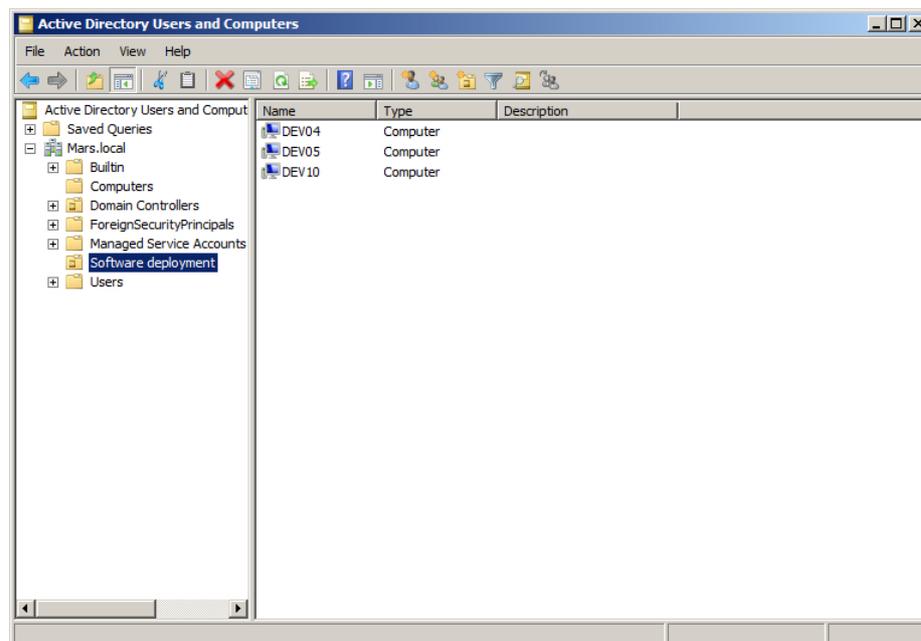


Figure 24. List of the organizational unit hosts

19) After the period of the group policy 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](#)<sup>(21)</sup>).

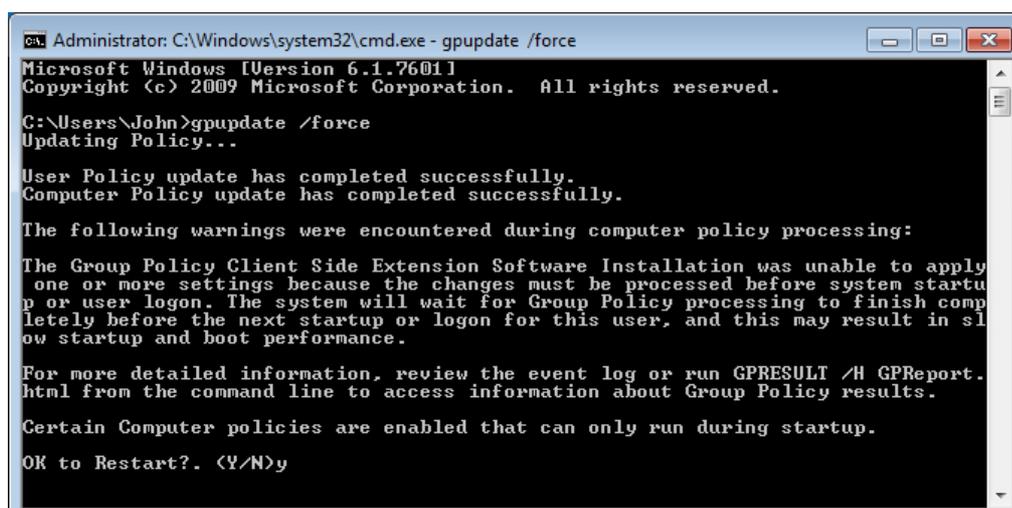


Figure 25. Updating the group policy manually

## 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 *svrimp.exe* command prompt utility is intended for remote installation of the ARUDIT SECURITY, LLC client components. Download the utility here: [http://updates.safensoft.com/<license\\_number>/39/T00LS/svrimp.exe](http://updates.safensoft.com/<license_number>/39/T00LS/svrimp.exe).

