SoftControl

Service Center 6.1.398

Administrator guide

Dear user!

ARUDIT SECURITY, LLC thanks you for choosing SoftControl Service Center. 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 Service Center helpful.

COPYRIGHT

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
Novovladykinsky 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
Sales team: sales@safensoft.com
Website: safensoft.com

Contents

1. Introduction

1.1 Purpose

SoftControl Service Center is the set of administrative tools for managing information security system that provides integrity of software environment of the network endpoints, protection against unauthorized data access by maintenance staff or violators, as well as monitors user activity. SoftControl Service Center consists of the following components.

- SoftControl Server is the server component;
- SoftControl Admin Console is the management console.

SoftControl Service Center supports operations with the following client components.

- SoftControl ATM Client / Enpoint Client / SClient (hereafter referred to as SoftControl SysWatch) are the client components of proactive protection of self-service devices, corporate network workstations and servers,respectively;
- SoftControl DLP Client is the client component for monitoring and data collection;
- SoftControl SysCmd is the client component for centralized management of client computers from the server (running processes on client computers and exchanging files with client computers);
- SoftControl DeCrypt, the client component designed to encrypt the hard disks of self-service devices, corporate network workstations and servers.

1.2 Notational conventions and terms

1.2.1 Notational conventions

Table 1 lists notational conventions used in this document.

Table 1. Notational conventions

Notation example	Description
ℹ	Important information.
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.

Notation example	Description
`C:\Program Files\SoftControl`	Paths to directories, files, or registry keys.
`%windir%\system32\msiexec.exe /i`	Source code, command and configuration file fragments.
<SoftControl Service Center installation directory>	Fields with specific names to be replaced with actual values.
Appendix 6	Links to internal resources (document sections) with the page numbers, or links to external resources (URL).

1.2.2 List of acronyms

This documents uses the following acronyms:

- **CPU** – central processing unit;
- **DBMS** – database management system;
- **GUI** – graphical user interface;
- **HDD** – hard disk drive;
- **ISS** – information security system;
- **OS** – operating system;
- **RAM** – random access memory.

1.2.3 Glossary

Table 2. Glossary

Term	Description
Proactive protection	A series of prevention techniques-based measures designed to prevent harmful effects.
Prevention techniques	The advanced data protection technologies that are based on the analysis of the activity on the user's computer. This can be the operation of any applications, OS services, user actions, external activity, etc. Unlike reactive techniques which are the basis of protections such as antivirus and personal firewalls, prevention techniques do not analyze an object code, but track the potentially dangerous actions the object performs. Therefore, the tools of proactive protection do not require the bases of malicious code and their updates that are necessary for traditional protections.
Reactive (signature) techniques	A mode of operation of antivirus software and intrusion detection systems. In this method, the program refers to the database of known viruses and checks whether some part of the code of the object being scanned corresponds to the known virus code (signature) in the database.
Control policy	A complete set of **activity control rules**.
Activity control rule	A set of conditions that determine an application's activity and how SoftControl SysWatch reacts to this activity.
System profile	A database that is stored locally on the **client host** and contains the checksums of

Term	Description
	the **executable modules**. The profile is the result of the SoftControl SysWatch automatic setup (profile gathering).
Application in the profile	An application with its checksum in the **system profile**.
Tracked application	An application that has run on the **client host** and that SoftControl SysWatch has detected during its operation, after the installation.
Trusted application	**Tracked application** from the **trusted execution zone**.
Restricted application	**Tracked application** from the **restricted execution zone**.
Blocked application	**Tracked application** from the **blocked execution zone**. SoftControl SysWatch blocks such applications on the client host.
Execution zone (trusted, restricted, blocked)	Separate **control policy** that applies to the subset of **tracked applications**. There are three execution zones on each **client host**: trusted, restricted, and blocked zones. Any **tracked application** belongs to one of these zones.
Installer	The application that SoftControl SysWatch has heuristically detected as software designed to install other software; otherwise, it is the application that the user has marked as an installer. The installer gives certain privileges for a process to run (see below 'Software update mode').
Software update mode	An application launch mode that places the application and all PE files it has created or modified, to the system profile. The child processes of the application inherit the software update mode.
V.I.P.O. (Valid Inside Permitted Operations)	User account with restricted rights (a limited set of system privileges and no access to system objects). The account is used to arrange the 'sandbox' when running the applications and provides additional protection from possible harmful actions of the applications that are not entirely trustworthy. Only **restricted applications** can run under the V.I.P.O. account.
Role	An aggregate of user rights to use certain SoftControl Admin Console features.
PE file	An executable file of the PE format (Portable Executable). The format is used in Microsoft® Windows® operating systems for executable files (EXE), dynamic link libraries (DLL) and some other types of files.
Client host	A computer (a workstation, a server, a self-service terminal) with the installed SoftControl SysWatch.

2. Hardware and software requirements

2.1 SoftControl Server system requirements

Table 3. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
Client operating systems:	3GHz	4GB	100MB + extra 4GB (for embedded DBMS installation)
Microsoft® Windows® 7 (SP1) *32-bit/64-bit*			
Microsoft® Windows® 8 *32-bit/64-bit*			
Microsoft® Windows® 8.1 *32-bit/64-bit*			
Microsoft® Windows® 10 *32-bit/64-bit*			
Microsoft® Windows® 11 *64-bit*			
Server operating systems:			
Microsoft® Windows® Server 2008 R2 *64-bit*			
Microsoft® Windows® Server 2012 *64-bit*			
Microsoft® Windows® Server 2012 R2 *64-bit*			
Microsoft® Windows® Server 2016 *64-bit*			
Microsoft® Windows® Server 2019 *64-bit*			
Microsoft® Windows® Server 2022 *64-bit*			

Additional requirements:

- Microsoft® .NET Framework 4.5.
- Supported databases: Microsoft® SQL Server® 2008, SQL Server® 2012, SQL Server® 2014 SP1, SQL Server® 2016, SQL Server® 2017, PostgreSQL® 11.
- For SQL Server® 2014 Express SP1 or SQL Server® 2012 installation on Windows Server 2008 R2, Service Pack 1 (SP1) should be installed in the system.
- For server operating systems, only desktop installation options are supported.
- Microsoft® Windows® 11 may require the TPM 2.0 and Secure Boot in UEFI mode. A CPU with two or more cores is also recommended.

2.2 SoftControl Admin Console system requirements

Table 4. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
Client operating systems:	3GHz	4GB	100MB
Microsoft® Windows® 7 (SP1) *32-bit/64-bit*			
Microsoft® Windows® 8 *32-bit/64-bit*			

OS	CPU frequency	RAM size	HDD free space
Microsoft® Windows® 8.1 *32-bit/64-bit*			
Microsoft® Windows® 10 *32-bit/64-bit*			
Microsoft® Windows® 11 *64-bit*			
Server operating systems:			
Microsoft® Windows® Server 2008 R2 *64-bit*			
Microsoft® Windows® Server 2012 *64-bit*			
Microsoft® Windows® Server 2012 R2 *64-bit*			
Microsoft® Windows® Server 2016 *64-bit*			
Microsoft® Windows® Server 2019 *64-bit*			
Microsoft® Windows® Server 2022 *64-bit*			

Additional requirements:

- Microsoft® .NET Framework 4.5.
- For server operating systems, only desktop installation options with installed component Desktop Experience are supported.
- Microsoft® Windows® 11 may require the TPM 2.0 and Secure Boot in UEFI mode. A CPU with two or more cores is also recommended.

3. Installing and setting up SoftControl Service Center components

This section describes how to install[11] the SoftControl Server ('the server') and the SoftControl Admin Console components, set up[21] SoftControl Server when running[26] SoftControl Admin Console for the first time, and also gives instructions on how to register client applications[26].

3.1 Installing SoftControl Server and SoftControl Admin Console

There are the following ways to deploy SoftControl Service Center.

- typical[11]: install product components without the embedded DBMS;
- complete[14]: install product components including the embedded DBMS;
- custom[18]: install the components chosen by user.

Select typical installation if a configured DBMS is available on the network, or if it is to be installed separately. Information about separate DBMS installation is given in the appendix[187].

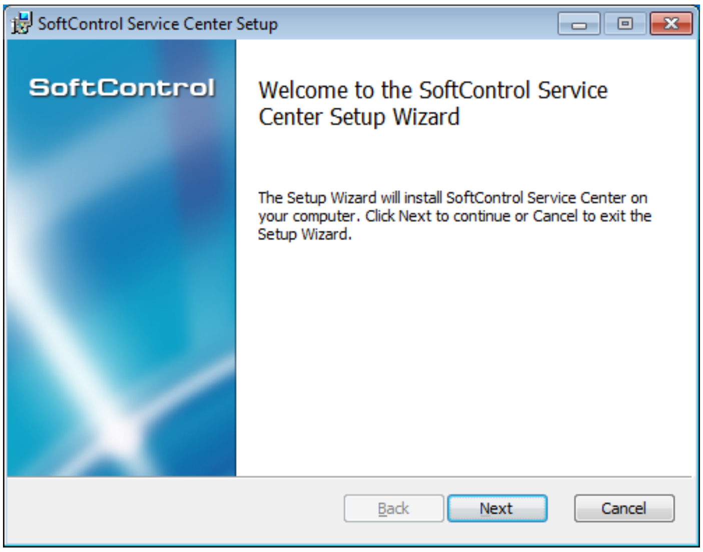
Complete installation is the fastest way to deploy and configure. This way, all the essential operations including DBMS installation are performed by the SoftControl Service Center installer automatically. The SoftControl Service Center installer includes free Microsoft® SQL Server® 2014 Express SP1 DBMS that has all the functionality required for the server to work.

If you prefer to install the server component, DBMS, and the management console onto the different computers, select custom installation.

3.1.1 Typical installation

1) Run the *Service.Center.msi* installation package.

2) Click **Next** in the **SoftControl Service Center Setup** window (fig. Running the installation program[11]).

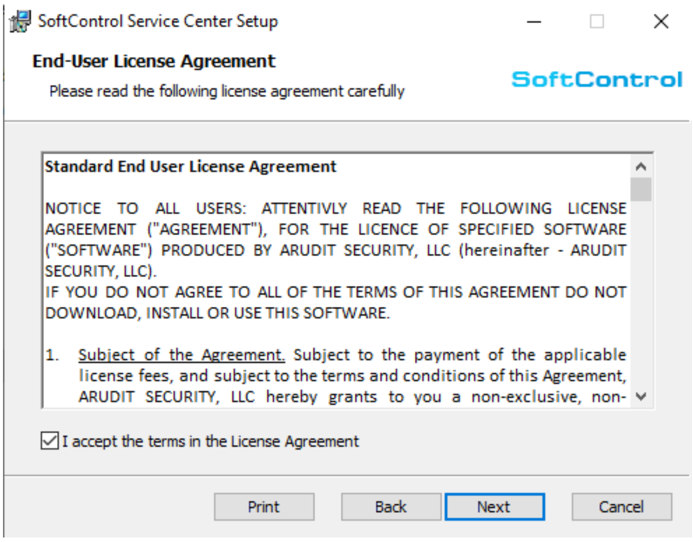


Welcome to the SoftControl Service Center Setup Wizard

The Setup Wizard will install SoftControl Service Center on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 1. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement 12).



End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

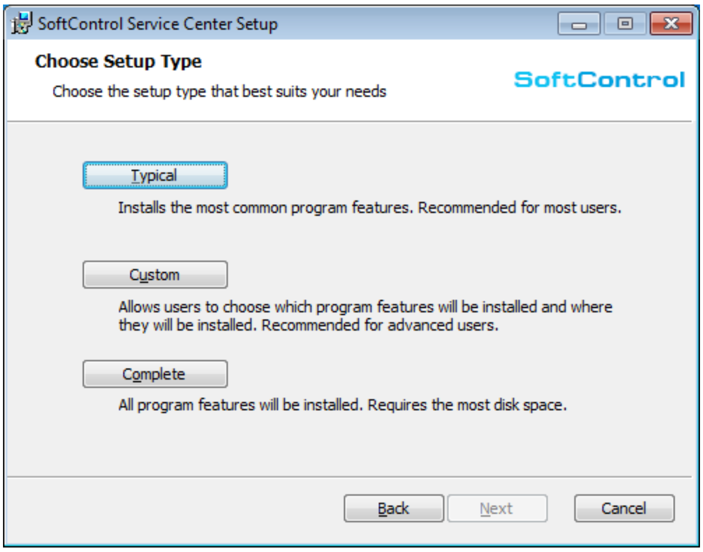
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

Figure 2. License agreement

4) Click **Typical** to select standard installation type (fig. Installation types 12).



SoftControl Service Center Setup

Choose Setup Type

Choose the setup type that best suits your needs

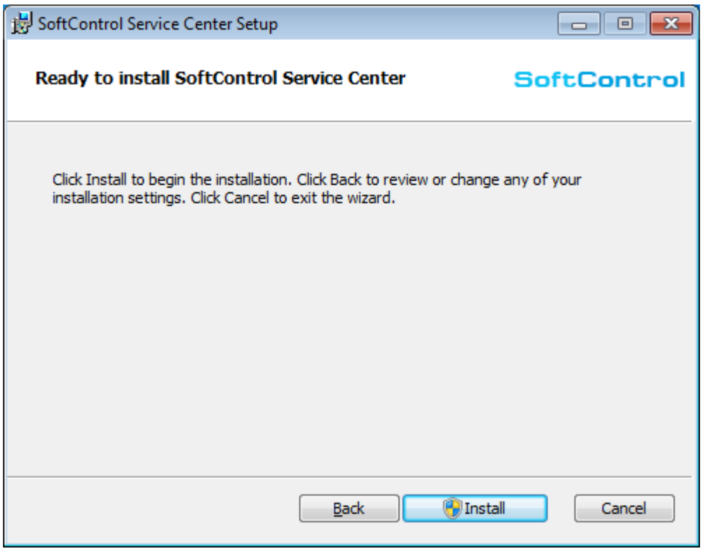
Installs the most common program features. Recommended for most users.

Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

All program features will be installed. Requires the most disk space.

Figure 3. Installation types

5) Click **Install** (fig. Ready to install (13)).



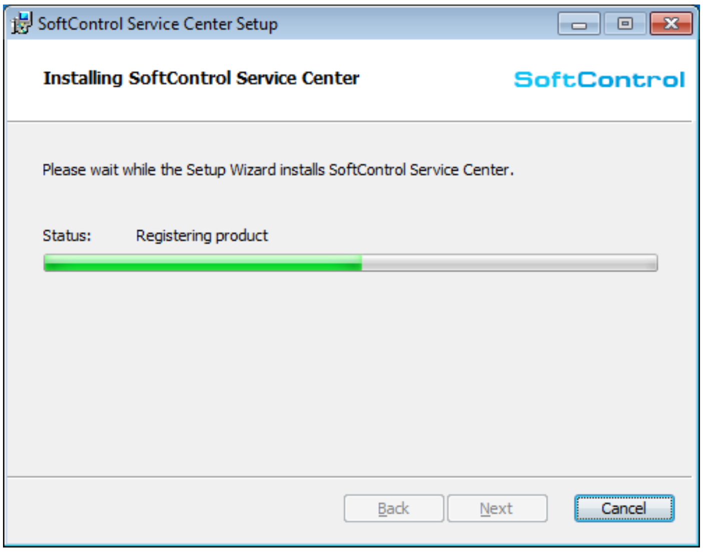
SoftControl Service Center Setup

Ready to install SoftControl Service Center

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 4. Ready to install

6) Wait until installation is complete (fig. Installation progress (13)).



SoftControl Service Center Setup

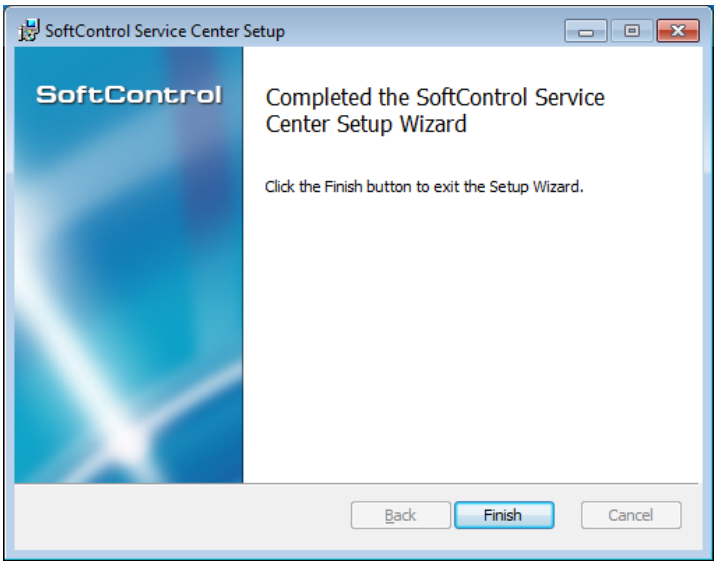
Installing SoftControl Service Center

Please wait while the Setup Wizard installs SoftControl Service Center.

Status: Registering product

Figure 5. Installation progress

7) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Installation is complete[14]).



SoftControl Service Center Setup

Completed the SoftControl Service Center Setup Wizard

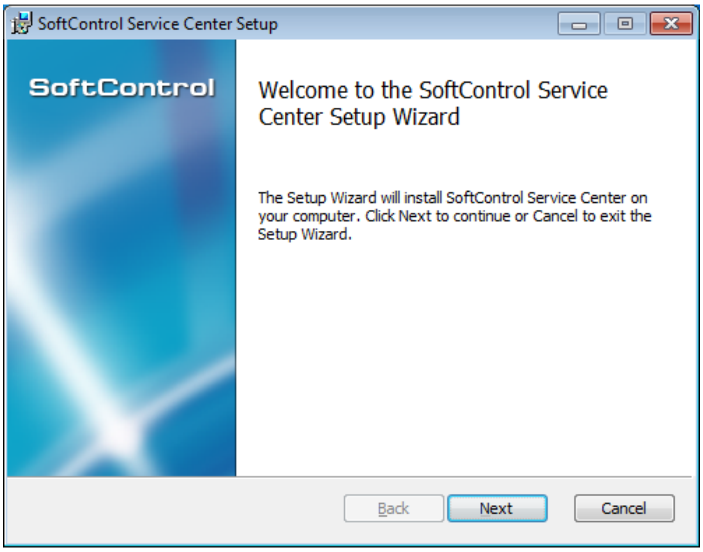
Click the Finish button to exit the Setup Wizard.

Figure 6. Installation is complete

3.1.2 Complete installation

1) Run the *Service.Center.msi* installation package.

2) Click **Next** in the **SoftControl Service Center Setup** window (fig. Running the installation program[14]).

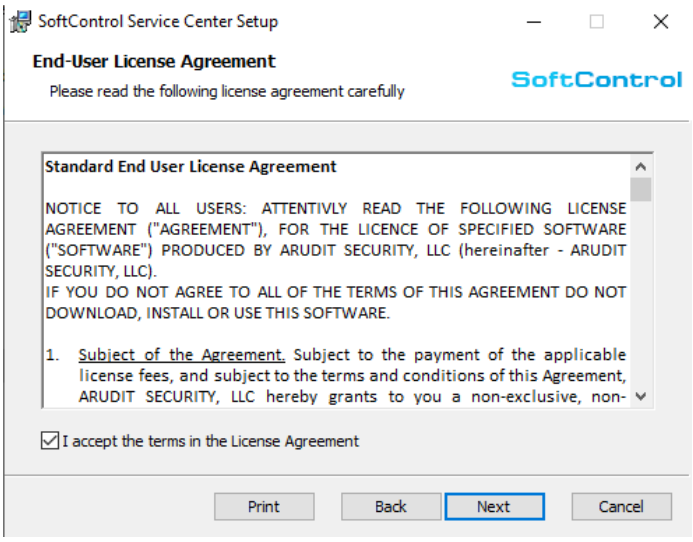


Welcome to the SoftControl Service Center Setup Wizard

The Setup Wizard will install SoftControl Service Center on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 7. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement [15]).



End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

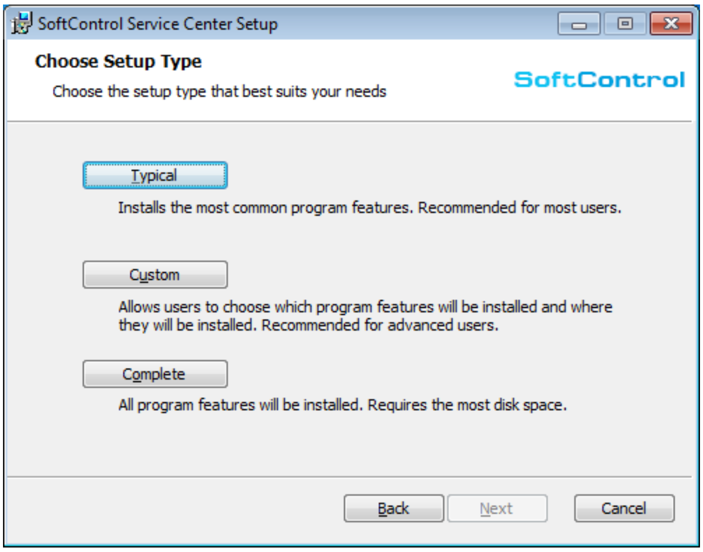
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

Figure 8. License agreement

4) Click **Complete** to select full installation type (fig. Installation types [15]).



SoftControl Service Center Setup

Choose Setup Type

Choose the setup type that best suits your needs

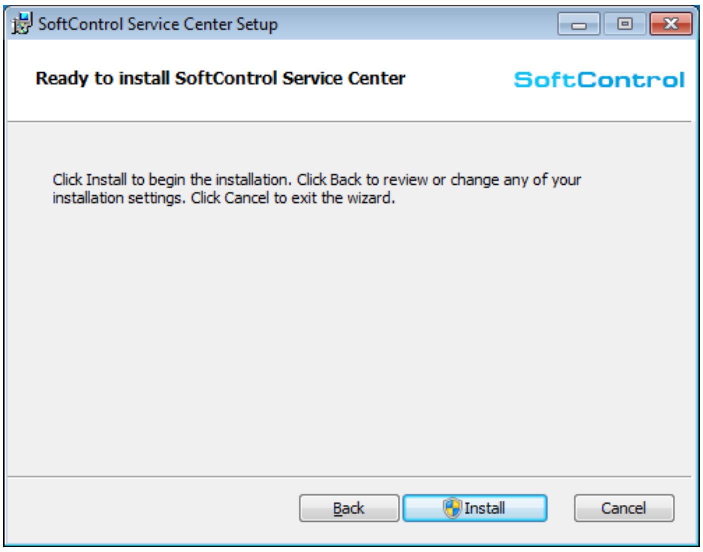
Installs the most common program features. Recommended for most users.

Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

All program features will be installed. Requires the most disk space.

Figure 9. Installation types

5) Click **Install** (fig. Ready to install[16]).



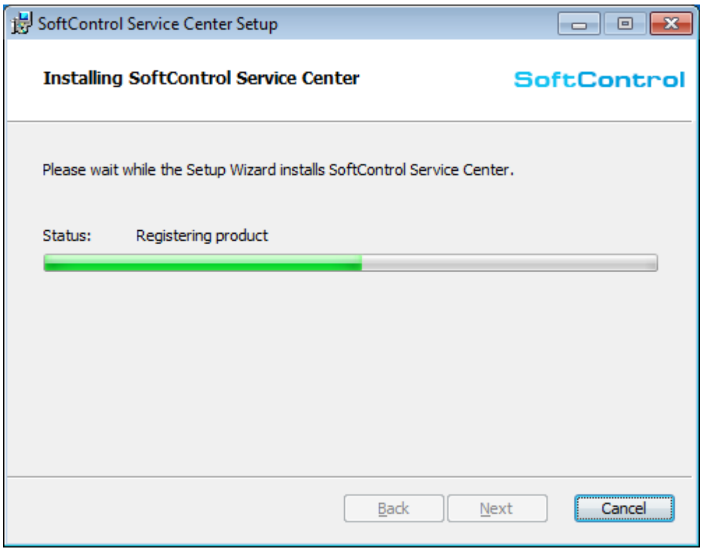
SoftControl Service Center Setup

Ready to install SoftControl Service Center

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 10. Ready to install

6) Wait until installation is complete (fig. Installation progress[16]).



SoftControl Service Center Setup

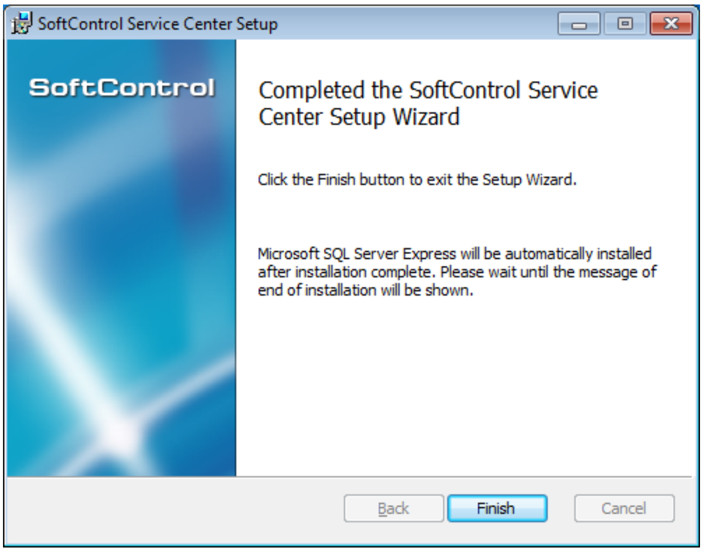
Installing SoftControl Service Center

Please wait while the Setup Wizard installs SoftControl Service Center.

Status: Registering product

Figure 11. Installation progress

7) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** to start Microsoft® SQL Server® 2014 Express SP1 installation (fig. SoftControl Service Center installation is complete (17)).



SoftControl Service Center Setup

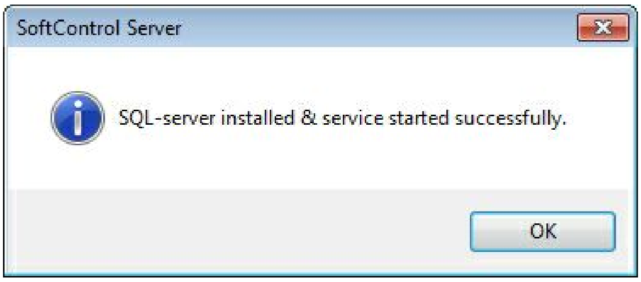
Completed the SoftControl Service Center Setup Wizard

Click the Finish button to exit the Setup Wizard.

Microsoft SQL Server Express will be automatically installed after installation complete. Please wait until the message of end of installation will be shown.

Figure 12. SoftControl Service Center installation is complete

8) Wait until Microsoft® SQL Server® 2014 Express SP1 installation is complete and then click **OK** (fig. Installation is complete (17)).


SoftControl Server

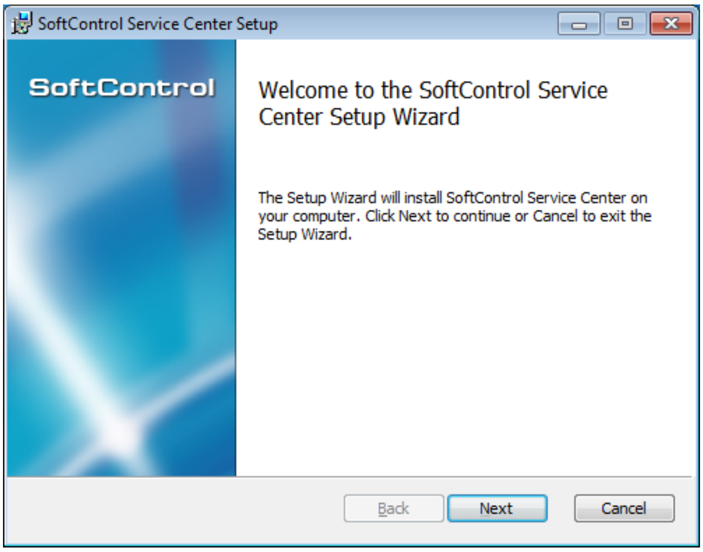
SQL-server installed & service started successfully.

Figure 13. Installation is complete

3.1.3 Custom installation

1) Run the *Service.Center.msi* installation package.

2) Click **Next** in the **SoftControl Service Center Setup** window (fig. Running the installation program [18]).

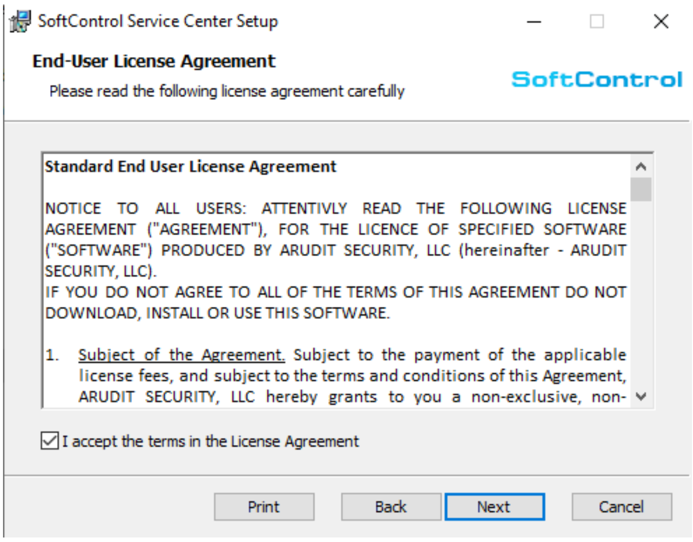

SoftControl Service Center Setup

Welcome to the SoftControl Service Center Setup Wizard

The Setup Wizard will install SoftControl Service Center on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 14. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement [18]).



End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

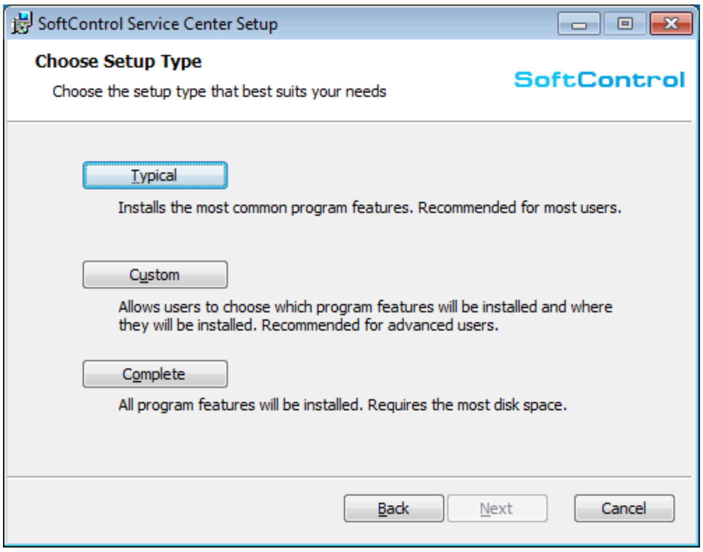
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

Figure 15. License agreement

4) Click **Complete** to select complete installation type (fig. Installation types [19]).



Choose Setup Type

Choose the setup type that best suits your needs

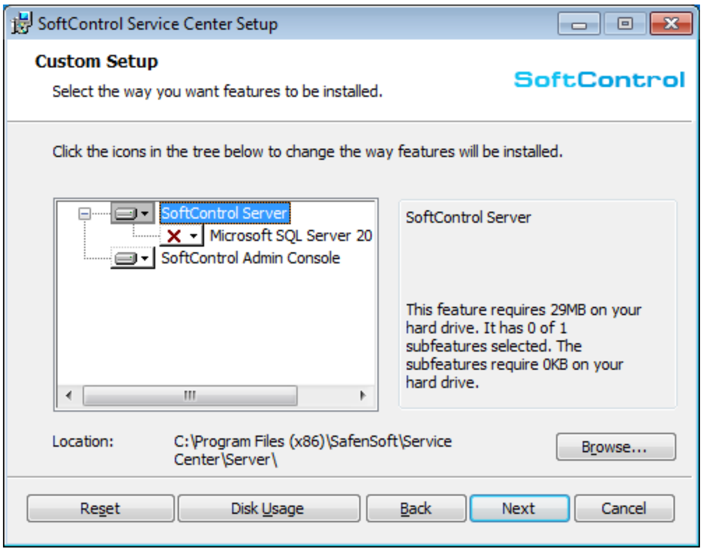
Typical: Installs the most common program features. Recommended for most users.

Custom: Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete: All program features will be installed. Requires the most disk space.

Figure 16. Installation types

5) Configure the component installation (fig. Component installation configuration [19]). Click the icon of the component that should not be installed and select the **Entire feature will be unavailable** option from the drop-down menu (fig. Component installation options [20]). The **Will be installed on local hard drive** option should been selected for the component to install (fig. Component installation options [20]). Click **Browse** to change installation path if necessary. By clicking **Disk usage** you can view total size of the components being installed and available disk space. Click **Next** when all settings are specified.



SoftControl Service Center Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

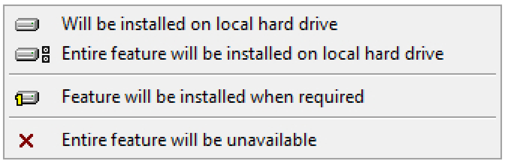
- SoftControl Server
  - Microsoft SQL Server 20
- SoftControl Admin Console

SoftControl Server

This feature requires 29MB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

Location: C:\Program Files (x86)\SafenSoft\Service Center\Server\

Figure 17. Component installation configuration



Will be installed on local hard drive

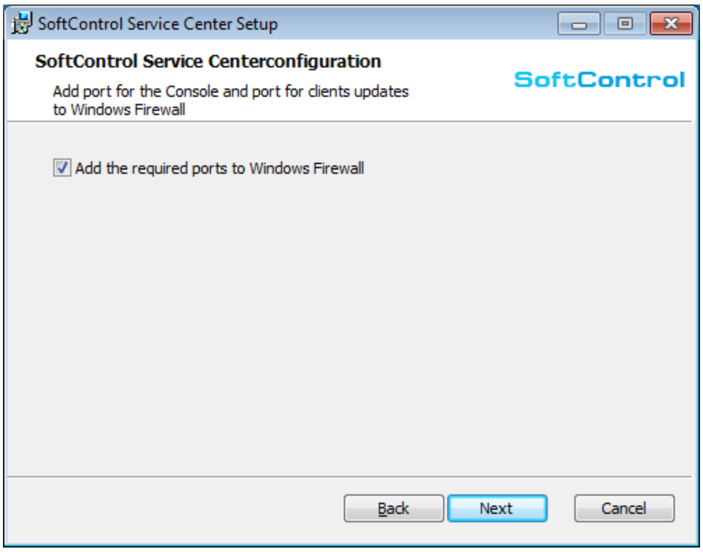
Entire feature will be installed on local hard drive

Feature will be installed when required

✗ Entire feature will be unavailable

Figure 18. Component installation options

6) Select the **Add the required ports to Windows Firewall** option to add the port of connection between SoftControl Admin Console and SoftControl Server to the firewall exceptions automatically (fig. 'Adding a port to the firewall exceptions' option 20). Otherwise, you should perform this operation manually (by default, port *8080* is used). To continue installation, click **Next**.



SoftControl Service Center Setup

SoftControl Service Centerconfiguration

Add port for the Console and port for clients updates to Windows Firewall

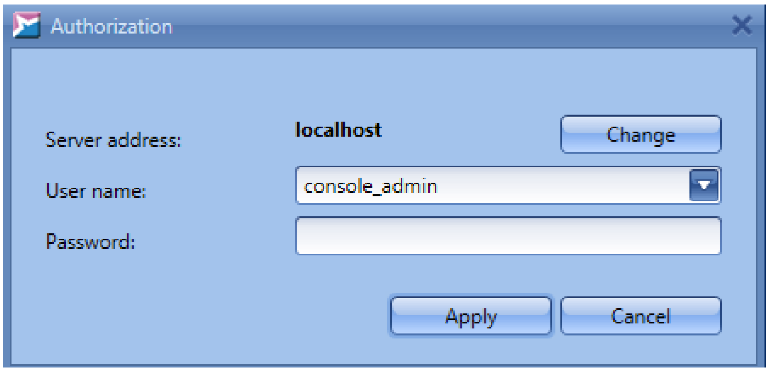
☑ Add the required ports to Windows Firewall

Figure 19. 'Adding a port to the firewall exceptions' option

7) If you have chosen SoftControl Admin Console and/or SoftControl Server without embedded DBMS installation, repeat actions 5-7 for typical installation[13]. If you have chosen SoftControl Server with the *Microsoft® SQL Server® 2014 Express SP1* component, repeat actions 5-8 for complete installation[16].

3.2 Setting up the server

To run SoftControl Admin Console, double-click the program desktop icon. If the server is not configured yet, enter the IP address of the computer with the installed SoftControl Server in the **Server address** field (you can use the *localhost* reserved name if SoftControl Server and SoftControl Admin Console are installed on the same computer), and click **Apply** (fig. Running SoftControl Admin Console for the first time[21]).



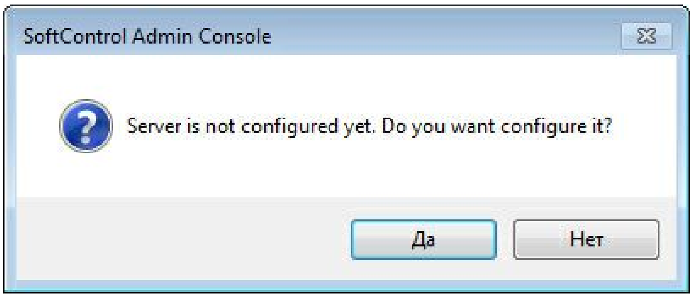
Server address: localhost

User name: console_admin

Password:

Figure 20. Running SoftControl Admin Console for the first time

Click **Yes** in the dialog box with the suggestion to create initial server configuration (fig. Suggestion to run server configuration wizard[21]).

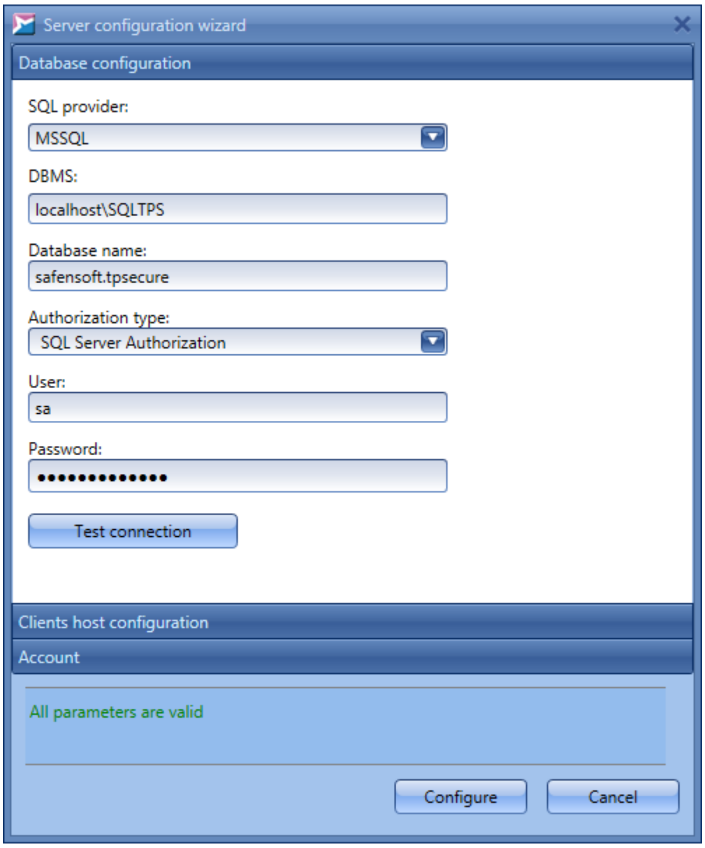


Server is not configured yet. Do you want configure it?

Figure 21. Suggestion to run server configuration wizard

In the **Database configuration** section of the server configuration wizard window, you can specify the DBMS connection options and the name of the database that the SoftControl Server component will use. If SoftControl Service Center was installed along with the embedded DBMS, the fields are filled in with the default values. In other cases, or when you need to change typical values, enter the following parameters (the default values are in parentheses) (fig. Setting up the connection to the DBMS 22):

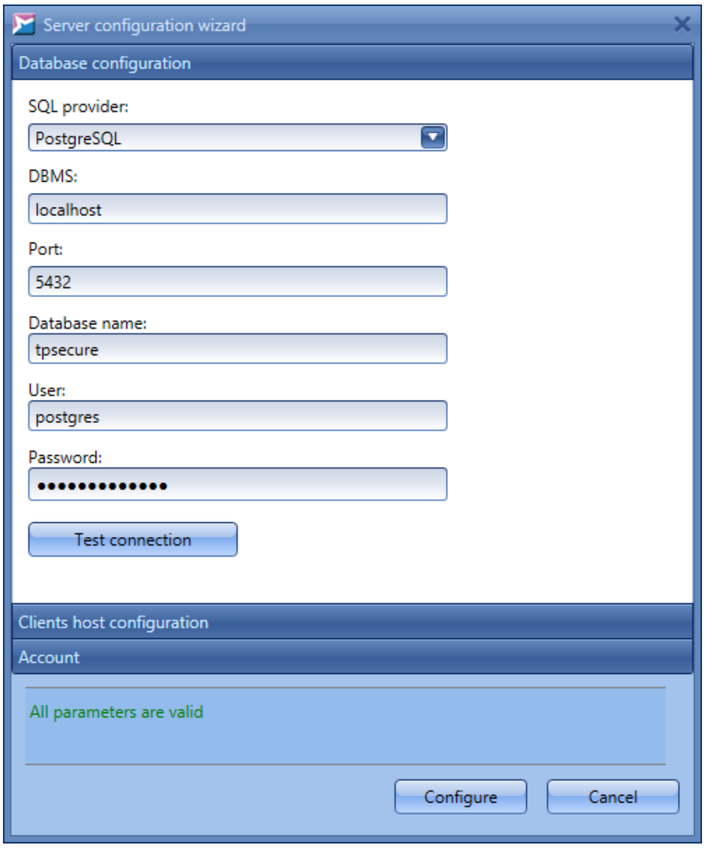
- **DBMS** is the network address (name) of the DBMS server (*localhost\SQLTPS*);
- **Database name** is the database name on the DBMS server (*safensoft.tpsecure*);
- **Authorization type** is the type of the account to log in to the DBMS server (*SQL Server Authorization*);
- **User** is the user name on the DBMS server (*sa*);
- **Password** is the user password on the DBMS server (*SafenSoft2007*).



SQL provider: MSSQL
DBMS: localhost\SQLTPS
Database name: safensoft.tpsecure
Authorization type: SQL Server Authorization
User: sa
Password: •••••••••••••

All parameters are valid

Figure 22. Setting up the connection to the DBMS for MS SQL Server


Server configuration wizard

Database configuration

SQL provider: PostgreSQL

DBMS: localhost

Port: 5432

Database name: tpsecure

User: postgres

Password: •••••••••••••

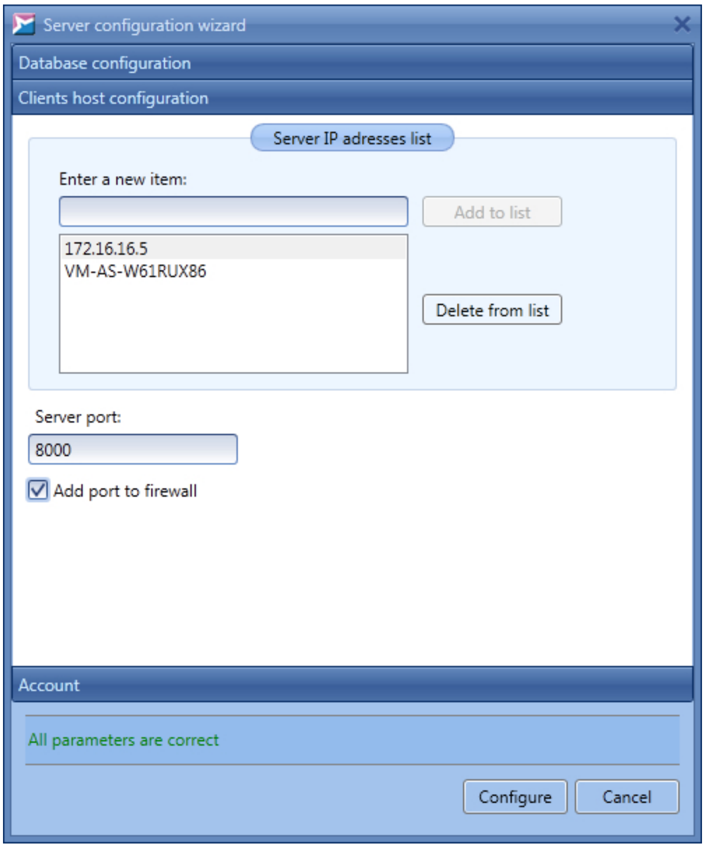
All parameters are valid

Figure 23. Setting up the connection to the DBMS for PostgreSQL

To check the connection to the DBMS and to check whether the SQL Server account is valid, click **Test connection**. If database with the specified name doesn't exist, it is created on the DBMS server when the configuration wizard completes its operation.

When accessing the PostgreSQL DBMS without specifying the database name, a connection is made to the user's database that matches his name. If the database user name differs from the database name, an error message will be displayed when you click the **Test connection** button.

In the **Clients host configuration** section, you can specify the parameters of connection between client applications and the server (fig. Setting up connection between client components and the server[23]).



Enter a new item:

172.16.16.5
VM-AS-W61RUX86

Server port: 8000

☑ Add port to firewall

All parameters are correct

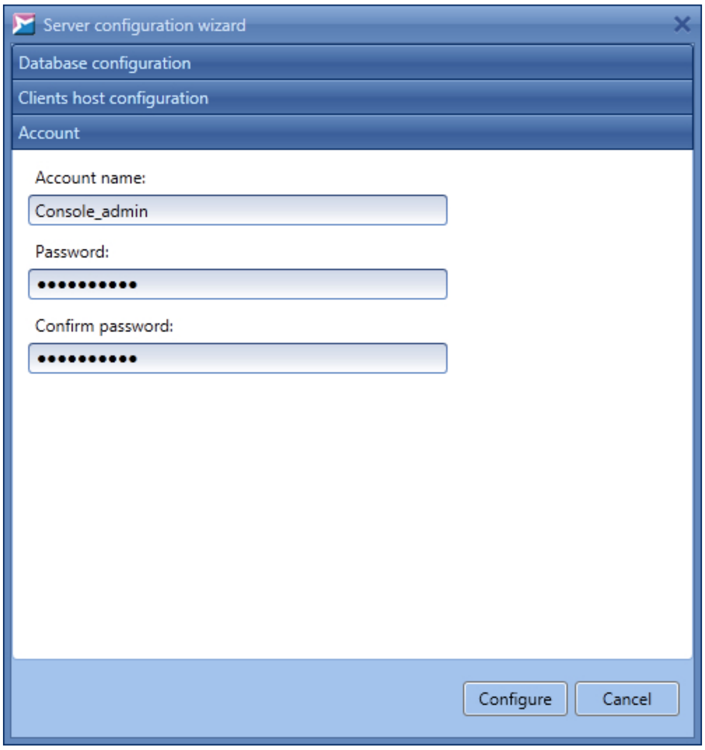
Figure 24. Setting up connection between client components and the server

By default, current server IP address and TCP port *8000* are used to connect to the server. Communication between the client applications and the server can also be performed through several standby channels. You can implement the option by specifying all IP addresses or names (DNS or NetBIOS) by which the server is accessible for the client applications. In this case, a client component connects to each of the addresses in turn until the request is successfully processed. Connection to the server is then established at this address. If there are no successful connections at any address, the client component searches through the list of addresses again after the heartbeat period expires. To add an address to the list, enter a new value to the corresponding field and click **Add to list**. To remove an address from the list, select it and click **Delete from list**. Specify the port of connection between client applications and the server in the **Server port** field (if SoftControl Server and SoftControl Admin Console are installed on the same computer, this port should not coincide with the connection port between SoftControl Server and SoftControl Admin Console[27]). Tick off the **Add port to firewall** checkbox, if the exception for the specified port is not added to the firewall.

We strongly recommend that you specify the server name in the address list, so that the client applications do not lose connection with the server even when its IP address changes automatically. If the connection is lost nevertheless, use the instructions on how to recover connection[208].

Create the first user account by specifying **Account name**, **Password** and **Confirm password** in the **Account** section (fig. Creating a user[25]). This user will have administrator privileges.

Note. You can change the user's password later by clicking **Change password** in the lower right corner of SoftControl Admin Console on any tab (see section Accounts[37]).



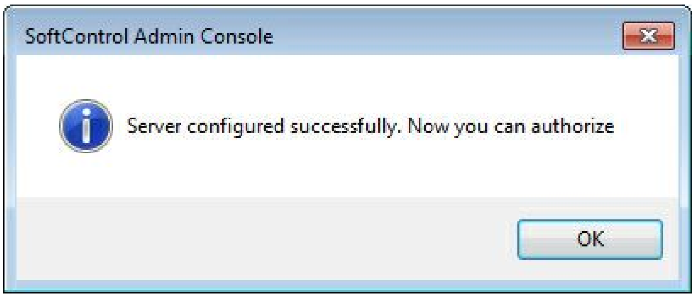
Account name: Console_admin

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Figure 25. Creating a user

When all settings are specified, click **Configure**. If the configuration is created successfully, the corresponding message is displayed (fig. Configuration is created successfully[25]).



SoftControl Admin Console

Server configured successfully. Now you can authorize

Figure 26. Configuration is created successfully

Use the created account to connect to SoftControl Server in the authorization window[26].

3.3 Registering client applications

After the initial setup[21] of the server, the encrypted configuration file is generated in the following path on the computer with the installed SoftControl Server:

```
C:\ProgramData\SafenSoft\ClientSettings.xmlc
```

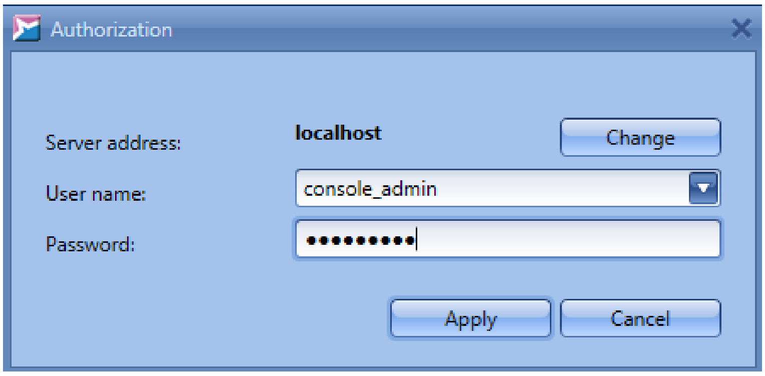
The file contains server connection parameters for the client applications, as well as common client certificate[205] that is used to establish secure connection by default. To register with SoftControl Service Center, apply the above-mentioned file on the devices with the client applications installed previously according to the documentation.

Connection to the server in the registration standby mode is performed with the help of common client certificate, and in this case, the client doesn't send data to the server. Interaction is performed in regular mode after the client component switches to the **Active** status[42].

For detailed description of how to apply the file, see 'SoftControl ATM Client / Endpoint Client / SClient user's guide' and 'SoftControl DLP Client installation guide' for the corresponding components.

3.4 Connecting to the server from the management console

To run SoftControl Admin Console, double click the program desktop icon. Enter **Server address**, **User name** and **Password**, select **Token** and enter its **PIN** in the **Authorization** window (fig. User authorization in SoftControl Admin Console[26]).



Server address: localhost

User name: console_admin

Password: ••••••••••

Figure 27. User authorization in SoftControl Admin Console

Click **Apply** to connect to the SoftControl Server component.

During user authentication, a session with unique ID is created on the server. All user operations with the management console are performed within current session, and connection between the server and management console is checked regularly. If the server cannot access management console for more than 2 minutes, current session is terminated.

By default TCP port *8080* is used for connection between SoftControl Admin Console and SoftControl Server. If the port cannot be used for some reason, change its value in the server component and management console configuration files.

The path of the server configuration file is as follows:

`C:\ProgramData\SafenSoft\Server.Config.xml`

The port value is specified in the *Port* attribute of the *WebApiHost* element.

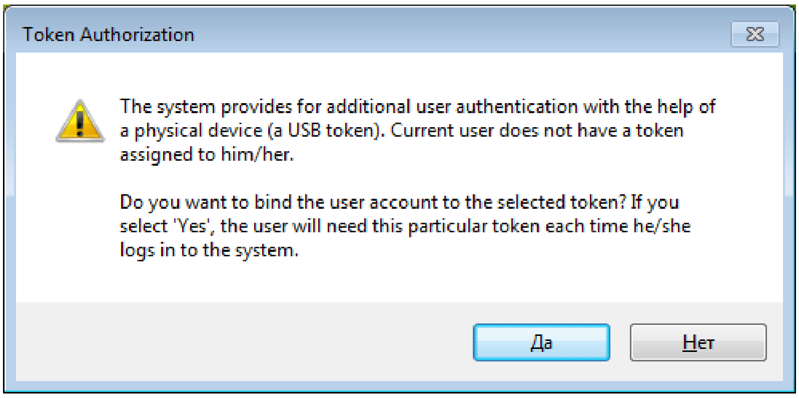
The path of the management console configuration file is as follows:

`C:\ProgramData\SafenSoft\SafenSoft.Enterprise.Console.exe.Config`

Port value is specified in the following part of the file:

```
<Databases>
  <Elements>
    <add name="<port value>" lastconnection="" />
  </Elements>
</Databases>
```

When you connect to SoftControl Service Center for the first time with the use of a token, SoftControl Admin Console displays a message that you should bind the account to the token (see fig. below[27]). Click **Yes** to log in to the system and start the centralized ISS management[29].


Token Authorization

The system provides for additional user authentication with the help of a physical device (a USB token). Current user does not have a token assigned to him/her.

Do you want to bind the user account to the selected token? If you select 'Yes', the user will need this particular token each time he/she logs in to the system.

Figure 28. Binding an account to a token

You can change the token the account is bound to, in the authorization window (see above[26]) or on any tab in SoftControl Admin Console, by clicking **Change token** in the lower right corner.

If the number of log-in attempts exceeds the specified value (5 by default), the user account is blocked. You can set the value in the server configuration file with the help of the *PasswordAttempts* parameter. You can specify the period (in seconds) when the account remains blocked, with the help of the *LockForSeconds* parameter. Only the administrator can unblock the account.

Besides, the account is blocked if it has not been used for 45 days (except for **System Administrators**).

The user session is blocked if the user is idle for 5 minutes. To continue working with SoftControl Server, the user needs to log in again.

4. Centralized ISS management

The SoftControl Admin Console management console enables remote centralized management of the SoftControl SysWatch, SoftControl DLP Client and SoftControl SysCmd applications, on the basis of the SoftControl Server component's service functions.

This section describes how to work with SoftControl Admin Console and is designed for the administrators of the information security system (hereafter referred to as ISS) on the basis of SoftControl Service Center.

4.1 SoftControl Admin Console interface

The SoftControl Admin Console interface consists of the program's main window which has the following tabs.

- Log 130;
- Security events 39;
- Windows event logs 142;
- Clients 42;
- Client settings 56;
- Security profiles 113;
- Organization units 49;
- Tasks 115;
- Accounts 35;
- Roles 33;
- Contacts 153;
- Notifications 155;
- Updates 168;
- Configuration snapshots 162

Graphical buttons in the upper part of the SoftControl Admin Console main window correspond to the tabs listed above. Besides, the Clients 42, Log 130, Security events 39, Windows event logs 142, Organization units 49, Client settings 56, Security profiles 113, Tasks 115, Contacts 153 and Notifications 155 tabs have their own graphical buttons which apply only for these tabs. Table 5 describes the common buttons.

Table 5. SoftControl Admin Console widgets

Button	Name	Description	Hot keys
	Event log	Open the **Event Log** tab for all devices.	
	Security events	Open the **Security events** tab.	
	Windows event logs	Open the **Windows event logs** tab.	
	Clients	Open the **Clients** tab.	F4
	Client settings	Open the **Client settings** tab.	
	Security profiles	Open the **Security profiles** tab.	
	Organization units	Open the **Organization units** tab.	
	Tasks	Open the **Tasks** tab.	
	Accounts	Open the **Accounts** tab.	
	Roles	Open the **Roles** tab.	
	Contacts	Open the **Contacts** tab.	
	Notifications	Open the **Notifications** tab.	
	Refresh	Refresh data in the current tab.	F5
	Choose columns	Modify which columns are displayed in the table.	F6
	Save view settings	Save the selected set of columns as a user filter. Applies only to the **Log** tab.	F2
	Print	Print out the list of current devices or the selection of events.	Ctrl + P
XLS	Export to Excel	Export the list of current devices or the selection of events to an *XLSX* (Microsoft® Excel®) file.	Ctrl + E
	Configuration snapshots	Open the **Configuration snapshots** tab.	
	Updates	Open the **Updates** tab.	
	Server	Open the server connection settings.	

Some of the functions that are called by the common buttons can also be accessed from the main program menu.

The lower part of the main window displays a string with the current user name and their roles.

You can perform the following additional operations in the main SoftControl Admin Console window.

Setting up the connection to the DBMS server

To view or modify the settings of connection between DBMS server and SoftControl Admin Console while the latter is working, click **Database**.

The connection settings window is similar to the authorization[26] window that is displayed when SoftControl Admin Console runs.

Setting up the interface

To modify the SoftControl Admin Console interface settings, select **View** → **Settings** in the main menu.

By default, the SoftControl Admin Console interface language is selected on the basis of the OS regional settings, when the program runs for the first time. To change the language, select it from the drop-down list in the **Settings** window (fig. Interface settings[31]):

- **ru-RU** – Russian;
- **en-US** – English (USA).

Restart the program to apply the changes.

Tick off **Run one instance only** if several instances of SoftControl Admin Console should not be allowed to run at the same time.

Specify the maximum number of events that should be displayed per page on the Log[144] tab, in the **Event page size** field.

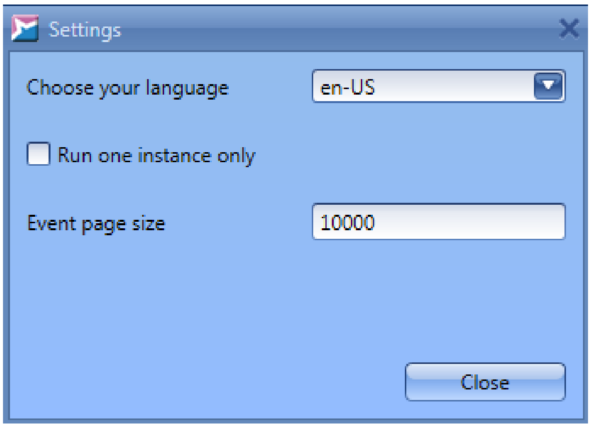

Settings
Choose your language: en-US
□ Run one instance only
Event page size: 10000

Figure 29. Interface settings

Viewing information about the program

Select **About** in the main menu.

4.2 The procedure

When you manage a SoftControl Service Center-based ISS from SoftControl Admin Console, we recommend that you follow the procedure as described below, in order to decrease the time spent and to increase the efficiency.

1) Run SoftControl Admin Console and connect to SoftControl Server (26).
2) On the **Roles** tab, create additional roles (33) if necessary and assign the roles (33) with the specified permissions to the user accounts (35). Supervise user actions (39) via management console with the help of the **Security events** tab.
3) Approve (46) or reject (47) registration requests from the client components which are installed on the protected endpoints, on the **Client settings** tab.
4) After you finish creating the workspace of the required devices, switch to the **Client settings** tab and add configurations (58) that should apply to the client applications.
5) After you configure the client settings, switch to the **Organization units** tab and create organization units (51) (groups) by any principle to distribute the registered components on the client hosts. When you create units, bind them to certain configurations (52).
6) Switch to the **Clients** tab and move client components (48) to the created organizational units.
7) Create the required tasks (115) for client applications on the **Tasks** tab.
8) Switch to the **Log** tab and start viewing the reports from the client components (130).
9) Additionally, you can set up notifications (155) about the incidents.The notifications will be sent to the specified e-mails (153). You also can export and print out (150) the required data.

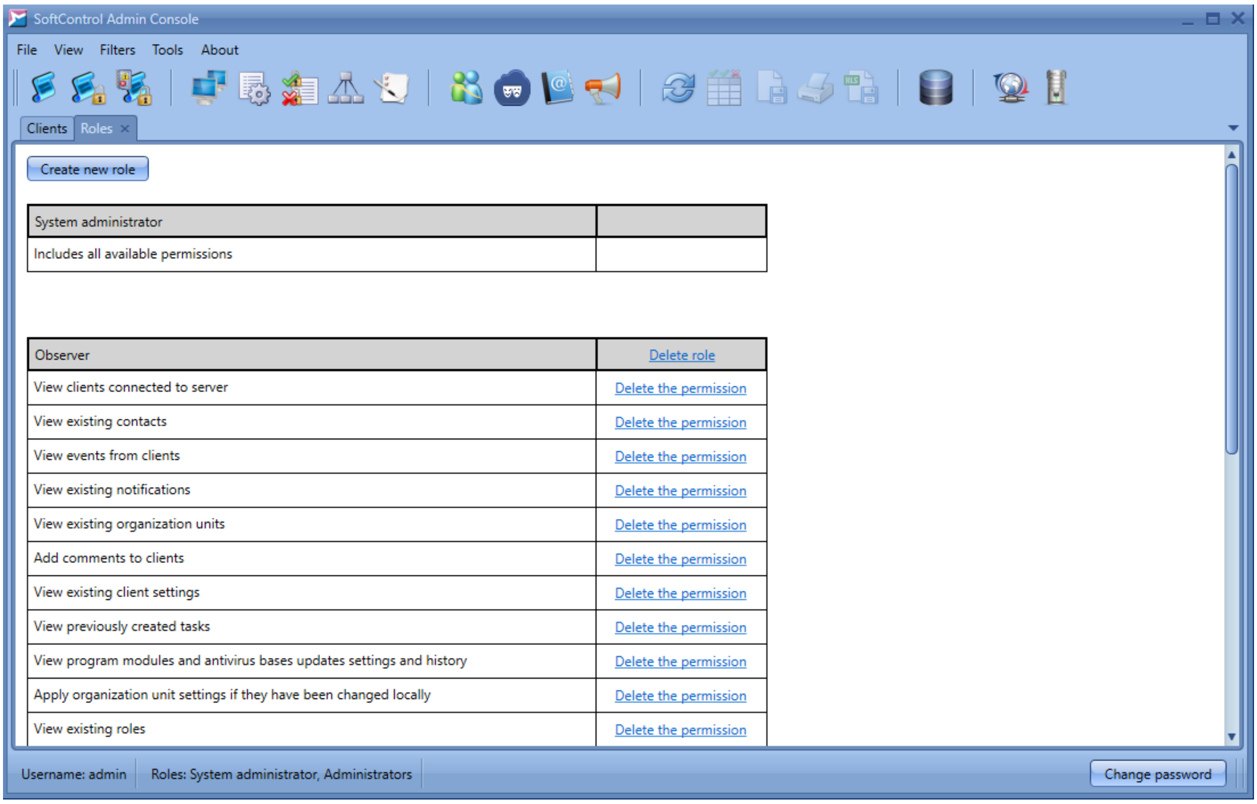
4.3 Role-based access control

SoftControl Service Center features the role-based access control (*RBAC*) subsystem. The subsystem allows you to regulate user (35) access to different functions of SoftControl Server and SoftControl Admin Console on the basis of their roles (33).

User actions are monitored through SoftControl Admin Console that registers the server security events[39].

4.3.1 Roles

The **Roles** tab allows you to manage the roles and set up the permissions for them (fig. The 'Roles' tab[33]).



System administrator	
Includes all available permissions	

Observer	Delete role
View clients connected to server	Delete the permission
View existing contacts	Delete the permission
View events from clients	Delete the permission
View existing notifications	Delete the permission
View existing organization units	Delete the permission
Add comments to clients	Delete the permission
View existing client settings	Delete the permission
View previously created tasks	Delete the permission
View program modules and antivirus bases updates settings and history	Delete the permission
Apply organization unit settings if they have been changed locally	Delete the permission
View existing roles	Delete the permission

Username: admin

Roles: System administrator, Administrators

Figure 30. The 'Roles' tab

The roles on the tab are displayed as tables, where the role name is specified in the first row, and the rights to perform certain operations in management console (permissions) are in the next rows.

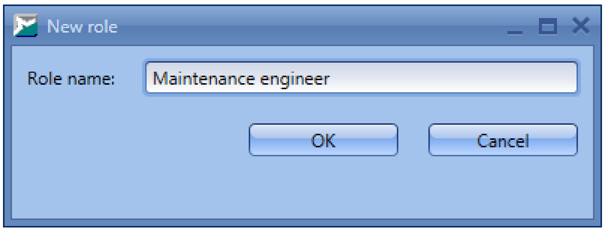
SoftControl Service Center includes two predefined roles:

- **System administrator** can access all the functionality of management console (recommended for advanced users and security officers).
- **Observer** can view most of information including all data on working with client applications (recommended for operators who monitor security incidents on the client hosts).

Besides, you can create new roles with their own sets of permissions. Operations with the roles on this tab are described below.

Creating a role

To add a role, click **Create new role** (fig. The 'Roles' tab[33]). Specify the **Role name** in the displayed window and click **OK** (fig. Creating a new role[34]).



Role name: Maintenance engineer

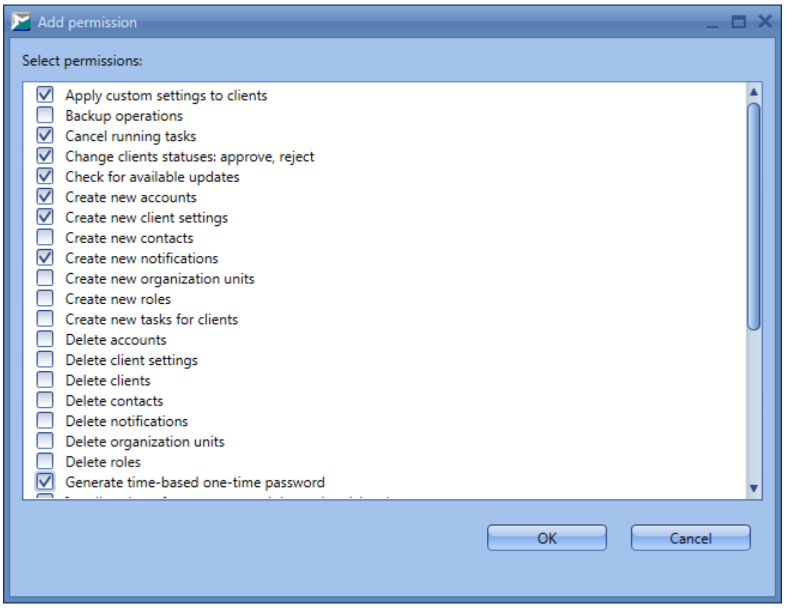
Figure 31. Creating a new role

The new role is added to the end of the role list. Set the permissions[34] for the role.

Modifying permissions

To add permissions to a role, click the **Add permission** button below the table with the role. Tick off the required permissions in the displayed window and click **OK** (fig. Adding permissions[34]).

To delete a permission, click the **Delete permission** link in the corresponding row of the table with a role (fig. The 'Roles' tab[33]).



Select permissions:

- ☑ Apply custom settings to clients
- □ Backup operations
- ☑ Cancel running tasks
- ☑ Change clients statuses: approve, reject
- ☑ Check for available updates
- ☑ Create new accounts
- ☑ Create new client settings
- □ Create new contacts
- ☑ Create new notifications
- □ Create new organization units
- □ Create new roles
- □ Create new tasks for clients
- □ Delete accounts
- □ Delete client settings
- □ Delete clients
- □ Delete contacts
- □ Delete notifications
- □ Delete organization units
- □ Delete roles
- ☑ Generate time-based one-time password

Figure 32. Adding permissions

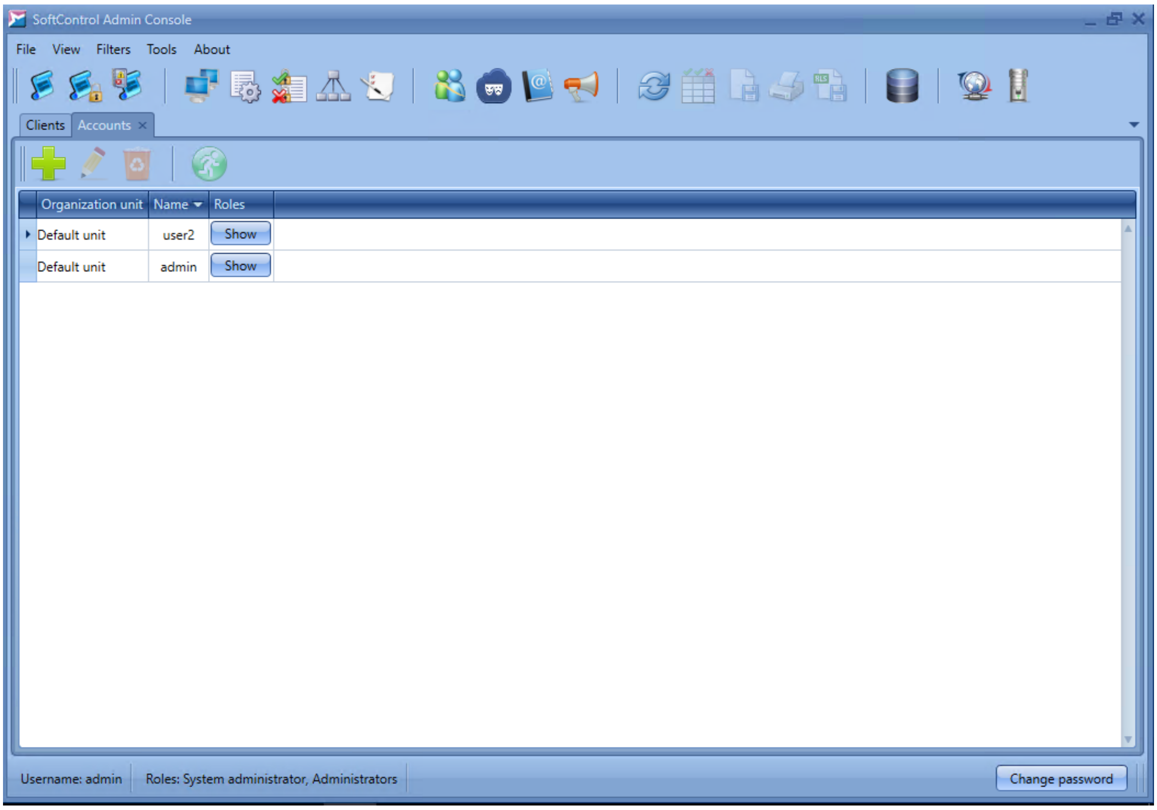
Removing a role

To remove a role, click the **Delete role** link in the table row with the role name (fig. The 'Roles' tab[33]) and confirm the removal in the dialog box.

You cannot remove roles that are assigned to current users (see section below[35]).

4.3.2 Accounts

You can manage user accounts and assign the roles for them on the **Accounts** tab (fig. The 'Accounts' tab[35]).



Organization unit	Name	Roles
Default unit	user2	Show
Default unit	admin	Show

Username: admin | Roles: System administrator, Administrators | Change password

Figure 33. The 'Accounts' tab

Basic operations with user accounts are performed with the help of the tab's graphical buttons which are described in table 6.

Table 6. The 'Accounts' tab widgets

Button	Name	Description
✚	New	Create a new account.
✏	Edit	Modify the selected account properties.
🗑	Delete	Remove the selected accounts.
🏃	Move	Move the selected user to another organization unit.

The list of the tab fields is given in table 7.

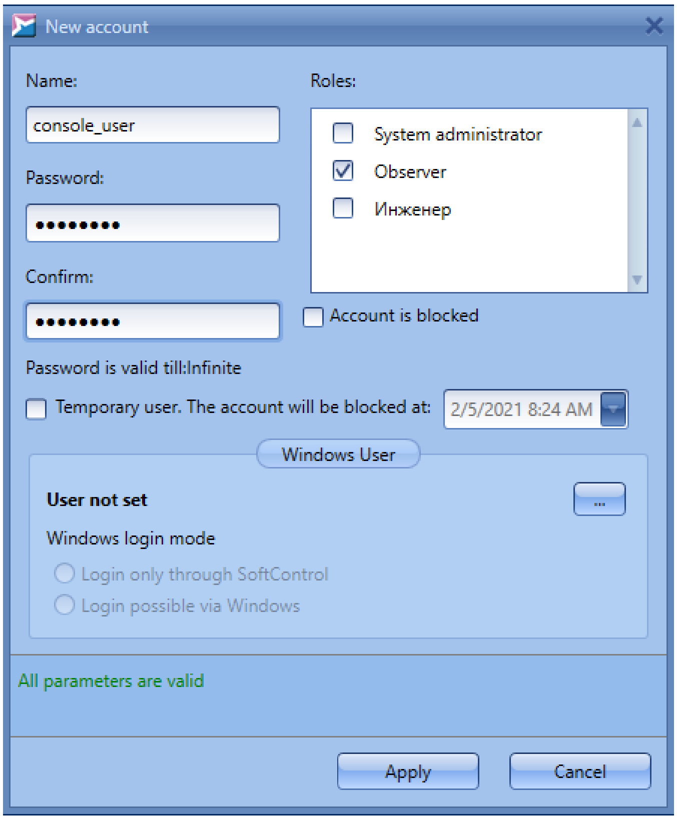
Table 7. The 'Accounts' tab fields

Field	Description
Organization unit	The organization unit that the current user is assigned to.
Name	User name.
Roles	User roles.

Basic operations on this tab are:

Creating user account

To create a new user account, click **New** (fig. The 'Accounts' tab[35]). Specify the user **Name**, enter **Password** and **Confirm** it in the displayed window. Select the required **Roles** for the user and then click **Apply** (fig. Creating an account[36]). Specify the minimum password length in the parameter *MinPasswordLength* of server configuration file (C:\ProgramData\SafenSoft\Server.Config.xml).


New account

Name: console_user

Password: ••••••••

Confirm: ••••••••

Roles:
- □ System administrator
- ☑ Observer
- □ Инженер

□ Account is blocked

Password is valid till:Infinite

□ Temporary user. The account will be blocked at: 2/5/2021 8:24 AM

Windows User

User not set

Windows login mode
- ○ Login only through SoftControl
- ○ Login possible via Windows

All parameters are valid

Figure 34. Creating an account

The Windows user area is for future use. Associated functionality has not been implemented in the current version.

All new user accounts are automatically added to the **Default** organization unit. You can move[38] the selected account to another unit.

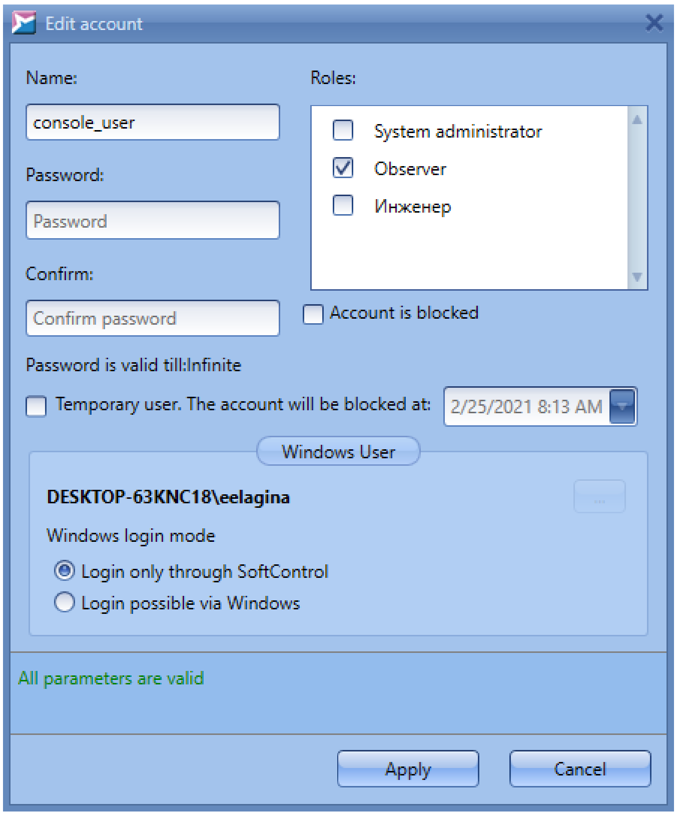
Depending on their role[33], the user can access data in the current unit and all its subsidiary units, but cannot access any data in the parent units.

You can make a temporary account by selecting **Temporary user** and specifying the date when the account should be blocked.

Modifying user account

To modify user account, click **Edit** (fig. The 'Accounts' tab[35]).

Modify the user **Name** and/or change the **Roles** in the corresponding area in the displayed window, and then click **Apply** (fig. Modifying an account[37]). The password does not change in this case. If you need to change the password, enter a new **Password** in the corresponding field and **Confirm** it.



Name: console_user

Password: Password

Confirm: Confirm password

Roles:
☐ System administrator
☑ Observer
☐ Инженер

☐ Account is blocked

Password is valid till:Infinite

☐ Temporary user. The account will be blocked at: 2/25/2021 8:13 AM

Windows User

DESKTOP-63KNC18\eelagina

Windows login mode
● Login only through SoftControl
○ Login possible via Windows

All parameters are valid

Figure 35. Modifying an account

Besides, any user can change his or her password in the window that is displayed when the user clicks **Change password** in the lower right corner of SoftControl Admin Console (see fig. The 'Accounts' tab[35]). The button is available on any tab.

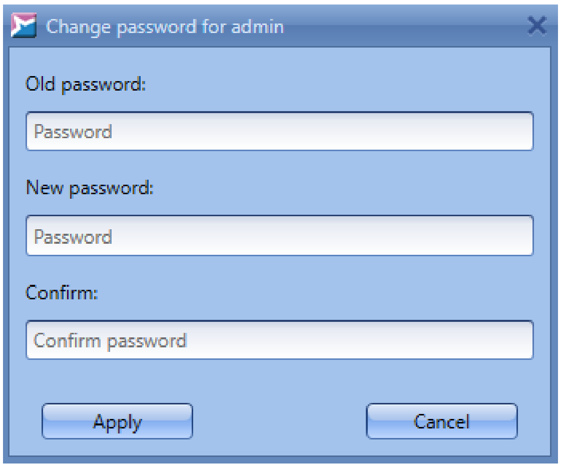


Figure 36. Changing user password

In this window, enter the **Old Password**, the **New Password**, **Confirm** it, and click **Apply**. When changing the password, the administrator can set its lifetime. To do so, the administrator specifies the required value (the number of days) for the *PasswordValidDays* parameter in the server configuration file (`C:\ProgramData\SafenSoft\Server.Config.xml`). It is 60 days by default; '0' means the lifetime is unlimited. You can specify the minimum time the password is valid for with the help of the *MinPasswordPeriodDays* parameter. This value cannot be greater than the value set for the *PasswordValidDays* parameter. You can also prevent the users from using a certain number of old passwords (from 1 to 10; with the *ForbidOldPasswordCount* parameter).

If you need to block the account, tick off **Account is blocked** (fig. Modifying an account[37]).

Removing an account

To remove a user account, select it, press **Delete** (fig. The 'Accounts' tab[35]) and confirm the removal in the dialog box.

Note. After you delete an account, you cannot create a new one with the same name in the next three years.

Moving an account

To move an account, select it, click **Move** and select the unit you need to move the user to, in the displayed window (fig. Moving an account[38]).

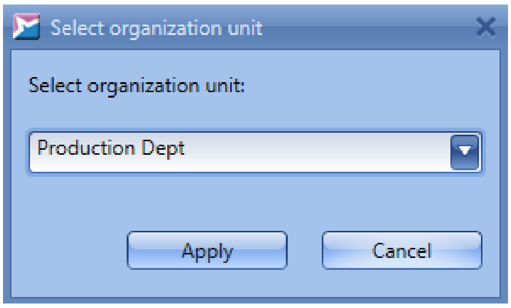


Figure 37. Moving an account

4.3.3 Server security events

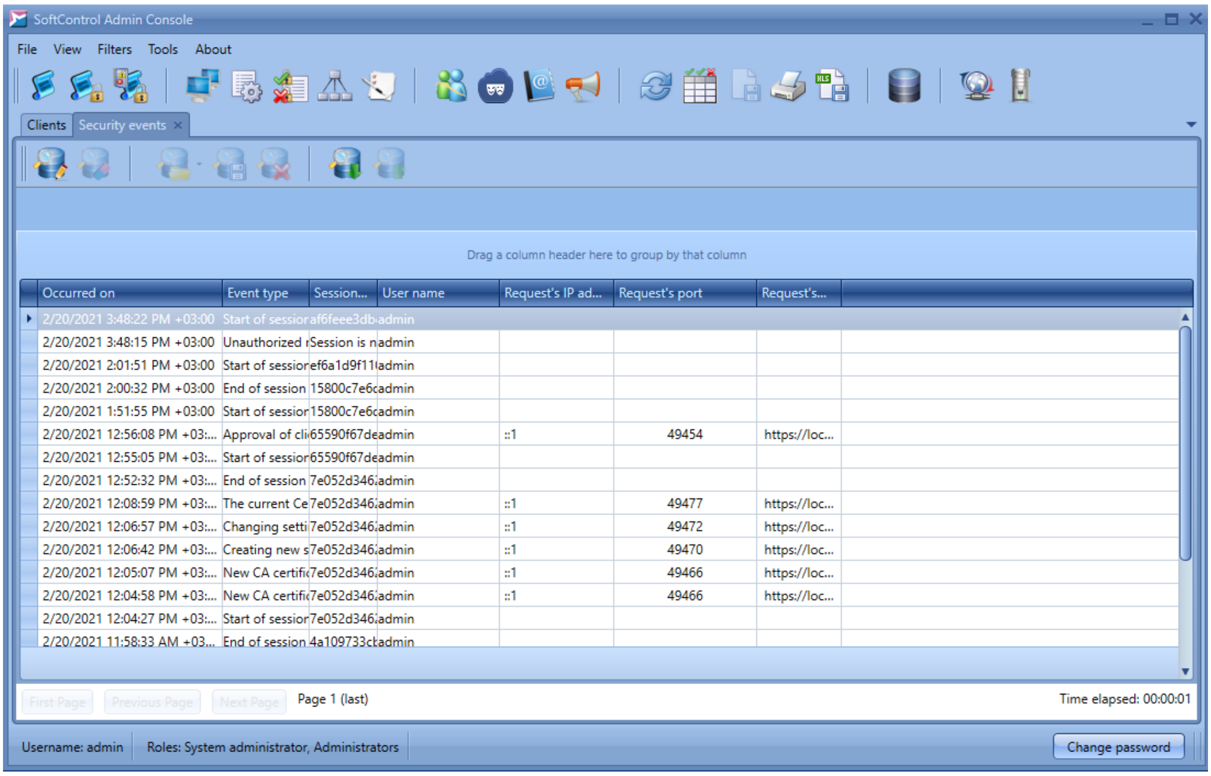
The administration console allows you to register user operations, so as to analyze them on the **Security events** tab (fig. The 'Security events' tab[39]).

The full list of the tab fields is given in table 8.

Table 8. The 'Security events' tab

Field	Description
Occurred on	Date and time when the event occurred.
Event type	Type of the registered event: • **Start of session**; • **End of session**; • **Role is created**; • **Role is deleted**; • **Adding permissions to role**; • **Role's permissions are removed**; • **Account is created**; • **Account is changed**; • **Account is deleted**; • **Approval of client**; • **Rejection of client**; • **Deletion of client**; • **Request to change a client certificate**; • **New certificate is assigned for client**; • **Moving object to another organization unit**; • **New organization unit is created**; • **Organization unit is deleted**; • **Creating new settings**; • **Changing settings for organization unit**; • **Assigning custom settings**; • **Settings are deleted**; • **Assigning organization unit settings**; • **Task is created**; • **Task is canceled**; • **Contact is created**;

Field	Description
	- **Contact is changed**; - **Contact is deleted**; - **Notification is created**; - **Notification is changed**; - **Notification is deleted**; - **Unauthorized request**; - **Insufficient permissions for request**; - **Error while processing request**.
Session ID	Checksum of the ID of the session that the event is associated with.
Account	User account associated with the event.
Request IP address	IP address of the computer with the installed SoftControl Admin Console from which a request to the server is received.
Request port	Port of the computer with the installed SoftControl Admin Console from which a request to the server is received.
Request Uri	Full URI of the SoftControl Admin Console request which is sent to the server.
Role name	Role name (only for the **Role is created**, **Role is deleted**, **Add permissions to role**, and **Role's permissions are removed** event types).
Role permissions	The list of added (only for the **Add permissions to role** event type) or deleted (only for the **Role's permissions are removed** event type) role permissions.
Account name	User account name (only for the **Account is created**, **Account is changed**, and **Account is deleted** event types).
Client's Guid	Unique ID of the client application (only for the **Approval of client**, **Rejection of client**, **Deletion of client**, and **Moving client to other organization unit** event types).
Client's name	The name of a client host (only for the **Approval of client**, **Rejection of client**, **Deletion of client**, **Request to change a client certificate**, **New certificate is assigned for client**, and **Moving object to another organization unit** event types).
Organization unit	Organization unit which the installed client component is moved to (only for the **Moving object to another organization unit**, **New organization unit is created**, and **Organization unit is deleted** event types).
Settings	The name of the client application configuration (only for the **Creating new settings**, **Changing settings for organization unit**, and **Settings are deleted** event types).
Settings creation time	Time when the client application configuration is created on the server (only for the **Creating new settings** event type).
Task ID	Task sequence number (only for the **Task is created** and **Task is canceled** event types).
Task type	Task type (only for the **Task is created** and **Task is canceled** event types).
Contact name	The name of the notification recipient (only for the **Contact is created**, **Contact is changed**, and **Contact is deleted** event types).
Notification name	Notification name (only for the **Notification is created**, **Notification is changed**, and **Notification is deleted** event types).
Error message	Message about the error during request processing.
Unauthorized request reason	The reason why authorization on the server is impossible (only for the **Unauthorized request** event type).


SoftControl Admin Console
File View Filters Tools About
Clients Security events
Drag a column header here to group by that column
First Page Previous Page Next Page

	Occurred on	Event type	Session...	User name	Request's IP ad...	Request's port	Request's...
▸	2/20/2021 3:48:22 PM +03:00	Start of sessior	af6feee3db	admin			
	2/20/2021 3:48:15 PM +03:00	Unauthorized r	Session is n	admin			
	2/20/2021 2:01:51 PM +03:00	Start of sessior	ef6a1d9f11	admin			
	2/20/2021 2:00:32 PM +03:00	End of session	15800c7e6c	admin			
	2/20/2021 1:51:55 PM +03:00	Start of sessior	15800c7e6c	admin			
	2/20/2021 12:56:08 PM +03:...	Approval of cli	65590f67de	admin	::1	49454	https://loc...
	2/20/2021 12:55:05 PM +03:...	Start of sessior	65590f67de	admin			
	2/20/2021 12:52:32 PM +03:...	End of session	7e052d346	admin			
	2/20/2021 12:08:59 PM +03:...	The current Ce	7e052d346	admin	::1	49477	https://loc...
	2/20/2021 12:06:57 PM +03:...	Changing setti	7e052d346	admin	::1	49472	https://loc...
	2/20/2021 12:06:42 PM +03:...	Creating new s	7e052d346	admin	::1	49470	https://loc...
	2/20/2021 12:05:07 PM +03:...	New CA certific	7e052d346	admin	::1	49466	https://loc...
	2/20/2021 12:04:58 PM +03:...	New CA certific	7e052d346	admin	::1	49466	https://loc...
	2/20/2021 12:04:27 PM +03:...	Start of sessior	7e052d346	admin			
	2/20/2021 11:58:33 AM +03...	End of session	4a109733cl	admin			

Page 1 (last)

Time elapsed: 00:00:01

Username: admin

Roles: System administrator, Administrators

Change password

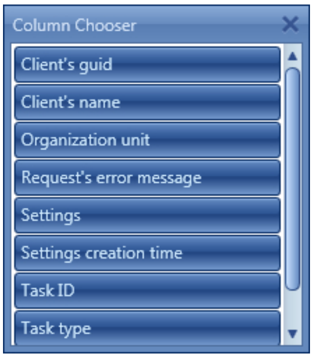
Figure 38. The 'Security events' tab

You can manage the data in the table with filters and database queries. These operations are described in Filtering the events 144 and Database queries 148.

Additional operations on this tab are described below:

Changing the displayed columns

If the required column is not in the table header, to add a new field to the current tab table, click **Choose columns** and drag the required field from the **Column chooser** window (fig. Selecting columns 41) to the required place in the table header.


Column Chooser

- Client's guid
- Client's name
- Organization unit
- Request's error message
- Settings
- Settings creation time
- Task ID
- Task type

Figure 39. Selecting columns

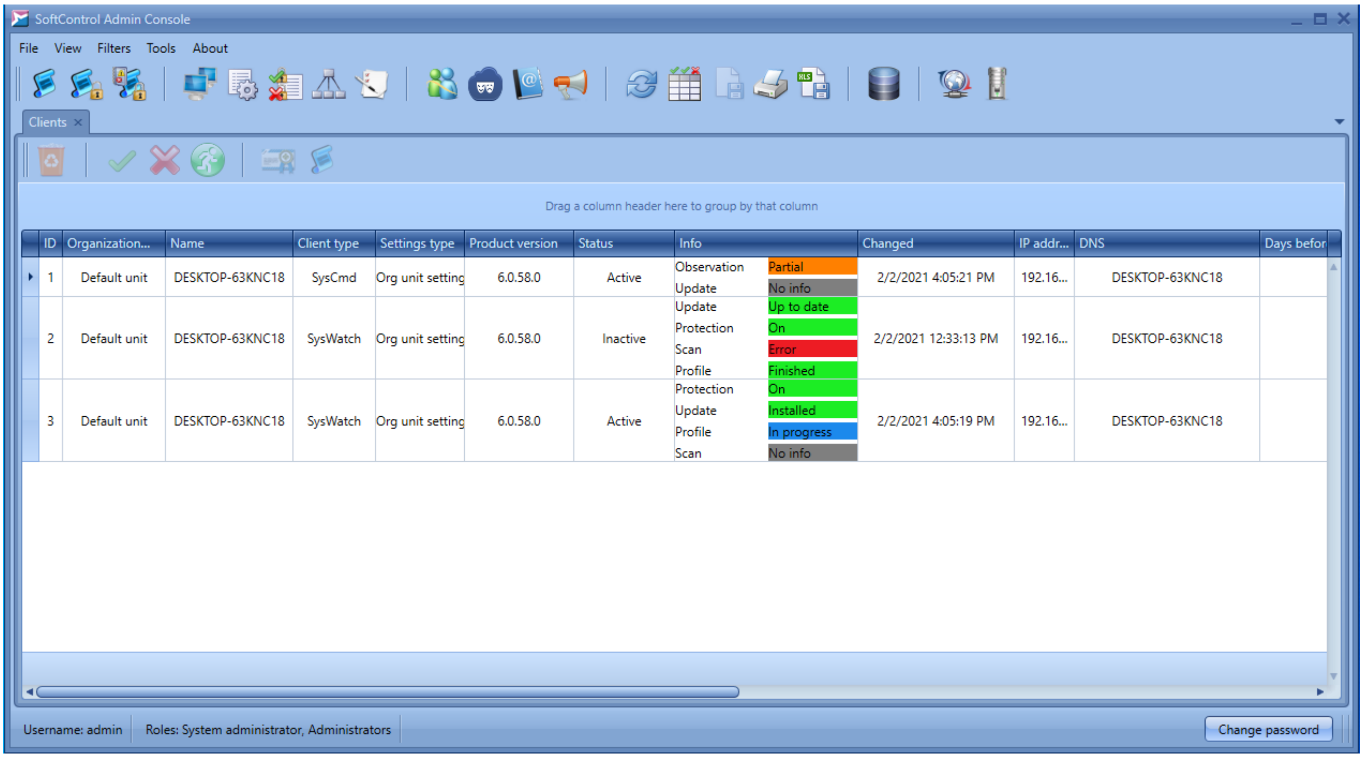
To remove an existing field, drag it to the **Column chooser** window or out of the table header.

Data grouping

For the convenience, information on the tab can be grouped by any field (category) except for **Occurrence time**. To do so, drag the column header to the panel between the table header and group of the tab buttons (fig. Selecting columns 41). If you group by several fields, category priority (nesting) decreases from left to right depending on the location on the panel.

4.4 Clients

The **Clients** tab allows you to register client applications, move them to the organization units, check the status and receive information about the hosts that the client components are installed on (fig. The 'Clients' tab 42).



Drag a column header here to group by that column

ID	Organization...	Name	Client type	Settings type	Product version	Status	Info		Changed	IP addr...	DNS	Days befor
1	Default unit	DESKTOP-63KNC18	SysCmd	Org unit setting	6.0.58.0	Active	Observation Update	Partial No info	2/2/2021 4:05:21 PM	192.16...	DESKTOP-63KNC18	
2	Default unit	DESKTOP-63KNC18	SysWatch	Org unit setting	6.0.58.0	Inactive	Update Protection Scan Profile	Up to date On Error Finished	2/2/2021 12:33:13 PM	192.16...	DESKTOP-63KNC18	
3	Default unit	DESKTOP-63KNC18	SysWatch	Org unit setting	6.0.58.0	Active	Protection Update Profile Scan	On Installed In progress No info	2/2/2021 4:05:19 PM	192.16...	DESKTOP-63KNC18	

Username: admin

Roles: System administrator, Administrators

Figure 40. The 'Clients' tab

Basic operations with the devices are performed with the help of the tab's graphical buttons which are described in table 9.

Table 9. The 'Clients' widgets

Button	Name	Description	Hot keys
✓	Approve	Approve the registration of a client component on the server.	
✗	Reject	Reject the registration of a client component on the server.	
📄	Refresh	Refresh the certificate of a client component's specific certificate.	
🗑	Delete	Delete the selected client component(s) from the database.	Delete
🏃	Move	Move the selected client components to other organization units.	
📜	Event log	Open the **Event Log** tab for the selected components.	

The full list of the tab fields is given in table 10.

Table 10. The 'Clients' tab fields

Field	Description
ID	The serial number of the client host.
Organization unit	The organization unit which the client component belongs to.
Name	The name of a client host.
Client type	Type of the installed client component on the client host: • **SysWatch** – proactive protection component (SoftControl ATM Client / Endpoint Client / SClient); • **DLP** – data acquisition component (SoftControl DLP Client). • **SysCmd** – component of remote command execution and file sharing (SoftControl SysCmd)
Settings type	Client component configuration type: • **Org unit settings** – settings that are common for the organization unit which the client component belongs to; • **Custom settings** – settings that are individual for a client component, regardless of the organization unit; • **Local settings** – settings that have been changed locally for a SysWatch component.
Product version	Version of the installed client component. If the component version is lower than the SoftControl Admin Console version, this cell is highlighted in red. If the component version is higher than the SoftControl Admin Console version, the cell is highlighted in orange.
Status	Possible statuses that display the client component state are described below: • **Pending**: the client component has sent the registration request, and the administrator's decision is pending. • **Approved**: the client component registration request is approved by the administrator. • **Rejected**: the client component registration request is rejected by the administrator. • **Active**: a registered client component has sent a connection request to the server for the period of time that is equal to double heartbeat period 60. • **Inactive**: a registered client component has not sent a connection request to the server for the double heartbeat period 60.
Info	Additional information on a client component state.

Field	Description
	A **SysWatch** component has the following indicators: • **Protection** – proactive protection status. – **On**: protection of all the control scopes is enabled; – **Off**: protection of all control scopes is disabled; – **Partial**: protection of some of the control scopes is enabled. • **Scan** – the status of the last antivirus scanning task. • **Profile** – the status of the last profile gathering (automatic setup) task. – **In progress**: the task is in progress; – **Stopped**: the task is stopped by the user; – **Finished**: the task has completed successfully; – **Error**: an error occurred during the task start or completion. • **Update** – the status of the last component update. – **Installed**: the update is installed successfully; – **Not found**: the component updates are not found; – **Needs reboot**: the client host reboot is required to complete the update. The **No info** status for the **Scan**, **Profile** and **Update** operations means that these actions have not been performed since the client application registration on the server. A **DLP** component has the following indicators: • **Observation** – the monitoring activity status. – **On**: the monitoring of all the data collection scopes is enabled (this does not include the subcategory of removable devices); – **Off**: the monitoring of all the data collection scopes is disabled; – **Partial**: the monitoring of some of the data collection scopes is enabled.
Changed	Time when the latest event has been registered by the client component.
IP address	IP address of the client host.
DNS	Network name of the client host in a workgroup or the domain.
Days before license expiration	The number of days left before the current license key of a client component expires.
Settings state	The status of the client component settings that have been received from the server. This field updates dynamically each time the settings are changed from the SoftControl Admin Console. Possible field states are: • **applied successfully**; • **waiting for response**; • **failed to apply**; • **local settings**; • **no info**.
Certificate expiration date	Expiration date of the client component's specific certificate.
User comments	The field to enter comments for the select client component.
Unique ID	Unique client component's identifier that is assigned automatically after the client component sends the first request to the SoftControl Server.
Permanent connection status	Possible statuses that display whether the **Hold permanent connection to Service Center** option is enabled (see section Common settings 61): • **Active**: permanent connection to SoftControl Service Center is enabled; • **Inactive**: permanent connection to SoftControl Service Center is turned off.
Disable local settings management	The flag that determines how the client host settings are managed. If this option is enabled, you can only change the settings from SoftControl Service Center. You can enable or disable this option in the client component settings (see section

Field	Description
	SoftControl SysWatch settings [63]).
Bases version	Information about the version and release date of the antivirus databases and antivirus engine installed on SoftControl Service Center client.

Basic operations on this tab are:

- managing the registration process [46];
- moving to the organization units [48];
- managing the list of files that can run [48].

Additional operations on this tab are described below:

Working with several components

The tab allows you to work with a single component as well as with several client components. To apply the operations to several components, select them with one of the selection methods and perform the required operations:

- selecting several random components: hold down the **Ctrl** key on the keyboard and select the required components;
- selecting a range of components: select the first component of the range, hold down the **Shift** key on the keyboard and select the last component of the range.

Data grouping

For the convenience, information on the tab can be grouped by specified fields. You can group data by the **Organization unit**, **Client Type**, **Product version**, **Status**, **IP address**, **DNS**, **Days before license expiration**, **Settings state** and **User comments** fields (categories). To do so, drag the column header to the panel between the table header and group of the tab buttons (fig. The 'Clients' tab [42]). If you group by several fields, category priority (nesting) decreases from left to right depending on the location on the panel.

Viewing logs

To open the Event Log [130] tab with the events list, select the required components and perform one of the following operations:

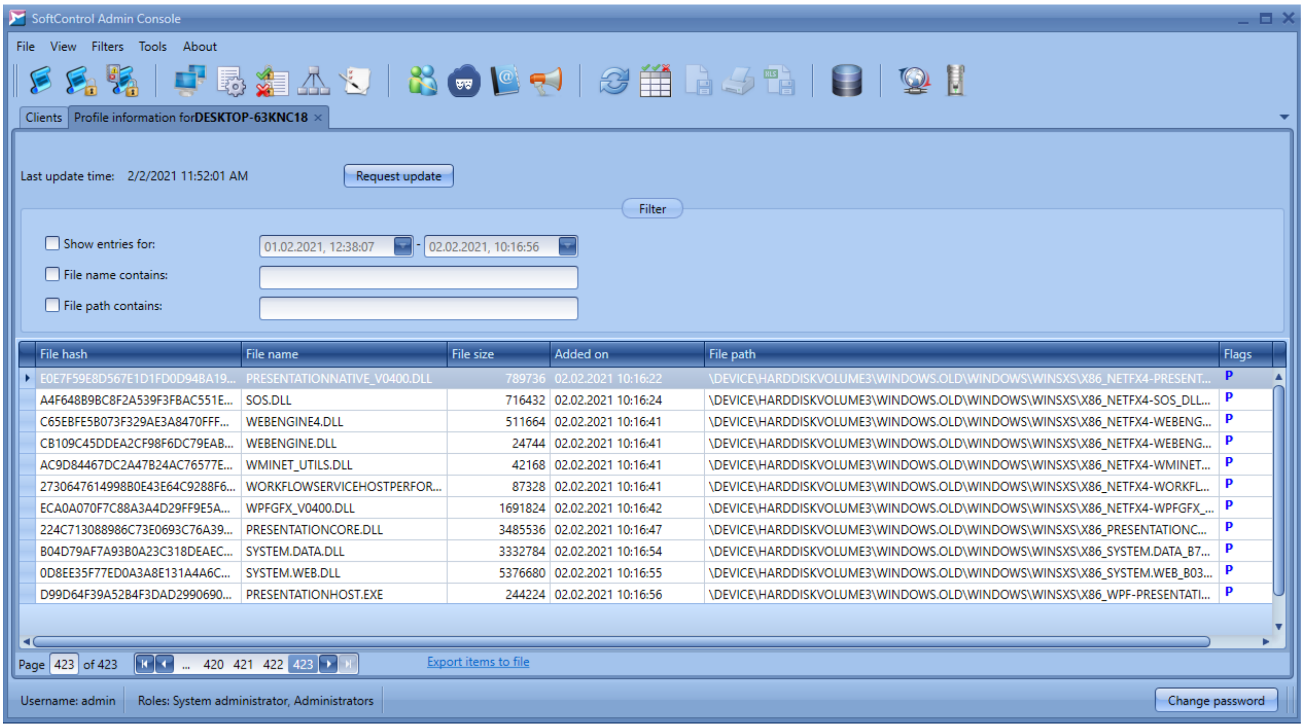
- click **Event log** in the group of buttons on the tab (fig. The 'Clients' tab [42]);
- invoke the context menu by right-clicking on the list of components and select the **Show**

Log command.

When you open the list of events, the header of the Log(130) tab displays the number of the selected components (fig. The 'Clients' tab(42)).

Viewing extended profile

Select a profile and invoke the context menu by clicking the right mouse button. Select the **Show extended profile info** command. The **Profile information** tab will open. You will see the list of checksums included in the selected profile. You can filter the displayed items. At the bottom of the window you will find the **Export items to file** hyperlink. Click on it to create an XML file with items on the screen. You can also remove items or copy checksums by right-clicking on an entry.



Last update time: 2/2/2021 11:52:01 AM

☐ Show entries for: 01.02.2021, 12:38:07 - 02.02.2021, 10:16:56

☐ File name contains:

☐ File path contains:

File hash	File name	File size	Added on	File path	Flags
E0E7F59E8D567E1D1FD0D94BA19...	PRESENTATIONNATIVE_V0400.DLL	789736	02.02.2021 10:16:22	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-PRESENT...	P
A4F648B9BC8F2A539F3FBAC551E...	SOS.DLL	716432	02.02.2021 10:16:24	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-SOS_DLL...	P
C65EBFE5B073F329AE3A8470FFF...	WEBENGINE4.DLL	511664	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WEBENG...	P
CB109C45DDEA2CF98F6DC79EAB...	WEBENGINE.DLL	24744	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WEBENG...	P
AC9D84467DC2A47B24AC76577E...	WMINET_UTILS.DLL	42168	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WMINET...	P
273064761499880E43E64C9288F6...	WORKFLOWSERVICEHOSTPERFOR...	87328	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WORKFL...	P
ECA0A070F7C88A3A4D29FF9E5A...	WPFGFX_V0400.DLL	1691824	02.02.2021 10:16:42	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WPFGFX_...	P
224C713088986C73E0693C76A39...	PRESENTATIONCORE.DLL	3485536	02.02.2021 10:16:47	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_PRESENTATIONC...	P
B04D79AF7A93B0A23C318DEAEC...	SYSTEM.DATA.DLL	3332784	02.02.2021 10:16:54	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_SYSTEM.DATA_B7...	P
0D8EE35F77ED0A3A8E131A4A6C...	SYSTEM.WEB.DLL	5376680	02.02.2021 10:16:55	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_SYSTEM.WEB_B03...	P
D99D64F39A52B4F3DAD2990690...	PRESENTATIONHOST.EXE	244224	02.02.2021 10:16:56	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_WPF-PRESENTATI...	P

Page 423 of 423 ... 420 421 422 423

Username: admin | Roles: System administrator, Administrators

Figure 41. 'Profile information' tab

4.4.1 Managing the registration process

Managing the registration process includes the following operations.

Approving the registration

Select the required client components that are in the **Pending** state and click **Approve** (fig. The 'Clients' tab(42)).

The **Status** field switches to the **Approved** state as soon as the registration is approved.

When the client component request is received next time, the component's certificate[205] is checked. If the certificate is common then the SoftControl Server component issues a specific (unique) certificate to authorize on the server. When the client component (with the specific certificate) sends a request next time, its status changes to **Active**. The client component is placed into operation since this moment: a secure encrypted communication channel is established between the server and the client.

Rejecting the registration

Select the required client components that are in the **Pending** state and click **Reject** (fig. The 'Clients' tab[42]).

Once the registration of selected clients are rejected, the **Status** field switches to the **Rejected** state. Interaction of the rejected clients with the server stops.

Once registration is rejected, you can only retry registration in the following way:

1) Remove the client components from the database with the help of the **Delete** button.

2) Retry registration on the server with the common certificate[205].

Updating client's certificate

Select the required client components that are in the **Active** or the **Inactive** state and click **Refresh** (fig. The 'Clients' tab[42]).

The **Certificate expiration date** field updates when the client component with the new specific certificate[205] sends a request next time. The client component cannot use the previous certificate anymore because the certificate is added to the black list of the certificates.

Removing the client component from the database

Select the required client components and click **Delete** (fig. The 'Clients' tab[42]). The specific certificate[205] is not withdrawn in this case, and after the heartbeat period the deleted components are displayed in SoftControl Admin Console again with the **Pending** status. To take the client components out of service completely, perform the following operations:

1) Place the specific certificate[205] of a client component to the black list with the help of the **Reject** button.

2) Remove the client components from the database with the help of the **Delete** button.

4.4.2 Moving to the organization units

To move the selected client components to another organization unit, click **Move** and select the required unit from the drop-down list in the displayed window (fig. Selecting an organization unit to move the component to[48]).

When moving client components to another organization unit, their settings automatically change to the configuration of the selected organization unit.

If you have the permission to move clients within a contiguous group, but not the permission to move clients to any organization units, and you try to move a client between two organization units that are not in one contiguous group, your request will be denied.

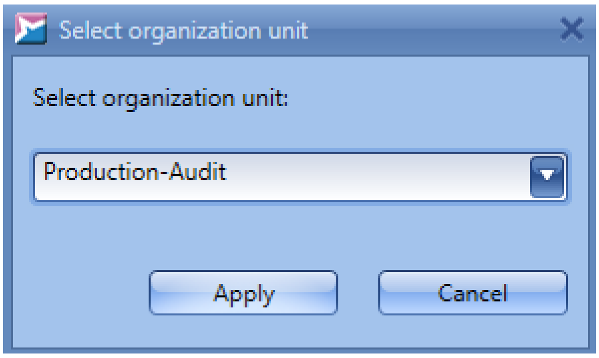
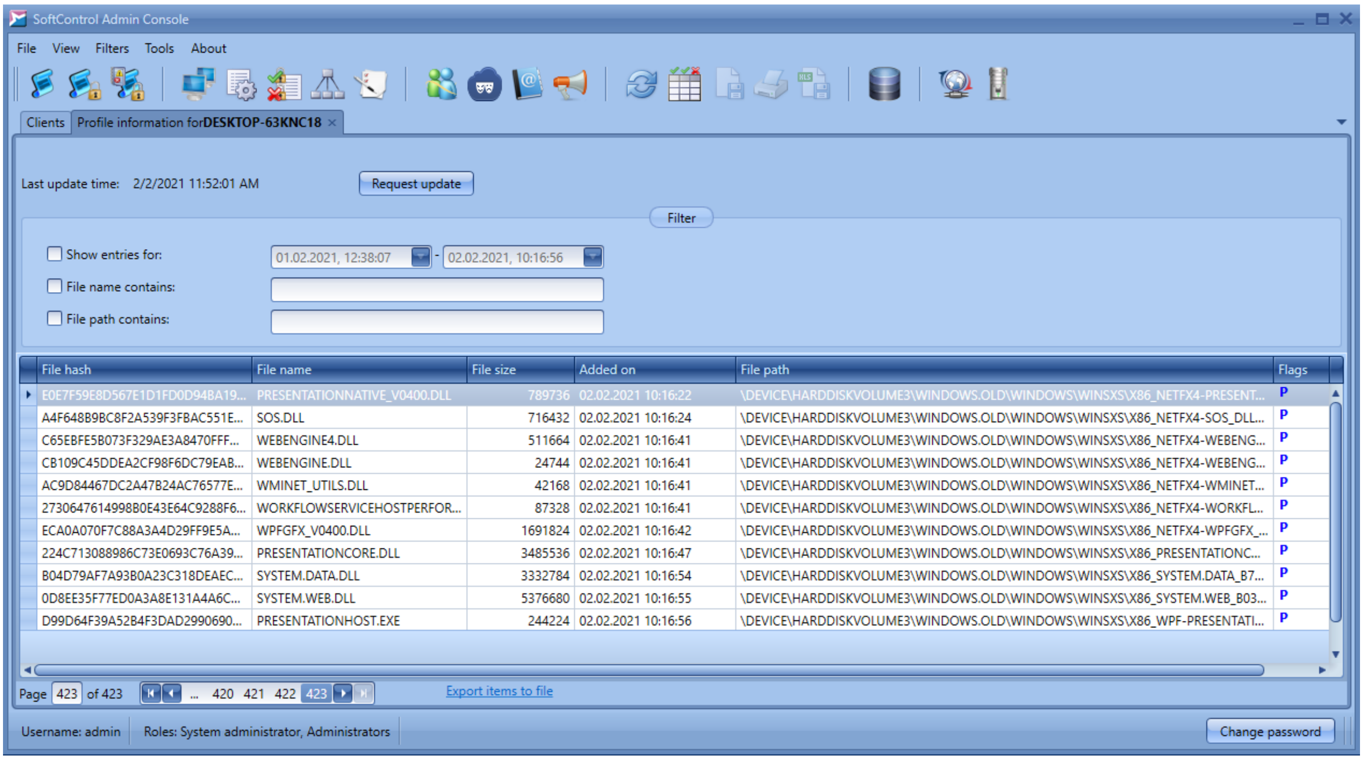


Figure 42. Selecting an organization unit to move the component to

4.4.3 Managing the list of allowed files

In SoftControl Admin Console, you can obtain the list of files that can run on a client host with installed SoftControl SysWatch, and revoke the permissions for the selected files.

To obtain the list of files, right-click the required SoftControl SysWatch application and select **Show extended profile info** in the context menu. This opens the **Profile information for <client_name>** tab (fig. The 'Profile information for...' tab[49]). To start collecting data about the profile, click **Request update**. SoftControl Admin Console displays the remaining time (approximately) while it collects the information. The list of files contains additional information such as the name of the file when it was added to the list, the check sum of the file, the full path, the date when the file was added, the size of the file, as well as the flag that indicates whether the file was added to the profile by the installer (**I**), during profile gathering (**P**) or by user through the settings (**U**).


SoftControl Admin Console
File View Filters Tools About
Clients
Profile information forDESKTOP-63KNC18
Request update
Filter
Export items to file
Change password

Last update time: 2/2/2021 11:52:01 AM

☐ Show entries for: 01.02.2021, 12:38:07 - 02.02.2021, 10:16:56

☐ File name contains:

☐ File path contains:

File hash	File name	File size	Added on	File path	Flags
E0E7F59E8D567E1D1FD0D94BA19...	PRESENTATIONNATIVE_V0400.DLL	789736	02.02.2021 10:16:22	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-PRESENT...	P
A4F648B9BC8F2A539F3FBAC551E...	SOS.DLL	716432	02.02.2021 10:16:24	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-SOS_DLL...	P
C65EBFE5B073F329AE3A8470FFF...	WEBENGINE4.DLL	511664	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WEBENG...	P
CB109C45DDEA2CF98F6DC79EAB...	WEBENGINE.DLL	24744	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WEBENG...	P
AC9D84467DC2A47B24AC76577E...	WMINET_UTILS.DLL	42168	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WMINET...	P
2730647614998B0E43E64C9288F6...	WORKFLOWSERVICEHOSTPERFOR...	87328	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WORKFL...	P
ECA0A070F7C88A3A4D29FF9E5A...	WPFGFX_V0400.DLL	1691824	02.02.2021 10:16:42	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_NETFX4-WPFGFX_...	P
224C713088986C73E0693C76A39...	PRESENTATIONCORE.DLL	3485536	02.02.2021 10:16:47	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_PRESENTATIONC...	P
B04D79AF7A93B0A23C318DEAEC...	SYSTEM.DATA.DLL	3332784	02.02.2021 10:16:54	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_SYSTEM.DATA_B7...	P
0D8EE35F77ED0A3A8E131A4A6C...	SYSTEM.WEB.DLL	5376680	02.02.2021 10:16:55	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_SYSTEM.WEB_B03...	P
D99D64F39A52B4F3DAD2990690...	PRESENTATIONHOST.EXE	244224	02.02.2021 10:16:56	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86_WPF-PRESENTATI...	P

Page 423 of 423 ... 420 421 422 423

Username: admin

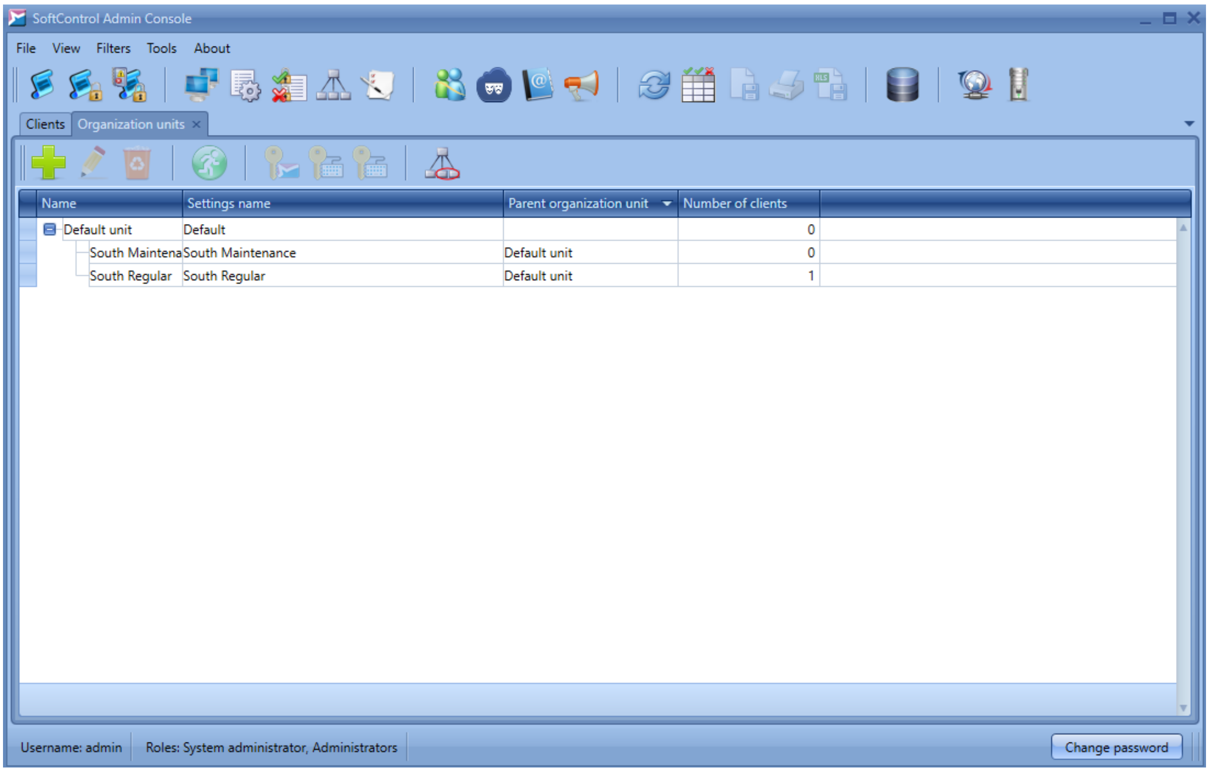
Roles: System administrator, Administrators

Figure43. The 'Profile information for...' tab

To view the list of files for a specified period, select the required dates in the **Filter** field. In the filter, you can specify a part of the file name and a part of the path to the file. To revoke permissions for certain files, select the files using **Shift** or **Ctrl** and click **Remove selected** in the context menu.

4.5 Organization units

The **Organization units** tab allows you to group client components by territorial, administrative or other attributes (fig. The 'Organization units' tab 49). Besides, you can bind organization units to the configurations and generate one-time passwords on this tab.



Name	Settings name	Parent organization unit	Number of clients
Default unit	Default		0
South Maintena	South Maintenance	Default unit	0
South Regular	South Regular	Default unit	1

Username: admin | Roles: System administrator, Administrators | Change password

Figure 44. The 'Organization units' tab

There is always at least one organization unit in the program, the **Default unit**, and you cannot delete it. All the new client components are moved to this organization unit automatically. The administrator can then create the required hierarchical structure of organization units (with any level of nesting), with the help of the **Move** button. When a unit is created, it is assigned a set of client settings.

Basic operations with the organization units are performed via the tab's graphical buttons which are described in table 11.

Table 11. The 'Organization units' tab widgets

Button	Name	Description
✚	New	Create a new organization unit.
✎	Edit	Modify the properties of the selected organization unit.
🗑	Delete	Remove the selected organization unit(s).
🏃	Move	Move the selected organization unit to another unit. You cannot move the **Default unit**. You cannot move a parent organization unit to a subsidiary unit.
🔑	One-time password for SysWatch	Open the one-time password generator window.
🔑	One-time password for keyboard (before 6.0)	Open the window to generate passwords that unlock the keyboard on a client host with version under 6.0.
🔑	One-time password for keyboard (after 6.0)	Open the window to generate passwords that unlock the keyboard on a client host with version 6.0 and later.

Button	Name	Description
	Contiguous groups	Manage groups for contiguous organization units.

List of the tab fields is given in table 12.

Table 12. The 'Organization units' tab fields

Field	Description
Name	Organization unit name.
Parent organization unit	The name of the parent organization unit.
Settings name	Client component configuration that applies to the organization unit.

Basic operations on this tab are:

- managing the organization units [51];
- generating one-time passwords [53];
- managing contiguous groups [54].

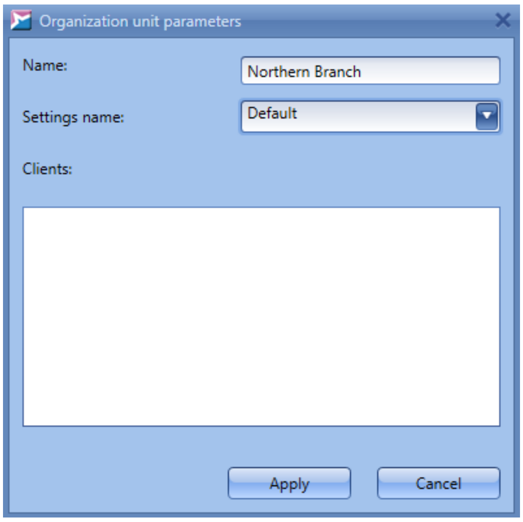
4.5.1 Managing the organization units

Managing the organization units includes the following operations.