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

### ▼ Installation conditions

- User account with full administrator rights 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\I$` and `\\host\ADMIN$` 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 Accounts** → **Change 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** op-

tion in the **HomeGroup Connections** section.

8) Click **Save changes**.

- Inbound 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. Svrrimp options**

Option	Description
<code>-h</code>	Brief information about the utility options.
<code>-i</code>	Switch to the installation mode. Mandatory keys and their values should be specified as described below.
<code>--login=&lt;login&gt;</code>	Login of the user that have administrator privileges on the remote host.
<code>--password=&lt;password&gt;</code>	Password of the user that have administrator privileges on the remote host.
<code>--client="&lt;path to installer&gt;"</code>	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).
<code>--config="&lt;path to configuration file&gt;"</code>	Path to the configuration file with the settings of connection to the remote server. It is necessary to send automatic request for <a href="#">registration</a> <sup>(25)</sup> to the SoftControl Server after the installation completes. If the file is in the utility

Option	Description
	execution folder, you can specify only the file name (without the quotes).
<code>--hostnames=&lt;name 1&gt; &lt;name 2&gt;...&lt;name N&gt;</code>	List of 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:

```
srvrmp -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 **Clients** 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](#)<sup>(26)</sup> and [remotely via SoftControl Service Center](#)<sup>(29)</sup>.

### 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 \(via GUI\)](#)<sup>(26)</sup>;
- [silent mode](#)<sup>(29)</sup>.

#### 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](#)<sup>(26)</sup>).



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](#)<sup>(26)</sup>).

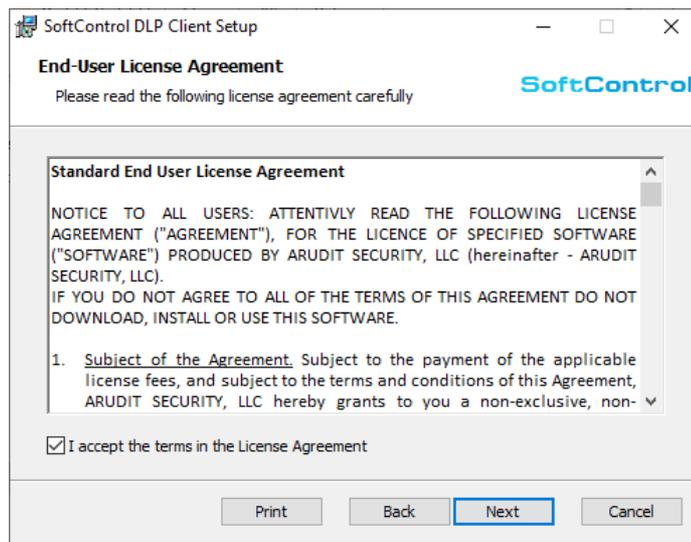


Figure 27. License agreement

4) Click **Update** (fig. [Ready to update](#)<sup>(27)</sup>).

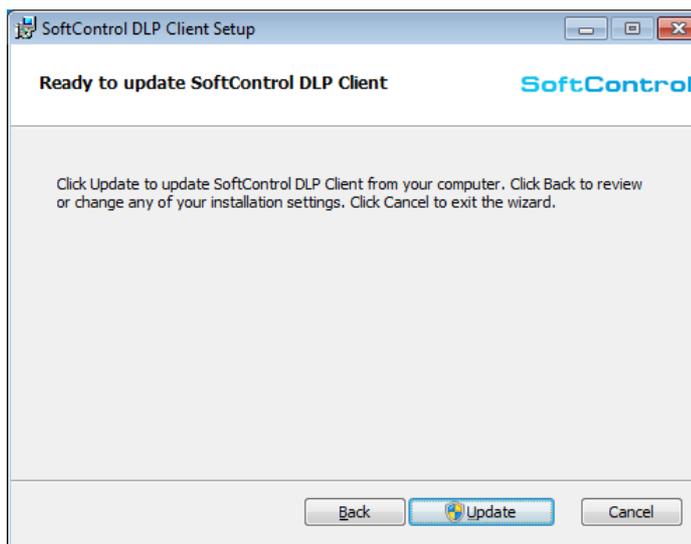