Creating an organization unit

To add a new organization unit, click **New** (fig. The 'Organization units' tab [49]).

Specify the **Name** of the organization unit in the displayed window and select **Settings name** in the drop-down list; then click **Apply** (fig. Creating an organization unit [51]).



Name: Northern Branch

Settings name: Default

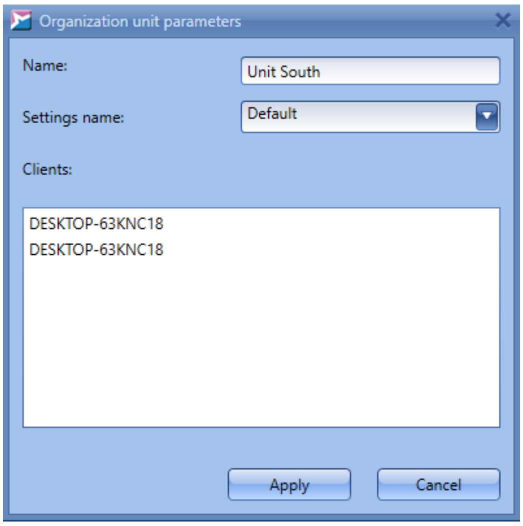
Clients:

Figure 45. Creating an organization unit

Modifying an organization unit properties

To modify an organization unit properties, click **Edit** (fig. The 'Organization units' tab 49).

Modify the **Name** of the organization unit and/or select another **Settings name** in the drop-down list; then click **Apply** (fig. Organization unit properties 51). If the organization unit contains components, they are displayed in the **Clients** list.



Organization unit parameters

Name: Unit South

Settings name: Default

Clients:

DESKTOP-63KNC18
DESKTOP-63KNC18

Figure 46. Organization unit properties

Removing an organization unit

To remove an organization unit, select it, press **Delete** (fig. The 'Organization units' tab 49) and confirm the removal in the dialog box. All the components from this organization unit are moved to its parent unit.

You cannot remove the **Default** organization unit.

Moving an organization unit

To move an organization unit, select it and click **Move**. In the displayed window, select the organization unit you want to move the current unit to (fig. Moving an organization unit 52).

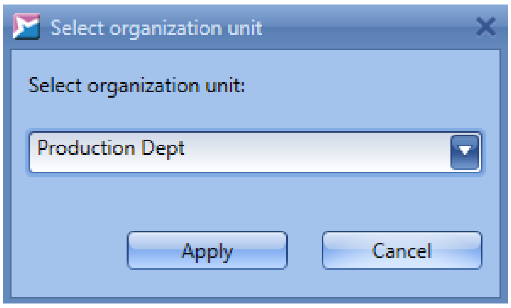


Figure 47. Moving an organization unit

You cannot move the **Default** organization unit. You cannot move a parent organization unit to a subsidiary unit.

4.5.2 Generating one-time passwords

SoftControl Service Center features the secure authentication subsystem based on the one-time password algorithm (TOTP). This algorithm has the high cryptographic strength and allows you to generate passwords that are valid only for a certain period of time. One-time passwords can be used to access the SoftControl SysWatch GUI/uninstaller when necessary (for example, if you need to give a one-time access to SoftControl SysWatch without disclosing the main password), as well as to unlock the keyboard on the client hosts (to unlock the keyboard, enter the password and then press the Enter key).

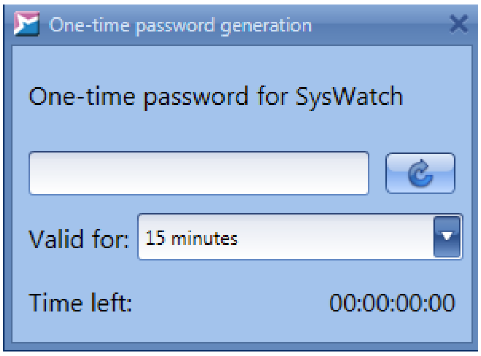
You should enable and set up the corresponding option (77) in the organization unit configuration to start working with the one-time password generator.

Note that one-time passwords for keyboard are generated depending on the version of SoftControl SysWatch installed on a client device (prior to 6.0 or 6.0 and later).

One-time password generation is performed within an organization unit: the generated password applies to all the SoftControl SysWatch applications in the organization unit. To open the generator window, select the organization unit and click (**One-time password for SysWatch**) or (**One-time password for keyboard** – one of the buttons depending on on the version of SoftControl SysWatch) (fig. The 'Organization units' tab (49)). In the displayed window, select **Time interval** for the password and click (**Generate password**). The **One-time password for SysWatch** (**One-time password for keyboard**) field contains the generated password. The **Time left** counter displays the password's lifetime in the *dd:hh:mm:ss* format (fig. The generator window (54)). After the lifetime expires, click again to generate a new password.

I) One-time passwords for SysWatch are designed for combined use with the main password. To access SoftControl SysWatch on a client host through the one-time passwords, main password protection[69] should be enabled. When SoftControl SysWatch GUI requests a password, tick off **Use TOTP password**.

II) As TOTP algorithm uses time as a parameter, you should synchronize the UTC time (i.e. regardless of time zone) on the computer with the installed SoftControl Admin Console and the host with the installed SoftControl SysWatch, so that the error is much less than the password lifetime.

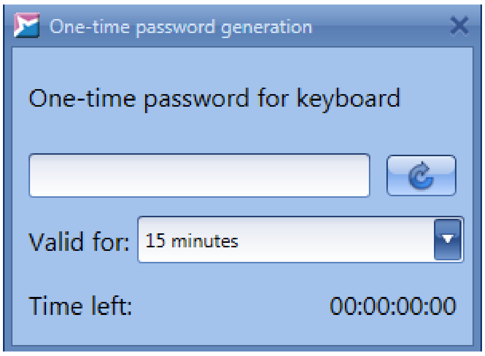

One-time password generation

One-time password for SysWatch

Valid for: 15 minutes

Time left: 00:00:00:00

Figure 48. The generator window for SysWatch


One-time password generation

One-time password for keyboard

Valid for: 15 minutes

Time left: 00:00:00:00

Figure 49. The generator window for keyboard

4.5.3 Contiguous groups

You can put organization units together in contiguous groups. This allows to do the following: a specific user can have the permission to move organization units within its group but not have the permission to move organization units between groups. It can be useful for performing maintenance procedures. For example, an operator can move the device that requires maintenance to a special unit with settings that allow performing of the required maintenance procedures. Once the maintenance works are done, the operator can then move the device back to its original organization unit. Besides moving clients within their contiguous groups, the operator does not have any other permissions.

Creating roles and assigning permissions is described in section Roles [33].

An organization unit can belong to only one contiguous group (or no contiguous groups at all).

To create contiguous groups and move organization units into them, click **Contiguous groups**.

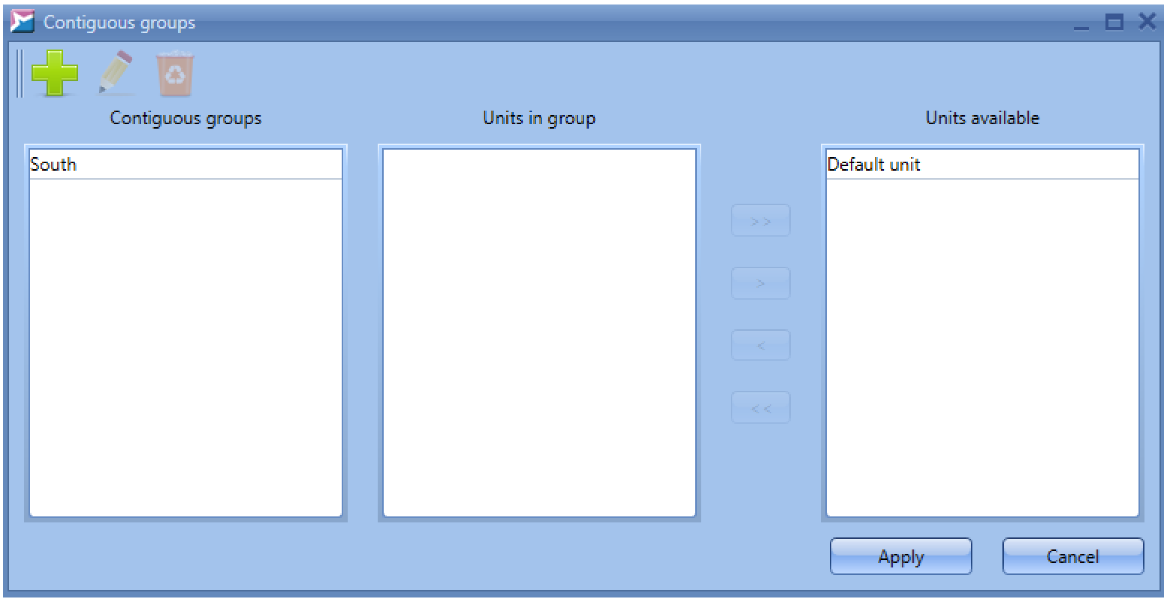


Figure 50. Contiguous groups

Existing contiguous groups are listed in the **Contiguous groups** area. To create a new group, click ➕. Enter the new group name and click **OK**.

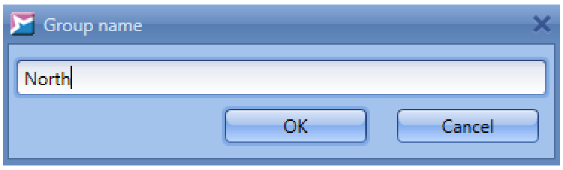


Figure 51. New contiguous group

To work with a group, select it in the list. The **Units in group** area will show names of the organization units that are in this group. The **Units available** area will show organization units that can be included in the group. Move organization units between these lists by using respective arrow buttons.

You can also rename and delete existing contiguous groups (without affecting organization units inside the groups).

Table 13. The "Contiguous groups" windows widgets

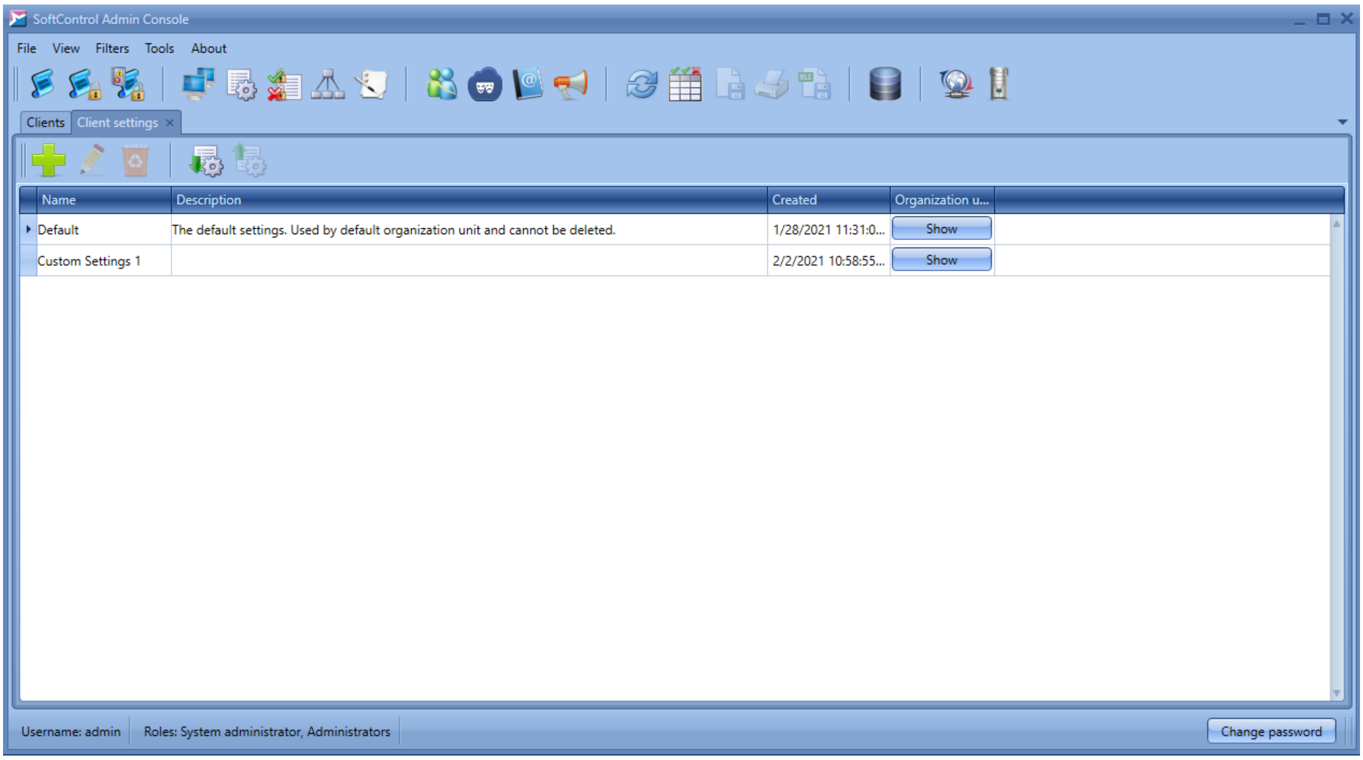
Button	Name	Description
➕	New group	Add new group
✏	Rename group	Rename selected group
♻	Delete group	Delete selected group

4.6 Setting up client components

The **Client settings** tab contains the list of the client application configurations (settings) (fig. The 'Client settings' tab 56).

SoftControl Admin Console has the following types of configurations:

- organization unit settings;
- custom settings;
- local settings (only for SoftControl SysWatch).



Name	Description	Created	Organization u...
Default	The default settings. Used by default organization unit and cannot be deleted.	1/28/2021 11:31:0...	Show
Custom Settings 1		2/2/2021 10:58:55...	Show

Username: admin | Roles: System administrator, Administrators

Figure 52. The 'Client settings' tab

By default, all client components receive the organization unit settings after registration on the server. Custom settings are intended for cases when you need to set a configuration that differs from the organization unit configuration, for a certain client component. The tab contains the list of all configurations including custom configurations. Information about how to work with custom settings is given below[58].

Basic operations with the configurations are performed via the tab's graphical buttons that are described in table 14.

Table 14. The 'Client settings' tab widgets

Button	Name	Description
➕	New	Create a new client component configuration.
✏	Edit	Modify the selected configuration.
🗑	Delete	Remove the selected configuration(s).
⬇	Import	Import a configuration from an XML file.
⬆	Export	Export the select configuration to an XML file.

The list of the tab fields is given in table 15.

Table 15. The 'Client settings' tab fields

Field	Description
Name	Client component configuration name.
Description	Client component configuration description.
Created	Date and time when the configuration was created.
Organization units	The list of the organization units which the configuration applies to.

SoftControl Admin Console has the following categories of the centrally managed settings of client components:

- common settings[59];
- SoftControl SysWatch settings[63];
- SoftControl DLP Client settings[104].
- SoftControl SysCmd settings[112].

Basic operations on this tab are:

Creating a configuration

To add a new configuration, click **New** (fig. The 'Client settings' tab [56]). Specify the configuration parameters in the **Client settings editor** window (see figures from The 'Name' section [60] to Update schedule settings [111]). If the **All parameters are correct** status is displayed in the lower part of the window, click **Apply** to add the created configuration; otherwise, modify invalid parameters.

Creating the configuration based on the current one

To add a new configuration that is based on the current one, select it and perform one of the following operations:

- click **Edit** in the tab's button group (fig. The 'Client settings' tab [56]);
- double-click the configuration.

In the the **Client settings editor** window, modify the configuration name (mandatory) and parameters (if necessary) as you do with a new configuration (see figures from The 'Name' section [60] to Update schedule settings [111]). If the **All parameters are valid** status is displayed in the lower part of the window, click **Apply** to add the created configuration; otherwise, modify invalid parameters.

Changing settings type

To change the type of the client component settings, go to the Clients [42] tab, invoke the context menu by right-clicking the required component and select one of the commands:

- **Use orgunit settings**:

  assign the settings of the organization unit that client component belongs to.
- **Use custom settings**:

  assign custom settings to the client component.
- **Resubmit client's settings**:

  assign the latest configuration from SoftControl Server to a SoftControl SysWatch client component with the locally changed settings.

Using custom configurations

To add a new custom configuration and assign it to a client component, go to the Clients [42] tab, invoke the context menu by right-clicking the required component and select **Use custom settings**. Click **Add** in the **Select custom settings** window to create a new custom configuration (fig. Managing custom settings 59).

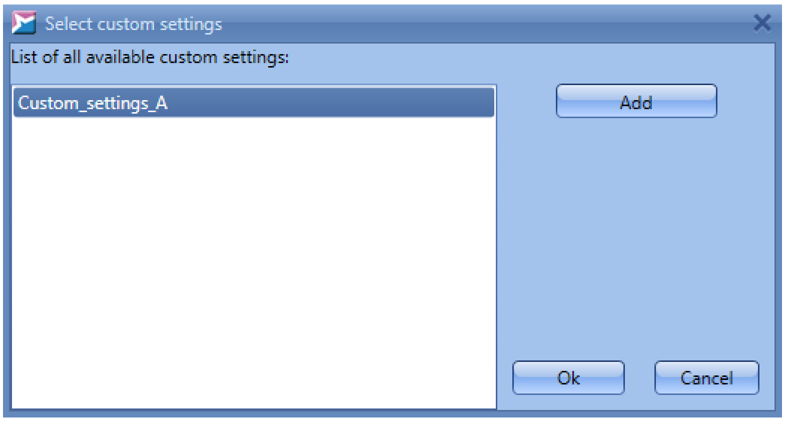


Figure 53. Managing custom settings

Specify the configuration parameters in the **Client settings editor** window (see figures from The 'Name' section 60 to Update schedule settings 111). If the **All parameters are valid** status is displayed in the lower part of the window, click **Apply** to add the created configuration; otherwise, modify invalid parameters. The created configuration is added to the custom configuration list. Select it from the list (or select a configuration that was created earlier) and click **OK** to apply the configuration to the client component.

Removing a configuration

To remove a configuration, select it, press **Delete** (fig. The 'Client settings' tab 56) and confirm the removal in the dialog box.

4.6.1 Common settings

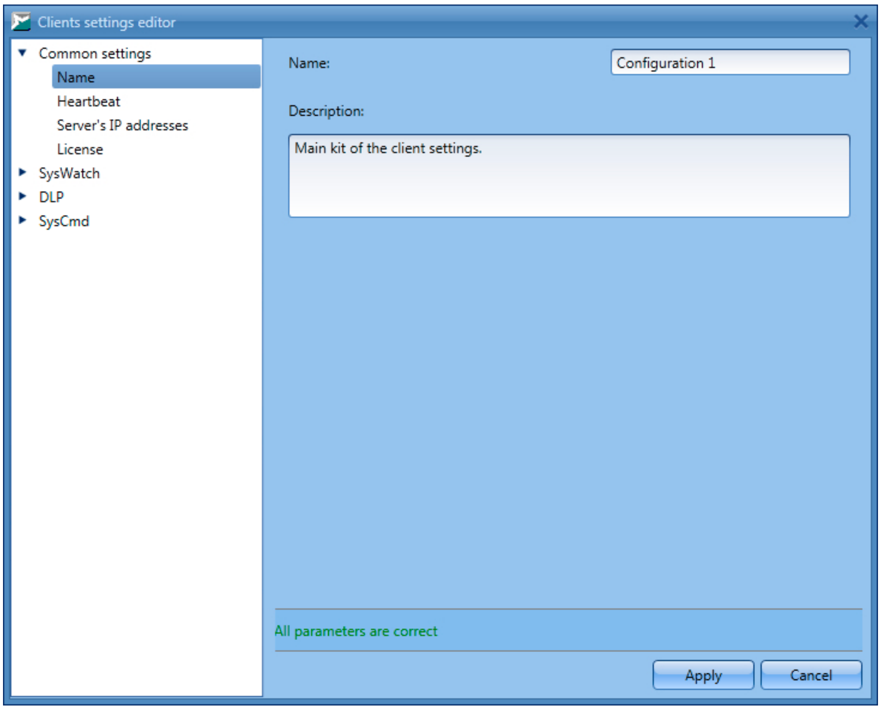
This category of settings includes common configuration parameters and the settings of interaction between the client applications and the server.

Name

The name of the client component configuration is required to identify a certain settings kit, while the configuration description provides brief information about the settings kit.

To specify the **Name** and the **Description**, enter them to the corresponding fields in the **Name** section of the **Common settings** category (fig. The 'Name' section 60).

The configuration name should be unique and should not coincide with the existing names.



Name: Configuration 1

Description: Main kit of the client settings.

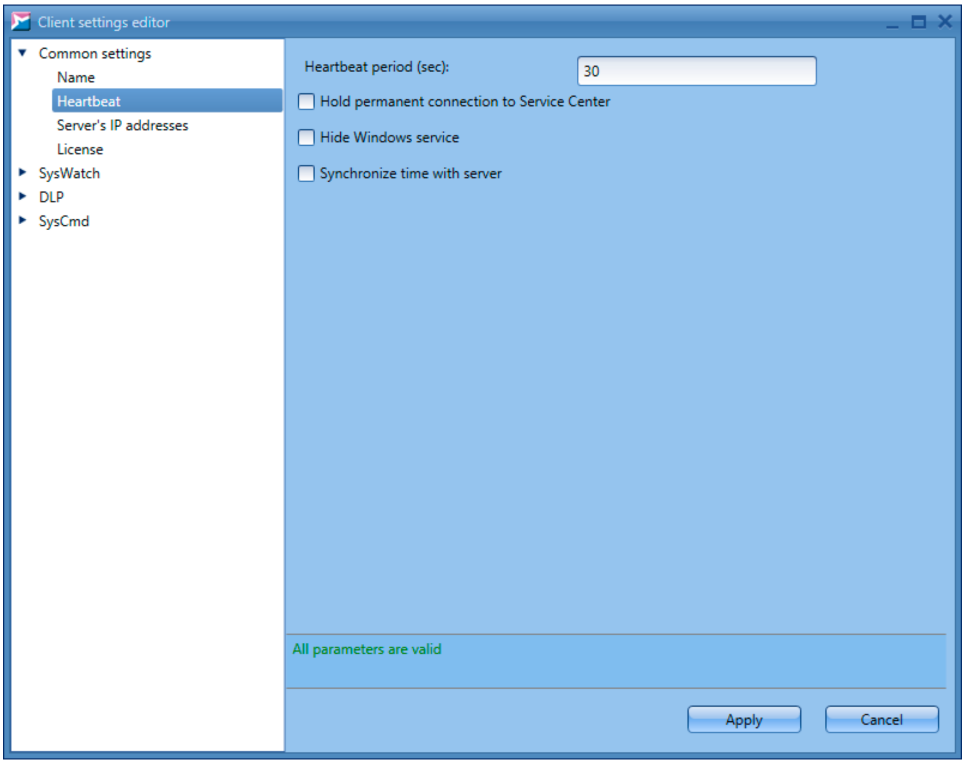
All parameters are correct

Figure 54. The 'Name' section

Heartbeat

Heartbeat is the client component parameter that specifies the period when a client component connects to the SoftControl Server component. The default value is 60 seconds (1 minute).

To modify the parameter, switch to the **Heartbeat** section of the **Common settings** category and enter the value (in seconds) in the **Heartbeat period (sec)** field (fig. The 'Heartbeat' section 61).



Heartbeat period (sec): 30

□ Hold permanent connection to Service Center

□ Hide Windows service

□ Synchronize time with server

All parameters are valid

Figure 55. The 'Heartbeat' section

Tick off **Hold permanent connection to Service Center** if you need to maintain connection to SoftControl Service Center in real time.

Besides, you need to tick off **Hold permanent connection to Service Center** if you need to enable video recording on request for SoftControl DLP Client. For video recording settings, see section SoftControl DLP Client settings 110.

Tick off **Hide Windows service** if the SoftControl SysWatch, SoftControl DLP Client and SoftControl SysCmd system services (*safensec.exe, eventsvc.exe and SysCmd.exe* respectively) should be hidden from the Windows **Services** snap-in.

Note: hiding system services does not work on Windows XP.

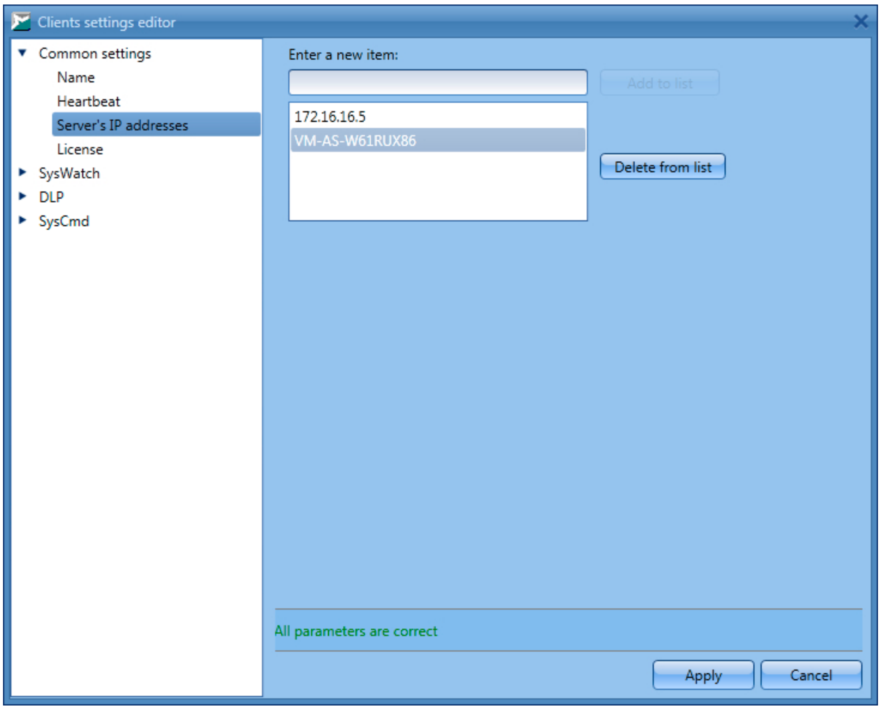
Note: if system services are hidden, you cannot manage them with any OS tools.

Tick off **Synchronize time with server** to allow SoftControl SysWatch to synchronize the time on the client computer with the time of SoftControl Server.

Specifying the server IP addresses

You can specify the server addresses that the client components can access, in the server configuration wizard 23.

To change the list of the addresses, switch to the **Server's IP addresses** section of the **Common settings** category and modify the list (fig. The 'Server's IP addresses' section 61).



172.16.16.5
VM-AS-W61RUX86

All parameters are correct

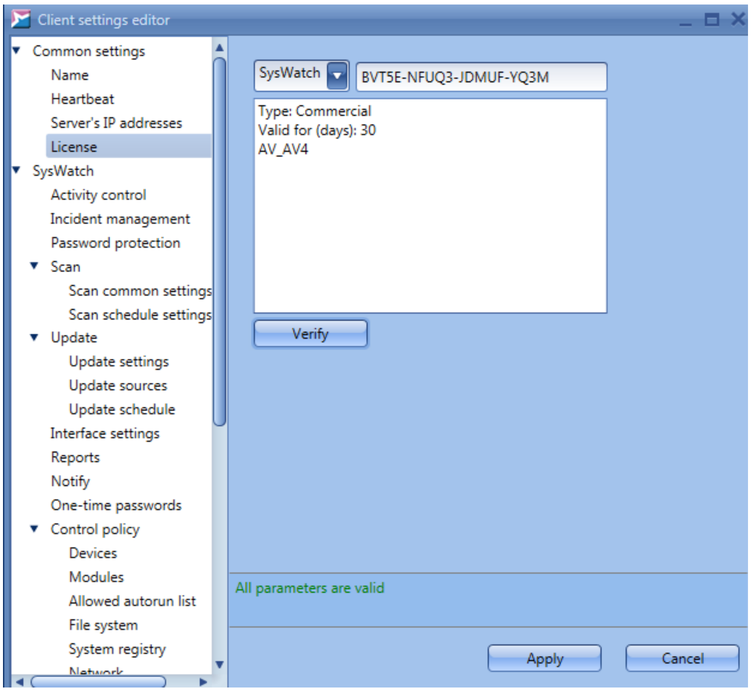
Figure 56. The 'Server's IP addresses' section

To add an address to the list, enter a new value of an IP address or a name to the corresponding field and click **Add to list**. To remove an address from the list, select it and click **Delete from list**.

License

The license key determines the functionality of the client components. The trial license is installed by default; it is valid for 30 days.

To specify the key, switch to the **License** section of the **Common settings** category, select the type of the client component in the drop-down list (**SysWatch**, **DLP**, **DeCrypt, SysCmd**), enter the key to the text field and click **Verify** to validate the license and display its parameters if the key is valid (fig. The 'License' section 62).



SysWatch BVT5E-NFUQ3-JDMUF-YQ3M

Type: Commercial
Valid for (days): 30
AV_AV4

All parameters are valid

Figure 57. The 'License' section

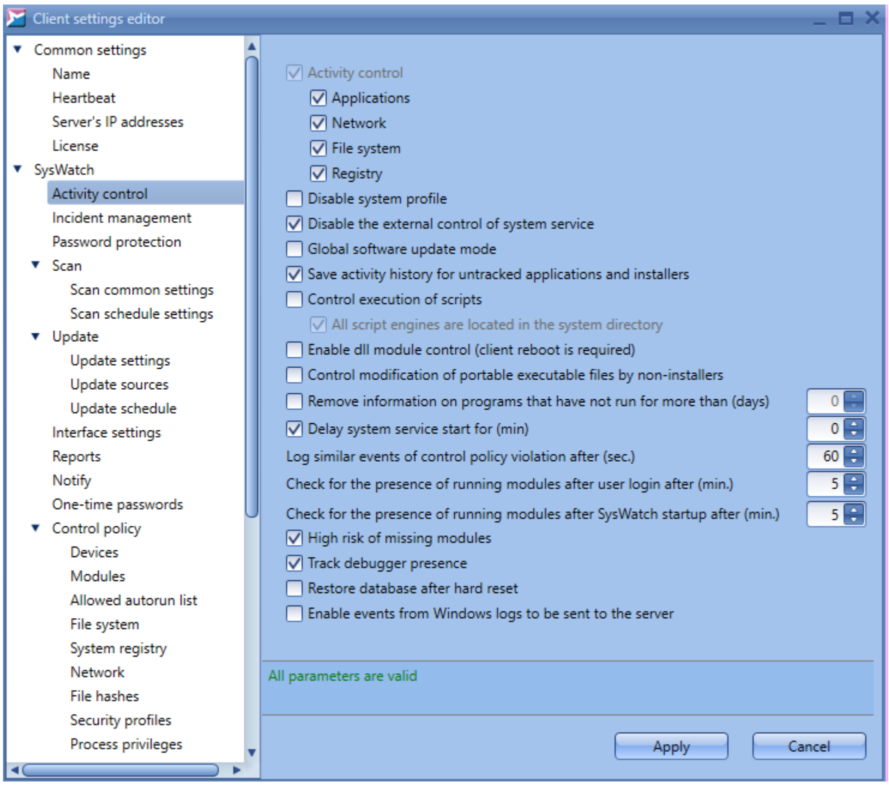
4.6.2 SoftControl SysWatch settings

This category of settings includes the SoftControl SysWatch component configuration that is similar to the configuration specified with the help of SoftControl SysWatch GUI, and the control policies.

Activity control

Tick off the checkboxes at the required control scopes in the **Activity control** section of the **SysWatch** category (fig. Activity control settings 63):

- □ **Activity control**:
  - □ **Applications**;
  - □ **Network**;
  - □ **File system**;
  - □ **Registry**.



☑ Activity control

☑ Applications

☑ Network

☑ File system

☑ Registry

□ Disable system profile

☑ Disable the external control of system service

□ Global software update mode

☑ Save activity history for untracked applications and installers

□ Control execution of scripts

☑ All script engines are located in the system directory

□ Enable dll module control (client reboot is required)

□ Control modification of portable executable files by non-installers

□ Remove information on programs that have not run for more than (days) 0

☑ Delay system service start for (min) 0

Log similar events of control policy violation after (sec.) 60

Check for the presence of running modules after user login after (min.) 5

Check for the presence of running modules after SysWatch startup after (min.) 5

☑ High risk of missing modules

☑ Track debugger presence

□ Restore database after hard reset

□ Enable events from Windows logs to be sent to the server

All parameters are valid

Figure 58. Activity control settings

Select the required additional options of the activity control below:

- ❑ **Disable system profile**:

  Turn off the monitoring of PE files on the client host.

- ❑ **Disable the external control of system service**:

  Do not allow unloading the SoftControl SysWatch system service from a client host RAM.

- ❑ **Global software update mode**:

  Execute all applications in installation mode.

  When this mode is active, all applications run as installers and are added to the profile (education mode). All modifications of the PE files are added to the profile as well. We recommend that you only use this mode on 'clean' systems, where all software has been installed from a master image. To enable or disable the mode, you need to restart the client host.

- ❑ **Save activity history for untracked applications and installers**:

  Automatically enable the activity history saving option when an application that is not in the profile or an unsigned installer runs for the first time.

- ❑ **Control execution of scripts**:

  Do not allow the interpreters to run untrusted scripts (except for the scripts that are signed with a digital signature from the whitelist of certificates). The following processes are blocked:

– wscript.exe (Microsoft ® Windows Based Script Host);

– cscript.exe (Microsoft ® Console Based Script Host);

– java.exe (Java™ Platform SE binary);

– javaw.exe (Java™ Platform SE binary);

– javaws.exe (Java™ Web Start Launcher).

In order to block specific processes, we recommend that you create the appropriate Control policy rules[85].

Note. If you select **Allow** for **Running script engine** in the **Incident management** section, the script execution will be allowed. The event will be logged.

❑ **All script engines are located in the system directory**:

Only processes started from a system directory (`C:\Windows\System32` or `C:\Windows\SysWOW64`) are blocked.

This option becomes active if **Control execution of scripts** is checked.

❑ **Enable dll module control (client reboot is required)**:

DLL module control works as follows. When an exe file tries to load a dll library, SoftControl SysWatch checks whether the library has a digital signature. If the library is signed and the digital signature certificate is considered trusted by Windows, SoftControl SysWatch allows the library to load, even if the library is not in the profile. If the library has no digital signature, SoftControl SysWatch checks whether it is in the profile. If the library is in the profile, SoftControl SysWatch allows it to load; otherwise, SoftControl SysWatch blocks it.

Note 1. Libraries that do not have an entry point (resource-only libraries without executable code) cannot be blocked.

Note 2. If you select **Allow** for **Loading untrusted DLL** in the **Incident management** section, the loading will not be blocked. The event will be logged.

❑ **Control modification of portable executable files by non-installers**:

Block modification of the executable files (exe, dll, etc.) by all applications except for the applications that work in the software update mode.

Note. If you select **Allow** for **Modification of PE file by non-installer** in the **Incident management** section, the file modification will not be blocked. The event will be logged.

❑ **Remove information on programs that have not run for more than (days)**:

Delete entries about inactive applications that meet the specified condition (the number of days without activity), from the SoftControl SysWatch database.

❑ **Delay system service start for (min)**:

Specify the delay of the SoftControl SysWatch system service start.

❑ **Log similar event of control policy violation after (sec.)**:

Specify the period of time after which SoftControl SysWatch starts logging similar events (60 seconds by default). Control policy violation events are considered *similar* and are not logged if the following conditions are met at the same time.

- the following parameters coincide for the events:
    - actions;
    - binary paths;
    - command lines;
    - process identifiers (PIDs);
- period of time after the previous event has been added is less than the specified value.

The text log on the client host with SoftControl SysWatch contains information about how many similar events have been skipped.

❑ **Check for the presence of running modules after SysWatch startup after (min.):**

Set the delay after SysWatch startup before the check of modules required for running at system startup. The required modules are the modules marked with the flag Must be running at system startup [84].

There are modules that are critical to operation of the system. SoftControl Service Center allows specifying modules to check and setting a delay after SysWatch startup following which presence of modules is checked. If some of the modules are missing, a respective security event is created.

❑**Check for the presence of running modules after user login after (min.):**

Set up the delay after user login before the check of modules required for running in user session. The required modules are the modules marked with the flag Must be running in user session [84].

There are modules that are critical during user sessions. SoftControl Service Center allows specifying modules to check and setting a delay after a user login following which presence of modules is checked. If some of the modules are missing, a respective security event is created.

❑ **High risk of missing modules:**

If the checkbox is marked and modules with the flags Must be running at system startup [84] and Must be running in user session (84) are not found in the memory during respective checks, and the log events will have the importance **Critical** instead of **High**.

❑ **Track debugger availability:**

If the checkbox is marked and the kernel-mode debugger or debugging of the process *safensec.exe* is detected, and the log event with the **Critical** importance will be generated.

❑ **Restore database after hard reset**:

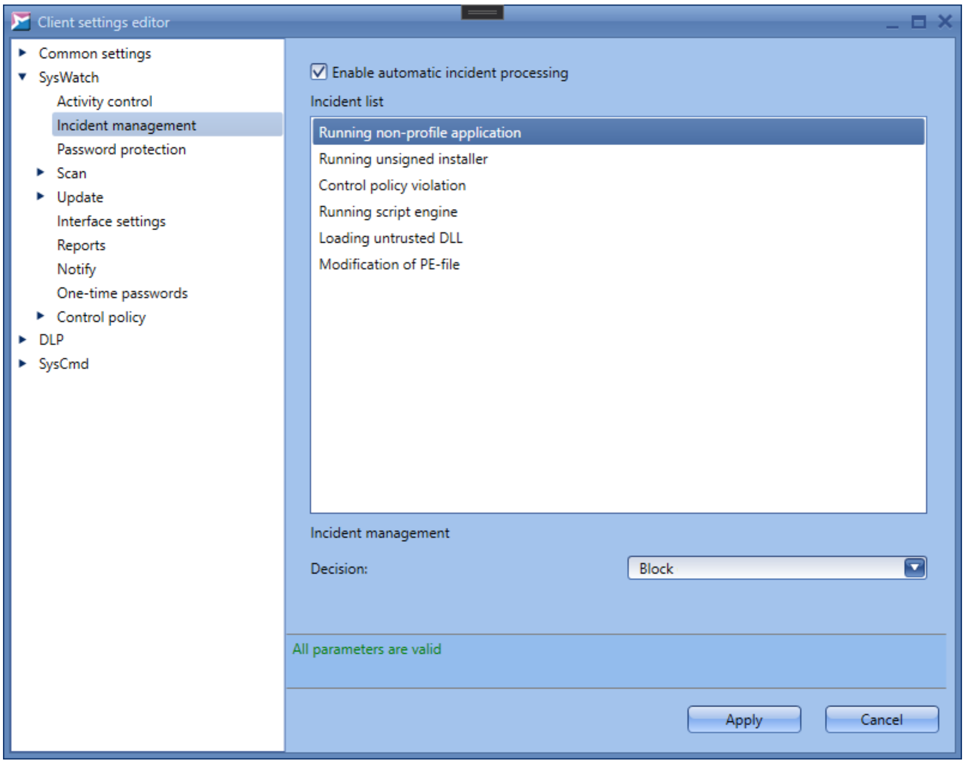
Restore the database from the most recent backup copy in case of a hard reset. SoftControl SysWatch backs up the database at startup, when new settings arrive from the server, or when you change settings locally.

❑ **Enable events from Windows logs to be sent to the server**:

Send events from Windows logs (System, Security, and Application) on the client devices to the server.

Incident management

Tick off the **Enable automatic incident processing** checkbox in the **Incident Management** section of the **SysWatch** category and specify the reaction to the incidents from the **Incident list** in the **Decision** drop-down list, according to table 16 (fig. Incident processing settings (67)).



☑ Enable automatic incident processing

Incident list

- Running non-profile application
- Running unsigned installer
- Control policy violation
- Running script engine
- Loading untrusted DLL
- Modification of PE-file

Incident management

Decision: Block

All parameters are valid

Figure 59. Incident processing settings

Table 16. Possible actions on incidents

Incident	Actions
Running non-profile application	• **Execute in the restricted mode** The application runs in the isolated environment ('sandbox') under the V.I.P.O. user account with limited permissions. The application is not added to the system profile but is moved to the restricted zone instead. The application can download child modules that are not added to the system profile either. Even if this application is harmful and it installs some extra components, SoftControl SysWatch prevents them from loading. • **Scan and execute in the restricted mode** The application runs in the restricted mode, if no malicious code has been found during the antivirus scanning. Otherwise, the application is blocked. • **Execute in the software update mode** The application runs under current user account without restrictions. The application and all its child modules are moved to the system profile and to the trusted execution zone. • **Scan and execute in the software update mode** The application runs in the software update mode, if no malicious code has been found during the antivirus scanning. Otherwise, the application is blocked. • **Block** The application is blocked.
Running unsigned installer	• **Install** The installer runs under current user account without restrictions. The application and all its child modules are moved to the system profile and to the trusted zone after installation. • **Scan and install** The installer runs in the software update mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Install in the restricted mode** The installer runs in the isolated environment ('sandbox') under the V.I.P.O. user account with limited permissions. The installer is not added to the system profile. • **Scan and install in the restricted mode** The installer runs in the restricted mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Block** The installer is blocked.
Control policy violation	• **Allow** Allow a process to perform an action that meets the conditions of the specified control policy rule, once or for a session. • **Scan and allow** Allow a process to perform an action that meets the conditions of the specified control policy rule once or for a session, if no malicious code has been found during the antivirus scanning. Otherwise, the action is blocked. • **Block** Do not allow the process to perform an action that meets the conditions of the specified control policy rule. • **Block and kill application** Do not allow the process to perform an action that meets the conditions of the specified control policy rule, and then kill the process.
Running script engine	• **Allow** Allow script engine running without restrictions. • **Block** Block script engine running.
Loading untrusted DLL	• **Allow** Allow loading without restrictions. • **Block**

Incident	Actions
	Block loading.
Modification of PE file by non-installer	• **Allow** Allow modification of a portable executable file. • **Block** Block modification.

To delegate the authorities to handle the incidents to a local SoftControl SysWatch user, deselect the **Enable automatic incident processing** checkbox.

Password protection

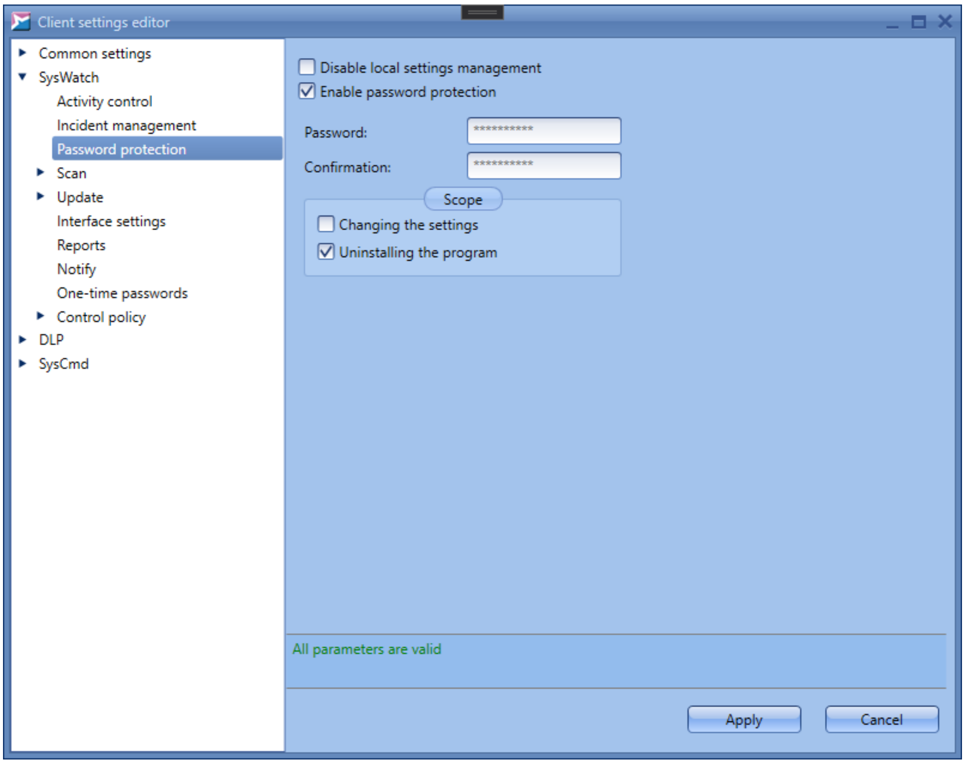
To enable common password protection of the SoftControl SysWatch interface and/or uninstaller on a client host, switch to the **Password protection** section of the **SysWatch** category and tick off the **Enable password protection** checkbox (fig. Password protection settings[69]). Enter a **Password** and its **Confirmation**, and select the **Scope**:

❑ **Changing the settings**:

Request the password when accessing SoftControl SysWatch GUI.

❑ **Uninstalling the program**:

Request the password when uninstalling SoftControl SysWatch.



☐ Disable local settings management
☑ Enable password protection
Password: **********
Confirmation: **********
Scope
☐ Changing the settings
☑ Uninstalling the program

All parameters are valid

Figure 60. Password protection settings

Select **Disable local settings management** if you need to prevent the modification of

SoftControl SysWatch settings from the client host. This flag is also displayed on the Clients[42] tab.

Scan settings

Specify the antivirus check parameters in the **Scan** → **Scan common settings** section of the **SysWatch** category (fig. Common scan settings[70]).

Select an action when threats are detected during the antivirus scanning, in the **Reaction to the threat** area:

- **Select action automatically**:

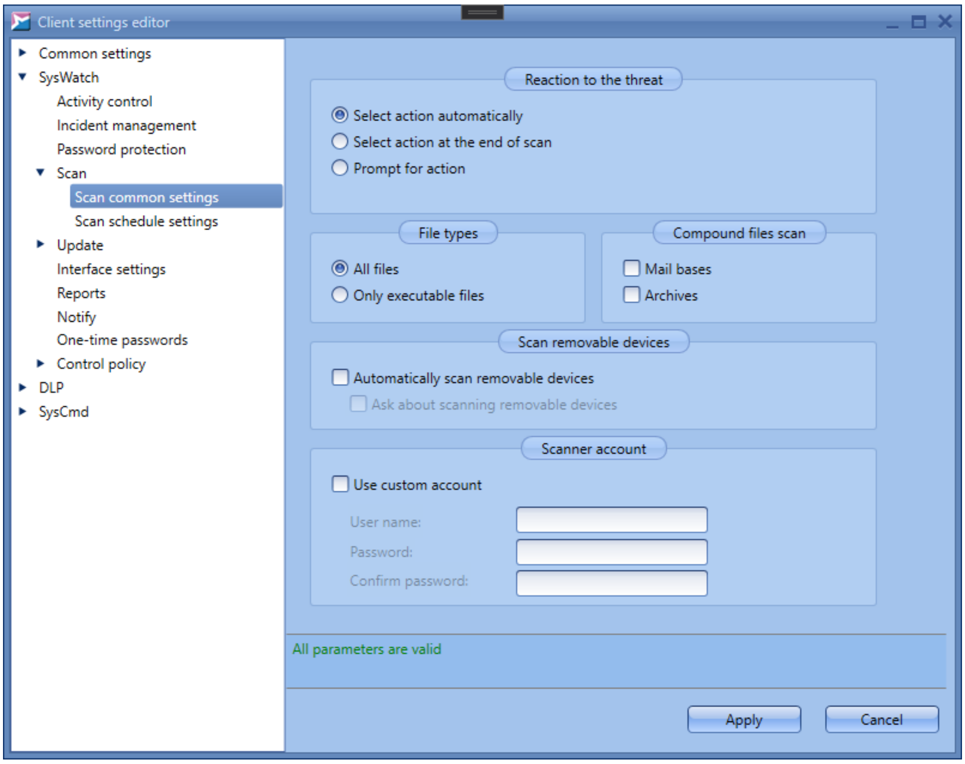
  Neutralize the infected object or delete it if it cannot be treated.

- **Select action at the end of scan**:

  After the check completes, SoftControl SysWatch prompts the local user to select actions for all the detected threats.

- **Prompt for action**:

  SoftControl SysWatch prompts the local user to select an action when a threat is detected.



Reaction to the threat

● Select action automatically
○ Select action at the end of scan
○ Prompt for action

File types

● All files
○ Only executable files

Compound files scan

□ Mail bases
□ Archives

Scan removable devices

□ Automatically scan removable devices
□ Ask about scanning removable devices

Scanner account

□ Use custom account

User name:
Password:
Confirm password:

All parameters are valid

Figure 61. Common scan settings

Select file types to scan in the **File types** area:

- **All files**:

Scan all types of files except for files not ticked off in the **Compound files scan** area (the **Mail bases** and **Archives** checkboxes).

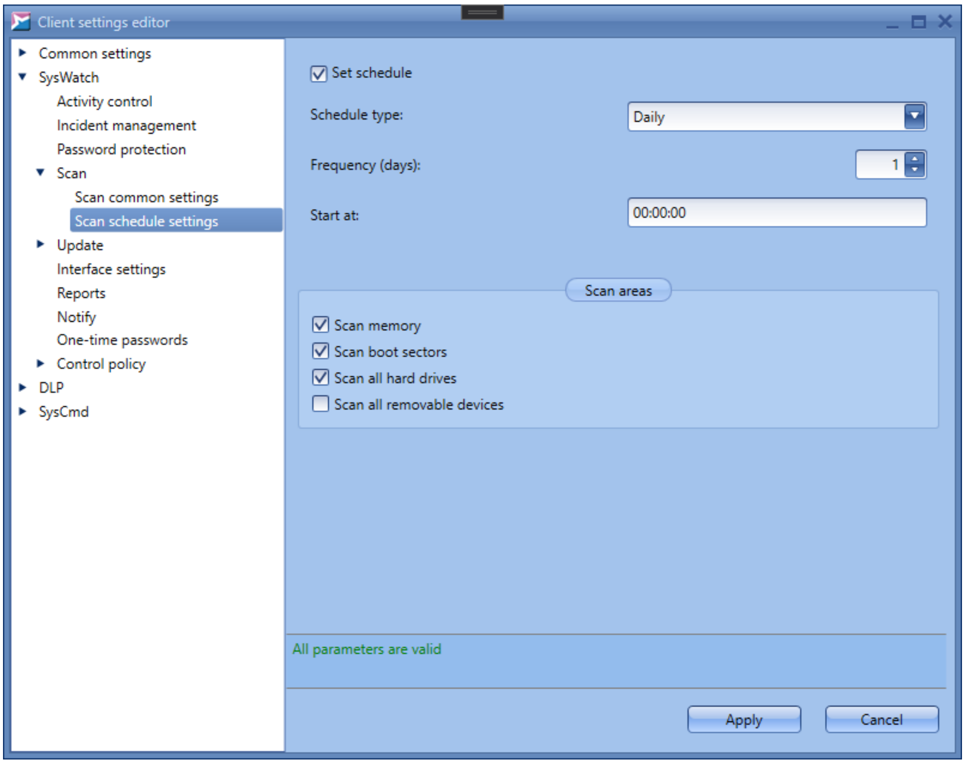
- **Only executable files**:

  Scan only PE files.

Tick off the **Automatically scan removable devices** checkbox in the **Scan removable devices** area, if you need to start the antivirus scanning of the USB devices automatically when they connect to a client host. Tick off **Ask about scanning removable devices** to show the dialog box with the scan suggestion on a client host.

Tick off **Use custom account** in the **Scanner account** area and specify the credentials, if it is required to specify an account other than the system account, to perform the scanning.

You can set the schedule of the antivirus check in the **Scan** → **Scan schedule settings** section of the **SysWatch** category. To do so, tick off the **Set schedule** checkbox and specify the parameters (fig. Scan schedule settings[71]). Specify frequency of the scanning task in the **Frequency (days)** counter, and the time of the task start in *hh:mm:ss* format in the **Start at** field. You can restrict the scan areas in the **Scan areas** section.



☑ Set schedule

Schedule type: Daily

Frequency (days): 1

Start at: 00:00:00

Scan areas

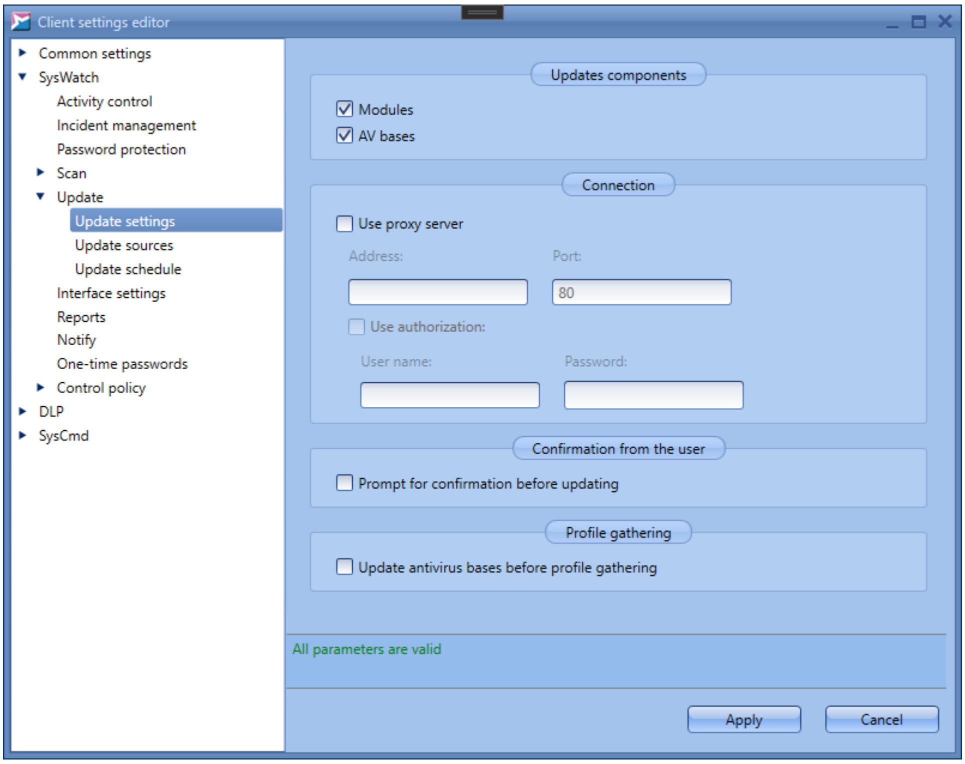
☑ Scan memory
☑ Scan boot sectors
☑ Scan all hard drives
☐ Scan all removable devices

All parameters are valid

Figure 62. Scan schedule settings

Update settings

Specify the update parameters in the **Update** → **Update settings** section of the **SysWatch** category (fig. Common update settings 72).



Updates components

☑ Modules
☑ AV bases

Connection

□ Use proxy server

Address: Port: 80

□ Use authorization:

User name: Password:

Confirmation from the user

□ Prompt for confirmation before updating

Profile gathering

□ Update antivirus bases before profile gathering

All parameters are valid

Figure 63. Common update settings

Select the required SoftControl SysWatch components to update in the **Update components** area:

❑ **Modules**;

❑ **AV bases**.

If a proxy server is used to connect to the update server, tick off **Use proxy server** and specify the required settings in the **Connection** area.

Tick off **Prompt for confirmation before updating** in the **Confirmation from the user** area to display the dialog box with the confirmation of the operation on a client host.

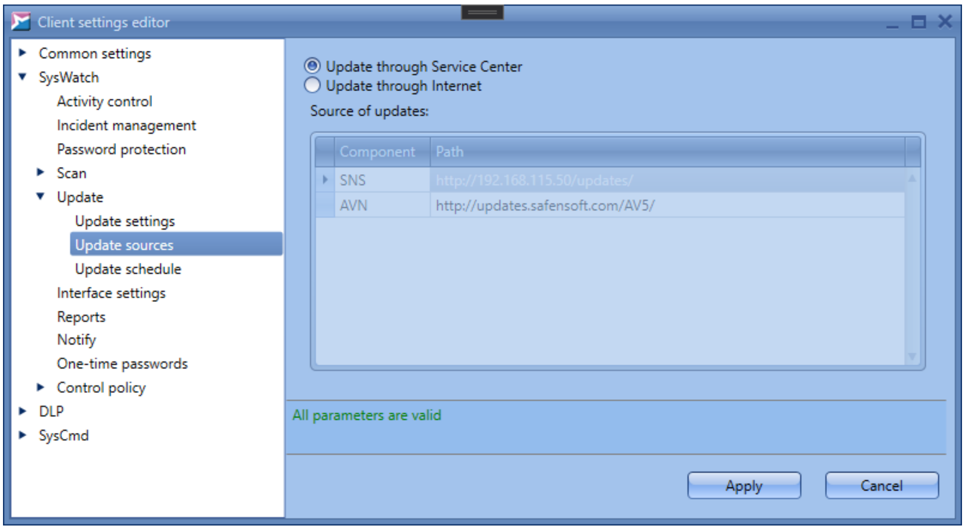
Tick off **Update antivirus bases before profile gathering** in the **Profile gathering** area if you need to update the antivirus bases on the client host before SoftControl SysWatch gathers the system profile.

You can select the update source in the **Update** → **Update sources** section of the **SysWatch** category:

o **Update through Service Center**: update via the intranet update server;

- ○ **Update through Internet**: update via ARUDIT SECURITY, LLC server available via the Internet.

In the **Source of updates** area, you can specify the addresses to update the proactive protection core and antivirus bases. Default values are taken from update settings for SoftControl Service Center.



● Update through Service Center
○ Update through Internet

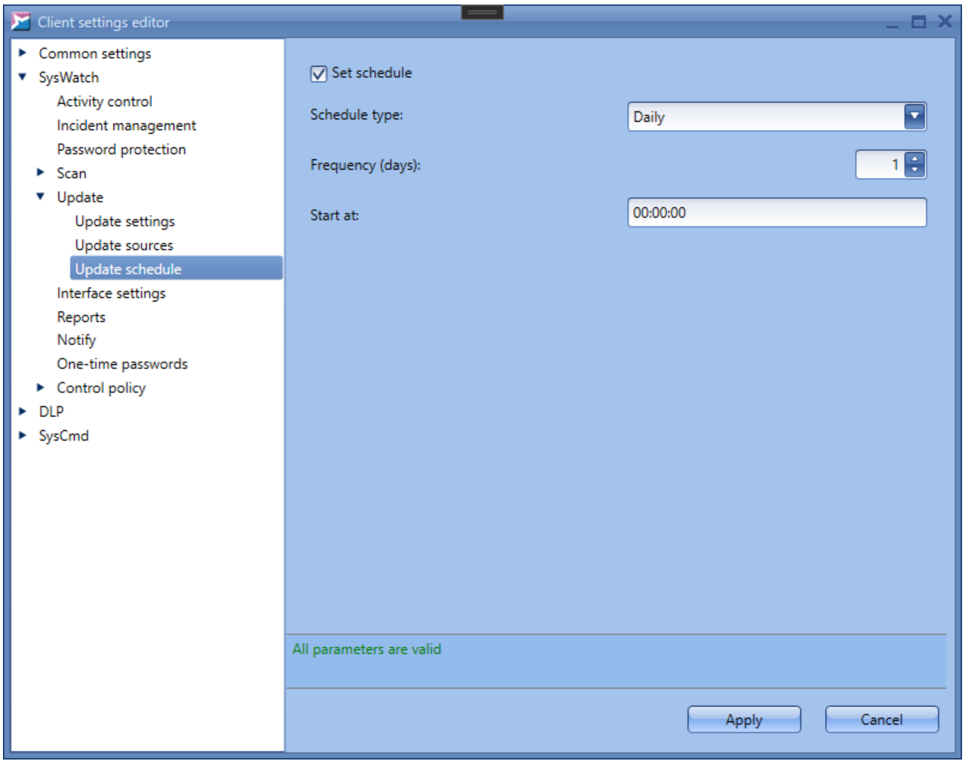
Source of updates:

Component	Path
SNS	http://192.168.115.50/updates/
AVN	http://updates.safensoft.com/AV5/

All parameters are valid

Figure 64. Update source settings

You can set the update schedule in the **Update** → **Update schedule** section of the **SysWatch** category. To do so, tick off the **Set schedule** checkbox and specify the parameters (fig. Update schedule settings 73). Specify the the frequency of the task in the **Days frequency** counter, and the start time in *hh:mm:ss* format in the **Invoke time** field.



☑ Set schedule

Schedule type: Daily

Frequency (days): 1

Start at: 00:00:00

All parameters are valid

Figure 65. Update schedule settings

Interface settings

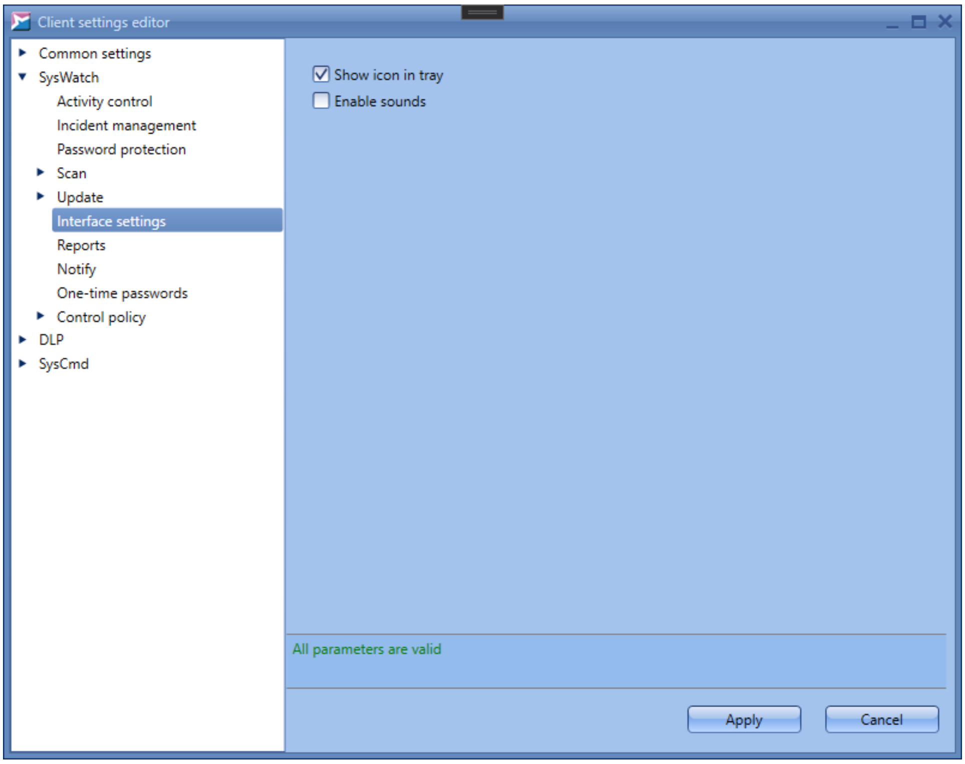
Select the required SoftControl SysWatch interface options on the client hosts, in the **Interface settings** section of the **SysWatch** category (fig. Interface settings 74):

❑ **Show icon in tray**:

show the SoftControl SysWatch icon in the Windows taskbar notification area.

❑ **Enable sounds**:

enable sound notifications about the incidents.



☑ Show icon in tray

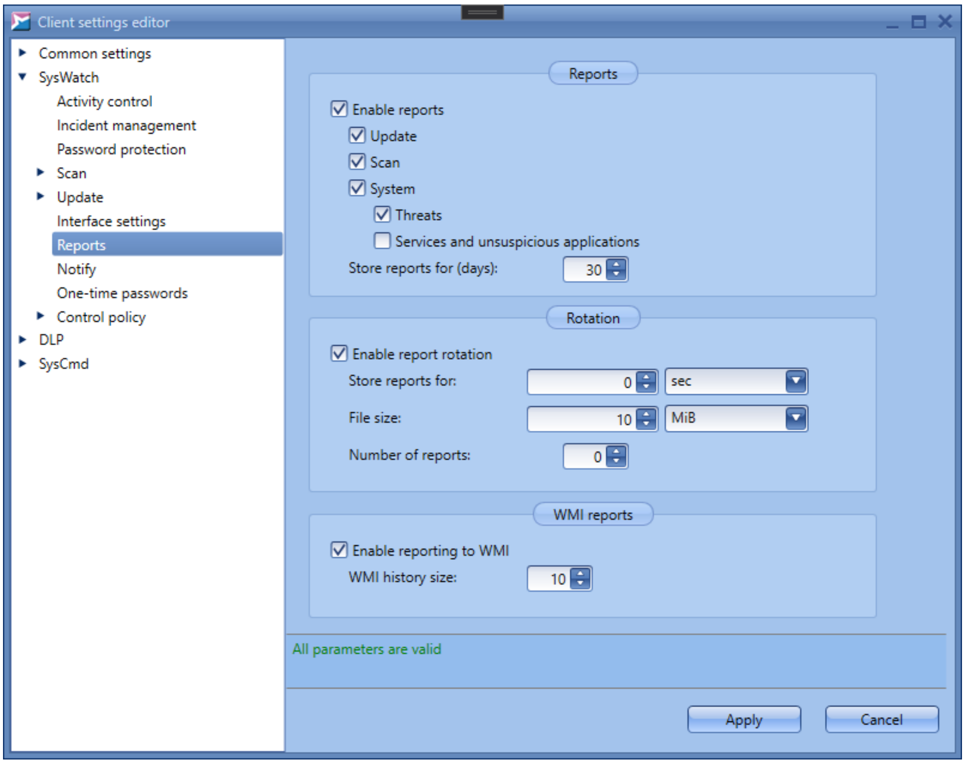
□ Enable sounds

All parameters are valid

Figure 66. Interface settings

Reports

In the **Reports** section of the **SysWatch** category, specify the SoftControl SysWatch parameters of logging to text files and registering events in WMI (fig. Report settings [75]).



Reports

☑ Enable reports

☑ Update

☑ Scan

☑ System

☑ Threats

□ Services and unsuspicious applications

Store reports for (days): 30

Rotation

☑ Enable report rotation

Store reports for: 0 sec

File size: 10 MiB

Number of reports: 0

WMI reports

☑ Enable reporting to WMI

WMI history size: 10

All parameters are valid

Figure 67. Report settings

Tick off the **Enable reports** checkbox in the **Reports** area to enable report generation and select the types of the events to be logged:

- ❑ **Update**;
- ❑ **Scan**;
- ❑ **System**:
  - ❑ **Threats**;
  - ❑ **Services and unsuspicious applications**.

Tick off **Services and unsuspicious applications** to enable the recording of events when the services start and stop. The services that have started before the *safensec.exe* system service are marked as *was started before* in the reports.

Specify the number of days when the event history is stored, in the **Store reports for (days)** counter.

Tick off the **Enable report rotation** checkbox in the **Rotation** area if necessary and specify the rotation options (one or several) that limit the quantitative data of the reports:

- **Store report for**:

  specify the time limit of a report file and select a unit from the drop-down list (seconds, minutes, hours, or days).

- **File size**:

  specify the size limit of a report file and select a unit from the drop-down list (bytes, KiB or MiB).

- **Number of reports**:

  specify the maximum number of the log file parts to be stored.

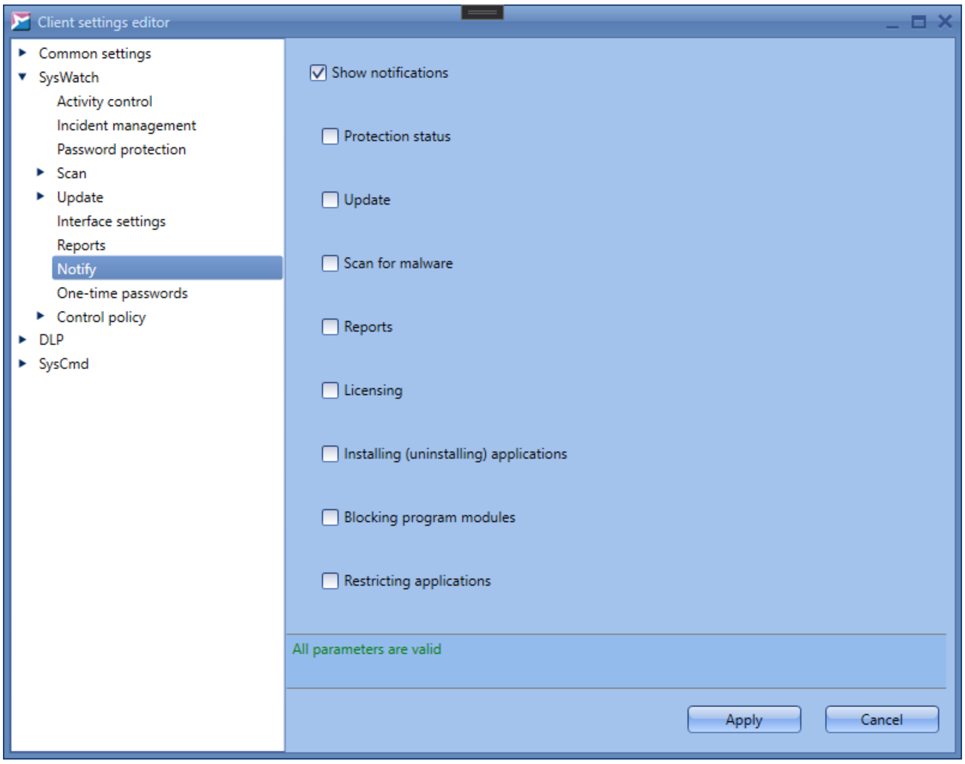
Tick off **Enable reporting to WMI** in the **WMI reports** area to enable the corresponding function and specify **WMI history size** in the corresponding field.

To prevent increased consumption of the system resources, we recommend that you do not set the history size to more than 100 events; 10-50 events is the optimal value.

Notify

To display SoftControl SysWatch local notifications on the client hosts, tick off the **Show notifications** checkbox in the **Notify** section of the **SysWatch** category and select the required types of messages (fig. Local notification settings 77):

- ❑ **Protection status**;
- ❑ **Update**;
- ❑ **Scan for malware**;
- ❑ **Reports**;
- ❑ **Licensing**;
- ❑ **Installing (uninstalling) applications**;
- ❑ **Blocking program modules**;
- ❑ **Restricting applications**.



☑ Show notifications

□ Protection status

□ Update

□ Scan for malware

□ Reports

□ Licensing

□ Installing (uninstalling) applications

□ Blocking program modules

□ Restricting applications

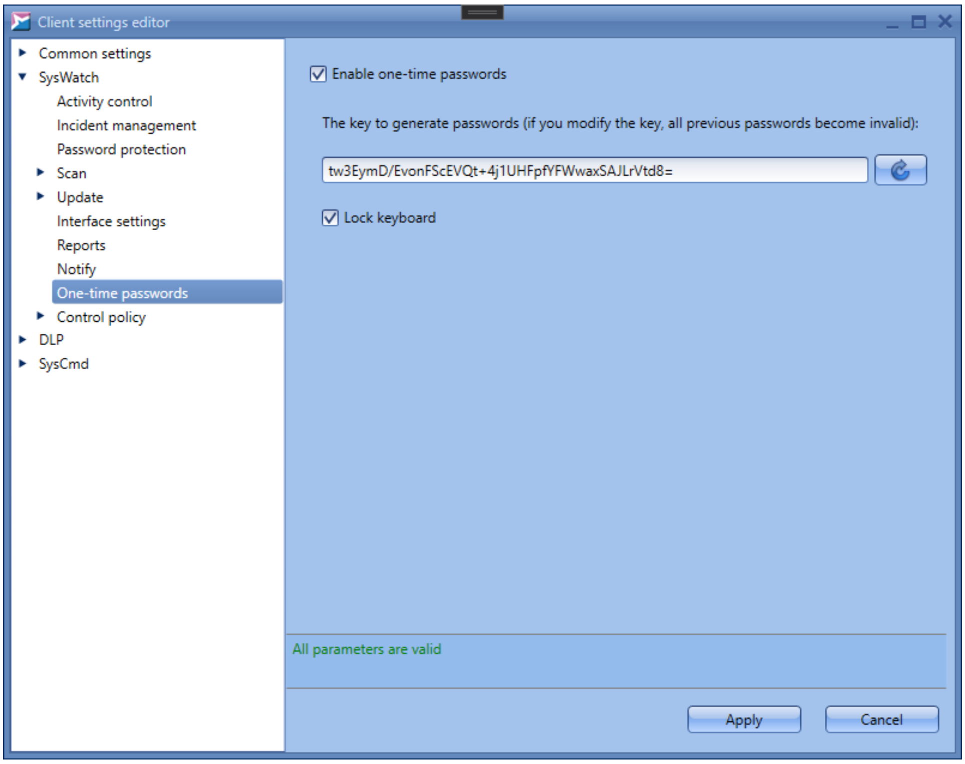
All parameters are valid

Figure 68. Local notification settings

One-time passwords

Tick off **Enable one-time passwords** in the **One-time passwords** section of the **SysWatch** category and click (**Generate key**) to generate a 256-bit key that is used to calculate one-time passwords (fig. One-time password settings 77).

Generating a new key makes all the previous passwords invalid.



☑ Enable one-time passwords

The key to generate passwords (if you modify the key, all previous passwords become invalid):

tw3EymD/EvonFScEVQt+4j1UHFpfYFWwaxSAJLrVtd8=

☑ Lock keyboard

All parameters are valid

Figure 69. One-time password settings

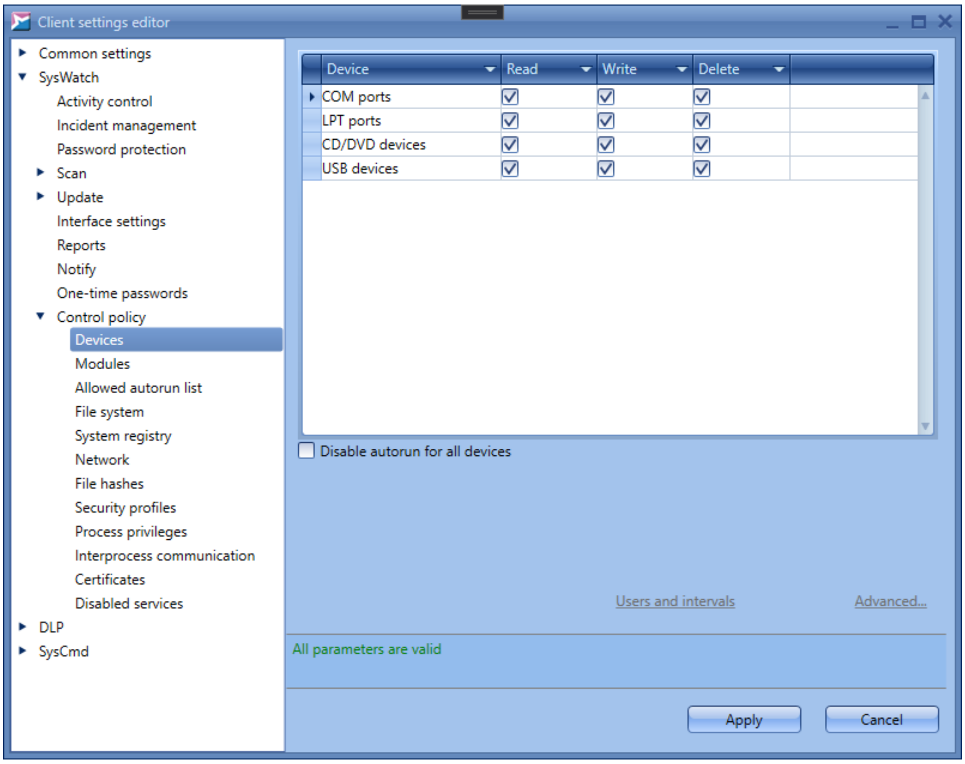
To lock the keyboard on the client host, tick off **Lock keyboard**. After SoftControl SysWatch receives the settings, the keyboard on the client host is locked. To unlock it, the user should enter a password. SoftControl SysWatch checks all sets of characters that the user enters. As soon as SoftControl SysWatch detects the password among the characters, it unlocks the keyboard. Besides, the keyboard unlocks when turning off and restarting the *safensec.exe* system service. If the user does not use the keyboard for 15 minutes, SoftControl SysWatch locks the keyboard again.

You can generate one-time passwords on the Organization units 53 tab.

Control policy: Devices

Specify the rules that control access to the following external system devices and ports on the client hosts, in the **Control policy** → **Devices** section of the **SysWatch** category (fig. Device control policy 78):

- COM ports;
- LPT ports;
- CD/DVD devices;
- USB devices.



Device	Read	Write	Delete
COM ports	☑	☑	☑
LPT ports	☑	☑	☑
CD/DVD devices	☑	☑	☑
USB devices	☑	☑	☑

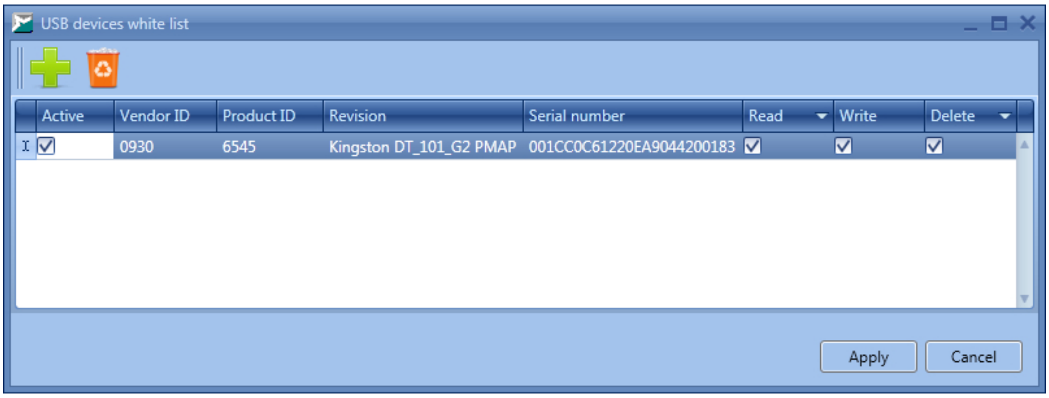
□ Disable autorun for all devices

All parameters are valid

Figure 70. Device control policy

To configure the permissions to access USB devices, specify them by ticking the corresponding checkboxes in the **Read**, **Write**, and **Delete** columns for the **USB devices** type.

Additionally, you can specify the exceptions for USB storage devices, i.e. select the devices that the rule does not apply to ('USB whitelist'). To do so, click **Advanced** and click ✚ (**Add**) in the displayed window (fig. Exceptions for USB storage devices 79).



Active	Vendor ID	Product ID	Revision	Serial number	Read	Write	Delete
☑	0930	6545	Kingston DT_101_G2 PMAP	001CC0C61220EA9044200183	☑	☑	☑

Figure 71. Exceptions for USB storage devices

Enter the USB storage device parameters in the corresponding fields. You can get the parameters of the USB device in the following way.

1) Insert the drive into the USB port of the computer.

2) Open the **Device Manager** tool of the Windows Control Panel.

3) Expand the **Disk drives** category and double-click the name of the required USB storage device.
4) Switch to the **Details** tab of the displayed window.
5) Select the **Parent** property from the drop-down menu. The **Value** field displays the string of the following type:

   USB\VID_<Vendor ID>&PID_<Product ID>\<Serial number>,

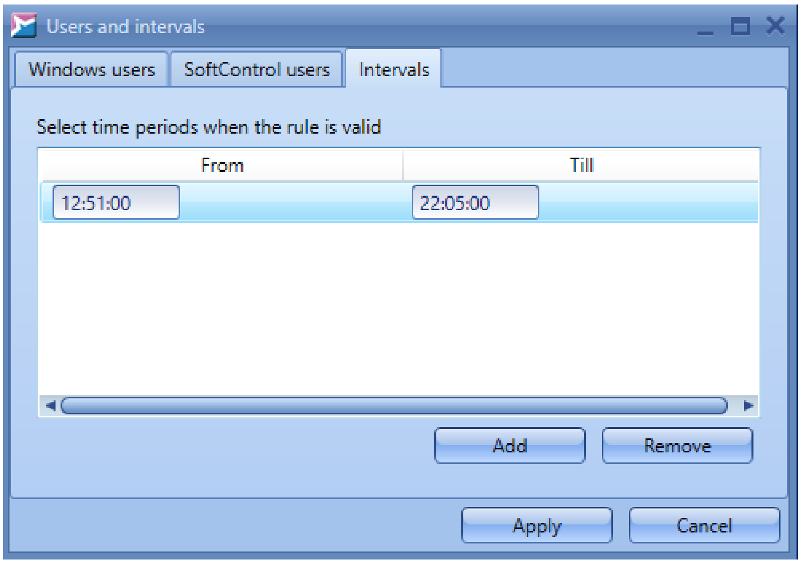
   where the corresponding numeric values of the **Vendor ID**, **Product ID**, and **Serial number** parameters are specified (shown in the angle brackets).
6) Select the **Hardware Ids** property from the drop-down menu. The **Value** field then displays the list of the hardware identifiers; use the first of the identifiers as the **Revision** parameter.

After you enter the parameters, select the access permissions for this device in the corresponding columns (**Read**, **Write** and **Delete**).

To remove a device from the list, click 🗑 (**Delete**).

To save the rules, click **Apply**.

For USB devices, you can specify time intervals and users (or groups) that the selected access rights apply to. To do it, click **Users and intervals**. In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Windows users** tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version). To confirm changes, click **Apply**.



Select time periods when the rule is valid

From	Till
12:51:00	22:05:00

Figure 72. Adding users and intervals for the rule

To block access to the CD/DVD devices, LPT ports and COM ports, deselect any box in the **Write**, **Read**, or **Delete** columns for the corresponding device types (all the boxes are then deselected for this type).

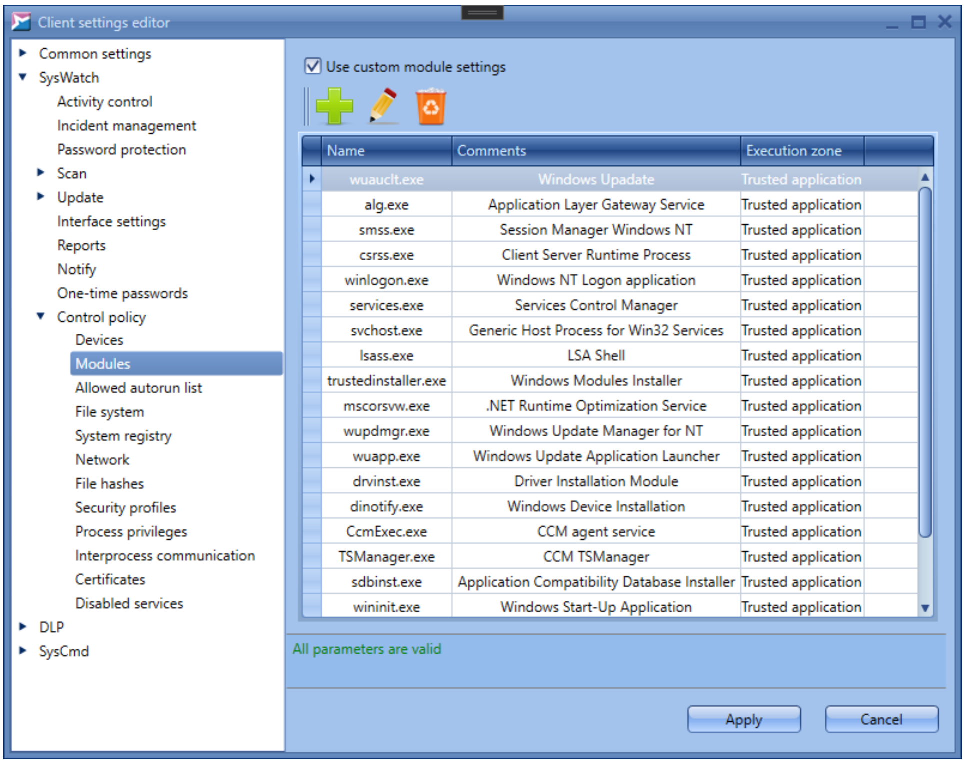
You should additionally reboot the system on the client hosts to change the access rights to the ports (COM, LPT).

Select the **Disable autorun for all devices** option, if you need to block autorun for the USB and CD/DVD devices.

Control policy: Modules

In the **Control policy** → **Modules** section of the **SysWatch** category, you can set the rules for certain applications installed on the client hosts (fig. Modules control policy 81). The feature is disabled by default. To enable it, select **Use custom module settings**.

If you tick off **Use custom module settings** and apply the settings on the client hosts, all local settings are deleted and cannot be restored.



☑ Use custom module settings

Name	Comments	Execution zone
wuauclt.exe	Windows Upadate	Trusted application
alg.exe	Application Layer Gateway Service	Trusted application
smss.exe	Session Manager Windows NT	Trusted application
csrss.exe	Client Server Runtime Process	Trusted application
winlogon.exe	Windows NT Logon application	Trusted application
services.exe	Services Control Manager	Trusted application
svchost.exe	Generic Host Process for Win32 Services	Trusted application
lsass.exe	LSA Shell	Trusted application
trustedinstaller.exe	Windows Modules Installer	Trusted application
mscorsvw.exe	.NET Runtime Optimization Service	Trusted application
wupdmgr.exe	Windows Update Manager for NT	Trusted application
wuapp.exe	Windows Update Application Launcher	Trusted application
drvinst.exe	Driver Installation Module	Trusted application
dinotify.exe	Windows Device Installation	Trusted application
CcmExec.exe	CCM agent service	Trusted application
TSManager.exe	CCM TSManager	Trusted application
sdbinst.exe	Application Compatibility Database Installer	Trusted application
wininit.exe	Windows Start-Up Application	Trusted application

All parameters are valid

Figure 73. Modules control policy

The window contains a number of Windows OS modules by default. To add a new module to the list, click ✚ (**Add**). The displayed window (fig. Creating rules for the module[82]) contains several tabs where you can add information about the module and specify rules for it.

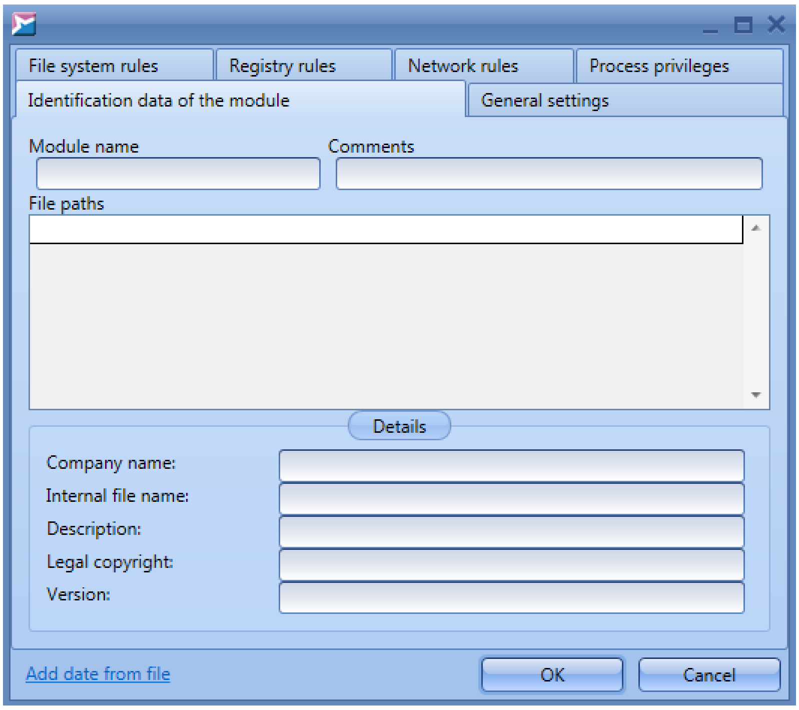


Figure 74. Creating rules for the module

You can add general information about the module on the **Identification data of the module** tab:

- **Module name** is the mandatory parameter.
- **File paths** are a set of possible paths to the file (the field can be empty).
- **Comments** is a short description of the module.

You can use masks in the **File paths** field to create rules for the objects you add. For example, you can specify part of the file path, with the help of masks. Below is the mask syntax:

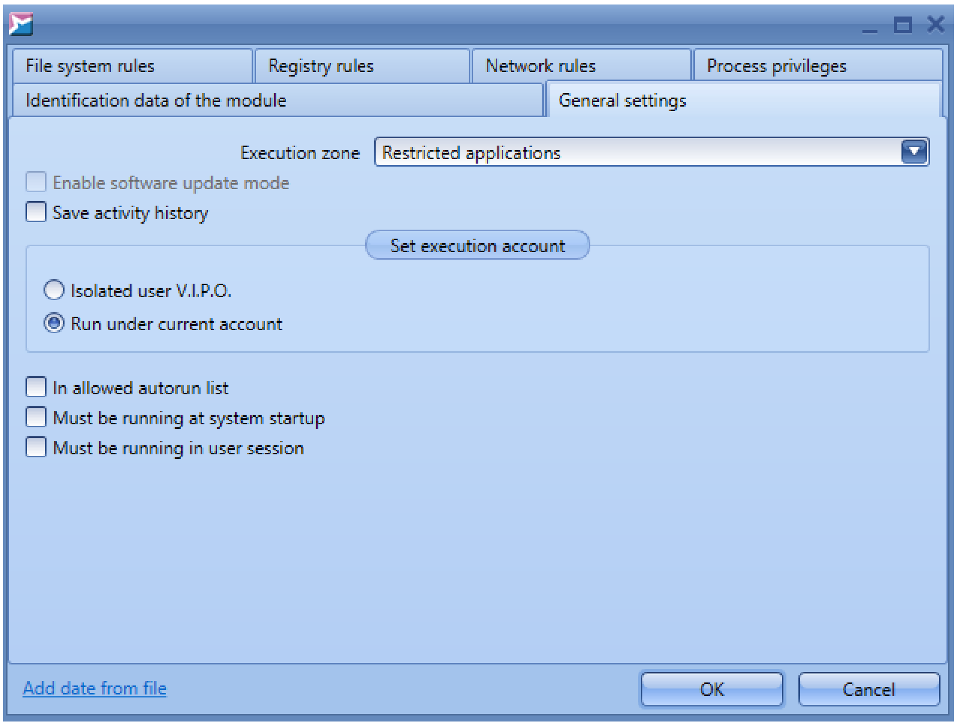
- **#*#** – mask replaces any number of characters except the '\' symbol;
- **#**#** – mask replaces any number of characters;
- **#?#** – mask replaces exactly one character (any character).

You can also select a module by clicking the **Add data from file** link (fig. Creating rules for the module[82]) and specifying the required file in the displayed window. The data on the **Identification data of the module** tab are filled in automatically in this case.

When you apply the settings on a client host, SoftControl Service Center compares the data of the executable modules on the client host and the identification data in the settings as follows. An executable module matches a description if all fields specified on the identification data tab coincide with the corresponding module data. The following should be considered as well:

– if several paths are specified for a module, any one of them should coincide with the module data;

– if information about the module version is in different languages, version description on any language should coincide completely with the module data.



Execution zone: Restricted applications

□ Enable software update mode

□ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

□ In allowed autorun list

□ Must be running at system startup

□ Must be running in user session

Figure 75. Creating rules for the module: General settings

You can specify module execution conditions on the **General settings** tab.

In the **Execution zone** area, select a zone to run the module:

- **Restricted applications;**
- **Blocked applications;**
- **Trusted applications.**

Tick off **Enable software update mode** if the module should run in this mode (for Trusted applications only). Tick off **Save launch history** to enable the activity history saving option for the module.

In the **Set execution account** area, select an account to run the application (for Restricted applications only):

- **Isolated user V.I.P.O.**
- **Run under current account.**

Select **In allowed autorun list** if you need to include the module in the allowed autorun list (see

Control policy → Allowed autorun list 84 for details).

Selecting **Must be running at system startup** enables the check if the module is loaded after the start of the system (see Activity control 66 for details).

Selecting **Must be running in user session** enables the check if the module is loaded after the logging in the user (see Activity control 66 for details).

On the **File system rules** tab, you can specify the application permissions to access the file system objects (similar to rules in section Control policy: File system 85).

On the **Registry rules** tab, you can specify the application permissions to access the system registry objects (similar to rules in section Control policy: System registry 88).

On the **Network rules** tab, you can specify the rules that control the application network activity (similar to rules in section Control policy: Network 91).

On the **Process Privileges** tab, restrictions are set on the use of Windows privileges by the process on client hosts (similar to rules in section Control Policy:Process privileges 98).

To modify information about a module, click ✎ (**Change**) or double-click the module and change the parameters, as you did when you added the module.

To delete a module from the list, click 🗑 (**Delete**).

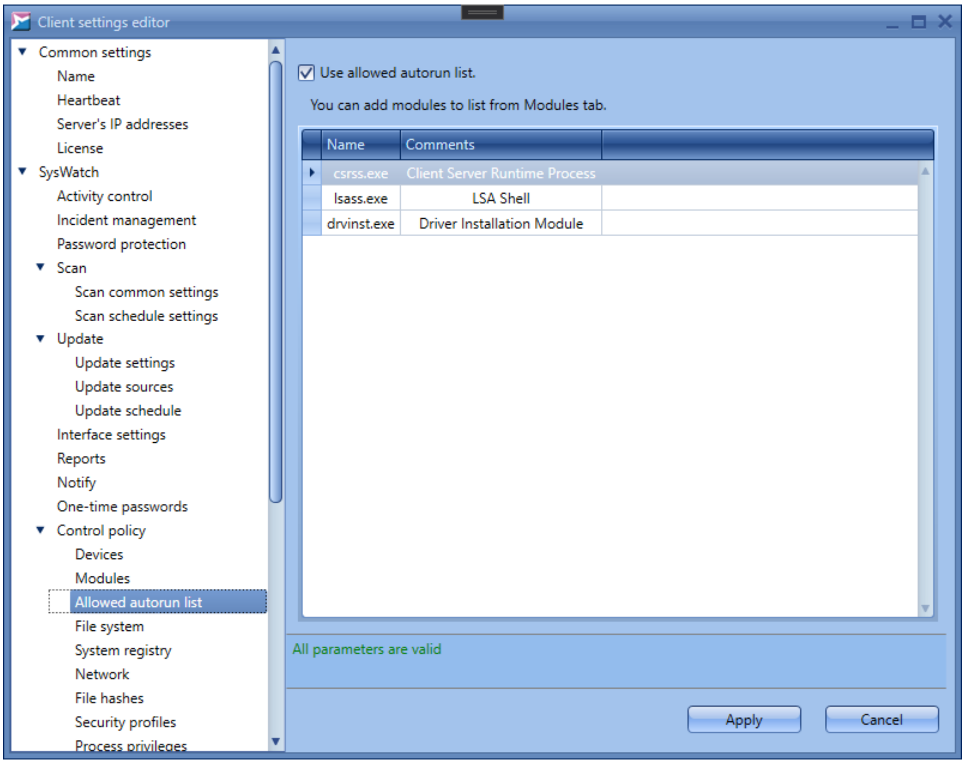
To confirm changes, click **Apply**.

Control policy: Allowed autorun list

The allowed autorun list is created in order to track launch of modules that are not included in this list. The allowed autorun list shall include modules that do not require creating a security event when launched.

The **Control policy** → **Allowed autorun list** section of the **SysWatch** category displays the list of modules that can start automatically on the client hosts (fig. Allowed autorun list 84). You can add modules to the list in the **Control policy** → **Modules** section (see above 83).

If **Use allowed autorun list** is checked, log records about launched processes specify if the processes were included in the allowed autorun list.



☑ Use allowed autorun list.

You can add modules to list from Modules tab.

Name	Comments
csrss.exe	Client Server Runtime Process
lsass.exe	LSA Shell
drvinst.exe	Driver Installation Module

All parameters are valid

Figure 76. Allowed autorun list

Control policy: File system

Specify the application permissions to access the file system objects on the client hosts, in the **Control policy** → **File system** section of the **SysWatch** category (fig. File system control policy 86):

- Reading a file or a folder;
- Writing to a file or to a folder (creating/changing a file or a folder);
- Deleting a file or a folder.

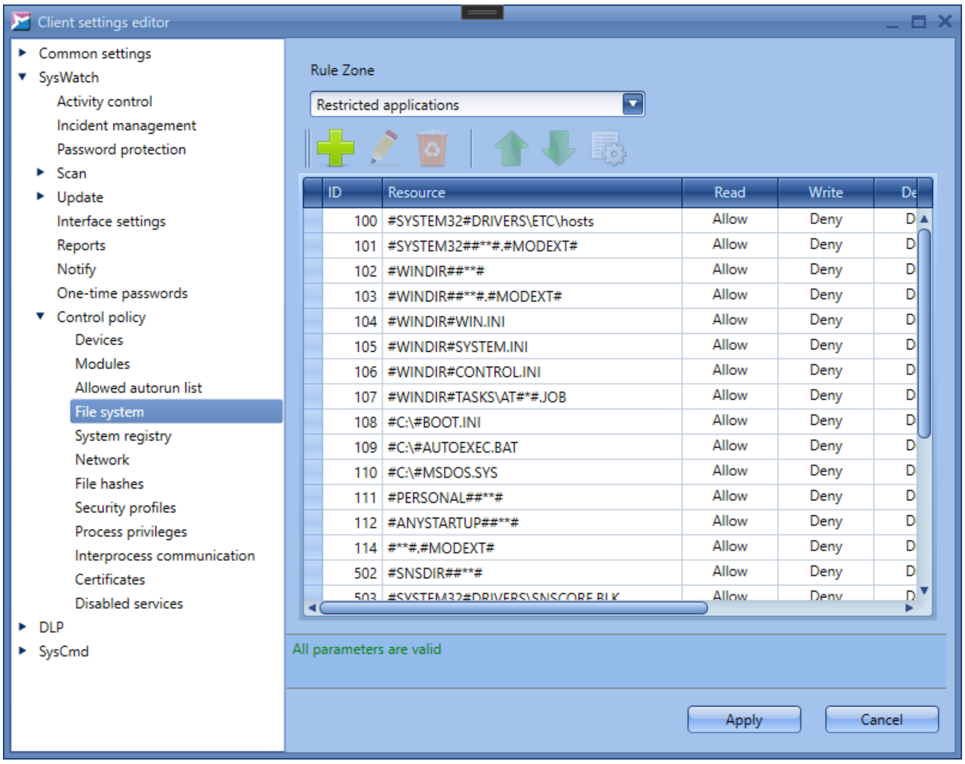
Rules are divided into lists for applications from the following execution zones:

- **Trusted applications**;
- **Restricted applications**.

To switch between the lists, select the required category from the **Rule Zone** drop-down list. If you need to move a rule to the list for applications from another execution zone, invoke the rule's context menu and select one of the options:

- **All** – create a rule for both execution zones, if the rule is only in one list;
- **Restricted** – move a rule to the list for the restricted applications;
- **Trusted** – move a rule to the list for trusted applications.

Each rule is an entry in the flat list and has its unique **ID**. The objects the rule applies to are specified in the **Resource** column, while their permissions are specified in the **Read**, **Write**, and **Delete** columns. The **Active** checkbox indicates whether the rule is active.



Rule Zone: Restricted applications

ID	Resource	Read	Write	De
100	#SYSTEM32#DRIVERS\ETC\hosts	Allow	Deny	D
101	#SYSTEM32##**#.#MODEXT#	Allow	Deny	D
102	#WINDIR##**#	Allow	Deny	D
103	#WINDIR##**#.#MODEXT#	Allow	Deny	D
104	#WINDIR#WIN.INI	Allow	Deny	D
105	#WINDIR#SYSTEM.INI	Allow	Deny	D
106	#WINDIR#CONTROL.INI	Allow	Deny	D
107	#WINDIR#TASKS\AT#*#.JOB	Allow	Deny	D
108	#C:\#BOOT.INI	Allow	Deny	D
109	#C:\#AUTOEXEC.BAT	Allow	Deny	D
110	#C:\#MSDOS.SYS	Allow	Deny	D
111	#PERSONAL##**#	Allow	Deny	D
112	#ANYSTARTUP##**#	Allow	Deny	D
114	#**#.#MODEXT#	Allow	Deny	D
502	#SNSDIR##**#	Allow	Deny	D
503	#SYSTEM32#DRIVERS\SNSCORE.BLK	Allow	Deny	D

All parameters are valid

Figure 77. File system control policy

If several rules have overlapping scopes, then the lowest rule in the list has the highest priority of execution. Rule position in the list can be changed by the ⬆ (**Up**) and ⬇ (**Down**).

A string in the **Resource** column is a path to the object or objects the rule applies to. In this string, you can use masks to create rules for the group of file system objects. For example, you can create a rule for a folder and all the objects inside it, or a rule for certain file types (extensions).

Below is the mask syntax:

- **#*#** – mask replaces any number of characters except the '\' symbol (if the mask is placed at the end of the string, the rule affects only root directory files);
- **#**#** – mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects root directory files, subdirectories and subdirectories files);
- **#?#** – mask replaces exactly one character (any character).

To create a rule, click ✚ (**Add**).

Type the full path to an object, or a mask in the **File or directory** field of the displayed window (fig. Creating a rule for the file system object(87)).

You can specify local folders as well as network folders. When you create a rule for network folders, the path is specified as follows: \\<*server_name*>\<*folder_name*>. You can use the **#**#** mask instead of '\\'. In this case, SoftControl SysWatch checks both network and local folders. Besides, you can specify IP address of the computer with the network folder.

> If you specify the computer's IP address in the rule, the rule is only valid when the user enters IP address to access the folder. It is not valid when the user enters the network path. Therefore, if you need to monitor the folders that the users access by both IP address and network path, create separate rules for each of the notations.

Select the security profile for the rule(95) in the corresponding drop-down list.

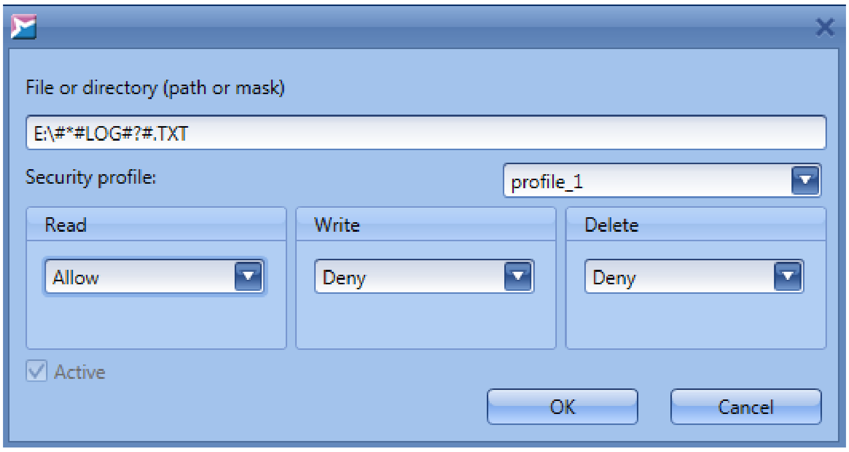
Note. You can only tick off or deselect the **Active** field if you select the default profile (**No group**). If you select any other profile you created yourself, the field is disabled. The value of the field is the same as the value of the corresponding field in the **Control policy** → **Security profiles** section.

Select the corresponding permissions to access the object, in the **Read**, **Write** and **Delete** areas:

- **Allow** – allow the application to perform an operation with the object;
- **Deny** – do not allow the application to perform an operation with the object.

Note that if reading is denied, writing and deleting are also automatically denied.

To add the created rule to the list and make it active, tick off the **Active** checkbox and click **OK**.



File or directory (path or mask)

E:\#*#LOG#?#.TXT

Security profile: profile_1

Read: Allow

Write: Deny

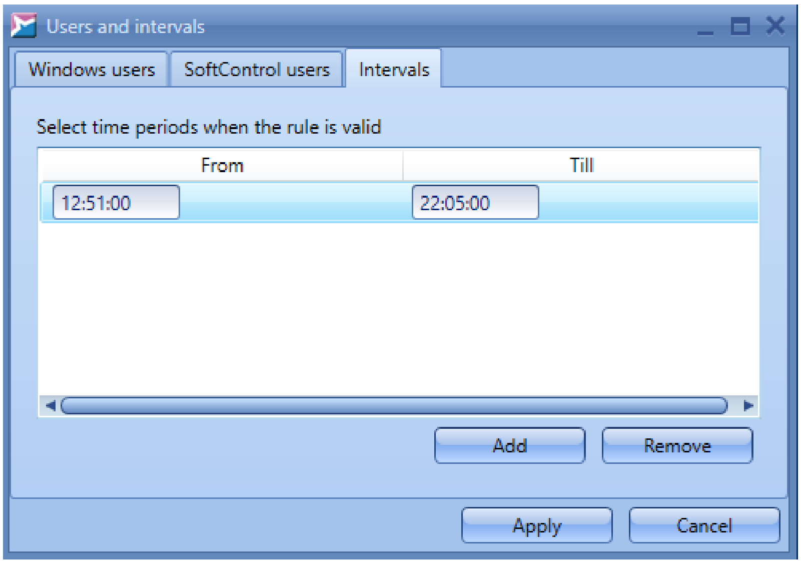
Delete: Deny

☑ Active

Figure 78. Creating a rule for the file system object

To edit a rule, click ✎ (**Change**) or double-click on it and set up the rule parameters, as with the creation of the rule.

To specify when the rule is valid and the users (or groups) it applies to, click (**Advanced**). In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Windows users** tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version). To confirm changes, click **Apply**.



Select time periods when the rule is valid

From	Till
12:51:00	22:05:00

Figure 79. Adding users and intervals for the rule

To delete a rule, click (**Delete**).

SoftControl SysWatch contains preset rules that apply to the system folders and the objects in the folders of the product components. Changing or deleting preset rules may cause violation of the system integrity protection.

Control policy: System registry

Specify the application permissions to access the system registry objects on the client hosts, in the **Control policy** → **System registry** section of the **SysWatch** category (fig. System registry policy[89]):

- Writing to a registry key or to a value (creating/changing a key or a value);
- Deleting a registry key or a value.

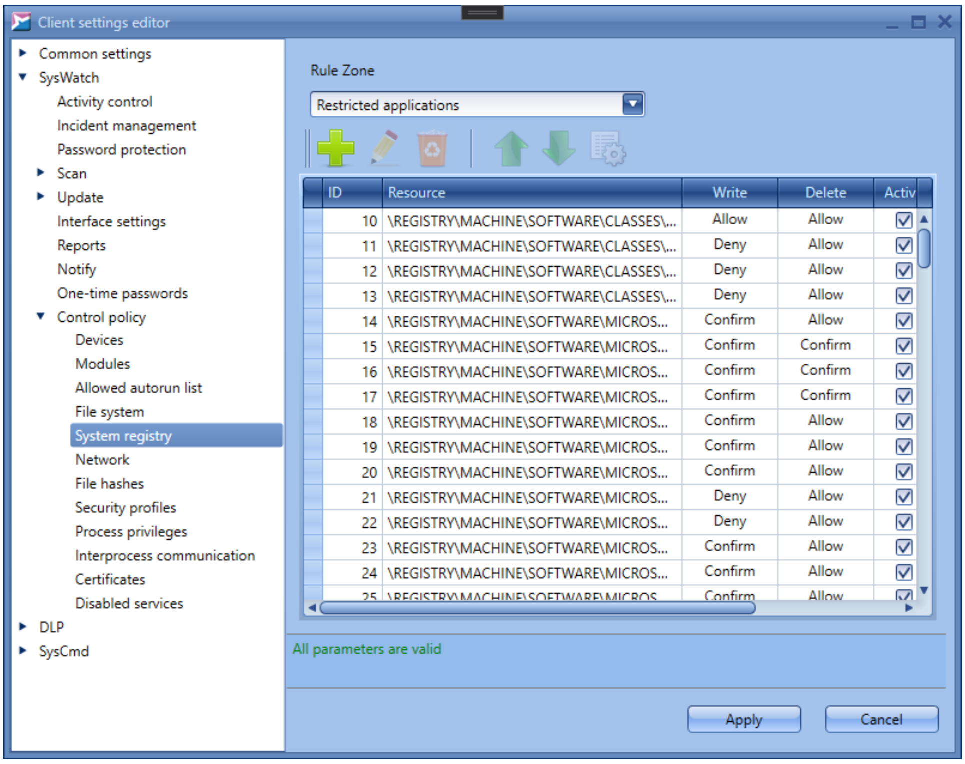
The rules are divided into lists for applications from the following execution zones.

- **Trusted applications**;
- **Restricted applications**.

To switch between the lists, select the corresponding category from the **Rule Zone** drop-down list. If you need to move a rule to the list for applications from another execution zone, invoke the rule's context menu and select one of the options:

- **All** – create a rule for both execution zones, if the rule is only in one list;
- **Restricted** – move a rule to the list for the restricted applications;
- **Trusted** – move a rule to the list for the trusted applications.

Each rule is an entry in the flat list and has its unique **ID**. The objects the rule applies to are specified in the **Resource** column, while their permissions are specified in the **Write** and **Delete** columns. The **Active** checkbox indicates whether the rule is active.



Rule Zone: Restricted applications

ID	Resource	Write	Delete	Activ
10	\REGISTRY\MACHINE\SOFTWARE\CLASSES\...	Allow	Allow	☑
11	\REGISTRY\MACHINE\SOFTWARE\CLASSES\...	Deny	Allow	☑
12	\REGISTRY\MACHINE\SOFTWARE\CLASSES\...	Deny	Allow	☑
13	\REGISTRY\MACHINE\SOFTWARE\CLASSES\...	Deny	Allow	☑
14	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
15	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Confirm	☑
16	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Confirm	☑
17	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Confirm	☑
18	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
19	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
20	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
21	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Deny	Allow	☑
22	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Deny	Allow	☑
23	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
24	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑
25	\REGISTRY\MACHINE\SOFTWARE\MICROS...	Confirm	Allow	☑

All parameters are valid

Figure 80. System registry policy

If several rules have overlapping scopes, then the lowest rule in the list has the highest priority of execution. The rule position in the list can be changed by the ⬆ (**Up**) and ⬇ (**Down**).

A string in the **Resource** column is a path to the object or objects the rule applies to. In this string, you can use masks to create rules for the group of system registry objects. For example, you can create a rule for a registry key and all objects inside it.

Below is the mask syntax:

- **#*#** – the mask replaces any number of characters except for the '\' symbol (if the mask is placed at the end of the string, the rule affects only the key values);
- **#**#** – the mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects the key values, subkeys and subkey values);

- **#?#** – the mask replaces exactly one character (any character).

To create a rule, click ✚ (**Add**).

Type the full path to an object, or a mask in the **Registry key or parameter** field of the displayed window (fig. Creating a rule for the system registry object[90]). The registry root keys in the specified path should be assigned as follows:

- *\REGISTRY\MACHINE\SOFTWARE\CLASSES\*, the HKEY_CLASSES_ROOT key;
- *\REGISTRY\MACHINE\*, the HKEY_LOCAL_MACHINE key;
- *\REGISTRY\USER\<SID>*, the HKEY_CURRENT_USER key for the user with the specified security identifier (<SID>);
- *\REGISTRY\USER\*, the HKEY_USERS key.

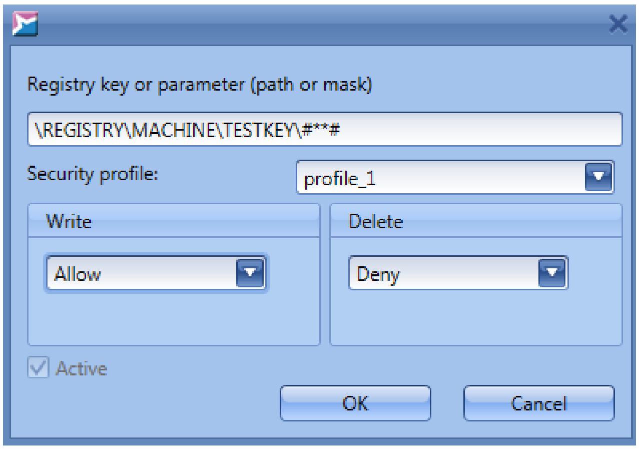
Select the security profile for the rule[95] in the corresponding drop-down list.

Note. You can only tick off or deselect the **Active** filed if you select the default profile (**No group**). If you select any other profile you created yourself, the field is disabled. The value of the field is the same as the value of the corresponding field in the **Control policy** → **Security profile** section.

Select the corresponding permissions to access the object, in the **Write** and **Delete** areas:

- **Allow** – allow the application to perform an operation with the object;
- **Deny** – do not allow the application to perform an operation with the object.

Note that if reading is denied, writing and deleting are also automatically denied.



Registry key or parameter (path or mask)
\REGISTRY\MACHINE\TESTKEY\#**#

Security profile: profile_1

Write: Allow

Delete: Deny

☑ Active

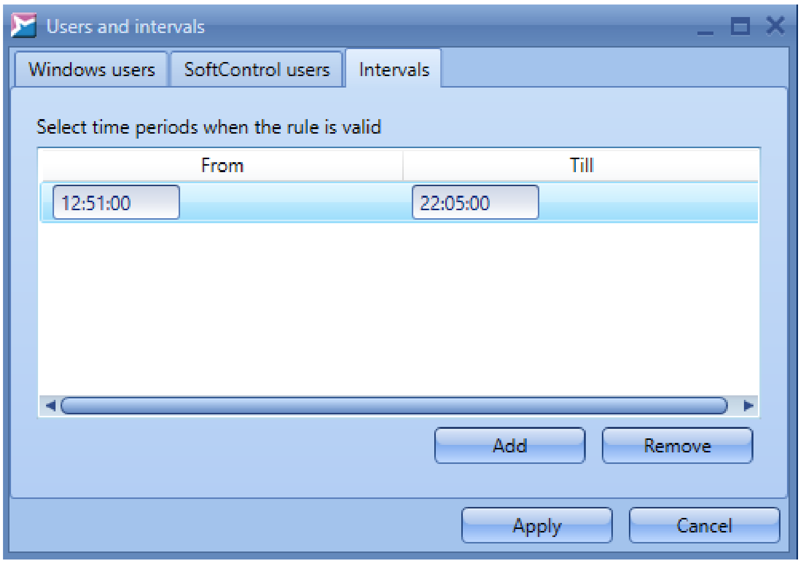
Figure 81. Creating a rule for the system registry object

To add the created rule to the list and make it active, tick off the **Active** checkbox and click **OK**.

To edit a rule, click ✎ (**Change**) and set up the rule parameters, as with the creation of the rule.

To specify when the rule is valid and the users (or groups) it applies to, click ⚙ (**Advanced**). In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Win-**

dows users tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version).



Select time periods when the rule is valid

From	Till
12:51:00	22:05:00

Figure 82. Adding users and intervals for the rule

To delete a rule, click 🗑 (**Delete**).

SoftControl SysWatch contains preset rules that apply to the system registry keys and values that affect the operation of the system and the product components. Changing or deleting preset rules may cause violation of the system integrity protection.

Control policy: Network

Specify the rules that control the application network activity on the client hosts, in the **Control policy** → **Network** section of the **SysWatch** category (fig. Network activity control policy[92]):

- Data receiving;
- Data sending.

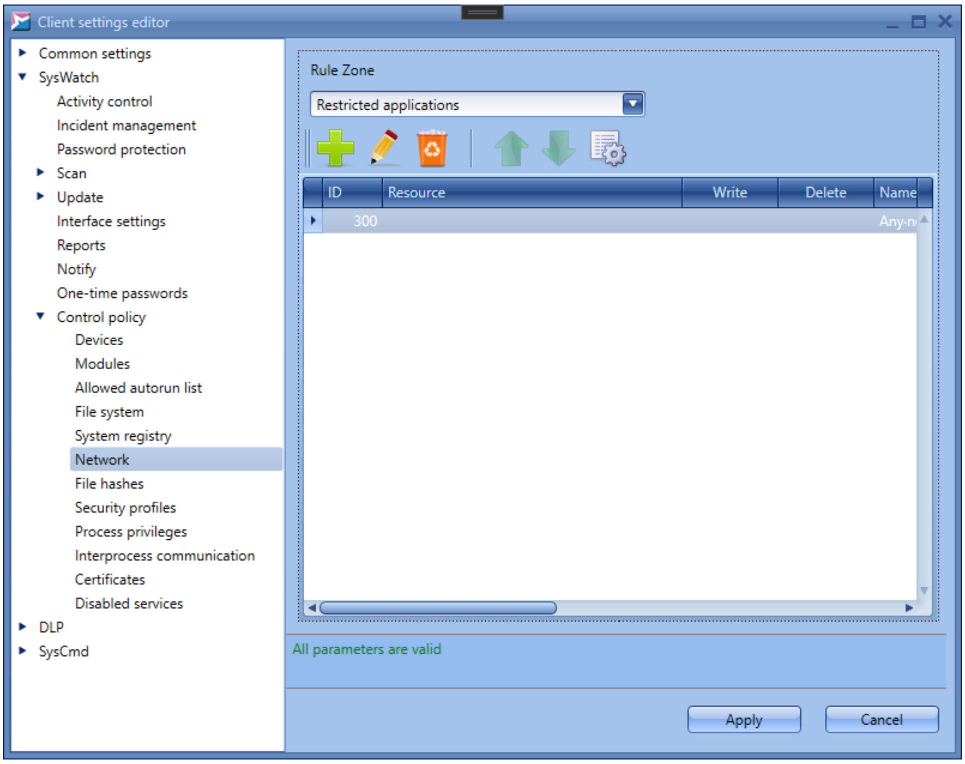
The rules are divided into lists for applications from the following execution zones:

- **Trusted applications**;
- **Restricted applications**.

To switch between the lists, select the corresponding category from the **Rule Zone** drop-down list. If you need to move a rule to the list for applications from another execution zone, invoke the rule's context menu and select one of the options:

- **All** – create a rule for both execution zones, if the rule is only in one list;

- **Restricted** – move a rule to the list for the restricted applications;
- **Trusted** – move a rule to the list for the trusted applications.



Rule Zone: Restricted applications

ID	Resource	Write	Delete	Name
300				Any-n

All parameters are valid

Figure 83. Network activity control policy

Each rule is an entry in the flat list and has its unique **ID**. The rule parameters are specified in the **Name**, **Direction**, and **Protocol** columns. Allowing or blocking network connection is indicated by the checkbox in the **Allow** column. If the event (when it occurs) should be processed by the local user, the checkbox in the **Allow** column is selected. The **Active** checkbox indicates whether this rule is active.

If several rules have overlapping scopes, then the lowest rule in the list has the highest priority of execution. The rule position in the list can be changed by the ⬆ (**Up**) and ⬇ (**Down**).

To create a rule, click ➕ (**Add**).

Specify the rule parameters in the displayed window (fig. Creating a network activity rule 93):

- **Name** is the rule name.
- **Direction** is the direction of the network activity from the point of view of the connection initiator:
  - **Inbound** is network connection initiated by the remote host;
  - **Outbound** is network connection initiated by the local host;
  - **Inbound/Outbound** is any direction.

- **Protocol** is the data transfer protocol:
  - **TCP**;
  - **UDP**;
  - **TCP/UDP** is either of these two.

Endpoints of data transfer on a client and remote hosts are specified on the **Source address** and **Remote address** tabs correspondingly. Select which network addresses and ports the rule applies to on both tabs and type values in the corresponding fields in a case of need:

- **Address** is the IP address of a host:
  - **Any address**;
  - **Specific address**;
  - **Address range**.
- **Port** is the network port:
  - **Any port**;
  - **Specific port**;
  - **Port range**.