Figure 28. Ready to update

5) Wait until the update completes (fig. [Updating progress](#)<sup>(27)</sup>).

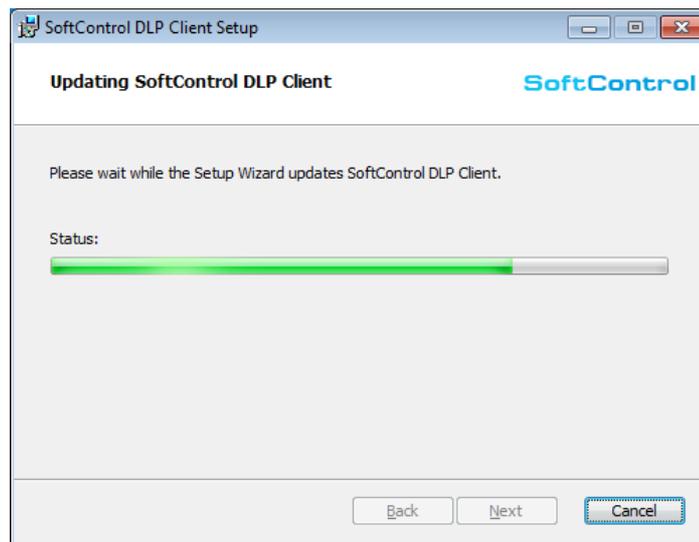


Figure 29. Update progress

6) After the **Completed the SoftControl DLP Client Setup Wizard** message is displayed, click **Finish** (fig. [Update completes](#)<sup>(28)</sup>).

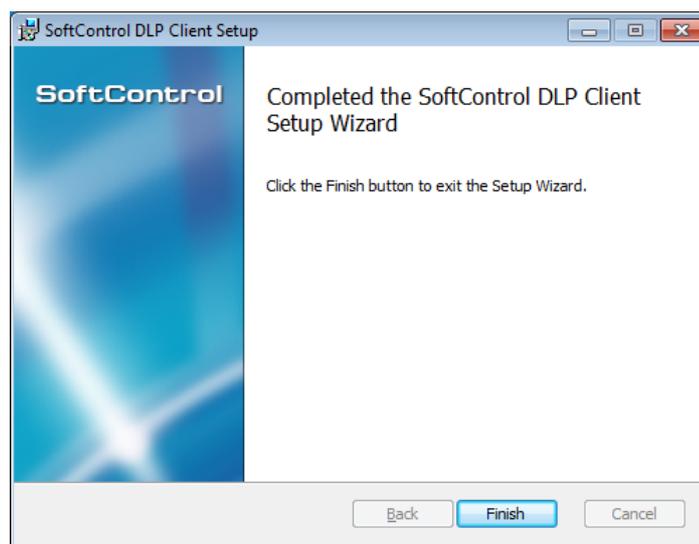


Figure 30. Update completes

7) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete the updates (fig. [Requesting system reboot](#)<sup>(28)</sup>).

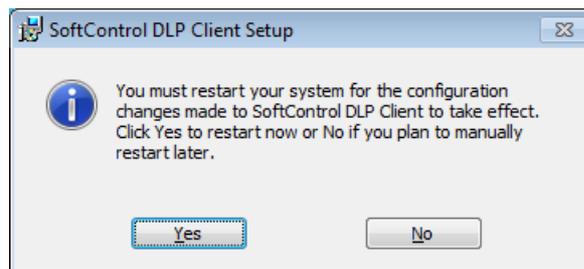


Figure 31. Requesting system reboot

## 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](#)<sup>(30)</sup> or in one of the [remote centralized](#)<sup>(31)</sup> methods.

### 5.1 Local uninstallation

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

- [standard mode \(via GUI\)](#)<sup>(30)</sup>;
- [silent mode](#)<sup>(30)</sup>.

#### 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](#)<sup>(30)</sup>).

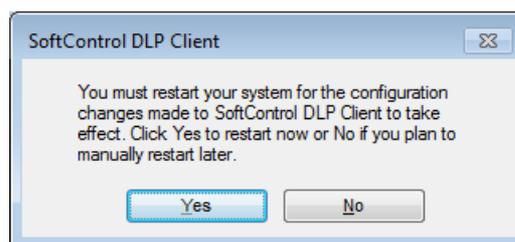


Figure 32. Requesting system restart