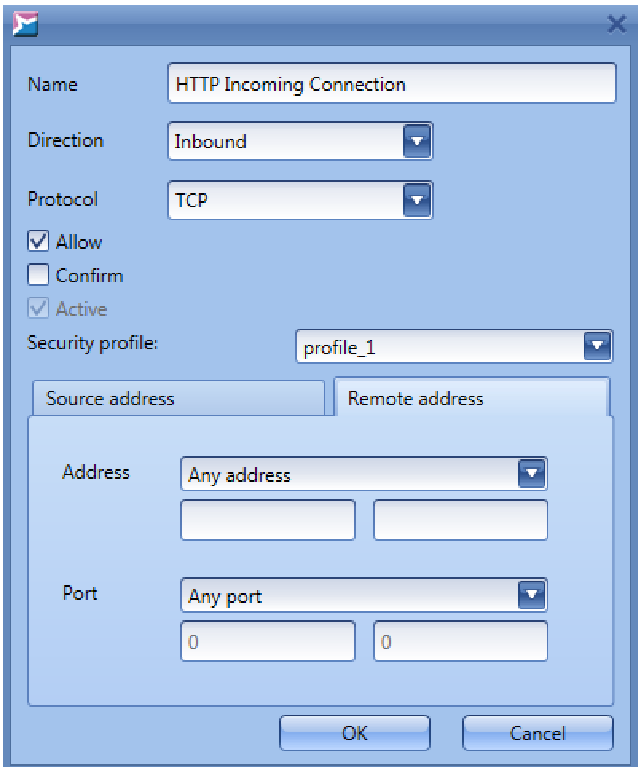

Name: HTTP Incoming Connection
Direction: Inbound
Protocol: TCP
☑ Allow
□ Confirm
☑ Active
Security profile: profile_1
Source address | Remote address
Address: Any address
Port: Any port
0 0

Figure 84. Creating a network activity rule

To enable network connection with the specified parameters, tick off the **Allow** checkbox; to deny the connection, deselect the checkbox. If it is assumed that the local user on a client host processes the application network activity incidents, tick off the **Confirm** checkbox (automatic processing of incidents[67] should be disabled).

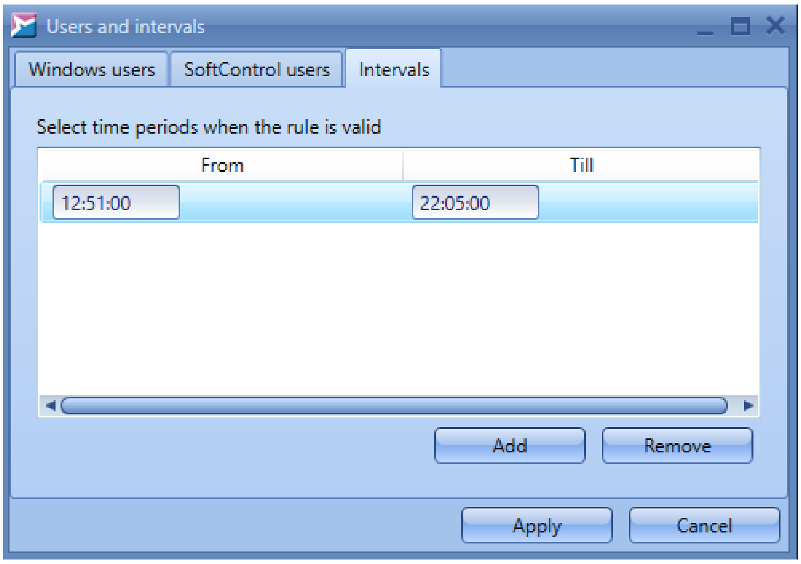
Select the security profile for the rule[95] in the corresponding drop-down list.

Note. You can only tick off or deselect the **Active** filed if you select the default profile (**No group**). If you select any other profile you created yourself, the field is disabled. The value of the field is the same as the value of the corresponding field in the **Control policy** → **Security profile** section.

To add the created rule to the list and make it active, tick off the **Active** checkbox and click **OK**.

To edit a rule, click (**Change**) or double-click on it and set up the rule parameters, as with the rule creation.

To specify when the rule is valid and the users (or groups) it applies to, click (**Advanced**). In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Windows users** tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version). To confirm changes, click **Apply**.



Select time periods when the rule is valid

From	Till
12:51:00	22:05:00

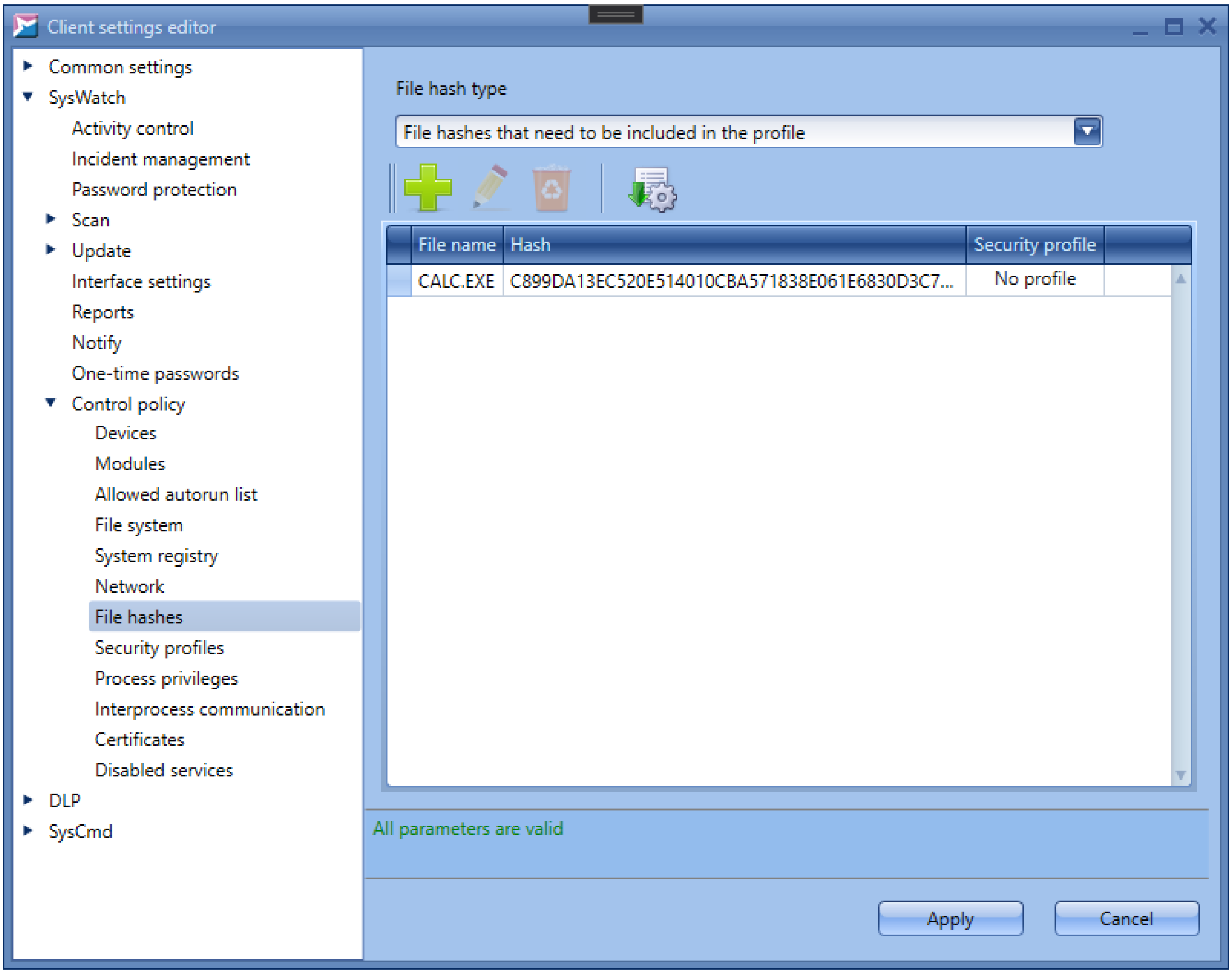
Figure 85. Adding users and intervals for the rule

To delete a rule, click (**Delete**).

Control policy: File hashes

In the **Control policy** → **File hashes** section, you can create a list of file hashes that need to be included in the profile, as well as a list of hashes that need to be excluded from the profile. These checksums are applied to the profile once, but the settings may be modified later, e.g., if you launch an installer.

You can add file checksums by using either the **Add** button or the **Import** button (to upload an XML file). You can copy file hashes from Profile information[46] and Profile comparison[167] tabs.



File hash type: File hashes that need to be included in the profile

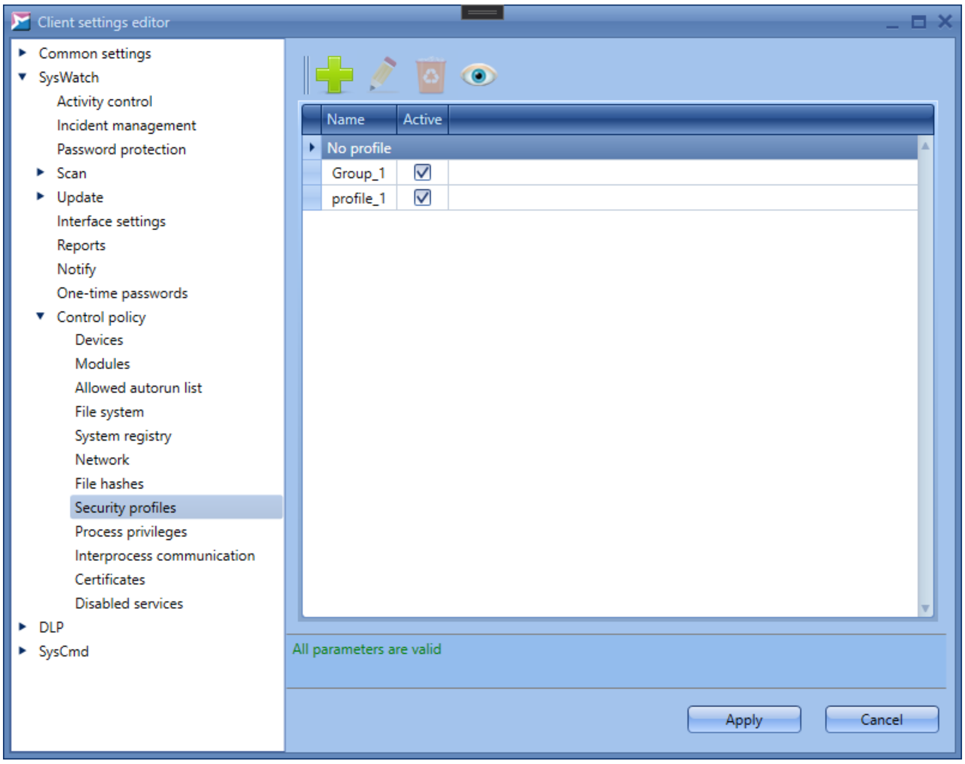
File name	Hash	Security profile
CALC.EXE	C899DA13EC520E514010CBA571838E061E6830D3C7...	No profile

All parameters are valid

Figure 86. File hashes

Control policy: Security profiles

In the **Control policy** → **Security profiles** section of the **SysWatch** category, you can load the security profiles from the SoftControl Service Center database. The security profiles group the activity control rules from different categories (fig. Security profiles[95]). You can create the profiles on the Security profiles[113] tab.

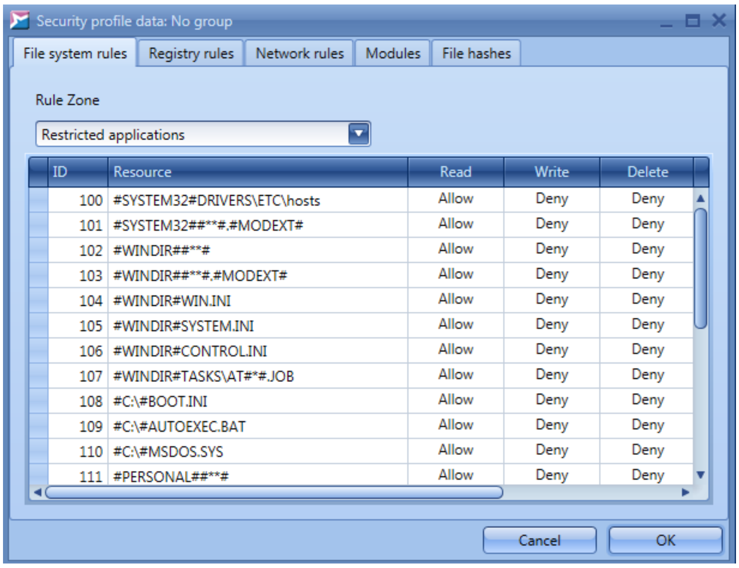


Name	Active
No profile	
Group_1	☑
profile_1	☑

All parameters are valid

Figure 87. Security profiles

The window contains a read-only profile by default (**No group**). The profile includes all file system, system registry, network and modules rules that are available in the corresponding sections of the settings windows (see figures File system control policy [86], System registry control policy [89], Network activity control policy [92] and Modules control policy [81]). You can neither edit nor remove the rules from this profile. To view profile details, double click on it or click 👁 (**View**).

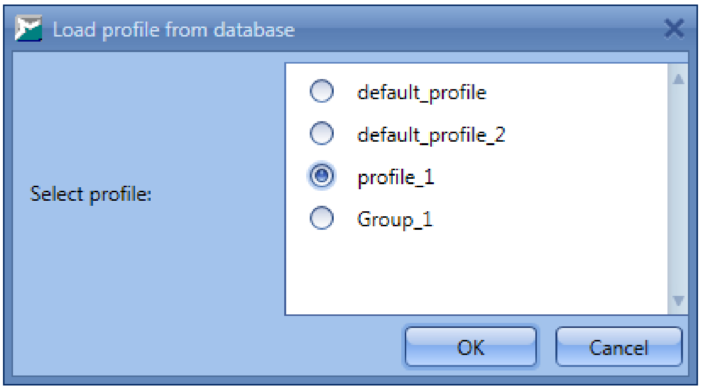


Rule Zone: Restricted applications

ID	Resource	Read	Write	Delete
100	#SYSTEM32#DRIVERS\ETC\hosts	Allow	Deny	Deny
101	#SYSTEM32##**#.#MODEXT#	Allow	Deny	Deny
102	#WINDIR##**#	Allow	Deny	Deny
103	#WINDIR##**#.#MODEXT#	Allow	Deny	Deny
104	#WINDIR#WIN.INI	Allow	Deny	Deny
105	#WINDIR#SYSTEM.INI	Allow	Deny	Deny
106	#WINDIR#CONTROL.INI	Allow	Deny	Deny
107	#WINDIR#TASKS\AT#*#.JOB	Allow	Deny	Deny
108	#C:\#BOOT.INI	Allow	Deny	Deny
109	#C:\#AUTOEXEC.BAT	Allow	Deny	Deny
110	#C:\#MSDOS.SYS	Allow	Deny	Deny
111	#PERSONAL##**#	Allow	Deny	Deny

Figure 88. Default security profile

To load a profile from the database, click ✚ (**Load**). Select the required profile in the displayed window (fig. Loading a security profile (97)).


Load profile from database

Select profile:

○ default_profile
○ default_profile_2
● profile_1
○ Group_1

Figure 89. Loading a security profile

If a profile with the select name already exists in the current settings, an error message is displayed and the process terminates.

To add a rule of a certain category to a profile, perform the following operations.

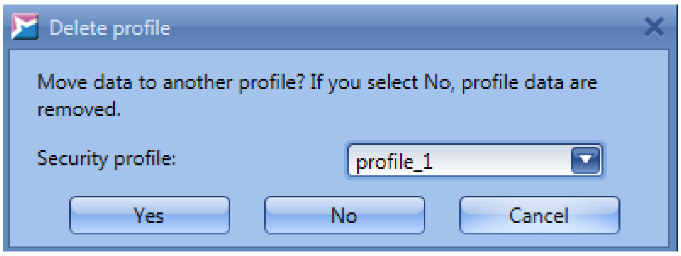
1. Go to the corresponding section of the SoftControl SysWatch settings.
2. Create a new rule or edit an existing one.
3. In the **Creating a new rule** window, select the required profile from the drop-down list (see figures Creating a rule for the file system object (87), Creating a rule for the system registry object (90), Creating a network activity rule (93)).
4. Click **OK**.

To remove a rule of a certain category from the profile, go to the corresponding section of the SoftControl SysWatch settings and delete the rule in that section.

To rename a profile, click ✎ (**Rename**) and specify the new profile name in the displayed window.

To view profile details, select the profile and click 👁 (**View**). The displayed window contains detailed profile information divided into rule categories (see fig. Default security profile (96)).

To delete a security profile, click 🗑 (**Delete**). If you need to save the rules from the profile, select a profile to move the rules to in the displayed window and click **Yes** (fig. Deleting a profile (97)). Otherwise, click **No**; all the rules are deleted in this case.


Delete profile

Move data to another profile? If you select No, profile data are removed.

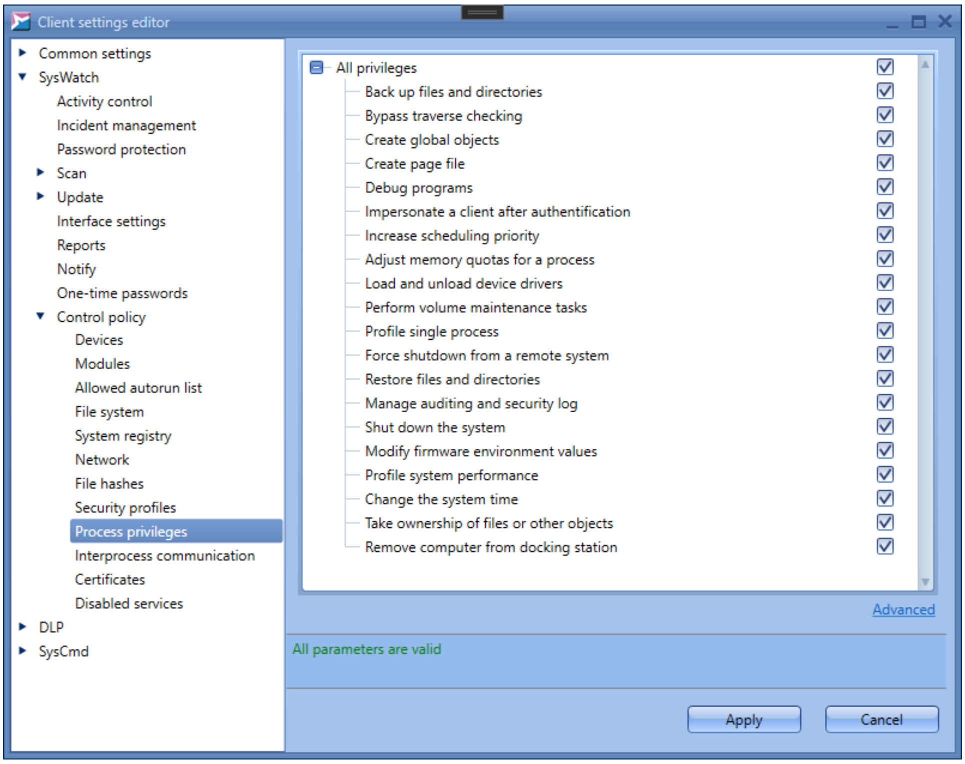
Security profile: profile_1

Figure 90. Deleting a profile

Control policy: Process privileges

In the **Control policy** → **Process privileges** section of the **SysWatch** category, specify the restrictions on the use of the following Windows privileges by processes on client hosts (fig. Process privileges control policy 98):

- Back up files and directories;
- Bypass traverse checking;
- Create global objects;
- Create page file;
- Debug programs;
- Impersonate a client after authentication;
- Increase scheduling priority;
- Adjust memory quotas for a process;
- Load and unload device drivers;
- Perform volume maintenance tasks;
- Profile single process;
- Force shutdown from a remote computer;
- Restore files and directories;
- Manage auditing and security log;
- Shut down the system;
- Modify firmware environment values;
- Profile system performance;
- Change the system time;
- Take ownership of files or other objects;
- Remove computer from docking station.



- All privileges ☑
  - Back up files and directories ☑
  - Bypass traverse checking ☑
  - Create global objects ☑
  - Create page file ☑
  - Debug programs ☑
  - Impersonate a client after authentification ☑
  - Increase scheduling priority ☑
  - Adjust memory quotas for a process ☑
  - Load and unload device drivers ☑
  - Perform volume maintenance tasks ☑
  - Profile single process ☑
  - Force shutdown from a remote system ☑
  - Restore files and directories ☑
  - Manage auditing and security log ☑
  - Shut down the system ☑
  - Modify firmware environment values ☑
  - Profile system performance ☑
  - Change the system time ☑
  - Take ownership of files or other objects ☑
  - Remove computer from docking station ☑

All parameters are valid

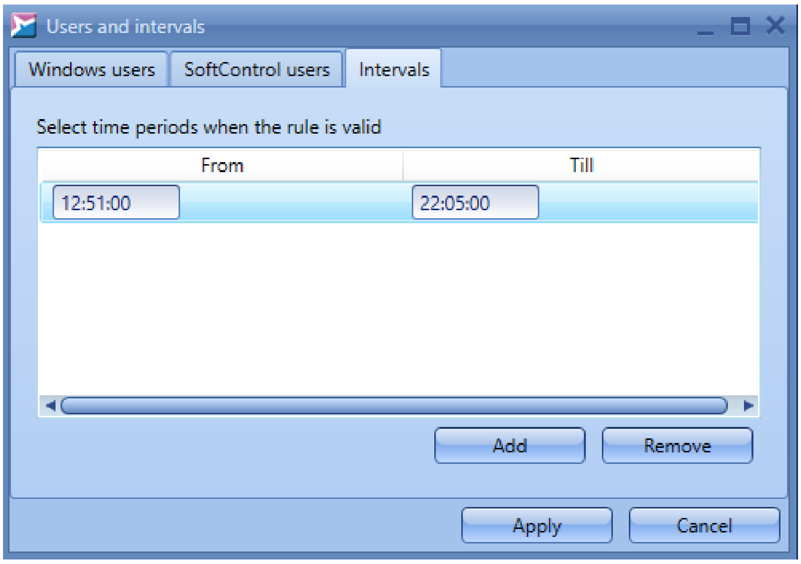
Figure 91. Process privileges control policy

Condition: the rules apply to all applications from the restricted execution zone.

By default, the applications (processes) have all the above-mentioned privileges; however, they can be limited by the OS. To restrict privileges manually, deselect checkboxes at the required privileges.

For description of the privileges and how they are applied, see section Supplemental information[212].

To specify when the rule is valid and the users (or groups) it applies to, click (**Advanced**). In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Windows users** tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version). To confirm changes, click **Apply**.



Select time periods when the rule is valid

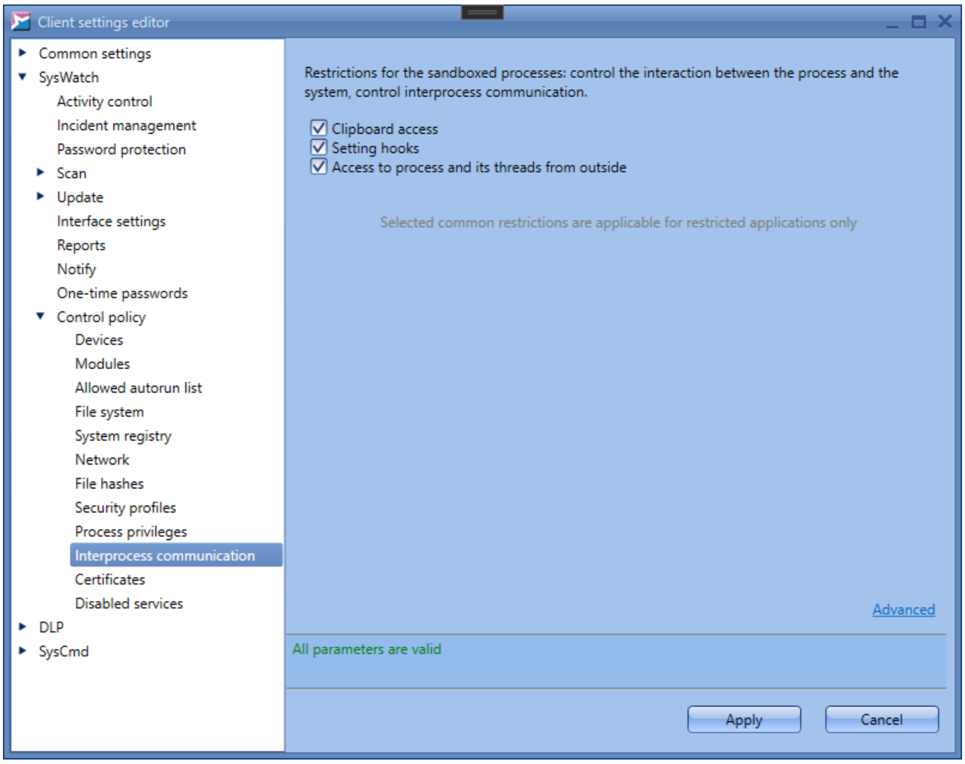
From	Till
12:51:00	22:05:00

Figure 92. Adding users and intervals for the rule

Control policy: Interprocess communication

In the **Control policy** → **Interprocess communication** section of the **SysWatch** category, specify the following permissions for interprocess communication (fig. Process interaction control policy[100]):

- Accessing the clipboard;
- Setting the hooks by an application;
- Accessing the process and its threads from the outside.



Restrictions for the sandboxed processes: control the interaction between the process and the system, control interprocess communication.

☑ Clipboard access
☑ Setting hooks
☑ Access to process and its threads from outside

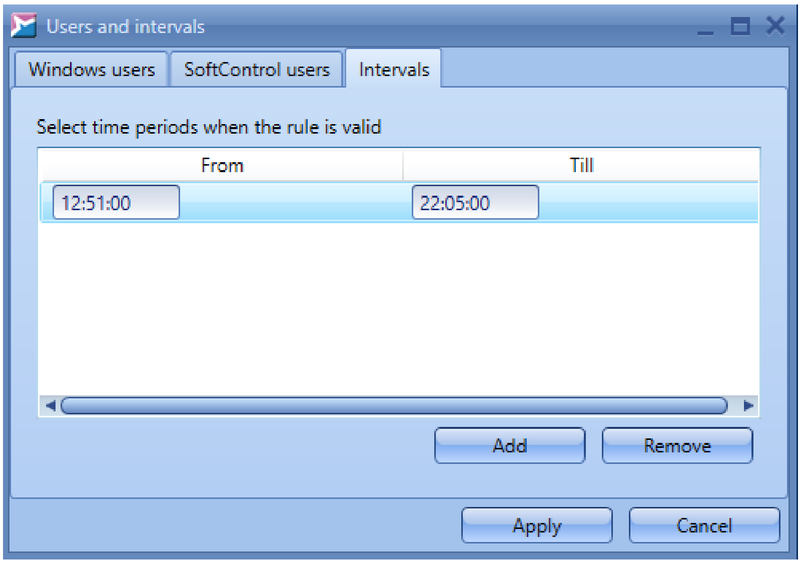
Selected common restrictions are applicable for restricted applications only

All parameters are valid

Figure 93. Process interaction control policy

Condition: the rules apply to the applications from the restricted zone that run under the V.I.P.O. user account.

To specify when the rule is valid and the users (or groups) it applies to, click **Advanced**. In the displayed window, set the time intervals on the **Intervals** tab and add users on the **Windows users** tab with the help of the **Add** button (functionality of the **SoftControl users** tab has not been implemented in the current version). To confirm changes, click **Apply**.



Select time periods when the rule is valid

From	Till
12:51:00	22:05:00

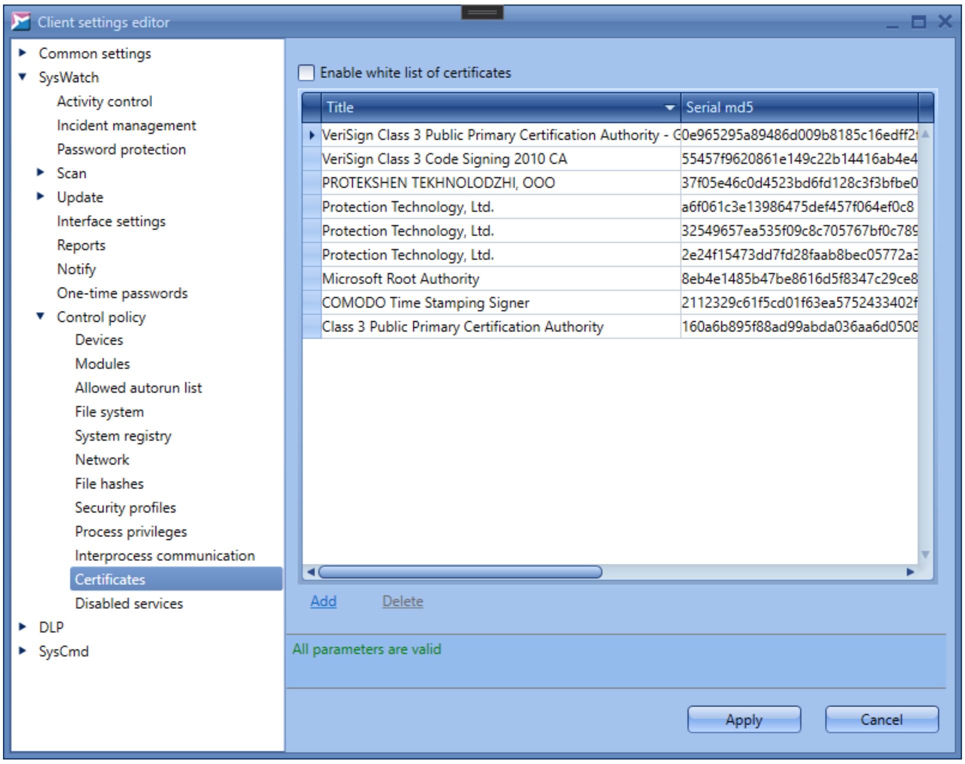
Figure 94. Adding users and intervals for the rule

Control policy: Certificates

Specify the whitelist of certificates for additional process activity control on client hosts, in the **Control policy** → **Certificates** section of the **SysWatch** category (fig. The whitelist of certificates[102]).

When an application runs, SoftControl SysWatch heuristically determines whether it is an installer or a script. By default, the installer runs in software update mode if it has a valid digital signature. Besides, it is possible to check whether a digital signature certificate is in the whitelist. To do so, tick off the **Enable whitelist of certificates** and create the list.

Initially, SoftControl SysWatch contains the basic list of the certificates by trusted vendors, including certificates by Protection Technology, Ltd. To add a new certificate to the list, click **Add** and specify an application, an installer or a script with the digital signature with the certificate to be included in the list, and then click **Open**. Tick off the boxes for the required certificates of the selected file in the **Add** column of the displayed window and click **OK** (fig. Selecting certificates to add[102]). Tick off the box in the **Trust** column for the added certificates (fig. The whitelist of certificates[102]).

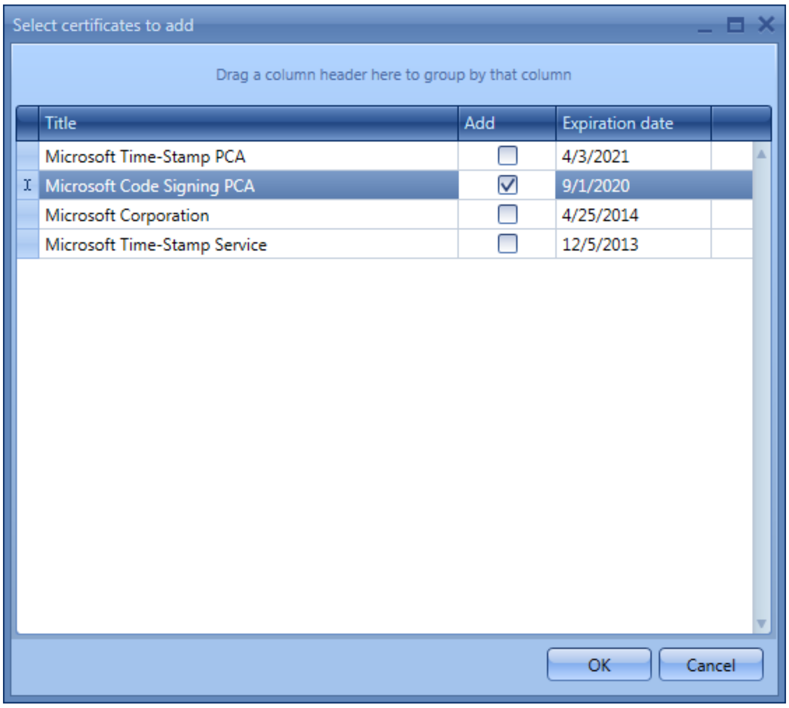


☐ Enable white list of certificates

Title	Serial md5
VeriSign Class 3 Public Primary Certification Authority - G	0e965295a89486d009b8185c16edff2
VeriSign Class 3 Code Signing 2010 CA	55457f9620861e149c22b14416ab4e4
PROTEKSHEN TEKHNOLODZHI, OOO	37f05e46c0d4523bd6fd128c3f3bfbe0
Protection Technology, Ltd.	a6f061c3e13986475def457f064ef0c8
Protection Technology, Ltd.	32549657ea535f09c8c705767bf0c789
Protection Technology, Ltd.	2e24f15473dd7fd28faab8bec05772a
Microsoft Root Authority	8eb4e1485b47be8616d5f8347c29ce8
COMODO Time Stamping Signer	2112329c61f5cd01f63ea5752433402f
Class 3 Public Primary Certification Authority	160a6b895f88ad99abda036aa6d0508

All parameters are valid

Figure 95. The white list of certificates


Select certificates to add
Drag a column header here to group by that column
OK
Cancel

Title	Add	Expiration date
Microsoft Time-Stamp PCA	□	4/3/2021
Microsoft Code Signing PCA	☑	9/1/2020
Microsoft Corporation	□	4/25/2014
Microsoft Time-Stamp Service	□	12/5/2013

Figure 96. Selecting certificates to add

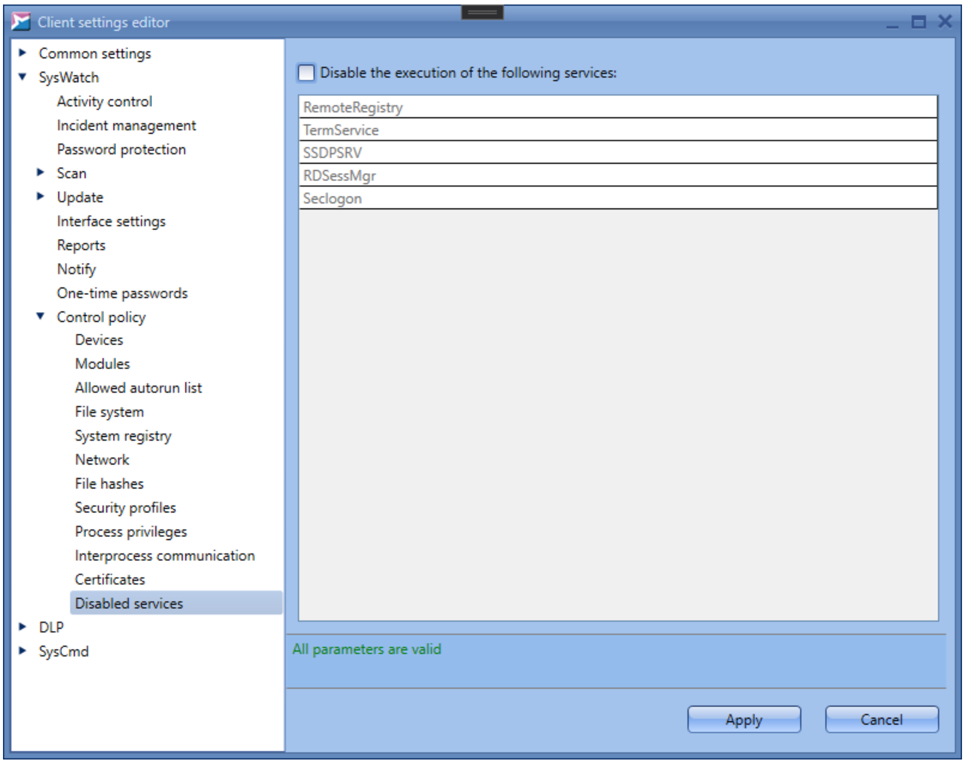
If you want to remove a certificate from the list of trusted certificates without deleting it, deselect the checkbox in the **Trust** column. To delete the certificate from the list completely, select it and click the **Delete** link (fig. The whitelist of certificates[102]).

Control policy: Disabled services

You can select services that should be blocked on the client hosts, in the **Control policy** → **Disabled services** section of the **SysWatch** category.

The following services are disabled by default: *RemoteRegistry*, *TermService*, *SSDPSRV*, *RDSessMgr*, and *Seclogon* (fig. Disabled services[103]). To add more services to the list, tick off **Disable following services execution**, enter the name of a service in the displayed cell and press **Enter**.

After you apply the settings on the client host, the status of the services from the list becomes *Disabled*. If a services has been running when the settings were applied, it continues to run.



□ Disable the execution of the following services:

RemoteRegistry
TermService
SSDPSRV
RDSessMgr
Seclogon

All parameters are valid

Figure 97. Disabled services

You can only enable the services from the list manually.

4.6.3 SoftControl DLP Client settings

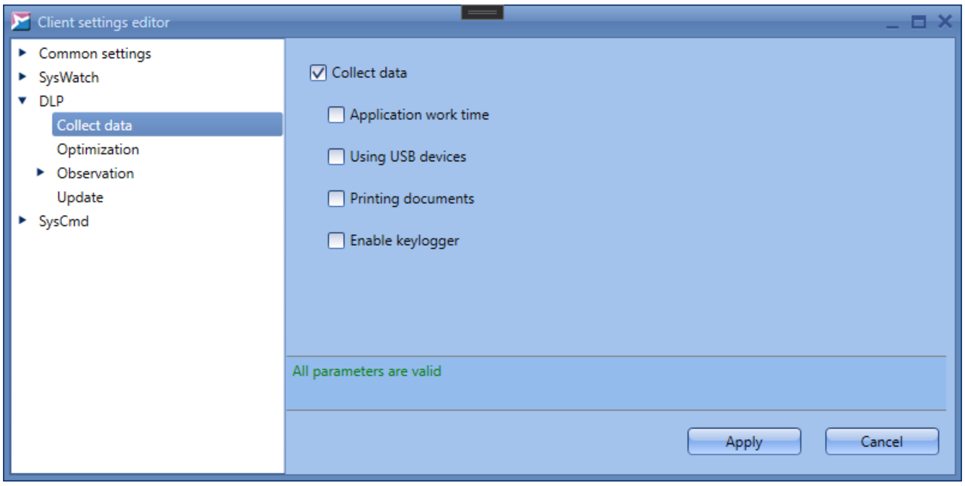
This category of settings includes the configuration of the SoftControl DLP Client component.

Collect data

Tick off **Collect data** in the **Collect data** section of the **DLP** category and select the required scopes of information (fig. Data collection settings[105]):

- ❑ **Application work time**;
- ❑ **Using USB devices**;
- ❑ **Printing documents**;
- ❑ **Enable keylogger**.

Observation over file system[105], system registry[107] and network traffic[109] is active if **Collect data** is checked and the rules are added to the corresponding subsections in the **Observation** section.



☑ Collect data

□ Application work time

□ Using USB devices

□ Printing documents

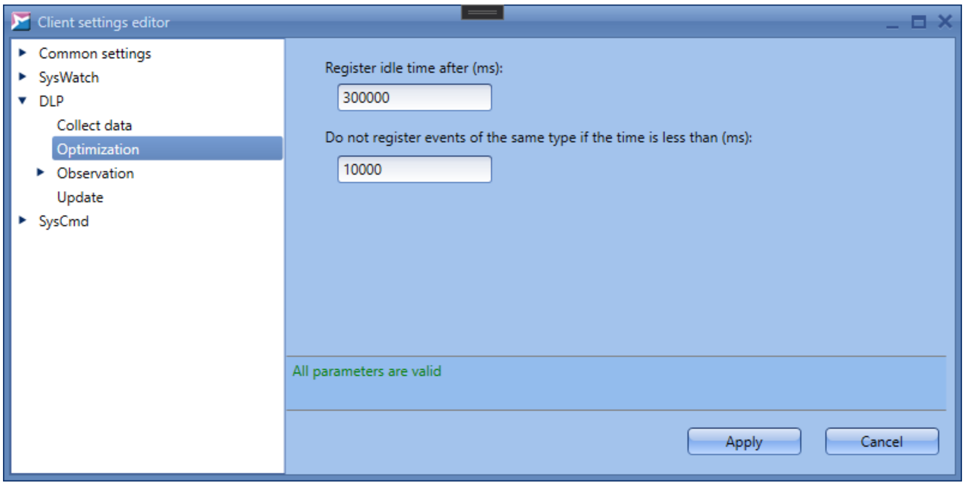
□ Enable keylogger

All parameters are valid

Figure 98. Data collection settings

Optimization

Time parameters of the event registration are specified in the **Optimization** section of the **DLP** category (fig. Optimization settings[105]).



Register idle time after (ms): 300000

Do not register events of the same type if the time is less than (ms): 10000

All parameters are valid

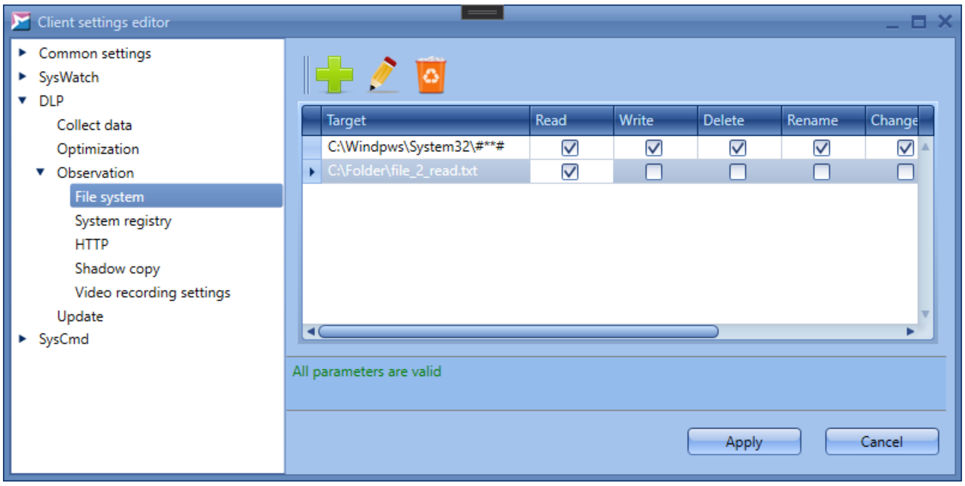
Figure 99. Optimization settings

Enter the **Register idle time after (ms)** and **Do not register events of the same type if the time is less than (ms)** time intervals in the corresponding fields (in milliseconds).

Note: the **Do not register events of the same type if the time (ms) is less than** option only applies when monitoring the file system resources. The **Register idle time after (ms)** option works when the **Application work time** option is enabled (see fig. Data collection settings[105]) and measures the time when an application is idle, i.e. when the user does not click any buttons or moves the mouse for the specified period.

Observation: File system

You can select the file system objects to monitor, in the **Observation** → **File system** section of the **DLP** category (fig. File system monitoring settings[106]).



Target	Read	Write	Delete	Rename	Change
C:\Windpws\System32\#**#	☑	☑	☑	☑	☑
C:\Folder\file_2_read.txt	☑	□	□	□	□

All parameters are valid

Figure 100. File system monitoring settings

To add an object to monitor, click ✚ (**Add**) and enter the full path to it in the displayed window (fig. Object under observation[107]).

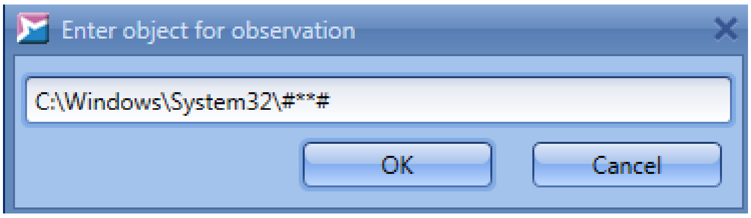
You can use masks to create rules for the group of file system objects. For example, you can create a rule for a folder and all the objects inside it, or a rule for certain file types (extensions). Below is the mask syntax:

- **#*#** – mask replaces any number of characters except the '\' symbol (if the mask is placed at the end of the string, the rule affects only root directory files);
- **#**#** –- mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects root directory files, subdirectories and subdirectories files);
- **#?#** – mask replaces exactly one character (any character).

For example, to enable observation of a folder and all included objects, add the #**# characters at the end of the string. Click **OK** to add the specified object to the list.

You can specify local folders as well as network folders. When you create a rule for network folders, the path is specified as follows: \\<*server_name*>\<*folder_name*>. You can use the **#**#** mask instead of '\\'. In this case, SoftControl SysWatch checks both network and local folders. Besides, you can specify IP address of the computer with the network folder.

> If you specify the computer's IP address in the rule, the rule is only valid when the user enters IP address to access the folder. It is not valid when the user enters the network path. Therefore, if you need to monitor the folders that the users access by both IP address and network path, create separate rules for each of the notations.



C:\Windows\System32\#**#

Figure 101. Object for observation

To change the path to the object, select it from the list and click ✎ (**Change**). To delete an object from observation, select it and click 🗑 (**Delete**).

For each of the objects, you can select the following operations that should be registered in reports:

- ❑ **Read**;
- ❑ **Write**;
- ❑ **Delete**;
- ❑ **Rename**;
- ❑ **Change**.

If an object is renamed on a client host, it is not monitored anymore.

The **Write** operation is registered when a new file is created with writing access rights. If the file already existed the **Change** operation is registered.

When the **Shadow copy** option is selected, a backup copy of the object under observation is saved before the object is modified, if the shadow copying (110) global option is enabled and **Delete** or **Change** fields are ticked off. If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters (110) when an incident occurs.

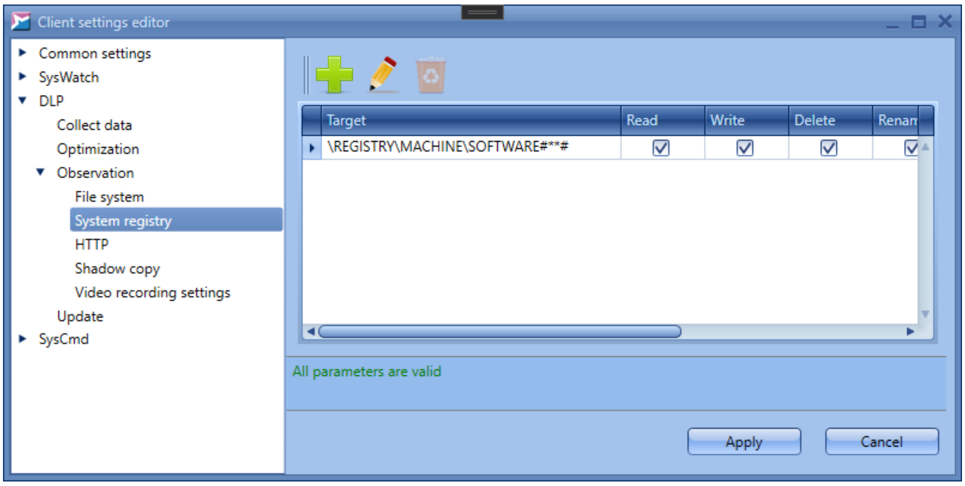
Observation: System registry

You can select the system registry objects to monitor, in the **Observation** → **Registry** section of the **DLP** category (fig. System registry monitoring settings (108)).

To add an object to monitor, click ✚ (**Add**) and enter the full path to it in the displayed window (fig. Object under observation (108)). The registry root keys in the specified path should be assigned as follows:

- *\REGISTRY\MACHINE\SOFTWARE\CLASSES\* – the HKEY_CLASSES_ROOT key;
- *\REGISTRY\MACHINE\* – the HKEY_LOCAL_MACHINE key;

- *\REGISTRY\USER\<SID>* – the HKEY_CURRENT_USER key for the user with the specified security identifier (<SID>);
- *\REGISTRY\USER\* – the HKEY_USERS key.



Target	Read	Write	Delete	Renam
\REGISTRY\MACHINE\SOFTWARE#**#	☑	☑	☑	☑

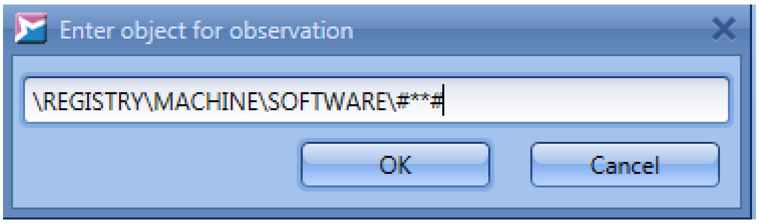
All parameters are valid

Figure 102. System registry monitoring settings

You can use masks to create rules for the group of system registry objects. For example, you can create a rule for a registry key and all objects inside it. Below is the mask syntax:

- **#*#** – the mask replaces any number of characters except for the '\' symbol (if the mask is placed at the end of the string, the rule affects only the key values);
- **#**#** – the mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects the key values, subkeys and subkeys values);
- **#?#** – the mask replaces exactly one character (any character).

For example, to enable observation of the registry key and all included objects, add the #**# characters at the end of the string. Click **OK** to add the specified object to the list.



\REGISTRY\MACHINE\SOFTWARE\#**#

Figure 103. Object for observation

To change the path to the object, select it from the list and click ✎ (**Change**). To delete an object from observation, select it and click 🗑 (**Delete**).

For each of the objects, you can select the following operations that should be registered in reports:

- ❑ **Read**;

□ **Write**;

□ **Delete**;

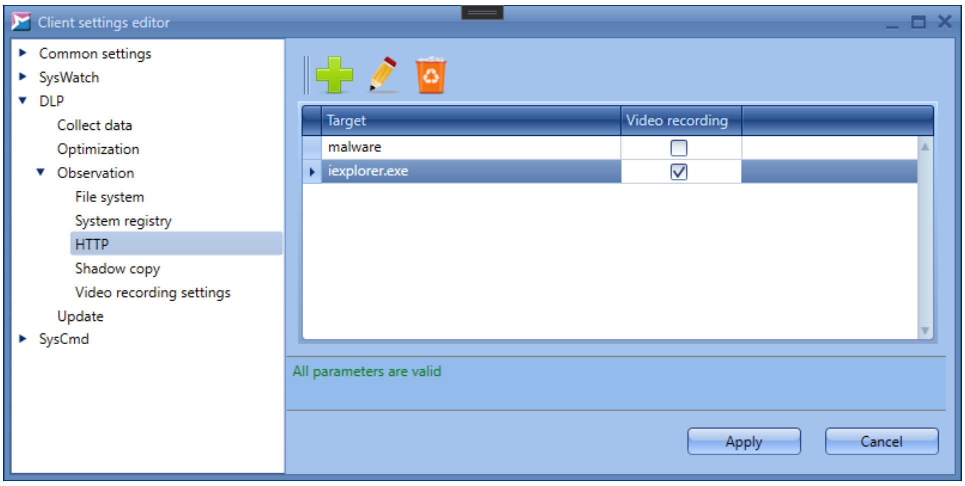
□ **Rename**.

If an object is renamed on a client host, it is not monitored anymore.

When the **Shadow copy** option is selected, a backup copy of the object under observation is saved before the object is modified, if the shadow copying [110] global option is enabled and **Delete** or **Write** fields are ticked off. If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters [110] when an incident occurs.

Observation: HTTP traffic

You can specify the network traffic data to be monitored, in the **Observation** → **HTTP** section of the **DLP** category (fig. Network traffic monitoring settings [109]).

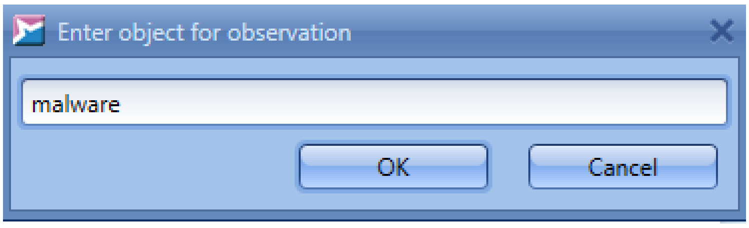


Target	Video recording
malware	□
iexplorer.exe	☑

All parameters are valid

Figure 104. Network traffic monitoring settings

To add data to monitor, click ✚ (**Add**) and enter a string in the displayed window (fig. Object under observation [109]). The presence of the specified text is traced during data transfer over the HTTP protocol. For example, it can be user's requests in search engines via an internet browser, or the name of the file transferred via the network. Click **OK** to add the string to the list.



malware

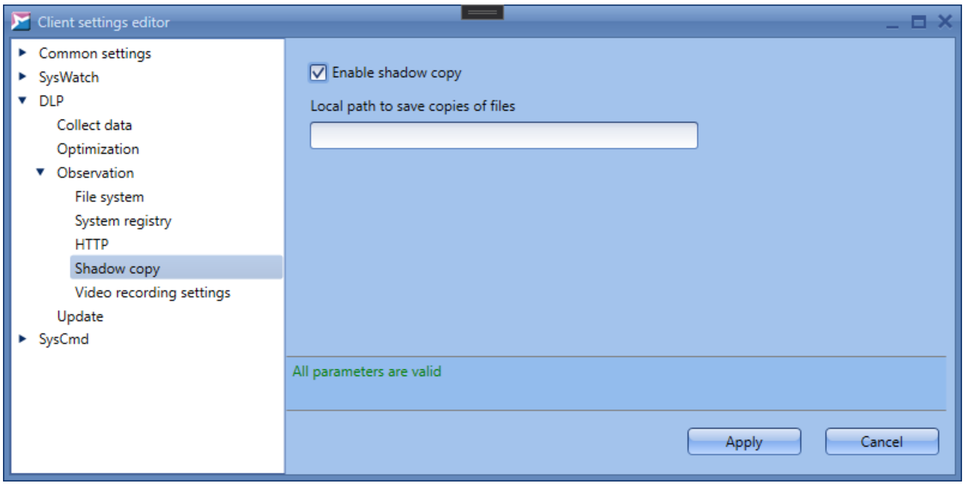
Figure 105. Object for observation

To change the traced text, select a string from the list and click ✎ (**Change**). To delete a text from observation, select a string and click 🗑 (**Delete**).

If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters[110] when an incident occurs.

Observation: Shadow copy

In the **Observation** → **Shadow copy** section of the **DLP** category, you can set up the saving of the shadow copies of the objects under observation (fig. Shadow copying settings[110]).



☑ Enable shadow copy

Local path to save copies of files

All parameters are valid

Figure 106. Shadow copying settings

Tick off the **Enable shadow copy** checkbox to enable the backups of the file system[105] and system registry[107] objects under observation, when the objects are modified (fig. Shadow copying settings[110]). You can enable the option for certain objects in the observation properties. Shadow copies of the objects are sent to the server and are available in the management console. They are also saved locally on the client hosts with the installed SoftControl DLP Client, by the path specified in the **Local path to save copies of files** field, or to the following default folder if no path is specified:

```
<SoftControl DLP Client installation folder>\Backups
```

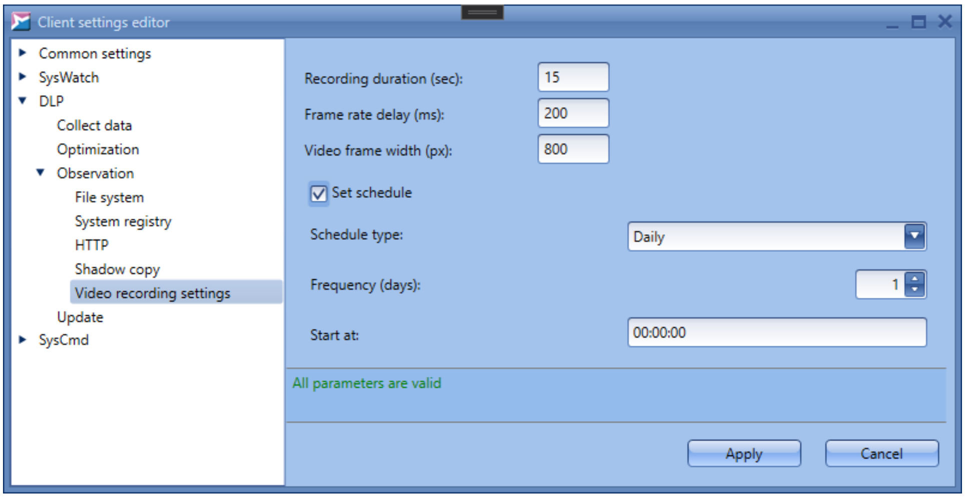
Observation: Video recording settings

In the **Observation** → **DLP video settings** section of the **DLP** category, you can set up the screen shots when the events under observation occur (fig. Video recording settings[111]).

Specify the following record parameters:

- **Recording duration** – duration of screen capturing, starting from the moment the event occurs (value range: 5 - 60 s);

- **Frame rate delay** – time interval between the screen captures (value range: 50 - 500 ms);
- **Video frame width** – screen shot width in pixels (value range: 0 - 1920).



Recording duration (sec): 15

Frame rate delay (ms): 200

Video frame width (px): 800

☑ Set schedule

Schedule type: Daily

Frequency (days): 1

Start at: 00:00:00

All parameters are valid

Figure 107. Video recording settings

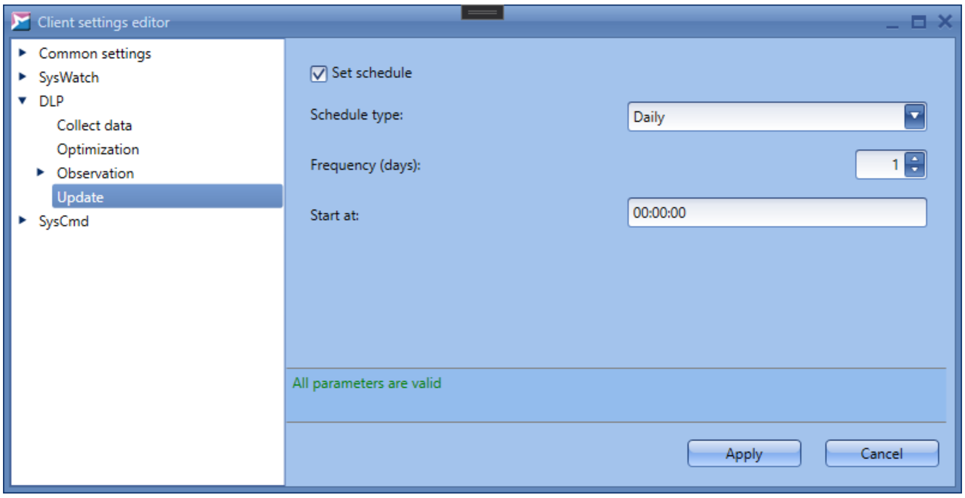
To start recoding the video in real time, right-click the required SoftControl DLP Client component on the Clients[42] tab and select **Start video recording** in the context menu.

You can enable video recording on schedule by ticking off **Set schedule**. Specify the following recording options:

- **Schedule type** – daily or hourly;
- **Frequency (days/hours)** – how often the task should run;
- **Invoke time** – time when the task should start (as *hh:mm:ss*).

Update settings

You can set the update schedule in the **Update** section of the **DLP** category. To do so, tick off the **Set schedule** checkbox and specify the parameters (fig. Update schedule settings[111]).



☑ Set schedule

Schedule type: Daily

Frequency (days): 1

Start at: 00:00:00

All parameters are valid

Figure 108. Update schedule settings

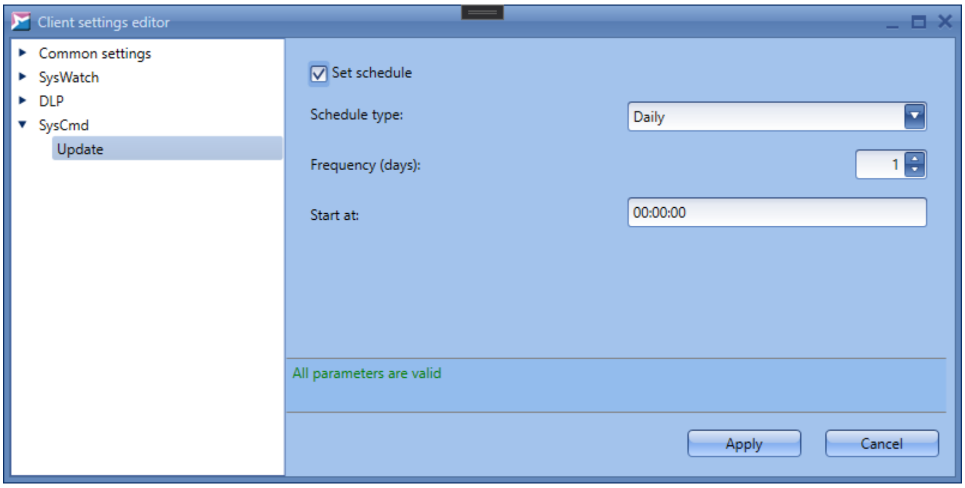
Select the **Schedule type** (daily or hourly), specify the frequency of the task in the **Frequency (days/hours)** counter, and the start time in *hh:mm:ss* format in the **Invoke time** field.

4.6.4 SoftControl SysCmd settings

This category of settings includes the configuration of the SoftControl SysCmd component.

Update settings

You can set the update schedule in the **Update** section of the **SysCmd** category. To do so, tick off the **Set schedule** checkbox and specify the parameters (fig. Update schedule settings[112]).



☑ Set schedule

Schedule type: Daily

Frequency (days): 1

Start at: 00:00:00

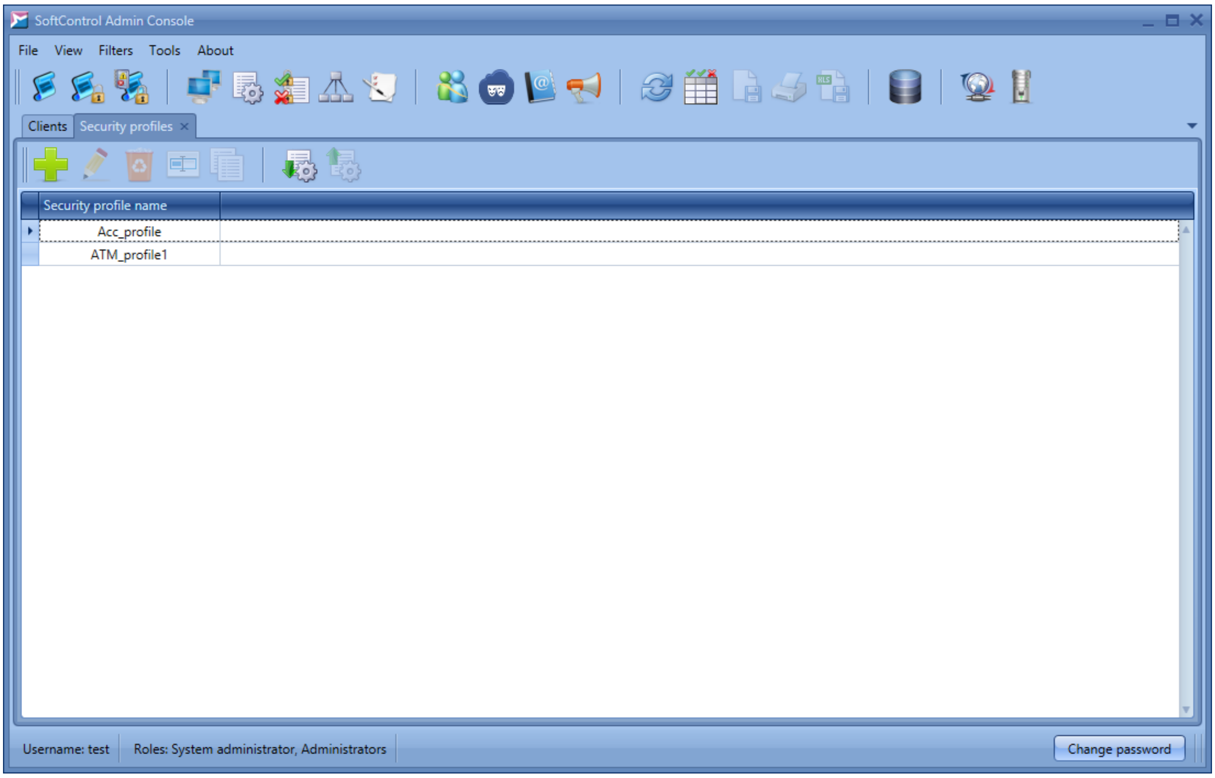
All parameters are valid

Figure 109. Update schedule settings

Select the **Schedule type** (daily or hourly), specify the frequency of the task in the **Frequency (days/hours)** counter, and the start time in *hh:mm:ss* format in the **Invoke time** field.

4.7 Security profiles

The **Security profile** tab allows you to work with the sets of security options (profiles) that include the rules for file system, system registry, network, and modules. The profiles combine activity control rules from different categories. The profiles you create are saved to the SoftControl Service Center database; you can use them in the client application settings (95).



Security profile name
Acc_profile
ATM_profile1

Username: test

Roles: System administrator, Administrators

Figure 110.'Security profiles' tab

Basic operations with the profiles are performed via the tab's graphical buttons that are described in table 17.

Table 17. The 'Security profiles' tab widgets

Button	Name	Description
✚	Add	Create a new security profile.
✎	Change	Modify the selected profile.
🗑	Delete	Remove the selected profile.

Button	Name	Description
	Rename	Rename the selected profile.
	Copy	Save the selected profile with a different name.
	Import	Import a profile from an XML file.
	Export	Export the select profile to an XML file.

Basic operations on this tab are:

Creating a profile

To create a security profile, click ✚ (**Add**) and specify the name of the profile. In the displayed **Security profile data: <profile_name>** window, set the rules for file system, system registry, network, and modules.

For details on how to add activity control rules, see the corresponding parts of the **SoftControl SysWatch settings** section (Control policy: File system [85], Control policy: System registry [88], Control policy: Network activity [91] and Control policy: Modules [81]).

Editing a profile

To modify a security profile, select it and click ✎ (**Change**) (fig. 'Security profiles' tab [113]). Edit the required data in the displayed **Security profile data: <profile_name>** window.

Deleting a profile

To delete a profile, select it, click 🗑 (**Delete**) (fig. 'Security profiles' tab [113]) and confirm the removal in the dialog box.

Renaming a profile

To rename a profile, select it, click (**Rename**) (fig. 'Security profiles' tab [113]) and specify the new name in the displayed window.

Copying a profile

To create a copy of a profile, select it, click (**Copy**) (fig. 'Security profiles' tab [113]) and specify the name of the new profile in the displayed window.

Importing a profile

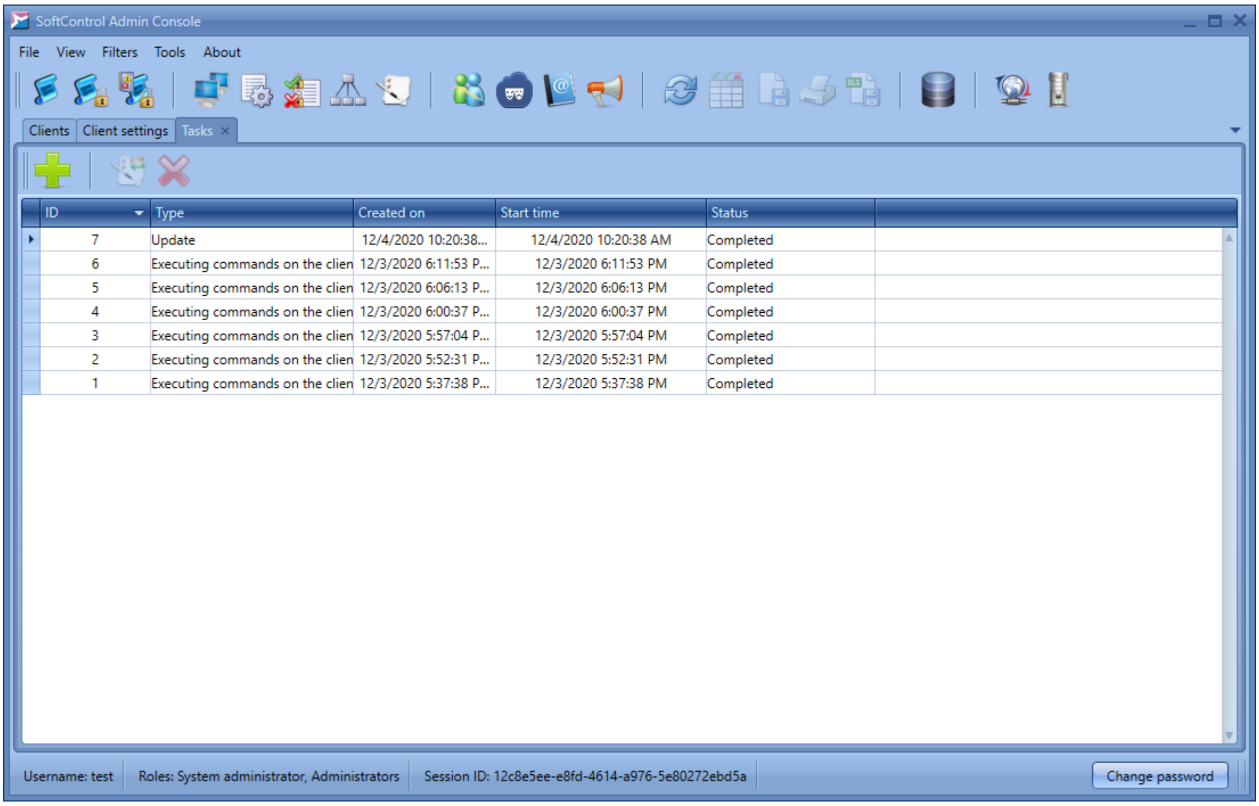
To load a security profile from an XML file, click (**Import**) (fig. 'Security profiles' tab [113]). Specify the name of the XML file in the dialog box and click **OK**.

Exporting a profile

To save a security profile to an XML file, click (**Export**). Specify the name and path of the XML file in the dialog box.

4.8 Tasks

The **Tasks** tab allows you to create tasks for client applications and watch the details of their execution (fig. The 'Tasks' tab [115]).



ID	Type	Created on	Start time	Status
7	Update	12/4/2020 10:20:38...	12/4/2020 10:20:38 AM	Completed
6	Executing commands on the clien	12/3/2020 6:11:53 P...	12/3/2020 6:11:53 PM	Completed
5	Executing commands on the clien	12/3/2020 6:06:13 P...	12/3/2020 6:06:13 PM	Completed
4	Executing commands on the clien	12/3/2020 6:00:37 P...	12/3/2020 6:00:37 PM	Completed
3	Executing commands on the clien	12/3/2020 5:57:04 P...	12/3/2020 5:57:04 PM	Completed
2	Executing commands on the clien	12/3/2020 5:52:31 P...	12/3/2020 5:52:31 PM	Completed
1	Executing commands on the clien	12/3/2020 5:37:38 P...	12/3/2020 5:37:38 PM	Completed

Username: test
Roles: System administrator, Administrators
Session ID: 12c8e5ee-e8fd-4614-a976-5e80272ebd5a

Figure 111. The 'Tasks' tab

The tab contains the list of all tasks and their parameters.

Basic operations with the tasks are performed via the tab's graphical buttons that are described in table 18.

Table 18. The 'Tasks' tab widgets

Button	Name	Description
✚	New	Create a new task for the client components.

Button	Name	Description
	Task status	View the report on the execution of the selected task.
❌	Cancel	Cancel a task in the **Pending** status.

The list of the tab fields is given in table 19.

Table 19. The 'Tasks' tab fields

Field	Description
ID	Task order number.
Type	Task type: • **profile**; • **scan**; • **update;** • **executing commands on the client.**
Created	Data and time of the task creation.
Start time	Date and time of the task start.
Status	Task completion status: • **pending** – none of the client component has started task execution; • **canceled** – task has been canceled before its execution. • **in process** – task execution has been started by at least one client component; • **completed** – task has been completed by all the client components.

Basic operations on this tab are:

Creating a task

To add a new task, click **New** (fig. The 'Tasks' tab [115]). Specify the task parameters depending on its type, in the **New task** window (see figures from The 'Task type' section [118] to The 'Clients' section [122] in section Updating [121]).

- profile gathering [118];
- antivirus scanning [119];
- updating [121];
- executing commands on the client [123].

Viewing task execution details

To view the details of task execution, select it and perform the one of the following operations:

- click **Task status** in the tab buttons group (fig. The 'Tasks' tab [115]);

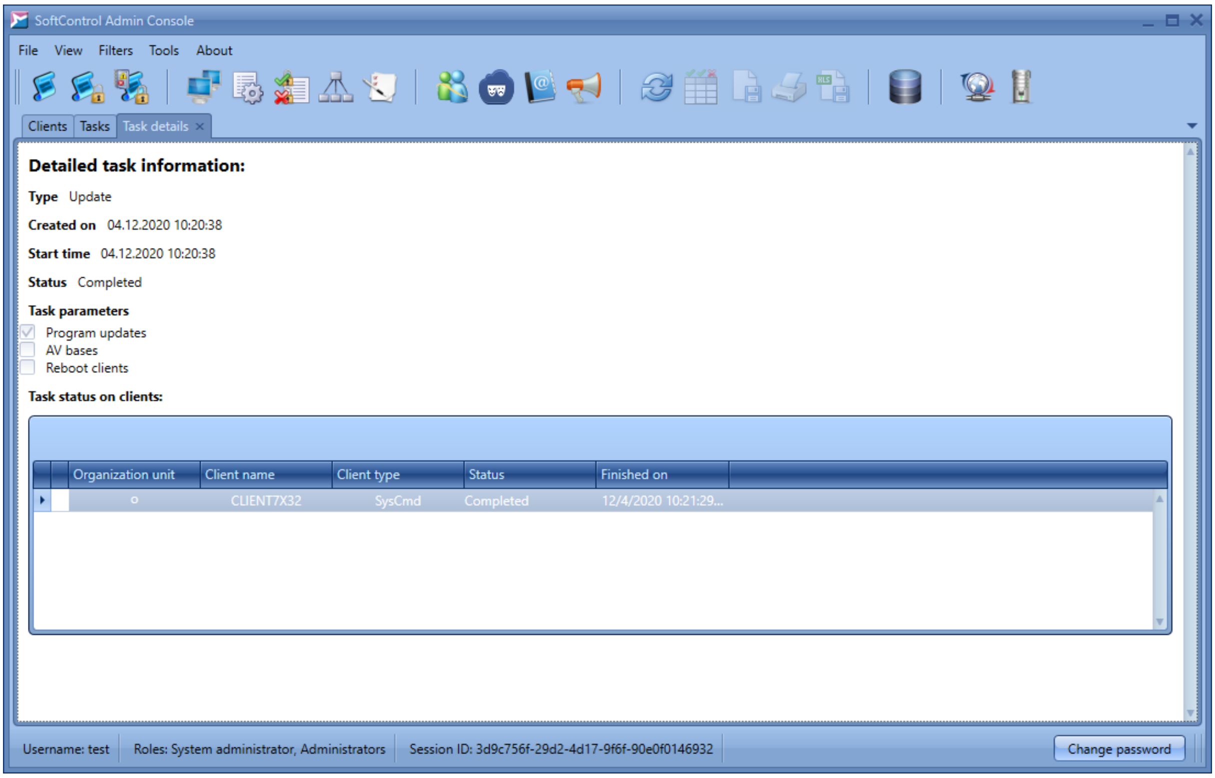
- double-click the task.

The displayed **Task: details** tab contains the detailed information about the task and the status of its execution for each of the client components (fig. Task execution details[117]).

Besides the main information (table 19) and the task parameters, the tab displays the **Status of task on clients** table. Description of its fields is given in table 20.

Table 20. The 'Status of task on clients' table fields

Field	Description
Organization unit	The organization unit which the client component belongs to.
Client name	The name of the client host which client component installed on.
Status	Task completion status: • **pending** – task execution has not started; • **starting** – the task start command has been sent to the client component successfully; • **start error** – the client component could not run the task; • **in process** – the client component is processing the task; • **process error** – an error occurred during task execution; • **canceled** – the task has been canceled; • **completed** – task execution has been finished; • **completion error** – an error occurred during task completion.
End time	The time of task completion on the client host.


SoftControl Admin Console
File View Filters Tools About
Clients Tasks Task details ×
Change password

Detailed task information:

Type Update

Created on 04.12.2020 10:20:38

Start time 04.12.2020 10:20:38

Status Completed

Task parameters

☑ Program updates
□ AV bases
□ Reboot clients

Task status on clients:

Organization unit	Client name	Client type	Status	Finished on
o	CLIENT7X32	SysCmd	Completed	12/4/2020 10:21:29...

Username: test | Roles: System administrator, Administrators | Session ID: 3d9c756f-29d2-4d17-9f6f-90e0f0146932

Figure 112. Task execution details

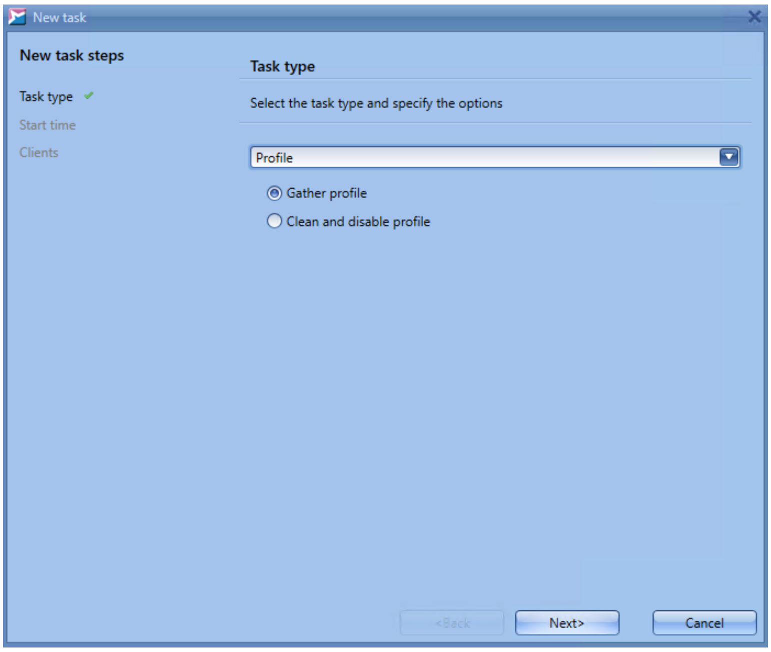
To view the report on the completed operations, go to the **Log** tab and apply filters[144] to the required types of operations. For detailed description of the report for the task **Executing commands on the client** see Executing commands on the client and file exchange[128] section.

4.8.1 Profile gathering

1) Select **Profile** from the drop-down list in the **Task type** section and click **Next** (fig. The 'Task type' section[118]):

   ○ **Gather profile** – gathering profile on SoftControl SysWatch components.

   ○ **Clean and disable profile** – clearing and disabling profile on SoftControl SysWatch components.



Task type

Select the task type and specify the options

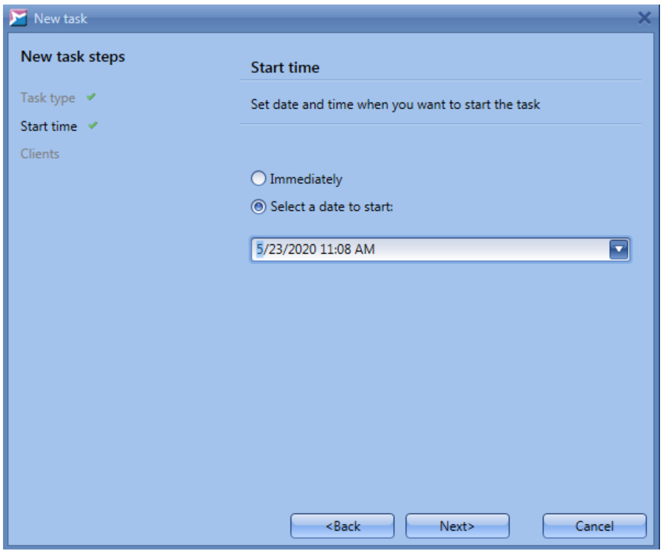
Profile

● Gather profile

○ Clean and disable profile

Figure 113. The 'Task type' section

2) Select the **Immediately** option in the **Start on** section to run the task right after you add it, or select **Choose a date to start** and specify the date and time of the start (fig. The 'Start date' section[118]). Click **Next** to continue.



New task

New task steps

Task type ✓
Start time ✓
Clients

Start time

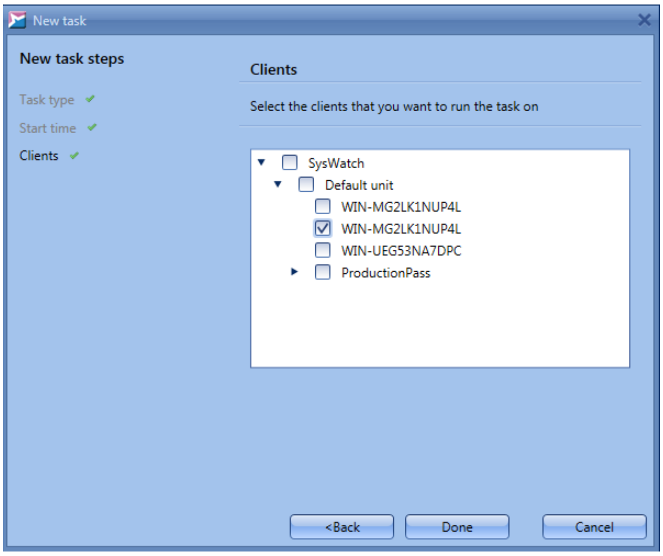
Set date and time when you want to start the task

○ Immediately
● Select a date to start:

5/23/2020 11:08 AM

Figure 114. The 'Start on' section

3) In the **Clients** section, tick off the client components which you want to create the task for (fig. The 'Clients' section[119]). If you select the **SysWatch** client type, the task is assigned to all client components. If you select an organization unit, the task is assigned to all client components of the organization unit. Click **Done** to create the task, or **Back** to change the task parameters.



New task

New task steps

Task type ✓
Start time ✓
Clients ✓

Clients

Select the clients that you want to run the task on

▾ □ SysWatch
  ▾ □ Default unit
    □ WIN-MG2LK1NUP4L
    ☑ WIN-MG2LK1NUP4L
    □ WIN-UEG53NA7DPC
  ▸ □ ProductionPass

Figure 115. The 'Clients' section

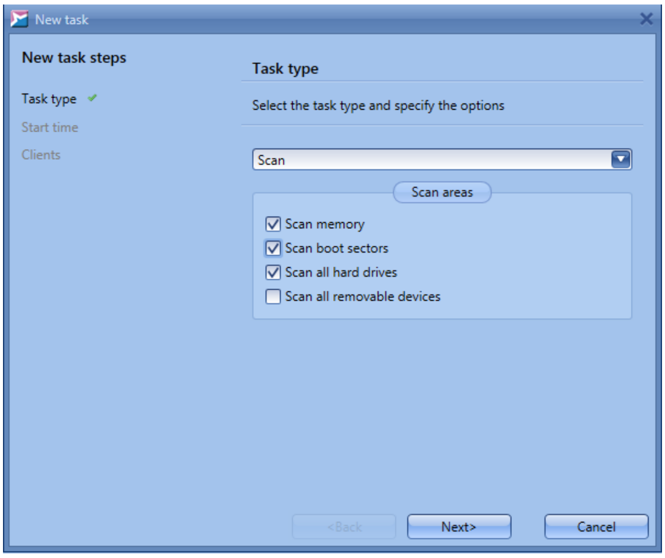
4.8.2 Antivirus scanning

1) Select **Scan** from the drop-down list in the **Task type** section and tick off the client host's areas to be scanned (fig. The 'Task type' section[120]):

- ❑ **Scan memory**;

- ❑ **Scan boot sectors**;
- ❑ **Scan all hard drives**;
- ❑ **Scan all removable devices**.

Click **Next** to continue.


New task

New task steps

Task type ✓
Start time
Clients

Task type

Select the task type and specify the options

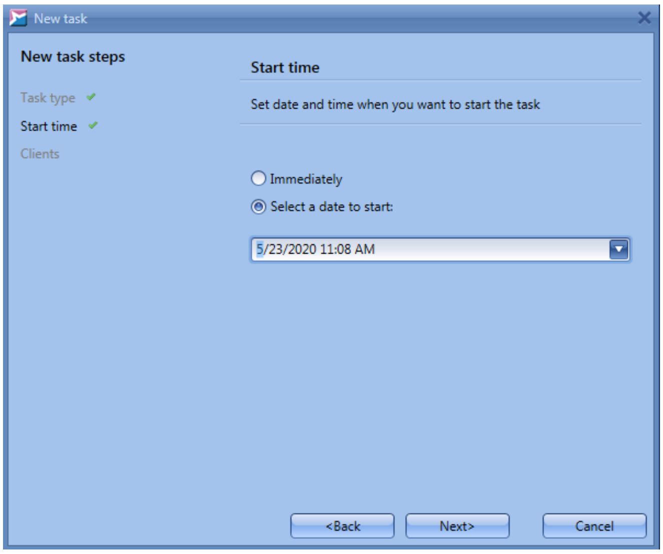
Scan

Scan areas

☑ Scan memory
☑ Scan boot sectors
☑ Scan all hard drives
☐ Scan all removable devices

Figure 116. The 'Task type' section

2) Select the **Immediately** option in the **Start on** section to run the task right after you add it, or select **Choose a date to start** and specify the date and time of the start (fig. The 'Start date' section[120]). Click **Next** to continue.


New task

New task steps

Task type ✓
Start time ✓
Clients

Start time

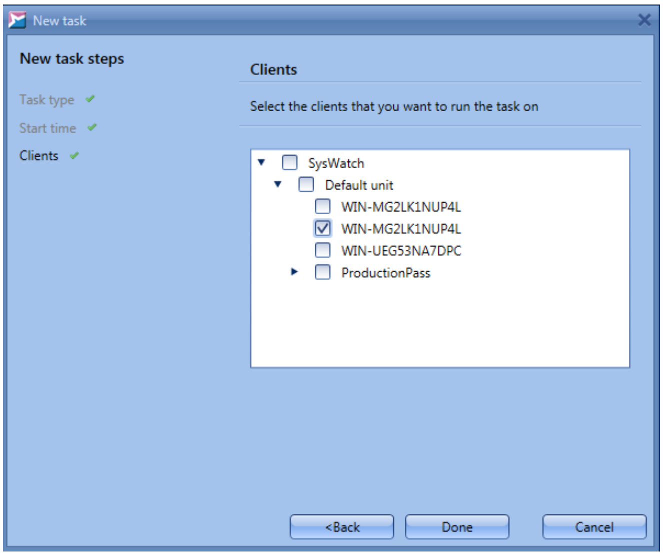
Set date and time when you want to start the task

○ Immediately
● Select a date to start:

5/23/2020 11:08 AM

Figure 117. The 'Start on' section

3) In the **Clients** section, tick off the client components which you want to create a task for (fig. The 'Clients' section[120]).



New task steps

Task type ✓
Start time ✓
Clients ✓

Clients

Select the clients that you want to run the task on

- ▾ □ SysWatch
  - ▾ □ Default unit
    - □ WIN-MG2LK1NUP4L
    - ☑ WIN-MG2LK1NUP4L
    - □ WIN-UEG53NA7DPC
  - ▸ □ ProductionPass

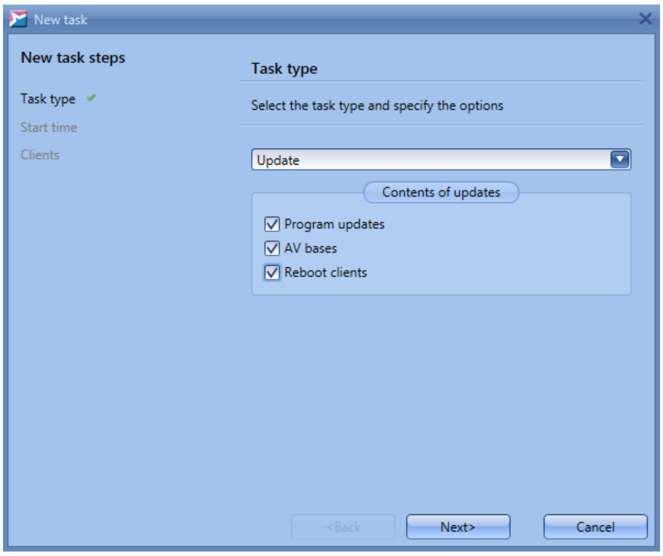
Figure 118. The 'Clients' section

If you select the **SysWatch** client type, the task is assigned to all client components. If you select an organization unit, the task is assigned to all the client components of the organization unit. Click **Done** to create the task, or **Back** to change the task parameters.

4.8.3 Updating

1) Select **Update** from the drop-down list in the **Task type** section, tick off the required components to update and the task options (fig. The 'Task type' section 121):

- ❑ **Program updates**: update SysWatch, DLP and SysCmd program modules.
- ❑ **AV bases**: update the antivirus bases of the SysWatch components.
- ❑ **Reboot clients**: reboot the client hosts when the update completes. If this option is not selected, you should reboot the client host locally to complete the program module updates. The corresponding message is displayed in the component's status in the Clients 42 tab and in the update events in logs 130. The SysCmd module does not require reboot after update, so this parameter is ignored for the module SysCmd.



New task

New task steps

Task type ✓
Start time
Clients

Task type

Select the task type and specify the options

Update

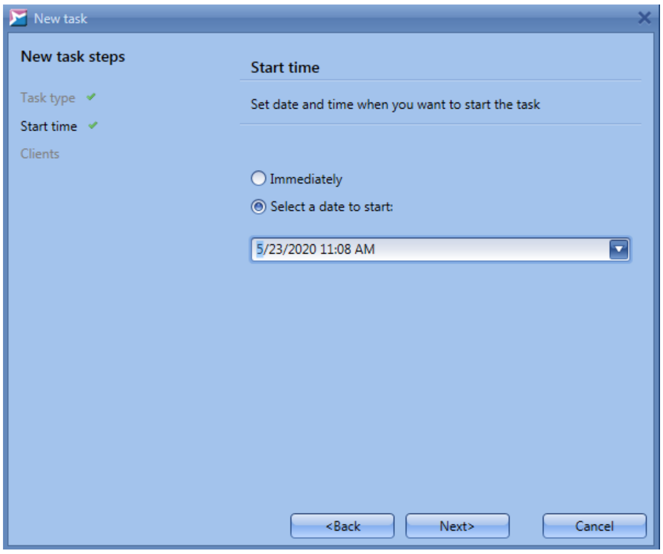
Contents of updates

☑ Program updates
☑ AV bases
☑ Reboot clients

Figure 119. The 'Task type' section

Click **Next** to continue.

2) Select the **Immediately** option in the **Start on** section to run the task right after you add it, or select **Choose a date to start** and specify the date and time of the start (fig. The 'Start date' section[122]). Click **Next** to continue.



New task

New task steps

Task type ✓
Start time ✓
Clients

Start time

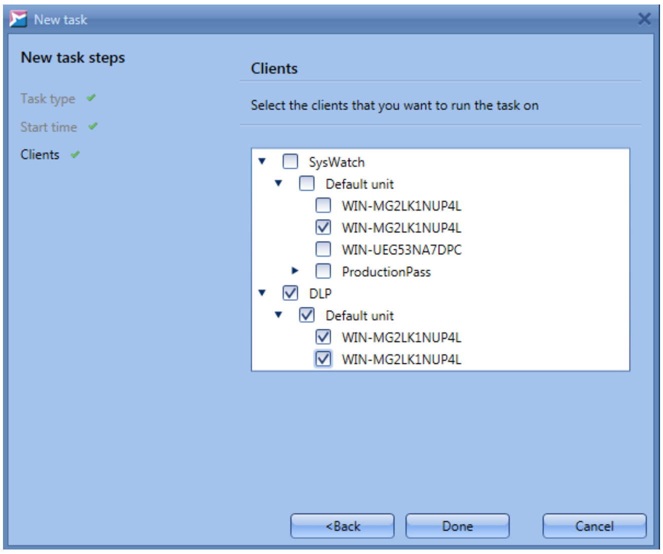
Set date and time when you want to start the task

○ Immediately
● Select a date to start:

5/23/2020 11:08 AM

Figure 120. The 'Start on' section

3) In the **Clients** section, tick off the client components which you want to create the task for (fig. The 'Clients' section[122]).



New task

New task steps

Task type ✓
Start time ✓
Clients ✓

Clients

Select the clients that you want to run the task on

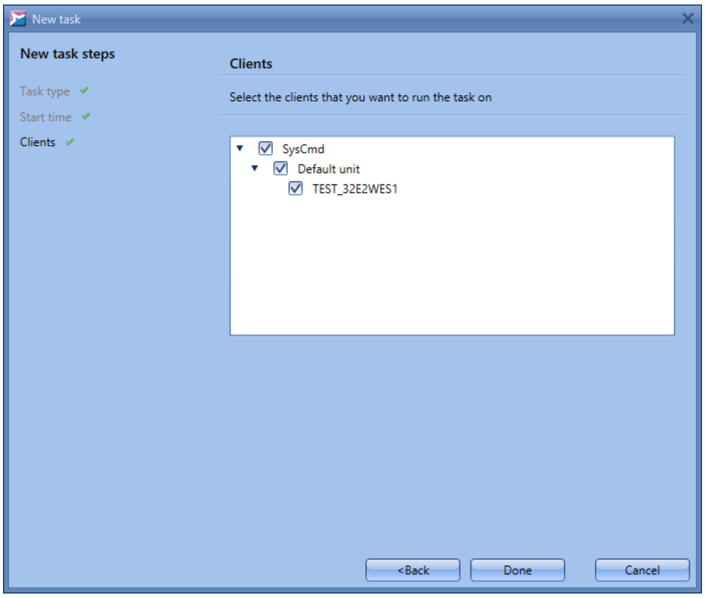
- ▾ □ SysWatch
  - ▾ □ Default unit
    - □ WIN-MG2LK1NUP4L
    - ☑ WIN-MG2LK1NUP4L
    - □ WIN-UEG53NA7DPC
  - ▸ □ ProductionPass
- ▾ ☑ DLP
  - ▾ ☑ Default unit
    - ☑ WIN-MG2LK1NUP4L
    - ☑ WIN-MG2LK1NUP4L

Figure 121. The 'Clients' section

If you select a client type, the task is assigned to all client components of the same type. If you select an organization unit, the task is assigned to all the client components of the organization unit. Click **Done** to create the task, or **Back** to change the task parameters.

4.8.4 Executing commands on the client and transferring files

A task of the type **Executing commands of the client** can run on a remote computer with an installed client SoftControl SysCmd. In one task, the following commands can be executed: uploading a file to the remote computer, running a process on the remote computer, downloading a file from the remote computer.



New task

New task steps

Task type ✓
Start time ✓
Clients ✓

Clients

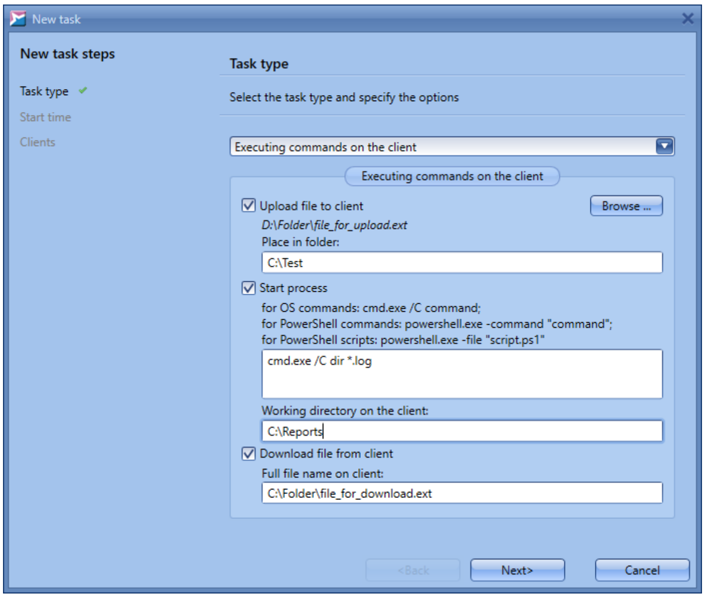
Select the clients that you want to run the task on

- ☑ SysCmd
  - ☑ Default unit
    - ☑ TEST_32E2WES1

Figure 122. The "Clients" section

4.8.4.1 Creating a task

1) Select **Executing commands on the client** from the drop-down list in the **Task type** section and mark commands[126] for executing (fig. The 'Task type' section[123]):



New task

New task steps

Task type ✓
Start time
Clients

Task type

Select the task type and specify the options

Executing commands on the client

Executing commands on the client

☑ Upload file to client

D:\Folder\file_for_upload.ext

Place in folder:

C:\Test

☑ Start process

for OS commands: cmd.exe /C command;
for PowerShell commands: powershell.exe -command "command";
for PowerShell scripts: powershell.exe -file "script.ps1"

```
cmd.exe /C dir *.log
```

Working directory on the client:

C:\Reports

☑ Download file from client

Full file name on client:

C:\Folder\file_for_download.ext

Figure 123. The 'Task type' section

❑ **Upload file to client** – copy a file from the local computer where SoftControl Admin Console is running to the remote computer with the installed module SoftControl SysCmd.

Parameters:

Select a file using the button **Browse** and enter the full target path on the remote computer to the **Place in folder** field. Both parameters are mandatory.

□ **Start process** – run specified file.

Parameters:

Executable file for running and command line arguments (mandatory parameter).

Working directory on the client (optional parameter).

You can specify the working folder that will be set as the current one for the process.

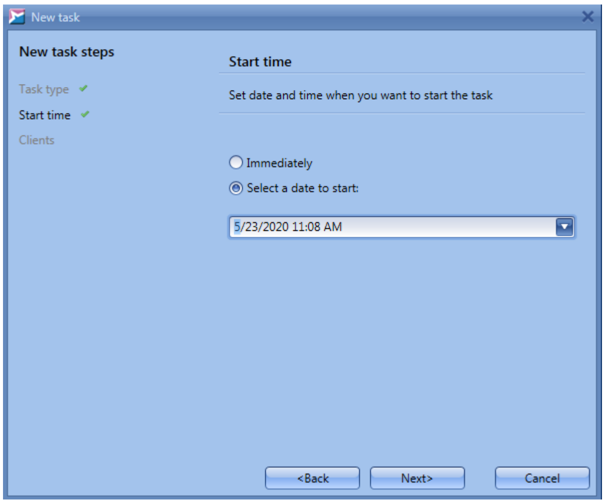
□ **Download file from client** – download a file from the remote computer with the installed module SoftControl SysCmd to the server SoftControl Server. Later, the downloaded file can be copied from the server to the local computer using SoftControl Admin Console.

Parameters:

Full path to the file on the client (mandatory parameter).

After filling in the data, click **Next**.

2) Select the **Immediately** option in the **Start on** section to run the task right after you add it, or select **Choose a date to start** and specify the date and time of the start (fig. The 'Start time' section[122]). Click **Next** to continue.



New task

New task steps

Task type ✓

Start time ✓

Clients

Start time

Set date and time when you want to start the task

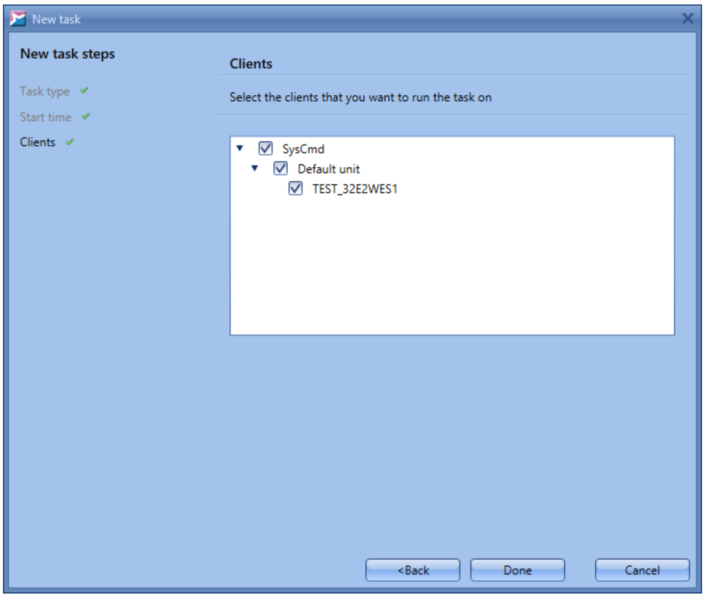
○ Immediately

● Select a date to start:

5/23/2020 11:08 AM

Figure 124. The 'Start time' section

3) In the **Clients** section, tick off the client components which you want to create a task for (fig. The 'Clients' section[122]).



Clients

Select the clients that you want to run the task on

☑ SysCmd
☑ Default unit
☑ TEST_32E2WES1

Figure 125. The 'Clients' section

If you select a client type, the task is assigned to all client components of the same type. If you select an organization unit, the task is assigned to all the client components of the organization unit. Click **Done** to create the task, or **Back** to change the task parameters.

4.8.4.2 Executing a task

During execution of the task with the type **Executing commands on the client**, the system performs the following actions:

Preparing the task. If the task contains the command of uploading a file to the client, SoftControl Admin Console transmits first the file to the server. The server stores the file in a folder specified in the paramenter *CmdFileStoreDir* of the server configuration file (C:\ProgramData\SafenSoft \Server.Config.xml), the default value is C:\ProgramData\SafenSoft\CmdFileStore. If the file has not been successfully transmitted to the server, SoftControl Admin Console shows the error message and the server does not create the task. Maximum file size for uploading to the client and for downloading from the client is specified in the parameter *MaxFileSizeByte* of the server configuration file.

Starting a task on the client. During a heartbeat, the client connects to the server and receives a list of tasks. The client creates a new thread for each task to execute commands from the task. Thus, different tasks can run in a non-specific order, but commands within one task run in the exact order as they are described in the task.

Uploading a file to the client. The client receives the file from the server and stores it according to the parameters of the command (path, name, times, and attributes). If a file with the same name already exists on the client, it will be overwritten. If the specified path does not exist, the client will try to create the path. The client returns the result code to the server. After finishing the command, the server deletes the file in any case (regardless of whether the command execution was successful or not). If file transfer from the server to the client is interrupted due to loss of connection or rebooting of the client device, uploading shall continue once connection is restored and the SysCmd service is running.

Running a process. The client creates the process according to the command arguments and starts reading the standard output streams (stdout and errout) of the process. After finishing reading data from the output streams, the client sends this data to the server. Buffer size for the process output is specified in the parameter *MaxCmdOutputChars* in the server configuration file. If the command restarts or shuts down the remote computer, it shall include a delay to give the client the time to wait for the next heartbeat and send the result to the server. For example, the *shutdown* command shall be used with the /t parameter. Since the client launches the process in a session without a GUI[7], it is not possible to run processes that expect user interaction for their execution or completion.

Downloading a file from the client. The client sends the file to the server, and the server stores the file in the folder specified in the parameter *CmdFileStoreDir* of the server configuration file. The client also sends to the server the file name, time, and attributes. If file transfer from a client to the server is interrupted due to loss of connection or rebooting of the client device, uploading shall continue once connection is restored and the SysCmd service is running.

Task completion. When all commands are completed, the server assigns the corresponding status to the task and sends the status to the server at the next heartbeat. It means that results of some commands might be accessible on the server before completion of the task.

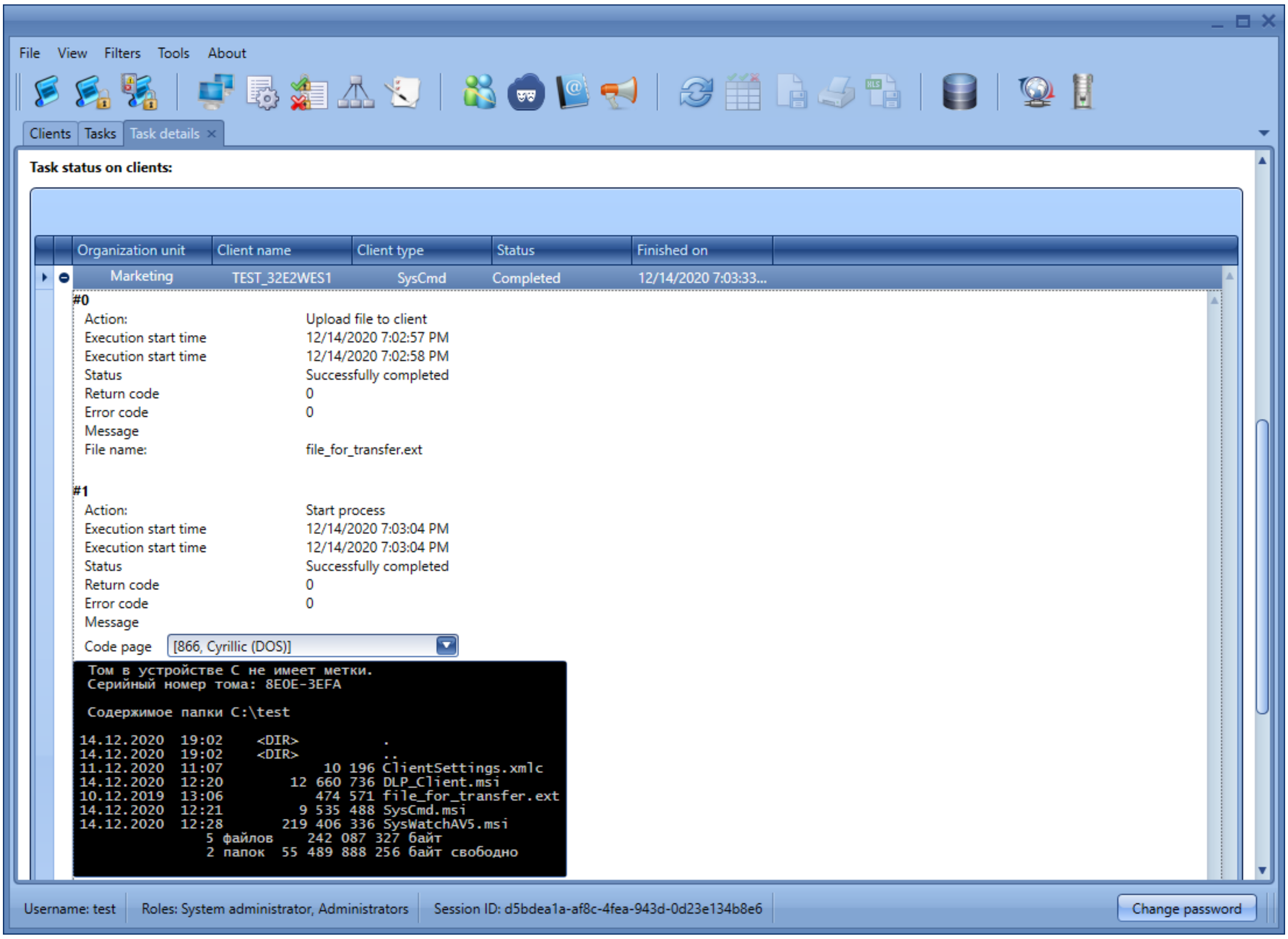
The total execution time of all commands in one task is limited by the parameter *MaxCmdExecTimeSec* of the server configuration file. If this time is exceeded, the command is interrupted and gets the "Timeout exceeded" status. (All commands that follow get the same status.) If the SoftControl SysCmd service is restarted or the client device is rebooted and execution of the commands in the task continues, time keeping is reset.

There are two types of errors that are possible during command execution. Critical errors (absence of the file to transfer or to run, an error during creation of a file or a path) interrupt execution of a command. In case of a non-critical error (network errors during file transfer), another attempt is made to perform the command until one of the three conditions is met: the command is finished successfully, a critical error occurs, or the time limit is reached. The next command in the task shall be executed only if the previous command 0is completed successfully. The server inserts a five-second delay between two successive commands.

Before and after execution of each file transfer command, the state of the command is saved on the client device in order to continue execution of unfinished commands after a service restart.

4.8.4.3 Analyzing the results of commands

Information about the results of command execution is accessible on the tab Task details[115] in the table **Task status on clients**. If results are already on the server, in first column the sign ⊕ will appear. The click on this sign expands detailed information of the results (figures Results of the file uploading and process starting commands[128] and Results of the file downloading command[129]).



Task status on clients:

Organization unit	Client name	Client type	Status	Finished on
Marketing	TEST_32E2WES1	SysCmd	Completed	12/14/2020 7:03:33...

#0

Action:	Upload file to client
Execution start time	12/14/2020 7:02:57 PM
Execution start time	12/14/2020 7:02:58 PM
Status	Successfully completed
Return code	0
Error code	0
Message	
File name:	file_for_transfer.ext

#1

Action:	Start process
Execution start time	12/14/2020 7:03:04 PM
Execution start time	12/14/2020 7:03:04 PM
Status	Successfully completed
Return code	0
Error code	0
Message	

Code page [866, Cyrillic (DOS)]

```
 Том в устройстве C не имеет метки.
 Серийный номер тома: 8E0E-3EFA

 Содержимое папки C:\test

14.12.2020  19:02    <DIR>          .
14.12.2020  19:02    <DIR>          ..
11.12.2020  11:07            10 196 ClientSettings.xmlc
14.12.2020  12:20        12 660 736 DLP_Client.msi
10.12.2019  13:06           474 571 file_for_transfer.ext
14.12.2020  12:21         9 535 488 SysCmd.msi
14.12.2020  12:28       219 406 336 SysWatchAV5.msi
               5 файлов    242 087 327 байт
               2 папок  55 489 888 256 байт свободно
```

Username: test | Roles: System administrator, Administrators | Session ID: d5bdea1a-af8c-4fea-943d-0d23e134b8e6

Figure 126. Results of the file uploading and process starting commands

The **Status** field can have the following values:

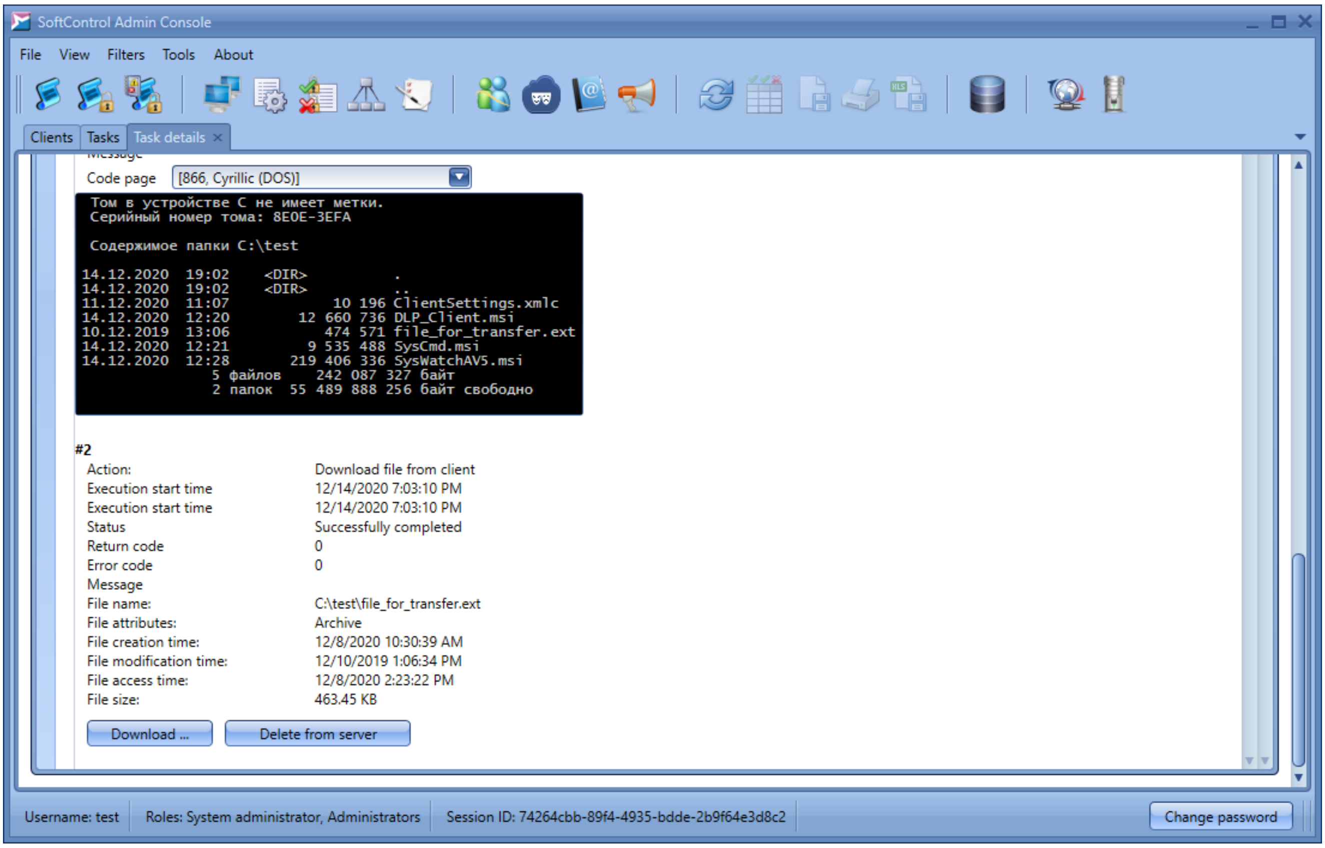
- Successfully completed.
- An error has occurred.
- Timeout exceeded.

The **Return code** field contains the code returned by the process in the command **Start process**.

If an error in module SoftControl SysCmd has occurred during calling Windows API functions, the **Error code** and **Message** fields contain the corresponding error code and description of the error.

For reading output data of the command **Start process**, the **Code page** can be selected.

If the command **Download file from client** has finished successfully, the file on the server can be managed by the **Download** and **Delete from server** buttons.


SoftControl Admin Console
File View Filters Tools About
Clients Tasks Task details ×

Code page [866, Cyrillic (DOS)]

```
 Том в устройстве C не имеет метки.
 Серийный номер тома: 8E0E-3EFA

 Содержимое папки C:\test

14.12.2020  19:02    <DIR>          .
14.12.2020  19:02    <DIR>          ..
11.12.2020  11:07            10 196 ClientSettings.xmlc
14.12.2020  12:20        12 660 736 DLP_Client.msi
10.12.2019  13:06           474 571 file_for_transfer.ext
14.12.2020  12:21         9 535 488 SysCmd.msi
14.12.2020  12:28       219 406 336 SysWatchAV5.msi
               5 файлов    242 087 327 байт
               2 папок  55 489 888 256 байт свободно
```

#2

Action:	Download file from client
Execution start time	12/14/2020 7:03:10 PM
Execution start time	12/14/2020 7:03:10 PM
Status	Successfully completed
Return code	0
Error code	0
Message	
File name:	C:\test\file_for_transfer.ext
File attributes:	Archive
File creation time:	12/8/2020 10:30:39 AM
File modification time:	12/10/2019 1:06:34 PM
File access time:	12/8/2020 2:23:22 PM
File size:	463.45 KB

Username: test | Roles: System administrator, Administrators | Session ID: 74264cbb-89f4-4935-bdde-2b9f64e3d8c2

Figure 127. Results of the file downloading command

4.9 Viewing reports

The **Log** tab is designed to view the consolidated reports from the client applications in SoftControl Admin Console. The tab allows tracing the events on several client hosts simultaneously in real time, and sampling the required data with the help of flexible filtering[144]. On the tab, the administrator can access the following data in a convenient format.

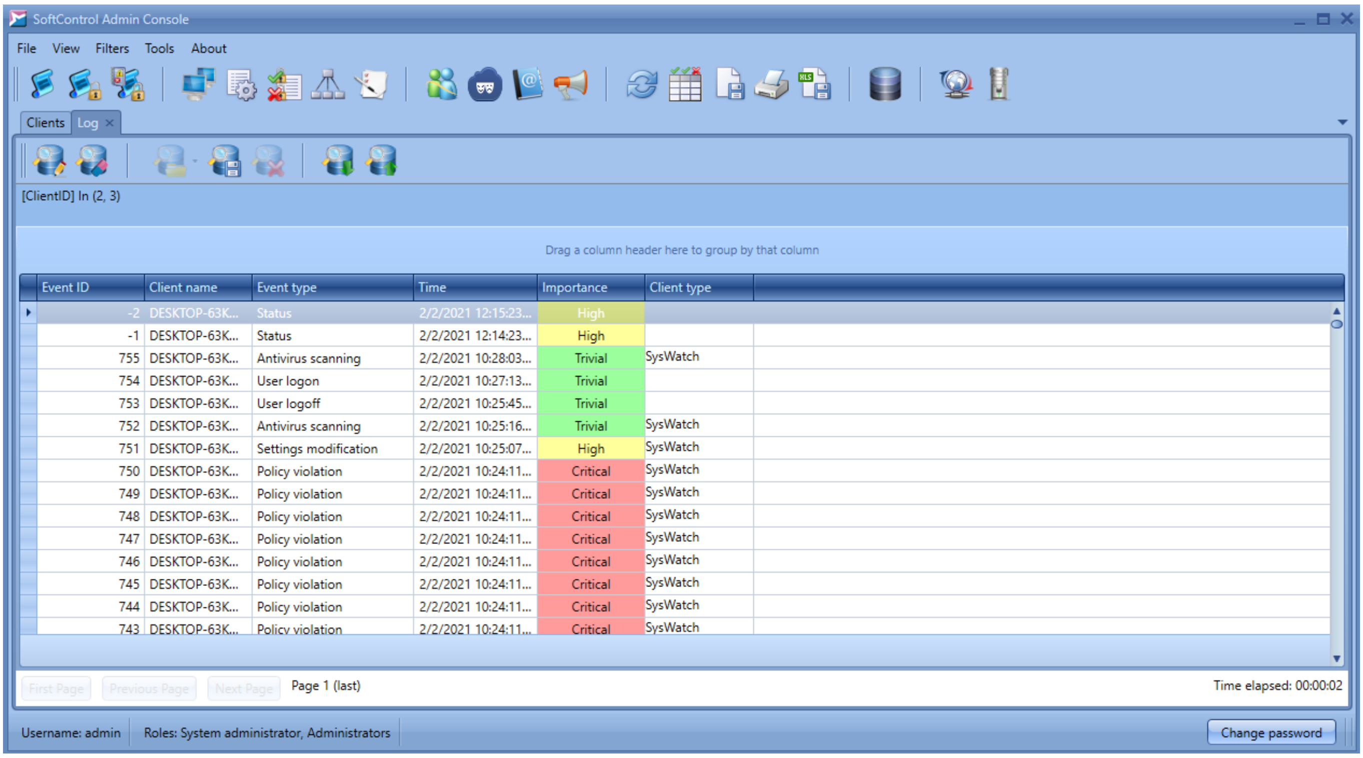
- SoftControl SysWatch logs[130];
- SoftControl DLP Client logs[136];
- SoftControl SysCmd logs[141].

The obtained reports can be printed or exported to a file[150].

Reports backup[151] is supported.

4.9.1 SoftControl SysWatch logs

The **Event Log** tab provides the detailed monitoring of the security events that are registered by SoftControl SysWatch on the client hosts (fig. The 'Log' tab for the SoftControl SysWatch component[130]). If you wish to browse all events from SysWatch clients, select those clients and follow the steps given in Clients[45].