#### 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](#)<sup>(31)</sup>;
- [via third party administrative tools](#)<sup>(33)</sup>.

### 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](#)<sup>(12)</sup> group policy object for the client application deployment (**Clients deployment**), and select **Edit** (fig. [Modifying a group policy object](#)<sup>(31)</sup>).
- 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](#)<sup>(32)</sup>).
- 4) Select **Immediately uninstall the software from users and computers** in the **Remove Software** dialog box and click **OK** (fig. [Selecting the removal method](#)<sup>(32)</sup>).

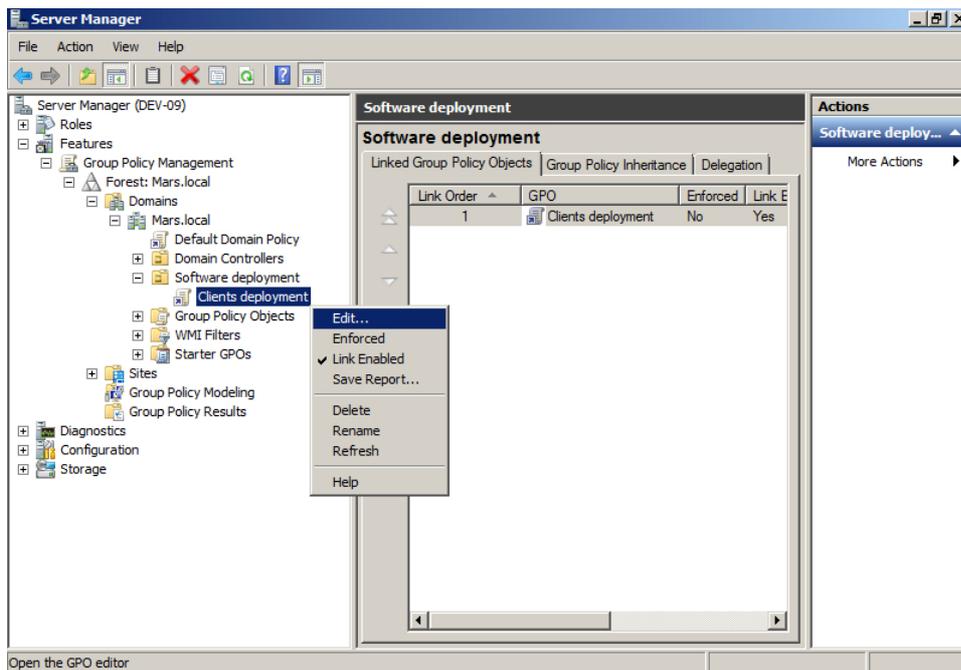


Figure 33. Modifying a group policy object

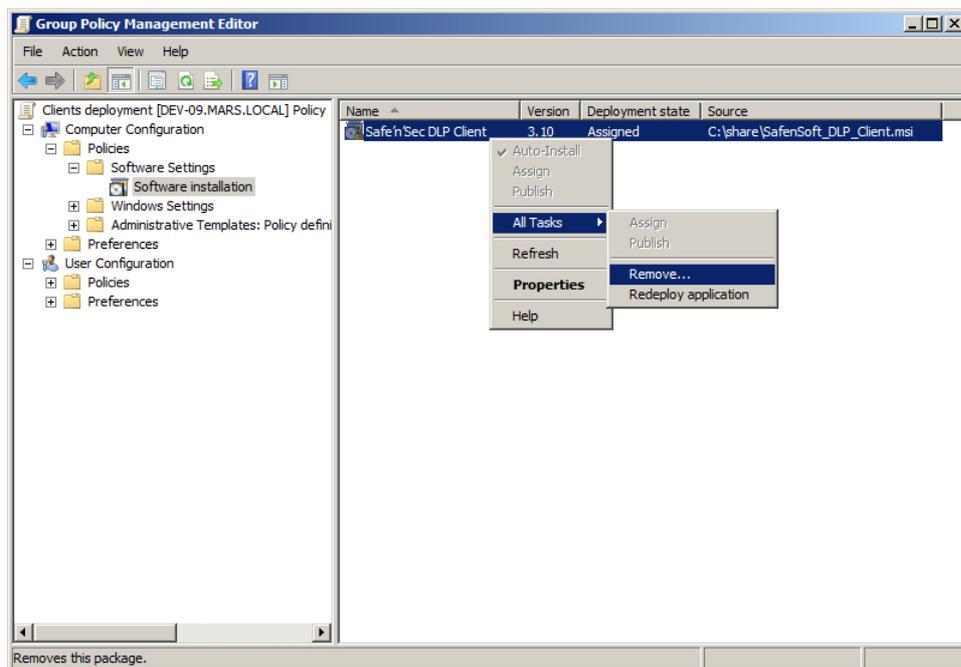


Figure 34. Invoking the application removal task

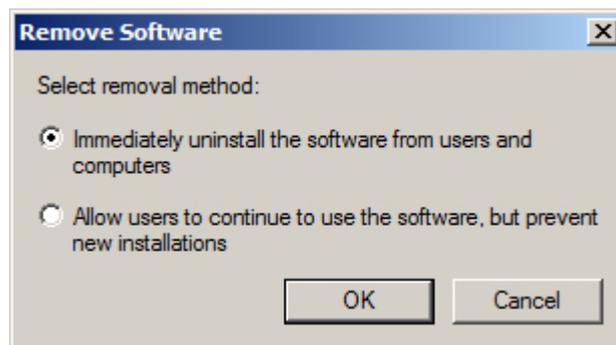


Figure 35. Selecting the removal method

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](#)<sup>33</sup>).

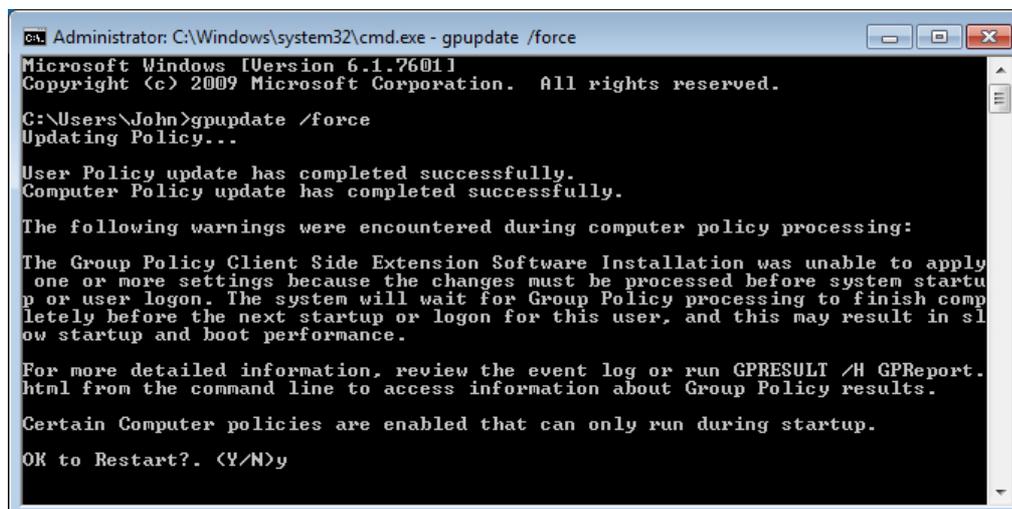


Figure 36. Updating the group policy parameters manually