SoftControl Admin Console
File View Filters Tools About
Clients Log ×

[ClientID] In (2, 3)

Drag a column header here to group by that column

Event ID	Client name	Event type	Time	Importance	Client type
-2	DESKTOP-63K...	Status	2/2/2021 12:15:23...	High	
-1	DESKTOP-63K...	Status	2/2/2021 12:14:23...	High	
755	DESKTOP-63K...	Antivirus scanning	2/2/2021 10:28:03...	Trivial	SysWatch
754	DESKTOP-63K...	User logon	2/2/2021 10:27:13...	Trivial	
753	DESKTOP-63K...	User logoff	2/2/2021 10:25:45...	Trivial	
752	DESKTOP-63K...	Antivirus scanning	2/2/2021 10:25:16...	Trivial	SysWatch
751	DESKTOP-63K...	Settings modification	2/2/2021 10:25:07...	High	SysWatch
750	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
749	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
748	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
747	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
746	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
745	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
744	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch
743	DESKTOP-63K...	Policy violation	2/2/2021 10:24:11...	Critical	SysWatch

Page 1 (last)

Time elapsed: 00:00:02

Username: admin

Roles: System administrator, Administrators

Figure 128. The 'Event Log' tab for the SoftControl SysWatch component

The full list of the tab fields for the SoftControl SysWatch component is given in table 21.

Table 21. The 'Event Log' tab fields for SoftControl SysWatch

Field	Description
Client name	The name of a client host.
Event ID	Unique event identifier. If SoftControl Admin Console receives an event with the duplicated identifier, the duplicated string is highlighted in red. If there is a break in the order of the identifiers (i.e. gaps in the sequence exist), the corresponding warning is added to the server component report in the Windows event log 182. The exception is the events of the **Status** type. The **Event ID** parameter can be either *-1* or *-2* for them.
Unique client ID	Unique identifier of a client host. The identifier is assigned automatically after SoftControl SysWatch sends a request to SoftControl Server for the first time.
Event type	Type of the security event (incident): • **policy violation**; • **activity control**; • **client update**; • **process start**; • **antivirus scanning**; • **settings modification**; • **status**; • **user logon**; • **user logoff;** • **DeCrypt events.**
Time	Date and time when the event occurred.
Importance	The event importance (priority) from the viewpoint of a threat to a client host's information security: • trivial; • high; • critical. Each priority level has the corresponding cell color.
Action	Action when a **policy violation** event occurs: • **reading the file**; • **changing the file**; • **renaming the file**; • **deleting the file**; • **opening the directory**; • **deleting the directory**; • **opening the registry key**; • **creating the registry key**; • **deleting the registry key**; • **changing the registry value**; • **deleting the registry value**; • **loading DLL module**; • **invalid password entered**. Action when a **process start** event occurs (the data are displayed in a single string): • **Installer**: yes/no; • **In profile**: yes/no (not available if the system profile is disabled on the client host, or the **Applications** checkbox in the **Activity control** section of the settings 63 is deselected); • **Valid certificate**: yes/no (for installers only);

Field	Description
	• **Whitelist is on**: yes/no (for installers only); • **Certificate is in whitelist**: yes/no (for installers only and when the whitelist is enabled); • **Global software update mode on**: yes/no (for installers only); • **Was tracked**: yes/no; • **Execute in software update mode**: yes/no. Action when an **antivirus scanning** event occurs: • **running the scanner**; • **running the profile gathering**; • **finishing the scan**; • **profile gathering completed**; • **scanning the object**. Action when a **client update** event occurs: • **starting the updates**; • **update completed**. Action when a **settings modification** event occurs: • **settings changed by user**; • **settings changed by server**. Action when the **DeCrypt events** occur: • **NOTIFY-DEV0;Boot with all devices present**; • **NOTIFY-PRETEST;Boot with unencrypted container**; • **NOTIFY-ERROR;Error at boot**; • **NOTIFY-PW;Boot with password**; • **NOTIFY-DEV1;Boot with 1 device missing**; • **NOTIFY-DEV2;Boot with 2 devices missing (CRITICAL)**; • **NOTIFY-ACTION: DEV-GET;Request list of found devices**; • **NOTIFY-ACTION: DEV-CHANGE;Update device list**; • **NOTIFY-ACTION: PW-CHANGE;Change password**; • **NOTIFY-ACTION: DISK-ENC STARTED;Disk encryption started**; • **NOTIFY-ACTION: DISK-ENC FINISHED;Disk encryption finished**; • **NOTIFY-ACTION: DISK-DEC STARTED;Disk decryption started**; • **NOTIFY-ACTION: DISK-DEC FINISHED;Disk decryption finished**; • **NOTIFY-ACTION: BOOT-PREPARE;Install boot loader**; • **NOTIFY-ACTION: BOOT-CLEAR;Uninstall boot loader**.
Action status	Action status when an **antivirus scanning** event occurs: • **scanner is running**; • **error when running the scanner**; • **scanner is stopped**; • **success**; • **failure**. Action status when a **client update** event occurs: • **update is running**; • **error when running the update**; • **no updates found**; • **update interrupted by user**; • **updates installed successfully**; • **system reboot is required**; • **update completed with errors**. Action status when the **DeCrypt events** occur: • **SUCCESS**;

Field	Description
	• **FAIL**.
Client status	The status of a registered client component: • **active**; • **inactive**; • **service was interrupted**; • **status error. invalid status**.
Binary path	The application or the installer that triggers the events of the **policy violation** or the **process start** types.
Command line	– Command that triggers the **process start** type event. – File system or registry object involved in the event of the **policy violation** type, or the name of the DLL module loaded by the process that caused the event of the **policy violation** type. – Invalid password.
User	User account under which the events of the **process start** or the **changing settings** types has occurred.
Zone	Application execution zone: • **trusted**; • **default** (restricted); • **blocked**.
PID	Unique process identifier in the OS for the event of the **process start** type.
Parent PID	Unique parent process identifier in the OS for the event of the **process start** type.
Parent process	The name of the parent process for the event of the **process start** type.
Decision	Decision for the application launch: • **permitted**; • **denied**. Each decision has the corresponding cell color.
Checked objects	The number of objects that have been checked during the antivirus scanning.
Threats found	The number of threats that have been detected during the antivirus scanning.
Threats neutralized	The number of threats that have been neutralized during the antivirus scanning.
Embedded certificates	The number of embedded certificates that have been detected during the automatic setup (profile gathering).
Catalog certificates	The number of catalog certificates that have been detected during the automatic setup (profile gathering).
Applications	Application activity control status: • **active**; • **inactive**.
File system	File system control status: • **active**; • **inactive**.
System registry	System registry control status: • **active**; • **inactive**.
Network control	Network activity control status: • **active**; • **inactive**.
Logon user name	The account that has been used to log on to a client host OS.

Field	Description
Logoff user name	The account that has been used to log out of a client host OS.
Error	Error code in the database on the server.
Client type	The type of the client the report is displayed for. The field is empty for common events (SysWatch and DLP).
Details	UID of the rule where the control policy has been violated.
Service name	System name of the service that has been started or stopped.
Display name	The name of the service in the Windows **Services** snap-in.
Service event	The service status: • **ServiceStarted**; • **ServiceFoundRunning**; • **ServiceStopped**.

The following events contain the extended information about an incident:

Antivirus scanner event

An antivirus scanner event allows you to view the detailed report about the results of the anti-virus scanning [119] of the client hosts.

Open the event list on the Log [130] tab for the SoftControl SysWatch component and select an event of the **Antivirus scanning** type with the **Finishing the scan** action. To open a report with additional information, perform one of the following operations for the selected event:

- double-click the event;
- invoke the context menu by right-clicking the event and select the **Show additional info for antivirus scanning event** command.

A report with the additional information only opens if threats are detected during the antivirus scanning (nonzero counter in the **Threats found** field), or if some threats have not been neutralized during previous check.

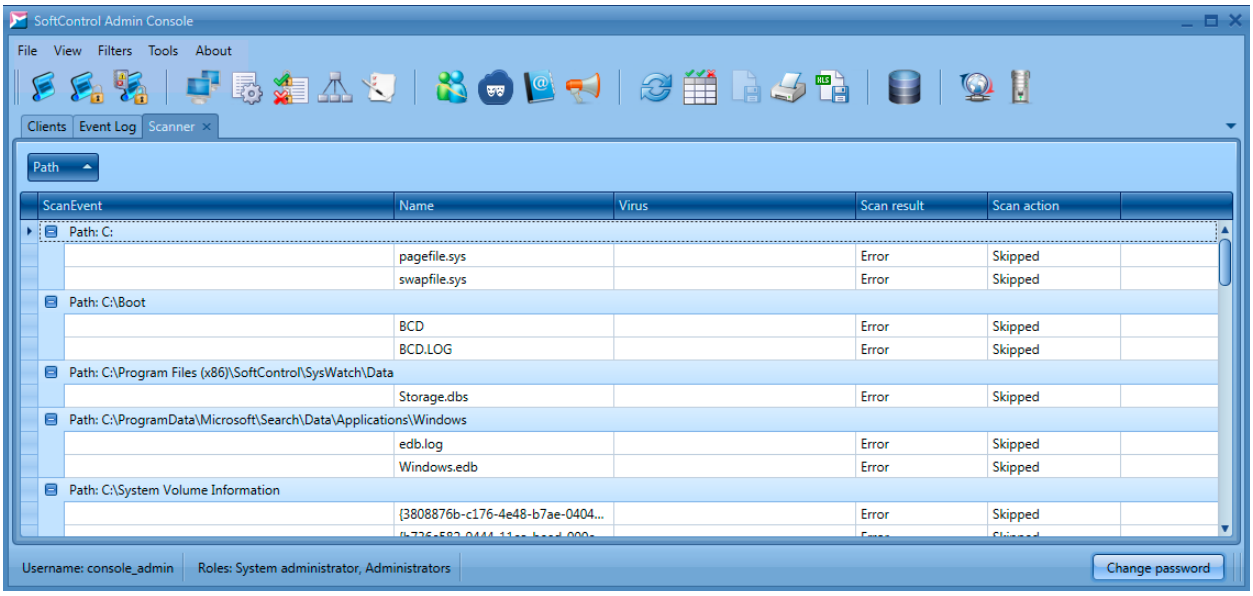
The displayed **Scanner** tab contains the list of all objects that contain the threats detected during the check (fig. Antivirus check results on the 'Scanner' tab [135]).

The full list of the tab fields is given in table 22.

Table 22. The 'Scanner' tab fields

Field	Description
ScanEvent	Date and time when the antivirus scanning has finished.
Path	The path to the object in the client host's file system.
Name	Object name.
Virus	Malicious code name.
Scan result	Profile gathering/antivirus scanning result:

Field	Description
	• **Clean**; • **Infected**; • **Suspicious**; • **Error**; • **Treatment error**; • **Error when moving**; • **Error when deleting**.
Scan action	Action that is performed for the object during the antivirus scanning: • **Treated**; • **Moved**; • **Skipped**; • **Deleted**; • **No action**.



ScanEvent	Name	Virus	Scan result	Scan action
Path: C:				
	pagefile.sys		Error	Skipped
	swapfile.sys		Error	Skipped
Path: C:\Boot				
	BCD		Error	Skipped
	BCD.LOG		Error	Skipped
Path: C:\Program Files (x86)\SoftControl\SysWatch\Data				
	Storage.dbs		Error	Skipped
Path: C:\ProgramData\Microsoft\Search\Data\Applications\Windows				
	edb.log		Error	Skipped
	Windows.edb		Error	Skipped
Path: C:\System Volume Information				
	{3808876b-c176-4e48-b7ae-0404...		Error	Skipped

Figure 129. Antivirus check results on the 'Scanner' tab

Settings modification event

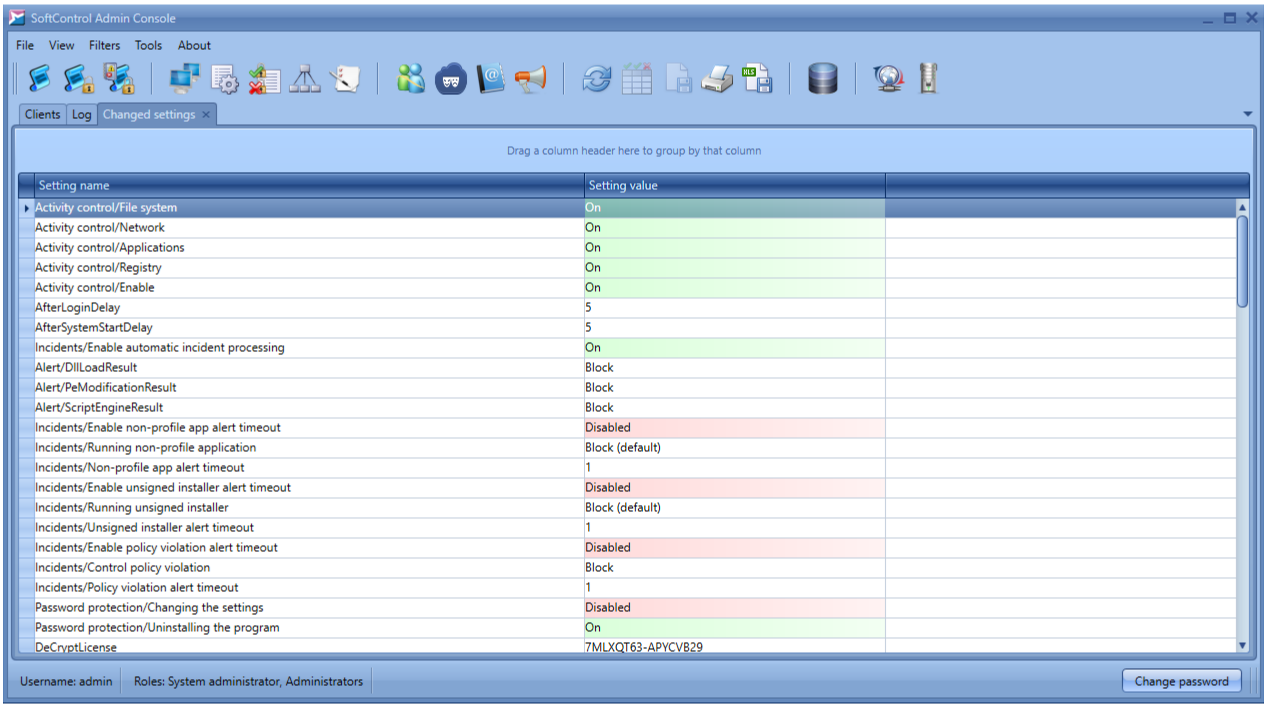
Settings modification event allows you to view the full list of the SoftControl SysWatch configuration changes. The SoftControl SysWatch settings can be changed as follows:

- by the administrator via SoftControl Admin Console [63];
- by the local user with the help of:
  – the program GUI;
  – the configuration file.

Open the list of events on the **Event Log**[130] tab for the SoftControl SysWatch component and select an event of the **Settings modification** type. To open the report with the additional information, perform one of the following operations with the selected object:

- double-click the event;
- invoke the context menu by right-clicking the event and select the **Show additional info for settings modification event** command.

The displayed **Settings modification** tab contains the list of the SoftControl SysWatch settings and their new status (fig. The 'Changed settings' tab[136]).


SoftControl Admin Console
File
View
Filters
Tools
About
Clients
Log
Changed settings
Drag a column header here to group by that column
Change password

Setting name	Setting value
Activity control/File system	On
Activity control/Network	On
Activity control/Applications	On
Activity control/Registry	On
Activity control/Enable	On
AfterLoginDelay	5
AfterSystemStartDelay	5
Incidents/Enable automatic incident processing	On
Alert/DllLoadResult	Block
Alert/PeModificationResult	Block
Alert/ScriptEngineResult	Block
Incidents/Enable non-profile app alert timeout	Disabled
Incidents/Running non-profile application	Block (default)
Incidents/Non-profile app alert timeout	1
Incidents/Enable unsigned installer alert timeout	Disabled
Incidents/Running unsigned installer	Block (default)
Incidents/Unsigned installer alert timeout	1
Incidents/Enable policy violation alert timeout	Disabled
Incidents/Control policy violation	Block
Incidents/Policy violation alert timeout	1
Password protection/Changing the settings	Disabled
Password protection/Uninstalling the program	On
DeCryptLicense	7MLXQT63-APYCVB29

Username: admin | Roles: System administrator, Administrators

Figure 130. The 'Changed settings' tab

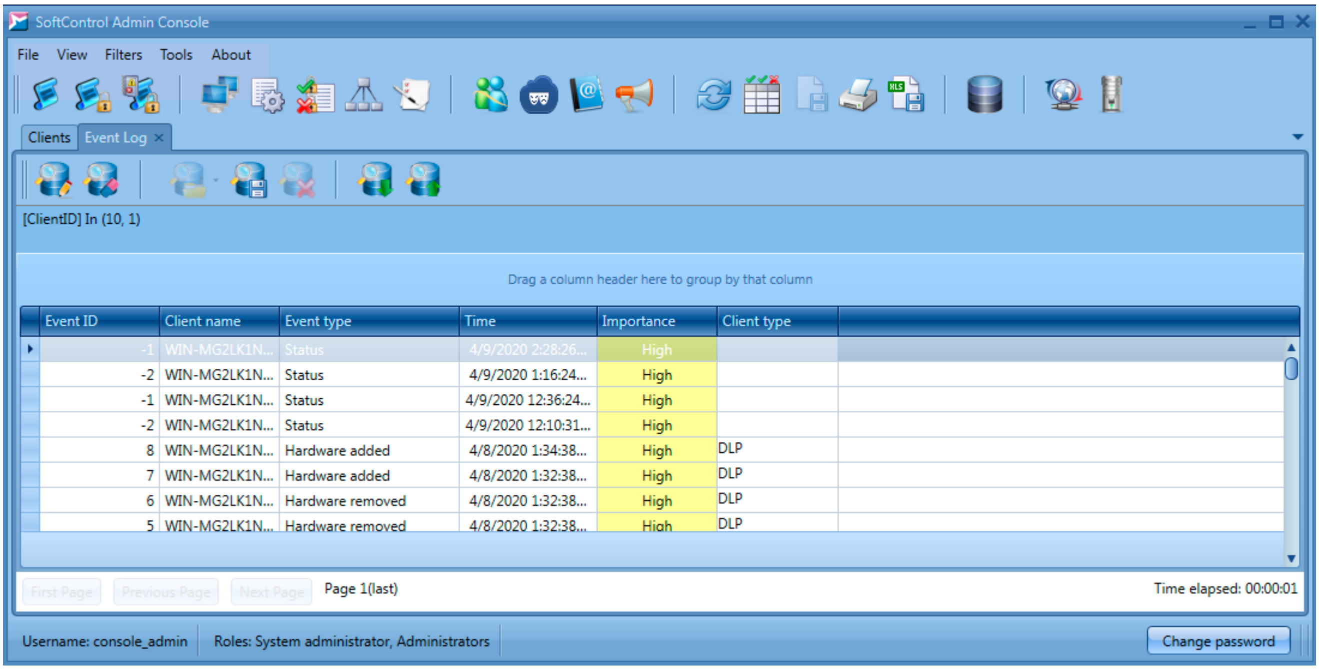
The full list of the tab fields is given in table 23.

Table 23. The 'Changed settings' tab fields

Field	Description
Setting name	The name of the settings.
Setting value	The new value of the settings that has been applied as a result of the event.

4.9.2 SoftControl DLP Client logs

The **Event Log** tab allows viewing the reports with the data that SoftControl DLP Client collects on the client hosts (fig. The 'Log' tab for the SoftControl DLP Client component[136]). If you wish to browse all events from DLP clients, select those clients and follow the steps given in Clients[45].



[ClientID] In (10, 1)

Event ID	Client name	Event type	Time	Importance	Client type
-1	WIN-MG2LK1N...	Status	4/9/2020 2:28:26...	High	
-2	WIN-MG2LK1N...	Status	4/9/2020 1:16:24...	High	
-1	WIN-MG2LK1N...	Status	4/9/2020 12:36:24...	High	
-2	WIN-MG2LK1N...	Status	4/9/2020 12:10:31...	High	
8	WIN-MG2LK1N...	Hardware added	4/8/2020 1:34:38...	High	DLP
7	WIN-MG2LK1N...	Hardware added	4/8/2020 1:32:38...	High	DLP
6	WIN-MG2LK1N...	Hardware removed	4/8/2020 1:32:38...	High	DLP
5	WIN-MG2LK1N...	Hardware removed	4/8/2020 1:32:38...	High	DLP

Page 1(last)

Time elapsed: 00:00:01

Username: console_admin

Roles: System administrator, Administrators

Figure 131. The 'Event Log' tab for the SoftControl DLP Client component

The full list of the tab fields for the SoftControl DLP Client component is given in table 24.

Table 24. The 'Event Log' tab fields for SoftControl DLP Client

Field	Description
Client name	The name of the client host.
Event ID	Unique event identifier. If SoftControl Admin Console receives an event with the duplicated identifier, the duplicated string is highlighted in red. If there is a break in the order of the identifiers (i.e., gaps in the sequence exist), the corresponding warning is added to the server component report in the Windows event log[182]. The exception is the events of the **Status** type. The **Event ID** parameter can be either *-1* or *-2* for them.
Unique client ID	Unique identifier of a client host. The identifier is assigned automatically after SoftControl DLP Client sends a request to SoftControl Server for the first time.
Event type	Type of the data collection event: • **hardware added**; • **file**; • **HTTP**; • **keylogger**; • **printer**; • **registry**; • **hardware removed**; • **work time.**
Time	Date and time when the event occurred.
Importance	The event importance (priority) from the viewpoint of a threat to a client host's information security: • trivial; • high; • critical.

Field	Description
	Each priority level has the corresponding cell color.
Client status	The status of the registered client component: • **active**; • **inactive**; • **service was interrupted**; • **status error. invalid status**.
Process path	The path to the process that triggers the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, and **printer** types.
Process description	Description of the process that triggers the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, and **printer** types.
User name	User account that is used to run the process that triggers the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, and **printer** types.
IP	Destination IP address of the HTTP request for the event of the **HTTP** type.
Url	Destination URL of the HTTP request for the event of the **HTTP** type.
Header	HTTP header for the event of the **HTTP** type.
Access mask	The type of the operation with the monitored object, for the events of the **file** and **registry** types: • **read**; • **write**; • **delete**; • **rename**; • **change**.
Backup file name	The local path to the shadow copy of the monitored object with the name of the *<Full name of the original object>_<N>.bkp*, where *N* is the order number of the locally saved backup, for the events of the **file**, **registry**, and **HTTP** types.
File path	The path to the monitored folder or file, for the event of the **file** type.
Drive type	The type of the drive with the monitored folder of file, for the event of the **file** type: • **fixed storage**; • **removable storage**.
Registry path	The path to the monitored registry key or registry key value, for the event of the **registry** type.
Keylogger time	The date when the keyboard input has been recorded, for the event of the **keylogger** type.
Keylogger data	Text entered by the user from the keyboard, for the event of the **keylogger** type.
Details	Description of the print source for the event of the **printer** type.
Device ID	Peripheral ID for the events of the **hardware added** and **hardware removed** types.
Device class	Peripheral class for the events of the **hardware added** and **hardware removed** types.
Device description	Peripheral description for the events of the **hardware added** and **hardware removed** types.
Start time	Time when the user started working with the application, for the events of the **work time** type.
End time	Time when the user finished working with the application, for the events of the **work time** type.
Duration	Duration of work with the application, for the events of the **work time** type.
File index	Index of the file for the event of the **HTTP** type.
Client type	The type of the client the report is displayed for. The field is empty for common events (SysWatch and DLP).

Field	Description
Printer name	The name of the printer the print job is sent to.

Events of the **file**, **registry** and **HTTP** types are highlighted in different colours, if they contain additional data (video records, shadow copies) (fig. Context menu of the event with additional data[139]).

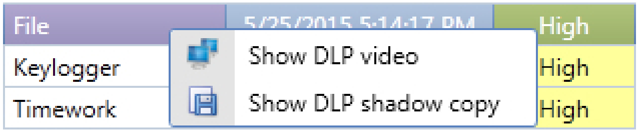


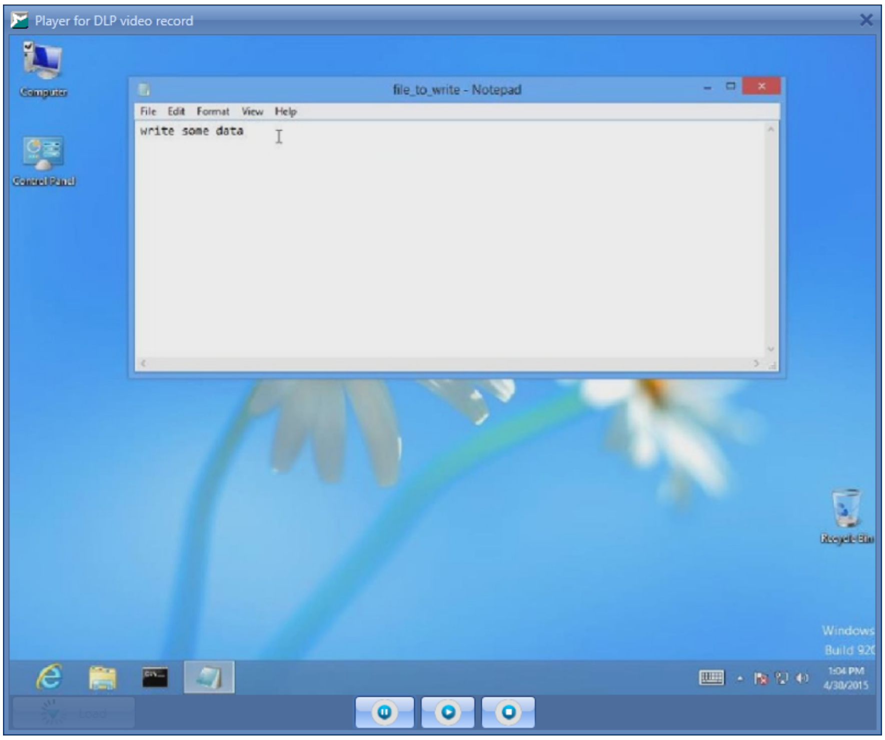
Figure 132. Context menu of the event with additional data

Viewing video records

SoftControl DLP Client saves the sequence of the client host's captured screen shots that can be played back as a video in the management console. Viewing video records is available for events of the **file**, **registry** and **HTTP** types, if **Video recording** option is selected in the monitored object settings. Invoke the context menu by right-clicking the event and select **Show DLP video** to open video record (fig. Context menu of the event with additional data[139]).

Click **Load** in the displayed video player window and manage the playback with the help buttons (fig. SoftControl DLP Client video player[139]) that are described in table 25.

To enable correct record processing by the SoftControl Server component on Microsoft® Windows® Server 2008 R2 and Microsoft® Windows® Server 2012 / 2012 R2, you should have the additional *Desktop Experience* component installed beforehand. Installation instructions are given in appendix[200].



write some data

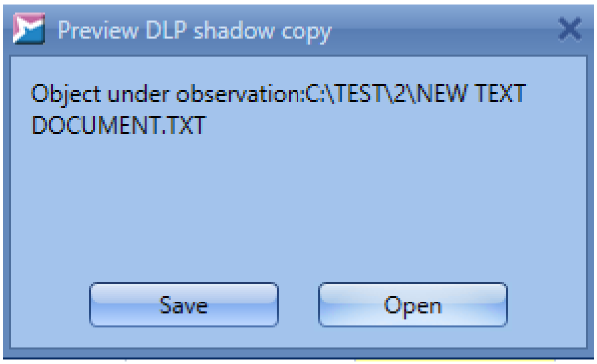
Figure 133. SoftControl DLP Client video player

Table 25. Video player widgets

Button	Name	Description
▶	Play	Play the record.
⏸	Pause	Pause playback.
■	Stop	Stop playback.

Viewing shadow copies

Viewing shadow copy of objects is available for events of the **file** and **registry** types, if **Shadow copy** option is selected in the monitoring settings for these objects. Invoke the context menu by right-clicking the event, select **Show DLP shadow copy** (fig. Context menu of the event with additional data[139]) and click **Open** in the displayed **Preview DLP shadow copy** window to view the saved copy of the specified object under observation or click the **Save** button to save a local shadow copy (fig. Shadow copy of the monitored object[140]).

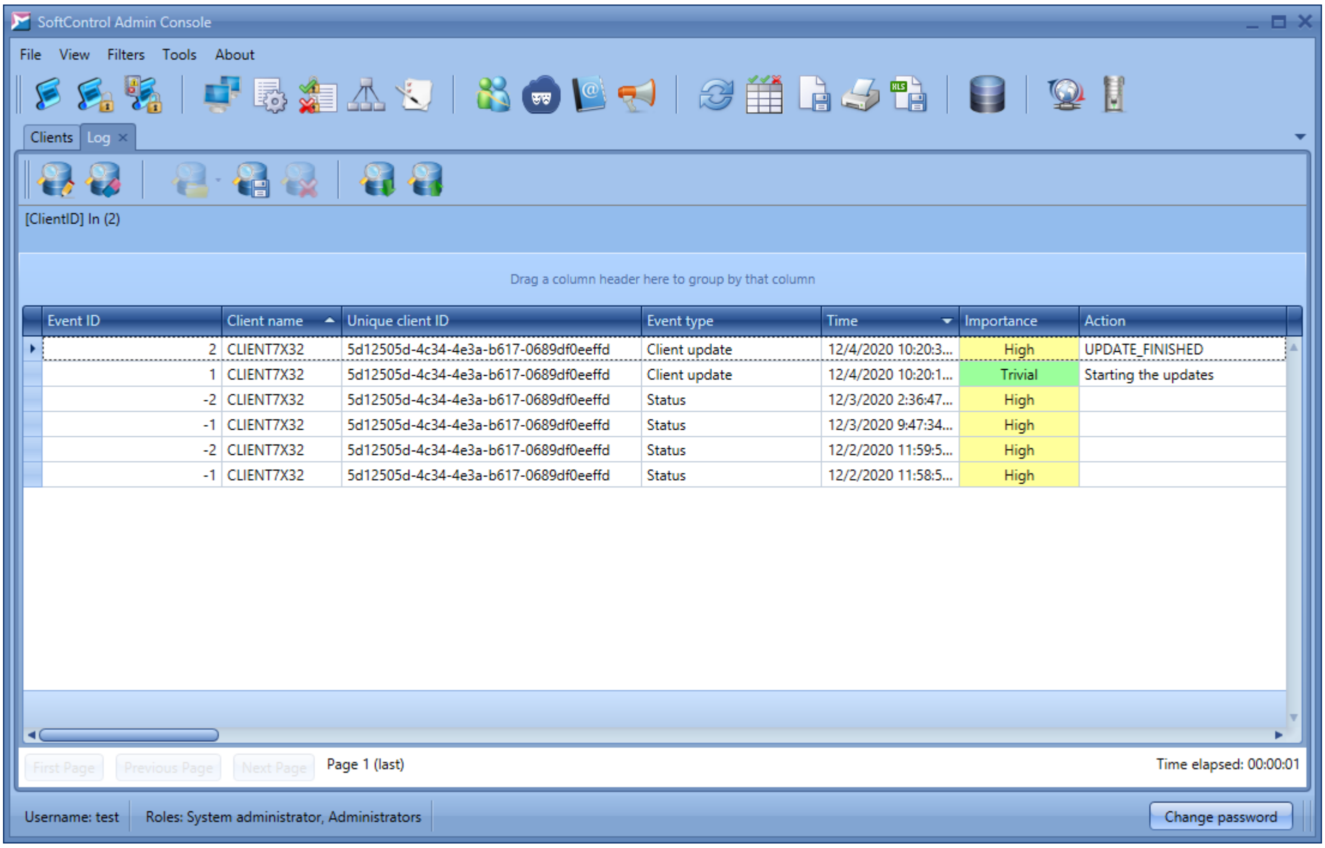


Object under observation:C:\TEST\2\NEW TEXT DOCUMENT.TXT

Figure 134. Shadow copy of the monitored object

4.9.3 SoftControl SysCmd logs

The **Event Log** tab allows viewing the reports with the data that SoftControl SysCmd collects on the client hosts (fig. The 'Log' tab for the SoftControl SysCmd component[141]). If you wish to browse all events from SysCmd clients, select those clients and follow the steps given in Clients[45].



[ClientID] In (2)

Event ID	Client name	Unique client ID	Event type	Time	Importance	Action
2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Client update	12/4/2020 10:20:3...	High	UPDATE_FINISHED
1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Client update	12/4/2020 10:20:1...	Trivial	Starting the updates
-2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Status	12/3/2020 2:36:47...	High	
-1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Status	12/3/2020 9:47:34...	High	
-2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Status	12/2/2020 11:59:5...	High	
-1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Status	12/2/2020 11:58:5...	High	

Page 1 (last)

Time elapsed: 00:00:01

Username: test

Roles: System administrator, Administrators

Figure 135. The 'Event Log' tab for the SoftControl SysCmd component

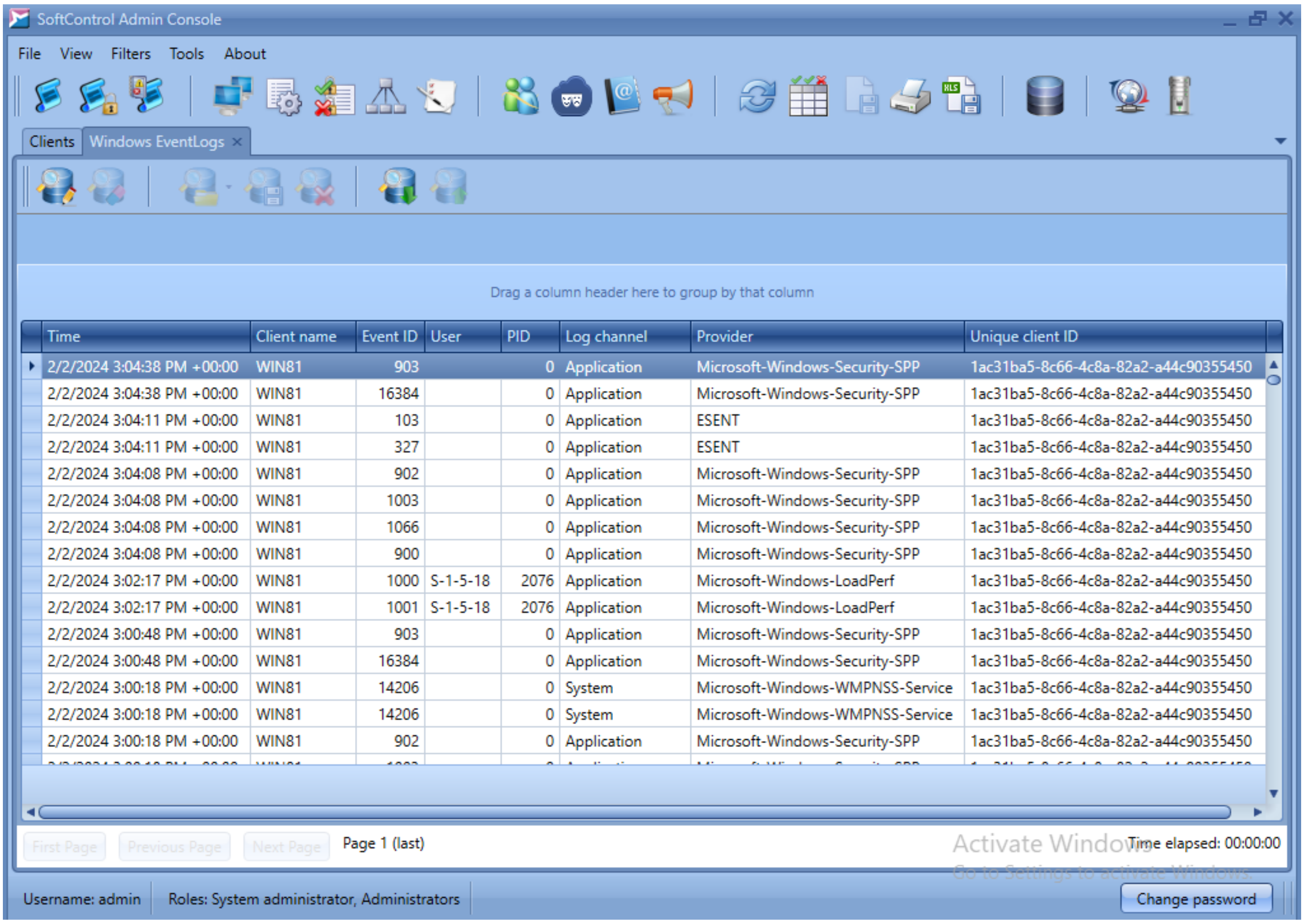
The full list of the tab fields for the SoftControl SysCmd component is given in table 26.

Table 26. The 'Event Log' tab fields for SoftControl SysCmd

Field	Description
Client name	The name of the client host.
Event ID	Unique event identifier. If SoftControl Admin Console receives an event with the duplicated identifier, the duplicated string is highlighted in red. If there is a break in the order of the identifiers (i.e., gaps in the sequence exist), the corresponding warning is added to the server component report in the Windows event log[182]. The exception is the events of the **Status** type. The **Event ID** parameter can be either *-1* or *-2* for them.
Unique client ID	Unique identifier of a client host. The identifier is assigned automatically after SoftControl SysCmd sends a request to SoftControl Server for the first time.
Event type	Type of the data collection event: • **client update**; • **status.**
Time	Date and time when the event occurred.
Importance	The event importance (priority) from the viewpoint of a threat to a client host's information security: • trivial; • high; • critical. Each priority level has the corresponding cell color.
Client status	The status of the registered client component: • **active**; • **inactive**; • **service was interrupted**; • **status error. invalid status**.
Action	Action when a **client update** event occurs: • **starting the updates**; • **update completed**.
Action status	Action status when a **client update** event occurs: • **update is running**; • **error when running the update**; • **no updates found**; • **update interrupted by user**; • **updates installed successfully**; • **system reboot is required**; • **update completed with errors**.

4.9.4 Windows Event Logs

The **Windows Event Logs** tab allows to view Windows event logs from client hosts (fig. The "Windows Event Logs" tab[142]).


SoftControl Admin Console
File View Filters Tools About
Clients Windows EventLogs
Drag a column header here to group by that column
First Page Previous Page Next Page Page 1 (last)
Activate Windows
Go to Settings to activate Windows.
Time elapsed: 00:00:00
Username: admin
Roles: System administrator, Administrators
Change password

Time	Client name	Event ID	User	PID	Log channel	Provider	Unique client ID
2/2/2024 3:04:38 PM +00:00	WIN81	903		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:38 PM +00:00	WIN81	16384		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:11 PM +00:00	WIN81	103		0	Application	ESENT	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:11 PM +00:00	WIN81	327		0	Application	ESENT	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:08 PM +00:00	WIN81	902		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:08 PM +00:00	WIN81	1003		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:08 PM +00:00	WIN81	1066		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:04:08 PM +00:00	WIN81	900		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:02:17 PM +00:00	WIN81	1000	S-1-5-18	2076	Application	Microsoft-Windows-LoadPerf	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:02:17 PM +00:00	WIN81	1001	S-1-5-18	2076	Application	Microsoft-Windows-LoadPerf	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:00:48 PM +00:00	WIN81	903		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:00:48 PM +00:00	WIN81	16384		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:00:18 PM +00:00	WIN81	14206		0	System	Microsoft-Windows-WMPNSS-Service	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:00:18 PM +00:00	WIN81	14206		0	System	Microsoft-Windows-WMPNSS-Service	1ac31ba5-8c66-4c8a-82a2-a44c90355450
2/2/2024 3:00:18 PM +00:00	WIN81	902		0	Application	Microsoft-Windows-Security-SPP	1ac31ba5-8c66-4c8a-82a2-a44c90355450

Figure 136. The "Windows event logs" tab

Note that in one heartbeat (the interval between requests by SoftControl SysWatch to SoftControl Server, 60 seconds by default) the client device sends not more than 1000 events. If for a long period of time a larger number of events is generated in Windows logs during one heartbeat, events will fail to be delivered to the server, which may lead to loss of events.

Specific fields for events from Windows Event Log described in table 27.

Table 27. Fields of the tab Windows Event Logs

Field	Description
<column without name>	For events with detailed information, the sign ⊕ allows to view it.
Time	Date and time of registration of the event.
Client name	The name of the client host.
Event ID	Event identifier in Windows Event Log.
User	The security identifier of the user (SID) under which the event occurred.
PID	The unique sequential process identifier (PID) in the OS for the event.
Log channel	Log name: • **Application;** • **System;**

Field	Description
	- **Security;** - **SafenSoft.** Events from the SafenSoft log are registered by SoftControl Server and can present in Windows Event Log if SoftControl SysWatch runs on the server.
Provider	Event source.
OpCode	Operation code defined by the provider for logical grouping of events.
Unique client ID	Unique identifier of a client host. The identifier is assigned automatically after SoftCon-trol SysWatch sends a request to SoftControl Server for the first time.

4.9.5 Filtering the events

Page representation

Information on the **Event Log** tab is displayed page by page. The maximum number of events per page is specified in the SoftControl Admin Console interface settings[31] (it is 10 000 events by default).

> We do not recommend that you set the **Events page size** parameter to more than 100 000 to prevent loss of performance.

Entries in the table are displayed on pages in chronological order, i.e., the most recent entries are on the first page. To navigate between pages, use the corresponding buttons at the bottom (fig. Page navigation[144]). You can only switch to the previous/next page.

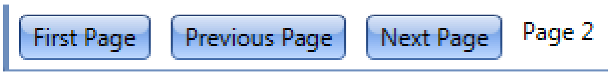


Figure 137. Page navigation

Data grouping

For the convenience, information on the **Event Log** tab can be grouped by any field (category). On the additional **Scanner** tab, you can group data by the **Path** (by default), **Virus**, **Scan result** and **Scan action** fields (categories). To do so, drag the column header to the panel between the table header and the group of buttons on the tab (see figures from The 'Log' tab for the SoftControl DLP Client component[136] to Shadow copy of the monitored object[140] in section above[136]). If you group by several categories, the priority (category nesting) decreases from left to right depending on the location on the panel.

Filtering by the preset filters

SoftControl Admin Console has the preset filters to make a sample of events.

To apply common built-in filters, open the **Filters** menu and select one of the options:

- **Default view** – display all types of events on fields that contain the main information (the filter applies by default when the tab opens).
- **Full view** – display all types of events on all fields.
- **Status** – display the events of changing the client application status.
- **Client updating** – display the events of updating the client applications.

To apply built in filters that correspond to the SoftControl SysWatch events, open the **Filters** → **SysWatch Events Filters** menu and select one of the options:

- **All**;
- **Policy violation**;
- **Activity control**;
- **Process start**;
- **Antivirus scanning**;
- **Settings modification**;
- **User logon**;
- **User logoff**;
- **Service event**.

To apply built-in filters that correspond to the SoftControl DLP Client events, open the **Filters** → **DLP Events Filters** menu and select one of the options:

- **All**;
- **Hardware added**;
- **File**;
- **HTTP**;
- **Keylogger**;
- **Printer**;
- **Registry**;
- **Hardware removed**;
- **Work time**.

Filtering applies to the entries on the current page only.

If there is a large number of events, progress bar is displayed while applying the filter. You can stop the process if necessary.

Filtering by custom filters

You can set up the selection options and save them as a custom filter that is invoked from the **Filters** → **User filters** menu.

To add a new field to the current tab's table, click **Choose columns** and drag the required field from the **Column chooser** window (fig. Choosing the columns[146]) to the required place in the table header. To remove an existing field, drag it to the **Column chooser** window, or out of the table header.

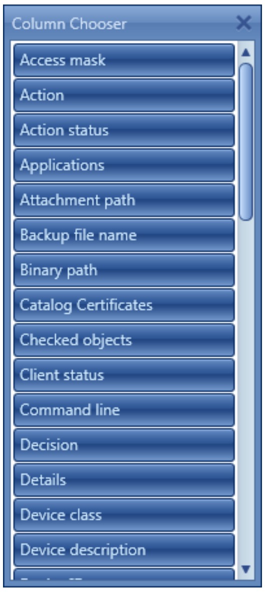


Figure 138. Choosing the columns

To filter the selection by field values, move the cursor to the field name, left-click the displayed key icon and specify the selection criteria in the drop-down list (fig. Filter by field[146]). The selection can be filtered by several fields at the same time. The key icon is constantly displayed in the headers of the fields that are filtered.

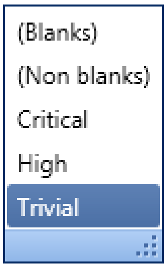
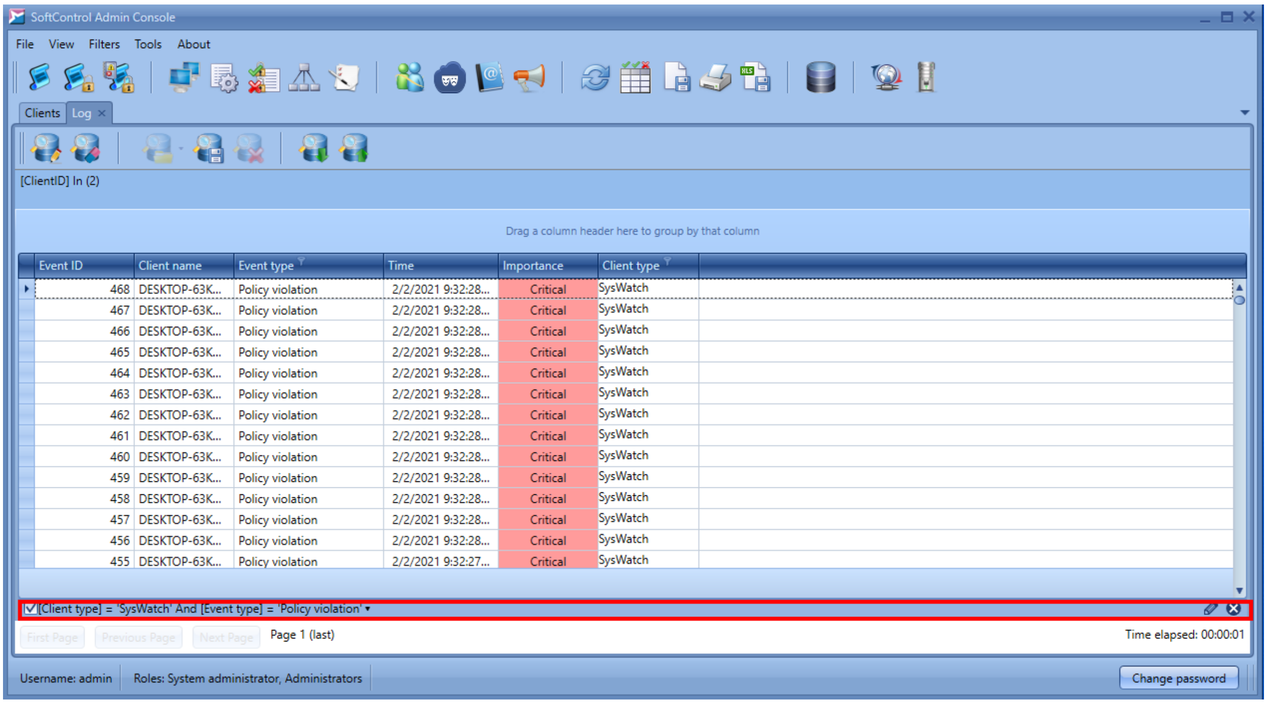


Figure 139. Filter by field

When you filter the entries, you will see the details about your filter at the bottom. You can reset or change it by clicking on the icons on the right.



[ClientID] In (2)

Event ID	Client name	Event type	Time	Importance	Client type
468	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
467	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
466	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
465	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
464	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
463	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
462	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
461	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
460	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
459	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
458	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
457	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
456	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
455	DESKTOP-63K...	Policy violation	2/2/2021 9:32:27...	Critical	SysWatch

☑ [Client type] = 'SysWatch' And [Event type] = 'Policy violation'

Page 1 (last)

Time elapsed: 00:00:01

Username: admin

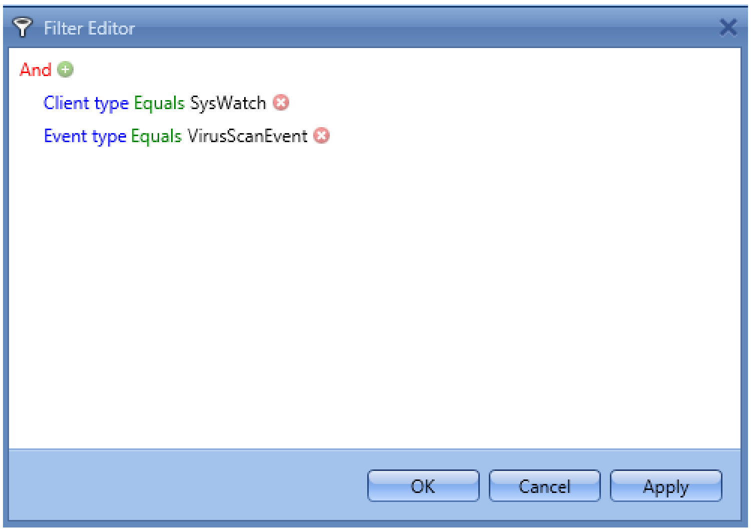
Roles: System administrator, Administrators

Figure 140. Filter settings

Click on the pencil icon to the right of the filter parameters to open the **Filter Editor**.

SoftControl Admin Console enables fine tuning the selection parameters via the **Filter Editor** tool. If a filter by some field is applied on the **Log** tab, a string with the filter parameters is displayed in the lower part of the tab.

The editor window is shown in fig. Filter editor 147.



And
Client type Equals SysWatch
Event type Equals VirusScanEvent

Figure 141. Filter editor

The first line contains logical operation (highlighted in red) that applies to the filter parameters. To change it, left-click it and select one of the following logical operators from the drop-down menu:

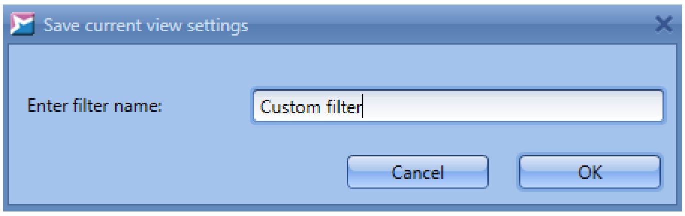
- And;
- Or;
- NotAnd;
- NotOr.

To add a new filter parameter, click the plus icon near the logical operation. Click **OK** to save filter parameters.

The string syntax for a filter parameter is as follows: *<filtered field> <condition> <value>*. Each element in the parameter string can be changed by clicking it. The conditions are detected automatically depending on the field type.

To sort the data in the tab tables by certain fields, left-click the required field and specify the direction of the sorting by clicking. The direction of the sorting is indicated by an arrow on the right-hand side of the field header.

To save the selection with the user-specified parameters for later use, click **Save view settings**, enter the filter name in the displayed window and click **OK** (fig. Saving the filter 148).



Enter filter name: Custom filter

Figure 142. Saving the filter

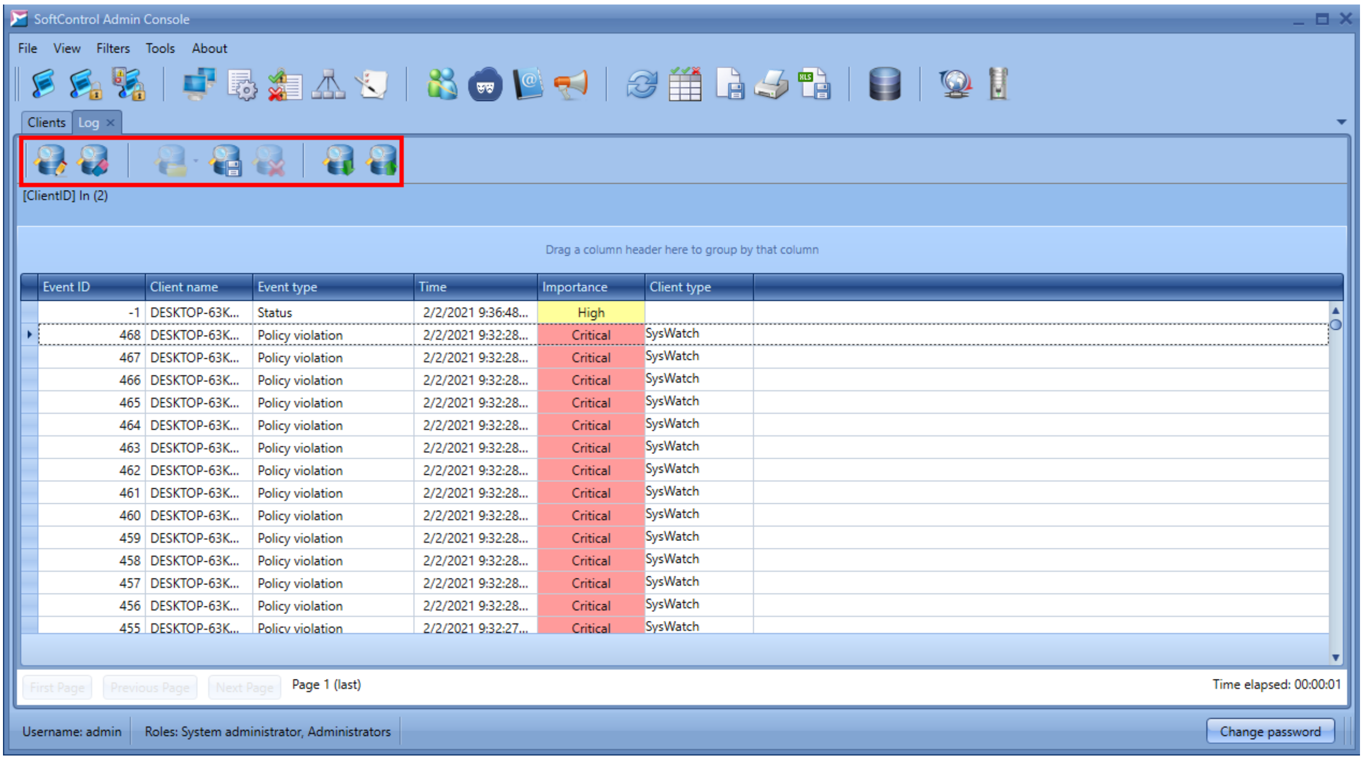
Filtering applies to the entries of the current page only.

If there is a large number of events, progress bar is displayed while applying the filter. You can stop the process if necessary.

4.9.6 Database queries

If you often search for entries that fall under a specific search query, you can save the query and then upload it from the memory to get the desired entries from the database.

Use icons located on the additional board to manage database queries.



SoftControl Admin Console
File View Filters Tools About
Clients Log
Drag a column header here to group by that column
First Page Previous Page Next Page Page 1 (last)
Change password

[ClientID] In (2)

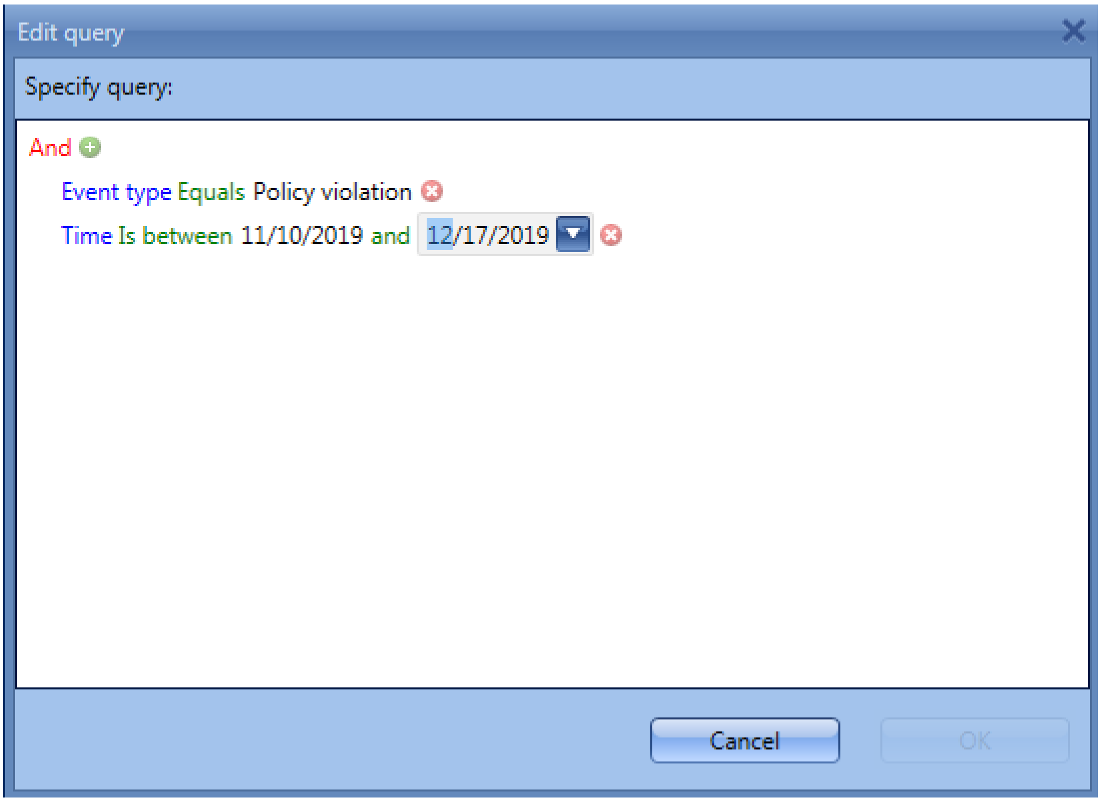
Event ID	Client name	Event type	Time	Importance	Client type
-1	DESKTOP-63K...	Status	2/2/2021 9:36:48...	High	
468	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
467	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
466	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
465	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
464	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
463	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
462	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
461	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
460	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
459	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
458	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
457	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
456	DESKTOP-63K...	Policy violation	2/2/2021 9:32:28...	Critical	SysWatch
455	DESKTOP-63K...	Policy violation	2/2/2021 9:32:27...	Critical	SysWatch

Time elapsed: 00:00:01

Username: admin Roles: System administrator, Administrators

Figure 143. Buttons for managing queries

To create a query, click (**Edit query**). The query editor window opens.



And

Event type Equals Policy violation

Time Is between 11/10/2019 and 12/17/2019

Figure 144. Query editor

The first line contains logical operation (highlighted in red) that applies to the filter parameters. To change it, left-click it and select one of the following logical operators from the drop-down menu:

- And;
- Or;
- NotAnd;
- NotOr.

To add a new filter parameter, click the plus icon near the logical operation. Click **OK** to save filter parameters.

The string syntax for a filter parameter is as follows: <*filtered field*> <*condition*> <*value*>. Each element in the parameter string can be changed by clicking it. The conditions are detected automatically depending on the field type.

Find all icons for managing queries in the table below.