## 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. 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](mailto:support@safensoft.com).

## 7. Supplemental information

### 7.1 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

### 7.2 Updating SoftControl SysWatch and antivirus bases on Windows XP

Depending on Service Pack, Windows XP either does not support new certificates at all or supports them not completely. It is related to the fact that newer algorithms (SHA-256) were used for generating the certificates.

To ensure that SoftControl products are updated properly, perform the operations described in this section for the update modules.

Follow steps in this section to ensure proper update of the SoftControl SysWatch application and antivirus bases on 32-bit Windows XP.

Note. If you install version 5.1.79 or later of SoftControl SysWatch and it is the first installation of the application on your computer, these actions are not required: all updates will be performed properly. For SoftControl DLP and SoftControl SysCmd, you do not need to perform instructions from this section if you have version 6.0.95 or later.

1. Open the client settings editor in SoftControl Admin Console.
2. Go to **Modules**.
3. Click on .
4. On **Identification data of the module** tab, enter the module name (the name of the executable file) and its path according to the table below.

**Table 6. Update modules**

Component for updating	Module name	Path
SoftControl SysWatch	snsupd.exe	C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH\
SoftControl SysCmd	upd.exe	C:\Program Files\SoftControl\SysCmd\Updater
SoftControl DLP Client	upd.exe	C:\Program Files\SafenSoft\DLP Client\Updater

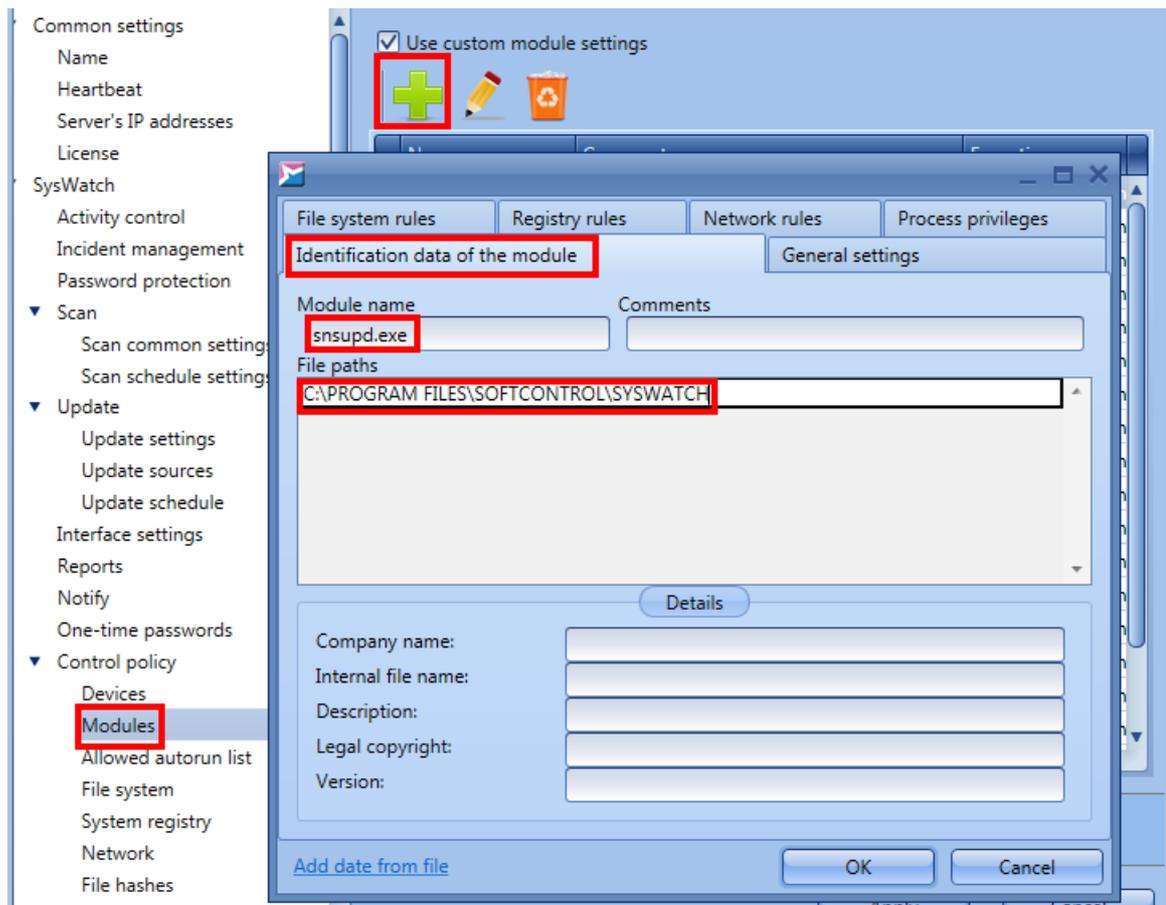


Figure 37. Setting up an update module (for SoftControl SysWatch)

5. On **General settings** tab, select **Trusted application** execution zone and check **Enable software update mode**.

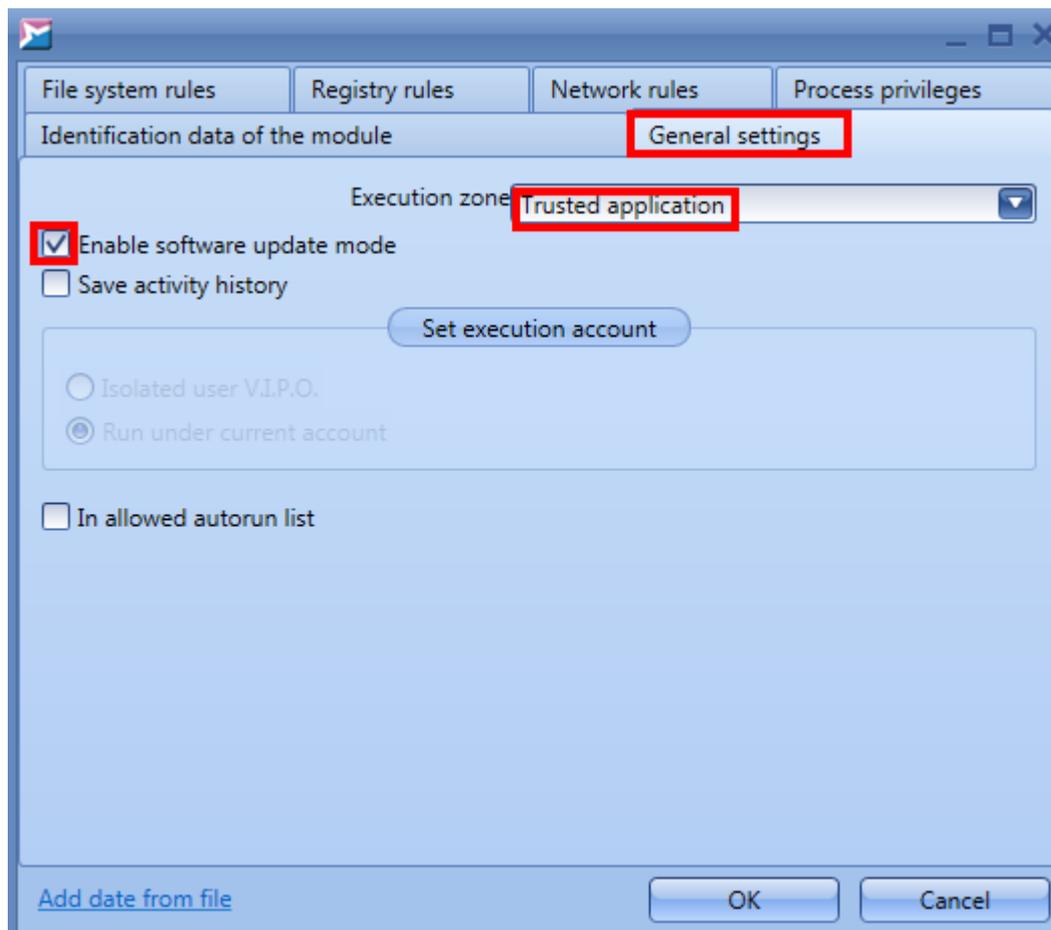


Figure 38. Adding the module to trusted applications

6. Click **OK**.
  7. Save the client settings under a new name and apply them to the organizational unit of the clients that require updating.
- If you are setting up updating for SoftControl SysWatch, now you can create a task to update the antivirus bases or wait for a scheduled update.