Table 28. Database queries

Icon	Name	Description
	Edit query	Opens the query editor. You can select parameters and their values here
	Clear query	Cancels active query criteria
	Select query	Allows to select a query from the list of your saved queries. The queries are stored here: `C:\ProgramData\SafenSoft\UserFilters\QueryCriteria.xml`
	Save query	Saves the active query in this file: `C:\ProgramData\SafenSoft\UserFilters\QueryCriteria.xml`
	Deleting queries	Opens the windows with your saved queries and allows to delete queries
	Import query	Allows to select an XML file and import a query from the file
	Export query	Exports the active query to an XML file

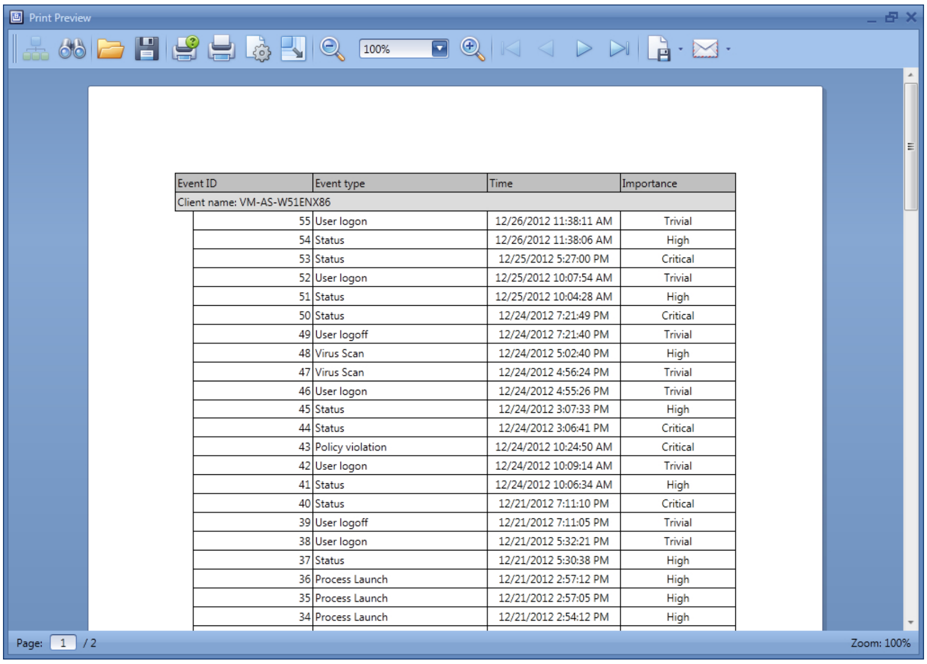
4.9.7 Printing out and exporting

SoftControl Admin Console allows you to export the information accumulated in the client application reports.

To print out a report, make a selection with the use of the required filters[144] and click **Print**. In the displayed print preview window, you can specify **Page setup** and **Scale** with the help of the corresponding buttons (fig. Print preview[151]).

Click **Print** to open standard printer settings window, or click **Quick Print** to print out the report instantly with the default printer settings.

To save a report to Excel, make a selection with the use of the required filters[144] and click **Export to Excel**. Specify the path to save the report and the report name in the dialog box and click **Save**.

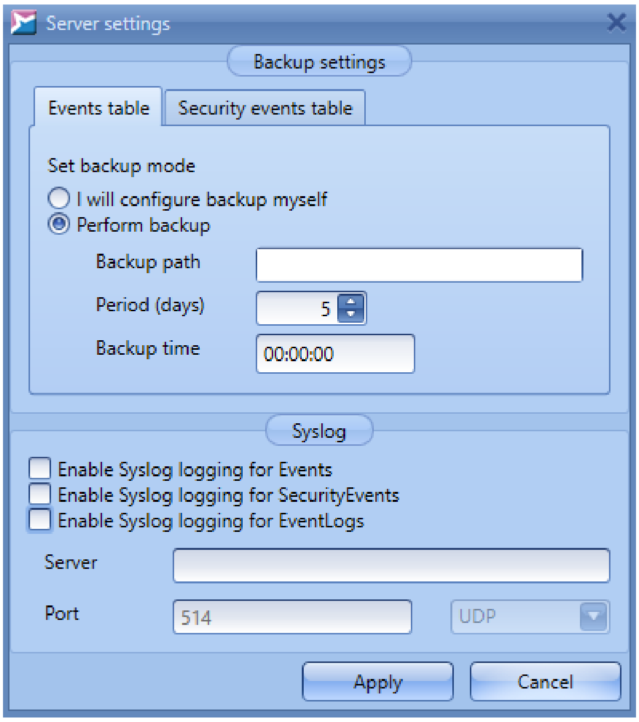


Event ID	Event type	Time	Importance
Client name: VM-AS-W51ENX86			
55	User logon	12/26/2012 11:38:11 AM	Trivial
54	Status	12/26/2012 11:38:06 AM	High
53	Status	12/25/2012 5:27:00 PM	Critical
52	User logon	12/25/2012 10:07:54 AM	Trivial
51	Status	12/25/2012 10:04:28 AM	High
50	Status	12/24/2012 7:21:49 PM	Critical
49	User logoff	12/24/2012 7:21:40 PM	Trivial
48	Virus Scan	12/24/2012 5:02:40 PM	High
47	Virus Scan	12/24/2012 4:56:24 PM	Trivial
46	User logon	12/24/2012 4:55:26 PM	Trivial
45	Status	12/24/2012 3:07:33 PM	High
44	Status	12/24/2012 3:06:41 PM	Critical
43	Policy violation	12/24/2012 10:24:50 AM	Critical
42	User logon	12/24/2012 10:09:14 AM	Trivial
41	Status	12/24/2012 10:06:34 AM	High
40	Status	12/21/2012 7:11:10 PM	Critical
39	User logoff	12/21/2012 7:11:05 PM	Trivial
38	User logon	12/21/2012 5:32:21 PM	Trivial
37	Status	12/21/2012 5:30:38 PM	High
36	Process Launch	12/21/2012 2:57:12 PM	High
35	Process Launch	12/21/2012 2:57:05 PM	High
34	Process Launch	12/21/2012 2:54:12 PM	High

Figure 145. Print preview

4.9.8 Backing up the reports

SoftControl Admin Console allows you to back up the tables with the event log and the security events. To set the backup options, select **Server settings** in the **File** menu in SoftControl Admin Console. In the displayed window (fig. Backing up the events[151]), switch to the **Events table** tab or to the **Security events table** tab depending on what events you need to back up. On either tab, select **Perform backup** and specify **Backup path** on the server to save the tables to, **Period** (in days), and **Backup time**.



Set backup mode

○ I will configure backup myself

● Perform backup

Backup path:

Period (days): 5

Backup time: 00:00:00

□ Enable Syslog logging for Events

□ Enable Syslog logging for SecurityEvents

□ Enable Syslog logging for EventLogs

Server:

Port: 514 UDP

Figure 146. Backing up the events

You can also back up the reports with the help of third-party software, without the use of SoftControl Service Center tools. Select **I will configure backup myself** in the **Server settings** window (see above[151]) in this case.

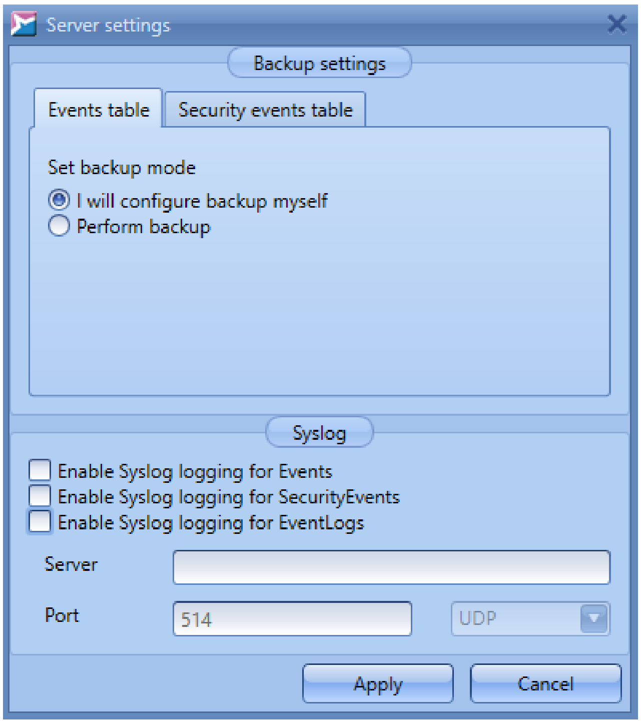
4.9.9 Sending events with Syslog protocol

You can send events to an external server with the Syslog protocol. To do this, select **Server settings** in the **File** menu in SoftControl Admin Console.

In the **Syslog** area, check necessary options:

- Enable Syslog logging for Events – all events from client devices (**Event**),
- Enable Syslog logging for SecurityEvents – all SoftControl management events (**SecurityEvent**),
- Enable Syslog logging for EventLogs – all events from tracked Windows logs on the devices (**EventLog**).

Then enter the name of the server, the port number, and select the protocol type.



Set backup mode

● I will configure backup myself

○ Perform backup

□ Enable Syslog logging for Events

□ Enable Syslog logging for SecurityEvents

□ Enable Syslog logging for EventLogs

Server

Port 514 UDP

Figure 147. Settings for Syslog

Messages sent to an external server using the Syslog protocol conform with the standard RFC 5424. You can find event details inside the STRUCTURED-DATA element of a Syslog message. Read more in the following articles:

- http://kb.safensoft.com/index.php/Sending_events_with_Syslog_protocol – elements of a Syslog message;
- http://kb.safensoft.com/index.php/Information_about_SoftControl_events – SoftControl events.

4.10 Events notifications

Notifications (warnings) about the events that are registered in SoftControl Service Center allow a security administrator to promptly react to the appearing threats, even if he/she does not have access to the workstation with the installed SoftControl Admin Console at the moment.

First of all, you need to specify the contacts 153 of the notification recipients; then you should set up notification sending parameters 155.

4.10.1 Contacts

You can specify the recipients of notifications on the **Contacts** tab (fig. The 'Contacts' tab 154).

Basic operations with the contacts are performed via the tab's graphical buttons that are described in table 29.

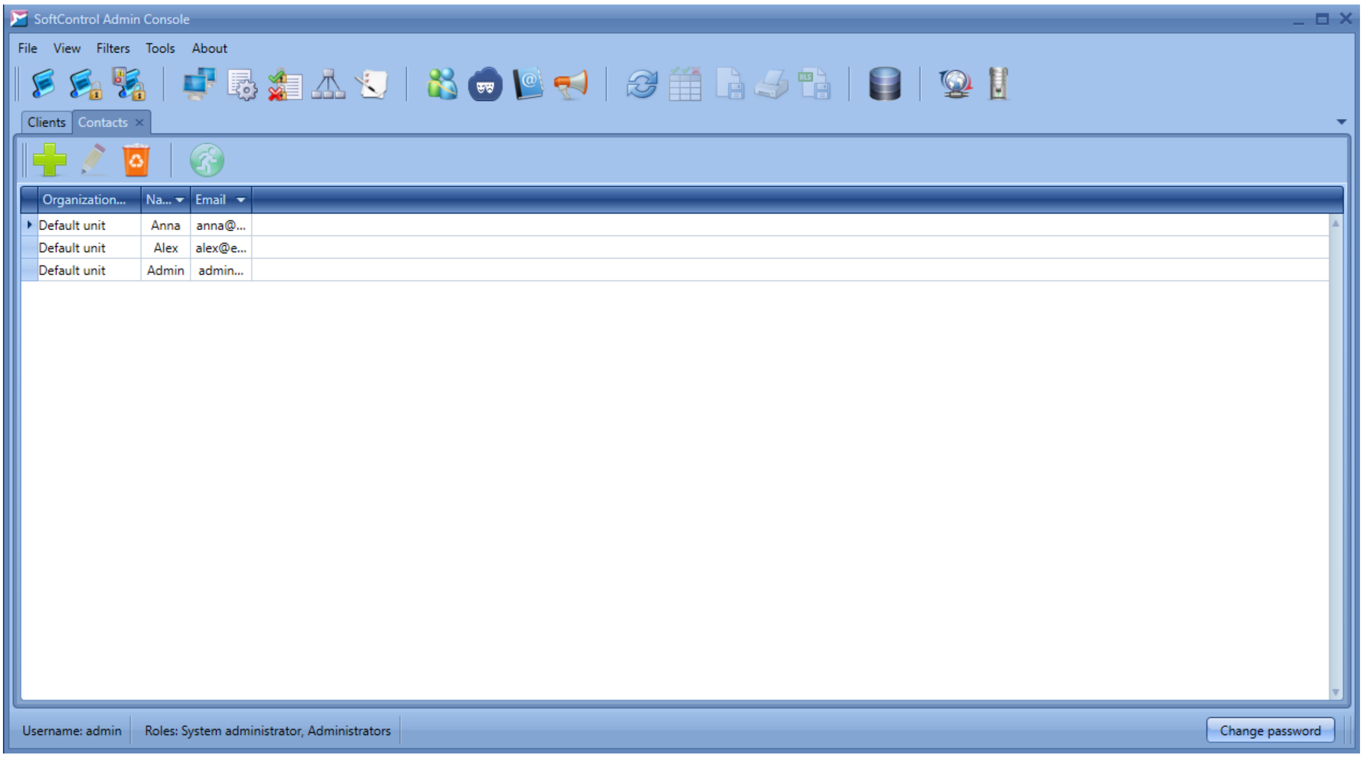
Table 29. The 'Contacts' tab widgets

Button	Name	Description
➕	New	Create a new contact.
✎	Edit	Modify the properties of the selected contact.
🗑	Delete	Remove the selected contact(s).
🏃	Move	Move the selected contact to another organization unit.

The list of the tab fields is given in table 30.

Table 30. The 'Contacts' tab fields

Field	Description
Organization unit	The organization unit that the contact is assigned to.
Name	The recipient's name.
Email	The recipient's e-mail address.

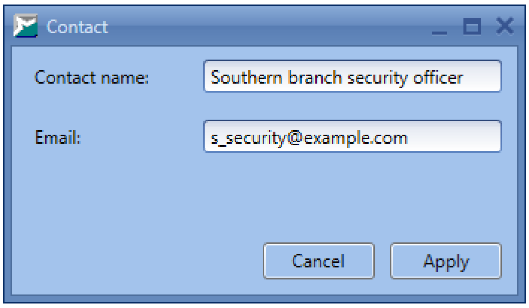


Organization...	Na...	Email
Default unit	Anna	anna@...
Default unit	Alex	alex@e...
Default unit	Admin	admin...

Figure 148. The 'Contacts' tab

To add a new recipient, click **New** (fig. The 'Contacts' tab[154]). Specify the recipient data in the **Contact Name** and **Email fields** and then click **Apply** (fig. Adding a contact[154]).

To modify and remove contacts, use the corresponding buttons.



Contact

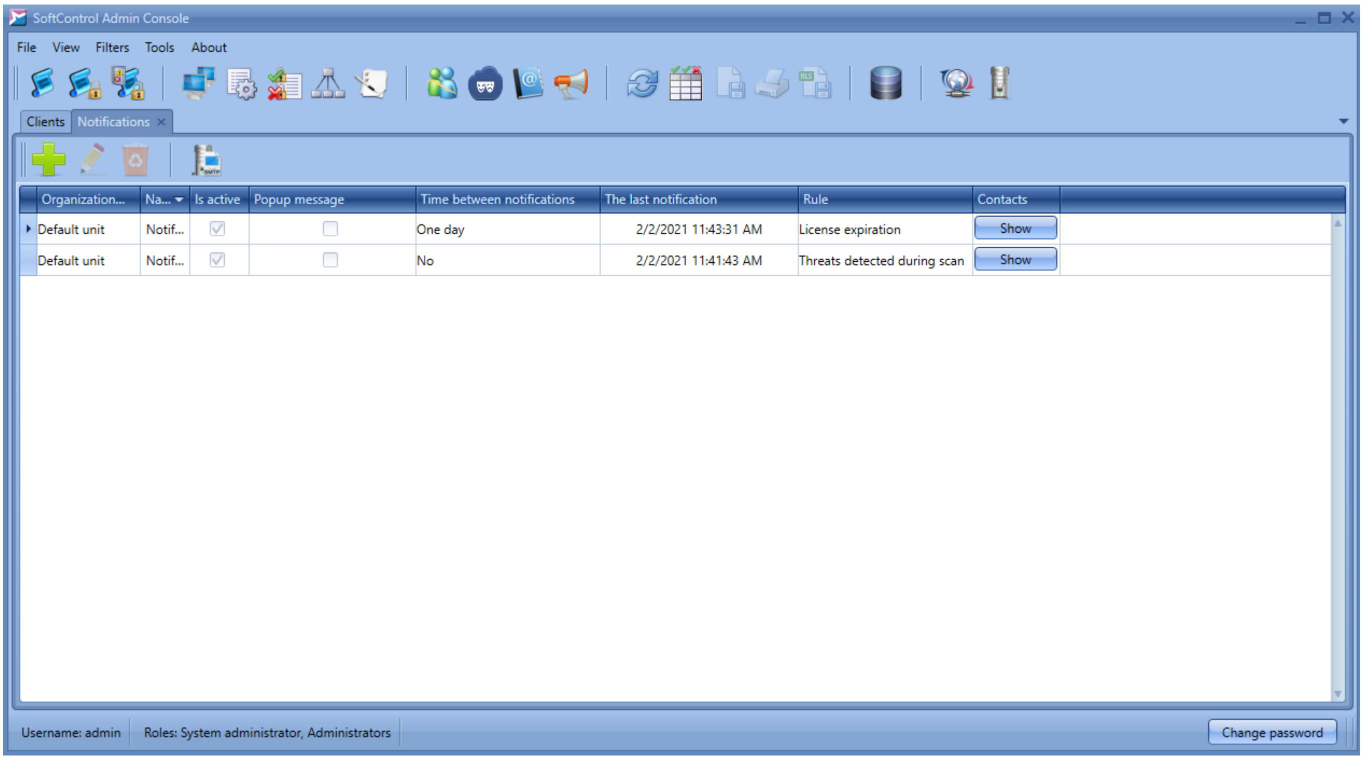
Contact name: Southern branch security officer

Email: s_security@example.com

Figure 149. Adding a contact

4.10.2 Setting up notifications

The **Notifications** tab is designed to set up the options of sending event notifications via email (fig. The 'Notifications' tab[155]).



	Organization...	Na...	Is active	Popup message	Time between notifications	The last notification	Rule	Contacts
▸	Default unit	Notif...	☑	□	One day	2/2/2021 11:43:31 AM	License expiration	Show
	Default unit	Notif...	☑	□	No	2/2/2021 11:41:43 AM	Threats detected during scan	Show

Username: admin Roles: System administrator, Administrators

Figure 150. The 'Notifications' tab

Basic operations with the notifications are performed via the tab's graphical buttons that are described in table 31.

Table 31. The 'Notifications' tab widgets

Button	Name	Description
✚	New	Create a new notification.
✏	Edit	Modify the properties of the selected notification.

Button	Name	Description
🗑	Delete	Remove the selected notification(s).
SMTP	SMTP	Set up the SMTP server.

The list of the tab fields is given in table 32.

Table 32. The 'Notifications' tab fields

Field	Description
Organization unit	The organization unit that the notification belongs to. You cannot move a notification to another organization unit. The organization unit of a notification is the same as the organization unit of the user who created the notification.
Name	Notification name.
Is active	Notification activity status flag.
Popup message	The flag that indicates whether a popup message is displayed when sending the notification.
Sending period	Minimum time interval after the previous notification has been sent. A new notification can be sent after this period expires.
The last notification	Time when the last modification has been sent.
Rule	The condition that triggers the notification.
Contacts	The list of the notification recipients.

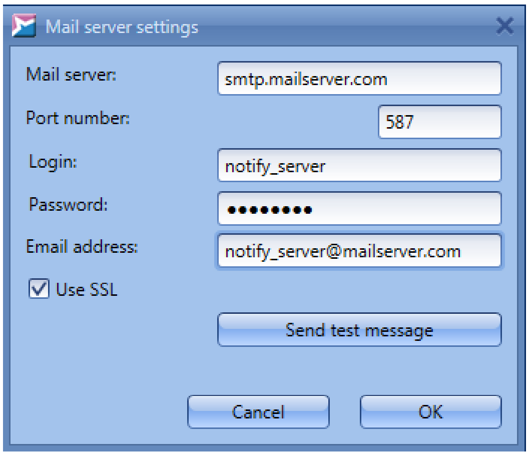
Basic operations on this tab are as follows.

Setting up the SMTP server

To enable notifications, you need to configure the outgoing mail server (SMTP). To do so, click **SMTP** (fig. The 'Notifications' tab[155]).

Specify the address of the mail server to send notifications in the **Mail server** field of the **Mail server settings** window, and **Port number** in the corresponding field (fig. Mail server settings[156]). Specify the account data in the **Login** and **Password** fields and **Email address** to send the notifications from. Tick off the **Use SSL** checkbox to secure enable data transfer.

To verify the specified settings, click **Send test message**.


Mail server settings

Mail server: smtp.mailserver.com

Port number: 587

Login: notify_server

Password: ●●●●●●●●

Email address: notify_server@mailserver.com

☑ Use SSL

Figure 151. Mail server settings

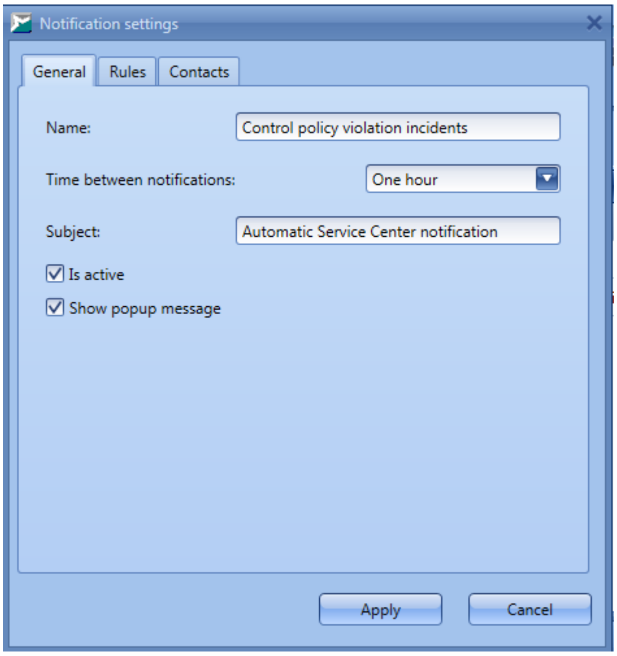
Click **OK** to apply settings.

Creating a notification

To add a new notification, click **New** (fig. The 'Notifications' tab[155]).

Specify the notification **Name** on the **General** tab of the displayed window, select the minimum **Time between notifications** in the drop-down list, enter the **Subject** of the message and tick off the **Is active** checkbox (fig. General notification parameters[157]).

To **Show popup message** when the notification is sent, tick off the corresponding checkbox. In this case, a pop-up message with the notification header is displayed after the notification is sent (fig. Pop-up message[157]).


Notification settings

Name: Control policy violation incidents

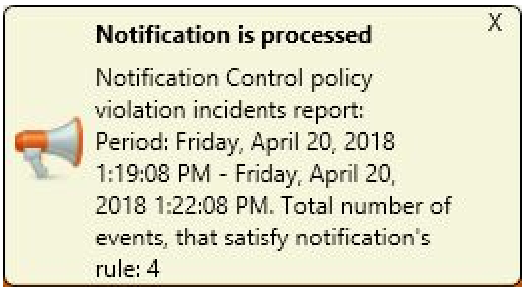
Time between notifications: One hour

Subject: Automatic Service Center notification

☑ Is active

☑ Show popup message

Figure 152. General notification parameters

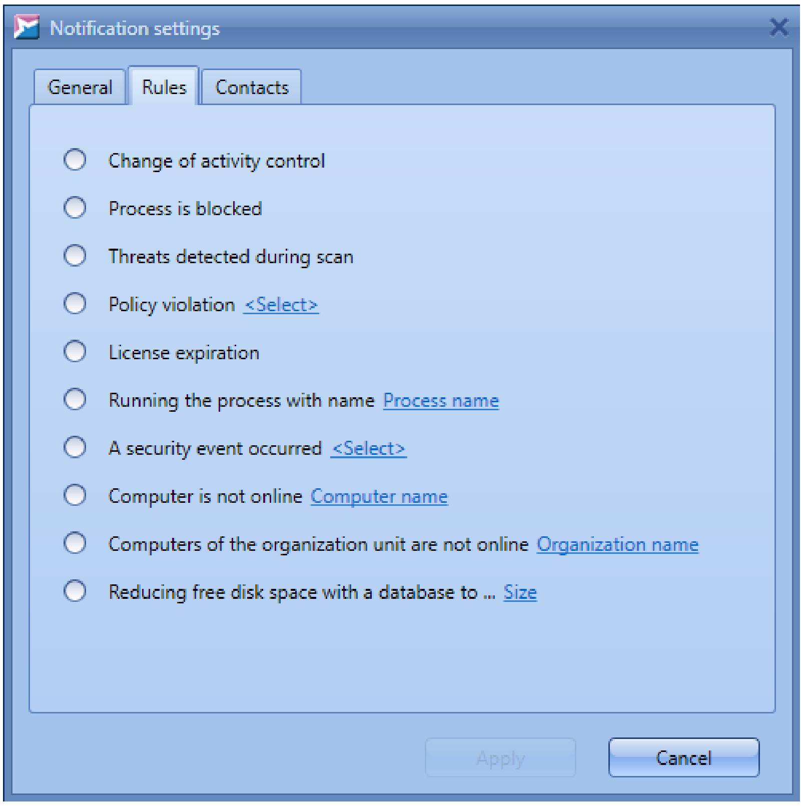


Notification is processed

Notification Control policy violation incidents report: Period: Friday, April 20, 2018 1:19:08 PM - Friday, April 20, 2018 1:22:08 PM. Total number of events, that satisfy notification's rule: 4

Figure 153. Pop-up message

On the **Rules** tab, select the condition that triggers the notification (fig. Conditions that trigger notification 158):



Notification settings

○ Change of activity control

○ Process is blocked

○ Threats detected during scan

○ Policy violation <Select>

○ License expiration

○ Running the process with name Process name

○ A security event occurred <Select>

○ Computer is not online Computer name

○ Computers of the organization unit are not online Organization name

○ Reducing free disk space with a database to ... Size

Figure 154. Conditions that trigger notification

○ **Change of activity control**:

the SoftControl SysWatch activity control status for any area has changed.

○ **Process is blocked**:

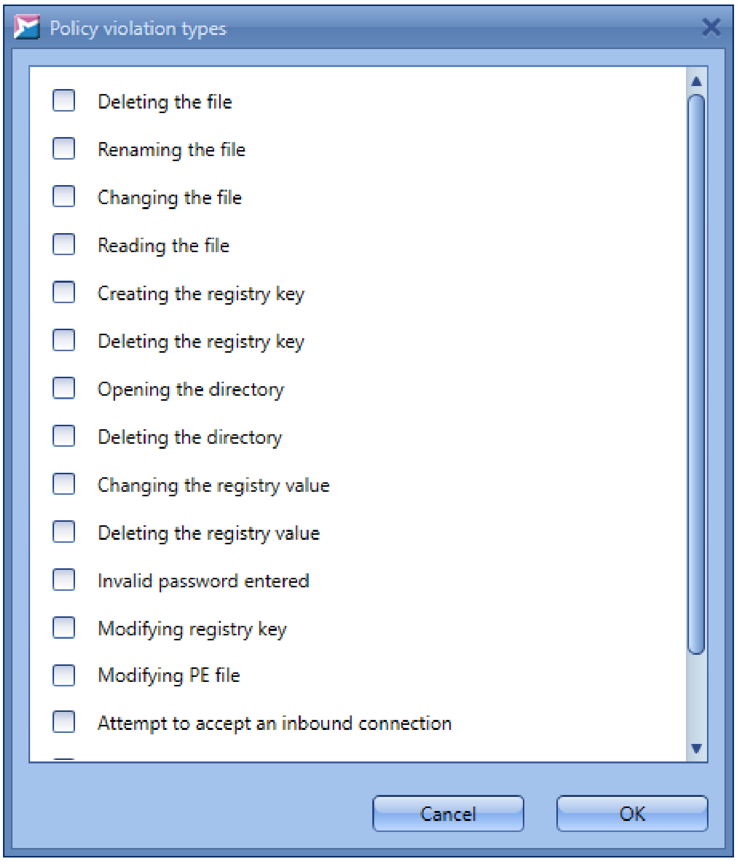
SoftControl SysWatch has registered the event of the **process start** type with the 'denied' decision.

○ **Threats detected during scan**:

SoftControl SysWatch has detected malicious code during antivirus check.

○ **Policy violation**:

SoftControl SysWatch has detected a **policy violation** event (or several events) that you can select by clicking **<Select>** (fig. Selecting control policy types to send notifications for[159]).



□ Deleting the file
□ Renaming the file
□ Changing the file
□ Reading the file
□ Creating the registry key
□ Deleting the registry key
□ Opening the directory
□ Deleting the directory
□ Changing the registry value
□ Deleting the registry value
□ Invalid password entered
□ Modifying registry key
□ Modifying PE file
□ Attempt to accept an inbound connection

Figure 155. Selecting control policy types to send notifications for

○ **License expiration**:

a client component's license key expires in less than 10 days.

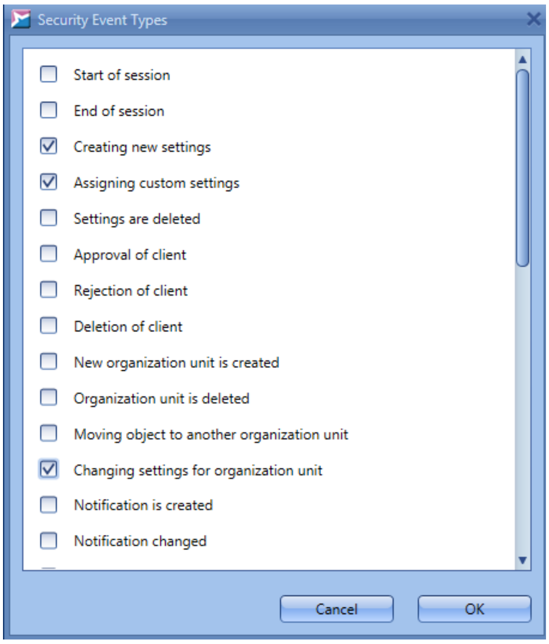
We strongly recommend that you set the **Time between notifications** parameter for this notification to at least 4 hours.

○ **Running the process with name**:

SoftControl SysWatch has registered the event of the **process start** type, with the specified **Process name**.

○ **A security events occured**:

SoftControl SysWatch has detected a security event (or several events) that you can select by clicking **<Select>** (fig. Selecting security events to send notifications for[159]).



- □ Start of session
- □ End of session
- ☑ Creating new settings
- ☑ Assigning custom settings
- □ Settings are deleted
- □ Approval of client
- □ Rejection of client
- □ Deletion of client
- □ New organization unit is created
- □ Organization unit is deleted
- □ Moving object to another organization unit
- ☑ Changing settings for organization unit
- □ Notification is created
- □ Notification changed

Figure 156. Selecting security events to send notifications for

○ **Computer is not online**:

The selected client does not communicate with the server for the specified time (in seconds). You cannot specify a time less than 2 heartbeat periods of the specified client settings.

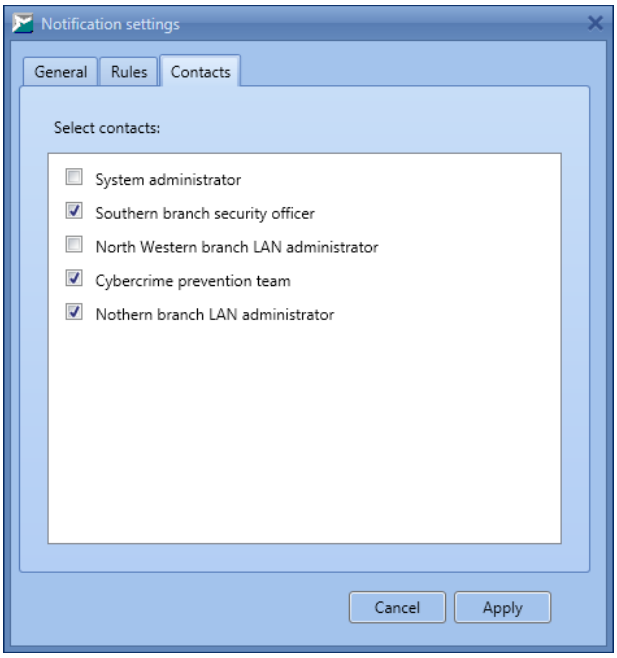
○ **Computers of the organization unit are not online**:

Clients from the selected organization unit do not communicate with the server during the specified time (in seconds). You cannot specify a time of less than 2 heartbeat periods of the specified unit settings.

○ **Reducing free disk space with a database to ...:**

Free space on the database hard drive has become less than the specified number of MB.

Switch to the **Contacts** tab and select the notification recipients (fig. Selecting notification recipients 160).



Select contacts:

☐ System administrator
☑ Southern branch security officer
☐ North Western branch LAN administrator
☑ Cybercrime prevention team
☑ Nothern branch LAN administrator

Figure 157. Selecting notification recipients

Click **Apply** to create the notification with the specified options.

Modifying notification properties

To change the notification properties, select the notification and perform one of the following operations:

- click **Edit** in the tab buttons group (fig. The 'Notifications' tab 155);
- double-click the notification.

In the the displayed window, modify the required parameters, as you do with a new configuration (fig. General notification parameters 157, Conditions that trigger notification 158, Selecting notification recipients 160).

Click **Apply** to confirm changes.

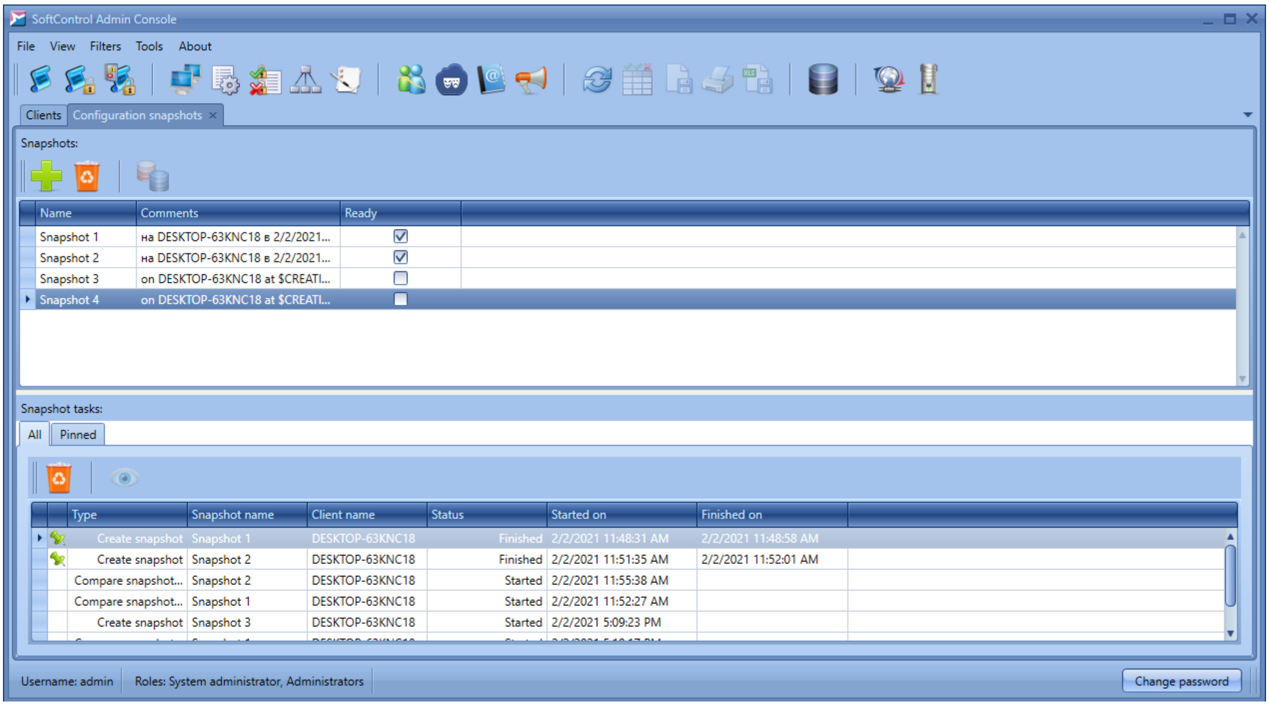
Disabling and removing notification

If you need to disable a notification without removing it from the list, open the notification settings window, deselect the **Is active** checkbox on the **General** tab and click **OK** (fig. General notification parameters 157).

To remove a notification, select it, press **Delete** (fig. The 'Notifications' tab 155) and confirm the removal in the dialog box.

4.11 Configuration snapshots

The **Configuration snapshots** tab is designed to create snapshots of the configuration of any connected client host. A configuration snapshot is the profile of the computer with the installed SoftControl SysWatch client application. SoftControl Admin Console allows you to compare snapshots with the current states of the selected client hosts.



Name	Comments	Ready
Snapshot 1	на DESKTOP-63KNC18 в 2/2/2021...	☑
Snapshot 2	на DESKTOP-63KNC18 в 2/2/2021...	☑
Snapshot 3	on DESKTOP-63KNC18 at $CREATI...	□
Snapshot 4	on DESKTOP-63KNC18 at $CREATI...	□

Type	Snapshot name	Client name	Status	Started on	Finished on
Create snapshot	Snapshot 1	DESKTOP-63KNC18	Finished	2/2/2021 11:48:31 AM	2/2/2021 11:48:58 AM
Create snapshot	Snapshot 2	DESKTOP-63KNC18	Finished	2/2/2021 11:51:35 AM	2/2/2021 11:52:01 AM
Compare snapshot...	Snapshot 2	DESKTOP-63KNC18	Started	2/2/2021 11:55:38 AM	
Compare snapshot...	Snapshot 1	DESKTOP-63KNC18	Started	2/2/2021 11:52:27 AM	
Create snapshot	Snapshot 3	DESKTOP-63KNC18	Started	2/2/2021 5:09:23 PM	

Figure 158. 'Configuration snapshots' tab

The **Configuration snapshots** button is only available to users who have all of the following permissions: **View clients connected to server**, **Create new tasks for clients**, **View existing organization units**.

The tab consists of two sections:

- snapshots[163];
- snapshot tasks[165].

4.11.1 Snapshots

Basic operations with the snapshots in the **Configuration snapshots** section are performed via the tab graphical buttons which are described in table 33.

Table 33. The 'Snapshots' section widgets

Button	Name	Description
✚	Add new	Create a new configuration snapshot.
🗑	Delete	Remove the selected snapshot.
🛢	Compare	Compare the created snapshot with a client host's profile.

List of the section fields is given in table 34.

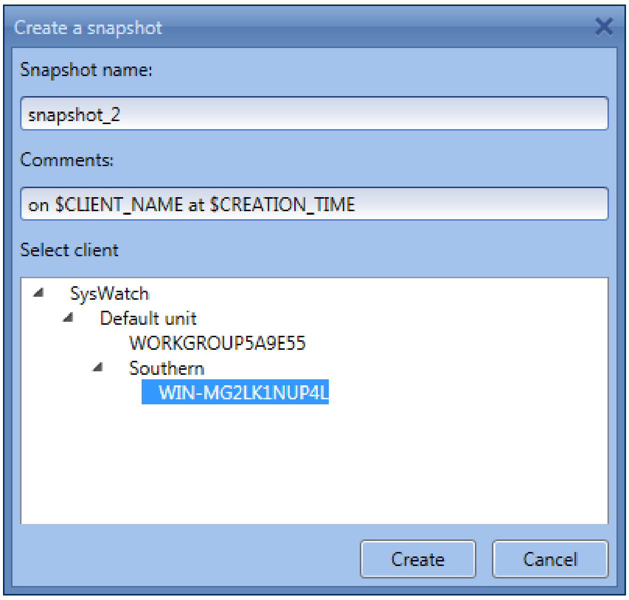
Table 34. The 'Snapshots' section fields

Field	Description
Name	The name of the task.
Comments	Text comments. The name of the client host and the snapshot creation time are specified by default.
Ready	The indication that the task is finished. This checkbox is ticked off after the client host responds.

Operations on this tab are described below.

Creating a snapshot

To create a configuration snapshot, click ✚ (**Add new**) (fig. 'Configuration snapshots' tab[162]). In the displayed window, specify the name of the snapshot, select a client host to snapshot and click **Apply** (fig. Creating a snapshot[163]). The snapshot creation task is then generated, and the corresponding entry appears in the table[166] in the **Snapshot tasks** section.



Create a snapshot

Snapshot name: snapshot_2

Comments: on $CLIENT_NAME at $CREATION_TIME

Select client

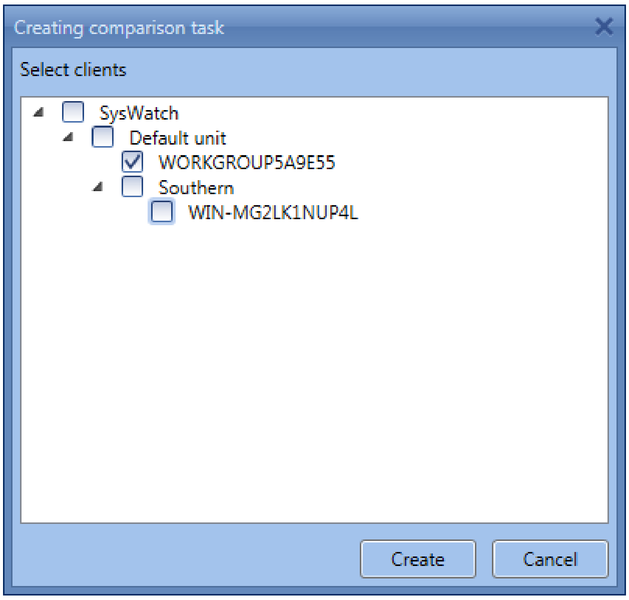
Figure 159. Creating a snapshot

The comments contain the following macros by default: $CLIENT_NAME and $CREATION_TIME. When a task is created, the macros are automatically replaced with the client host name and the task creation time, respectively.

Until the client host responds, the task status in the **Snapshot tasks** section (see below[166]) is **Started**. After the client host responds, the snapshot is marked as **Ready** (the corresponding column in the table[163] is ticked off). This completes the snapshot creation task, and the task status in the table changes to **Finished**.

Comparing configuration snapshots

To compare a configuration snapshot with the current state of the selected client host, select the snapshot and click (**Compare**) (fig. 'Configuration snapshots' tab[162]). In the displayed window, select the client host (or several client hosts) and click **Apply** (fig. Selecting client hosts to compare[164]). If you select several client hosts to compare, a comparison task is created for each of them.



- □ SysWatch
  - □ Default unit
    - ☑ WORKGROUP5A9E55
    - □ Southern
      - □ WIN-MG2LK1NUP4L

Figure 160. Selecting client hosts to compare

You can only use snapshots that are **Ready** for comparison.

Deleting a snapshot

To delete a snapshot, select it, click 🗑 (**Delete**) (fig. 'Configuration snapshots' tab[162]) and confirm the removal in the dialog box.

You can only remove snapshots that do not have any associated tasks. If a snapshot has tasks associated with it, you should delete these tasks first in order to remove the snapshot.

4.11.2 Snapshot tasks

The **Snapshot tasks** section contains the list of tasks performed on the **Configuration snapshots** tab (creating and comparing snapshots) and consists of two tabs, **All** and **Pinned**.

Basic operations with the tasks are performed via the tab's graphical buttons which are described in table 35.

Table 35. The 'Snapshot tasks' section widgets; 'All' tab

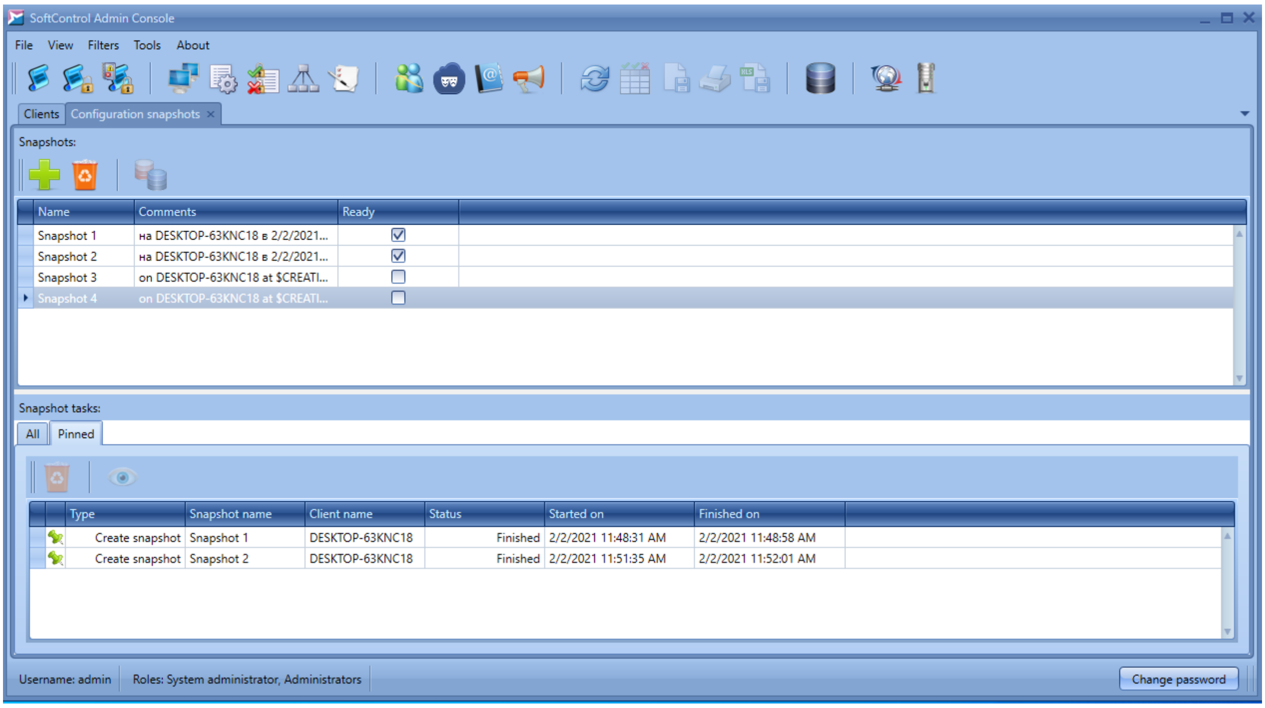
Button	Name	Description
🗑	Delete	Delete the selected snapshot.
👁	Show results	View how the configuration snapshot differs from the client host's profile.

List of the tab fields is given in table 36.

Table 36. The 'Snapshot tasks' section fields; 'All' tab

Field	Description
Type	The type of the task: **Create snapshot** or **Compare snapshot**.
Snapshot name	Task name as specified in section **Snapshots.**
Client name	The name of the client host.
Status	Task status: **Started**, **Finished**.
Started on	Date and time when the task was started.
Finished on	Date and time when the task was finished.

To pin the required task, select it in the table and click the left (empty) cell in the table. The cell is then marked as 📌. The task becomes **Pinned** and appears in the table on the **Pinned** tab (fig. Pinned tasks[166]). SoftControl Admin Console deletes the tasks that are not pinned 180 days after they are completed.



Name	Comments	Ready
Snapshot 1	на DESKTOP-63KNC18 в 2/2/2021...	☑
Snapshot 2	на DESKTOP-63KNC18 в 2/2/2021...	☑
Snapshot 3	on DESKTOP-63KNC18 at $CREATI...	□
Snapshot 4	on DESKTOP-63KNC18 at $CREATI...	□

	Type	Snapshot name	Client name	Status	Started on	Finished on
📌	Create snapshot	Snapshot 1	DESKTOP-63KNC18	Finished	2/2/2021 11:48:31 AM	2/2/2021 11:48:58 AM
📌	Create snapshot	Snapshot 2	DESKTOP-63KNC18	Finished	2/2/2021 11:51:35 AM	2/2/2021 11:52:01 AM

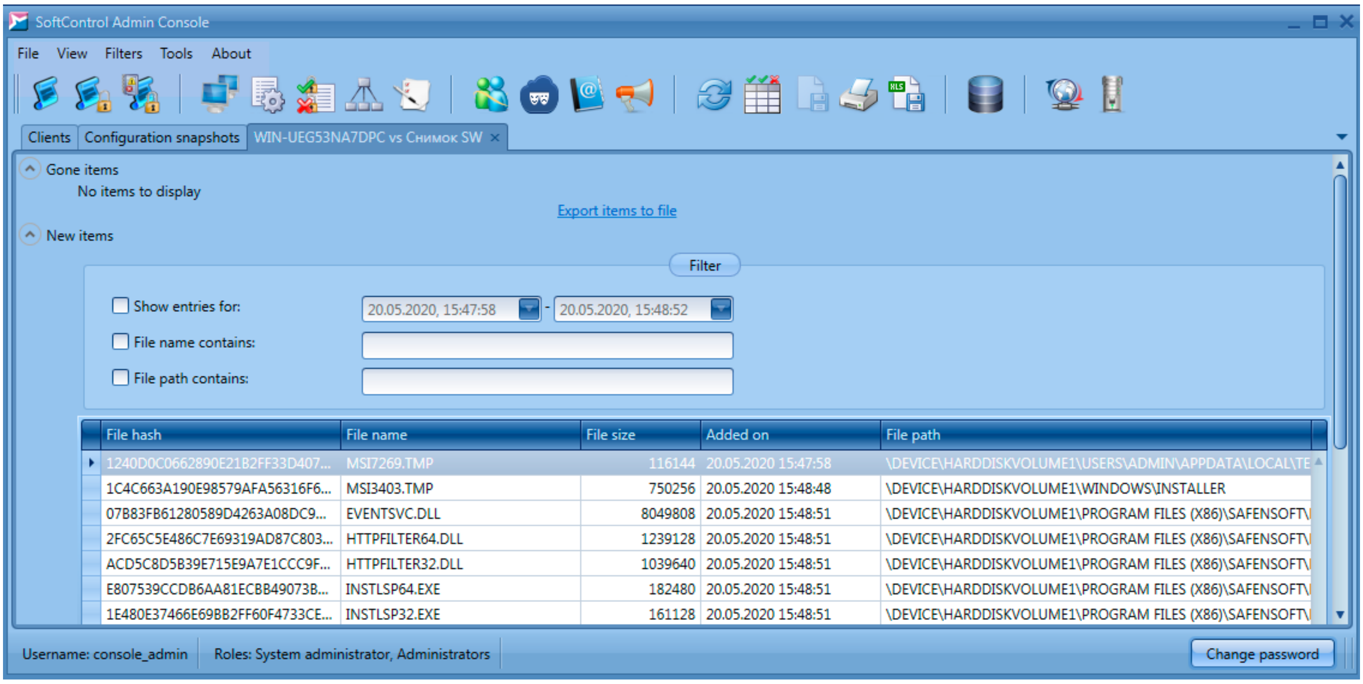
Username: admin

Roles: System administrator, Administrators

Figure 161. Pinned tasks

To view how a snapshot differs from the current configuration of a client host, select the required task and click 👁 (**Show results**). This opens the **<Client_name> vs <snapshot_name>** tab that contains two fields, **Gone items** and **New items** (fig. Comparing snapshots[166]).

You can invoke the context menu by right-clicking on an entry if you want to copy the checksum.


SoftControl Admin Console
File View Filters Tools About
Clients
Configuration snapshots
WIN-UEG53NA7DPC vs Снимок SW
Gone items
No items to display
Export items to file
New items
Filter
□ Show entries for: 20.05.2020, 15:47:58 - 20.05.2020, 15:48:52
□ File name contains:
□ File path contains:
Username: console_admin
Roles: System administrator, Administrators
Change password

File hash	File name	File size	Added on	File path
1240D0C0662890E21B2FF33D407...	MSI7269.TMP	116144	20.05.2020 15:47:58	\DEVICE\HARDDISKVOLUME1\USERS\ADMIN\APPDATA\LOCAL\TE
1C4C663A190E98579AFA56316F6...	MSI3403.TMP	750256	20.05.2020 15:48:48	\DEVICE\HARDDISKVOLUME1\WINDOWS\INSTALLER
07B83FB61280589D4263A08DC9...	EVENTSVC.DLL	8049808	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\
2FC65C5E486C7E69319AD87C803...	HTTPFILTER64.DLL	1239128	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\
ACD5C8D5B39E715E9A7E1CCC9F...	HTTPFILTER32.DLL	1039640	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\
E807539CCDB6AA81ECBB49073B...	INSTLSP64.EXE	182480	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\
1E480E37466E69BB2FF60F4733CE...	INSTLSP32.EXE	161128	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\

Figure 162. Comparing snapshots

To view the changes for a specified period, select the required dates in the **Filter** field. In the filter, you can specify a part of the file name and a part of the path to the file.

At the bottom of both sections you will find the **Export items to file** hyperlink. Click on it to create an XML file with entries on the screen.

5. Updating ISS components

SoftControl Service Center allows centralized updates for all the system components from an update server. This can be either the SoftControl server or an enterprise server. The **Updates** tab allows setting up and viewing the update history (fig. The 'Updates' tab for program modules 168, The 'Updates' tab for antivirus bases 172). You can change the update settings and view update history on the **Updates** tab (fig. The 'Updates' tab for program modules 168, The 'Updates' tab for antivirus bases 172).

The upper part of the tab contains two categories of settings to update the corresponding components:

- Program modules 168;
- Antivirus bases 172.

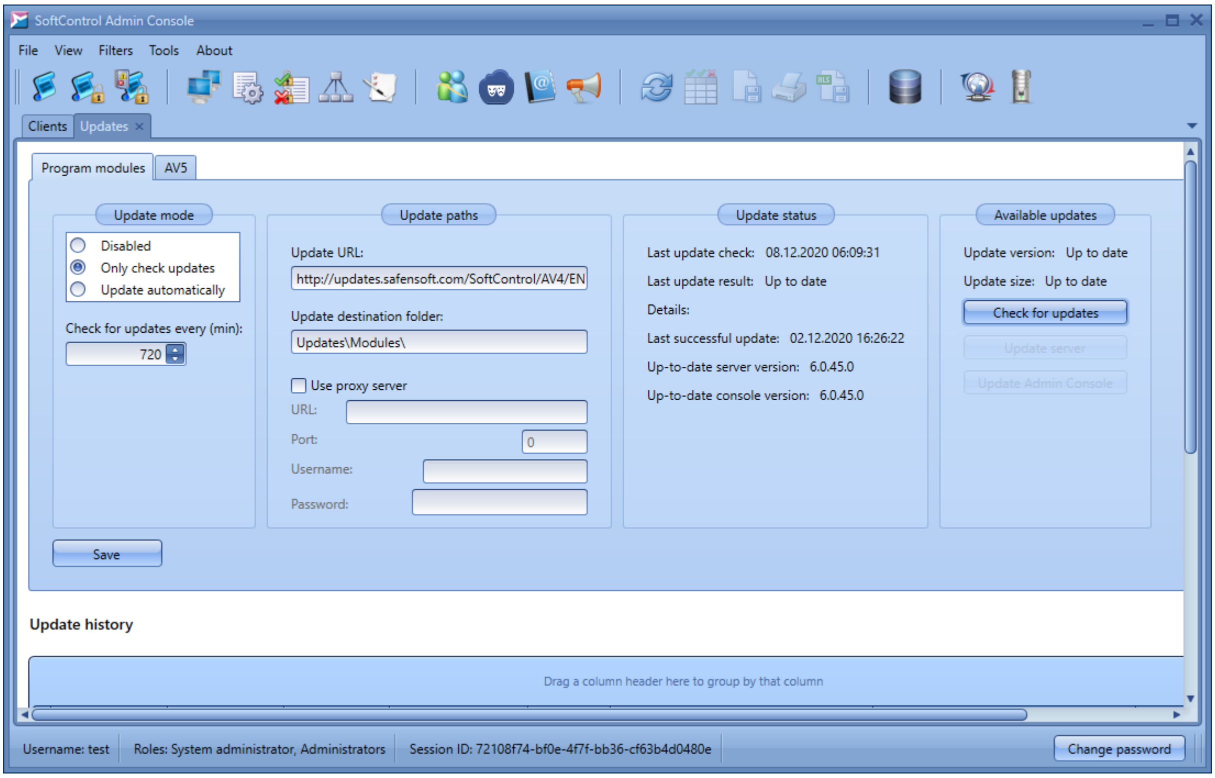
The lower part of the tab displays the update history that contains the list of the performed operations. The list of the fields is given in table 37.

Table 37. Fields of the update history list

Field	Description
Last check date	Date and time of the last check for updates.
Last update date	Date and time when the last updates have been installed.
Component	Name of the updated component.
Update status	Update state: • **Up to date**; • **Updates available**; • **Update downloaded**; • **Update installed**; • **Update process error**.
Update size	Update size in bytes.
Actual version	Current version of the installed component.
New version	The version of the component available for update.
Details	Additional information.

5.1 Setting up updates for program modules

This category of settings allows you to set up and manage the updates of the SoftControl Service Center components' modules as well as to manage the forwarding of the SoftControl SysWatch, SoftControl DLP Client and SoftControl SysCmd client components' modules, from the external (Internet) servers (fig. The 'Updates' tab for program modules 168).


SoftControl Admin Console
File View Filters Tools About
Clients Updates
Program modules AV5
Save
Check for updates
Update server
Update Admin Console
Drag a column header here to group by that column
Change password

Update mode
○ Disabled
● Only check updates
○ Update automatically
Check for updates every (min): 720

Update paths
Update URL: http://updates.safensoft.com/SoftControl/AV4/EN
Update destination folder: Updates\Modules\
□ Use proxy server
URL:
Port: 0
Username:
Password:

Update status
Last update check: 08.12.2020 06:09:31
Last update result: Up to date
Details:
Last successful update: 02.12.2020 16:26:22
Up-to-date server version: 6.0.45.0
Up-to-date console version: 6.0.45.0

Available updates
Update version: Up to date
Update size: Up to date

Update history

Username: test | Roles: System administrator, Administrators | Session ID: 72108f74-bf0e-4f7f-bb36-cf63b4d0480e

Figure 163. The 'Updates' tab for program modules

Setting up the update mode

You can select three working modes in the **Update mode** section:

□**Disabled**:

Update in automatic mode is disabled.

□**Only check updates**:

SoftControl Service Center automatically checks for updates on the external servers with the frequency specified in the **Check for updates every (min)** counter, but neither downloads nor installs them.

□**Update automatically**:

SoftControl Service Center automatically checks for updates on the external servers with the frequency specified in the **Check for updates every (min)** counter and forwards the update packages to the server, if versions newer than the installed ones are found. If a new SoftControl Service Center version is found, automatic update of the SoftControl Server and SoftControl Admin Console components is performed in the background mode on the server, after the installation packages are downloaded.

Client components are updated[176] from the created local 'mirror'.

If there is no Internet access or problems occurred during automatic update, you can update SoftControl Service Center in manual mode[174] if you have the required version of the installation package.

Setting up the update paths and proxy server parameters

The following parameters are specified in the **Update paths** section:

- **Update url**:

  Link to the external server. SoftControl Service Center uses the link to check for updates. You should specify your license number in the update url:

  `http://updates.safensoft.com/<license_number>/SoftControl/av4/en`

  Note. You should specify your license number manually.

- **Update destination folder**:

  The path to save the update packages from the external servers, relative to the following directory: `C:\ProgramData\SoftControl`. Specify the folder as follows:

  `Updates\Modules\`

Tick off the **Use proxy server** checkbox if it is required to connect to the external servers through a proxy server. In this case, specify the parameters of the proxy server:

- **URL**:

  IP address or name of the proxy server host.

- **Port**:

  Port number to connect to the proxy server (if not specified, port *80* is used by default).

- **Username**:

  Login for authentication on the proxy server.

- **Password**:

  Password for authentication on the proxy server.

Basic authorization type is supported. If authentication on the proxy server is not required, you should leave the **Username** and **Password** fields empty.

Checking and updating on demand

Operations on demand can be performed in the **Available updates** section with the help of the following buttons:

- **Check for updates**:

  Check for updates for the program modules. If any updates are found, **Update version** and **Update size** (in bytes) are displayed.
- **Install updates** (when SoftControl Server and SoftControl Admin Console are installed on the same computer):

  Check for updates for the program modules. If any updates are found, forward the installation package from the external servers and install the updates for SoftControl Server and SoftControl Admin Console.
- **Update server** (when SoftControl Server and SoftControl Admin Console are installed on different computers):

  Check for updates for the program modules. If any updates are found, forward the installation package from the external servers and install the updates for the server component (SoftControl Server).
- **Update Admin Console** (when SoftControl Server and SoftControl Admin Console are installed on different computers):

  Check for updates for the management console (SoftControl Admin Console) and install them, if any are found.

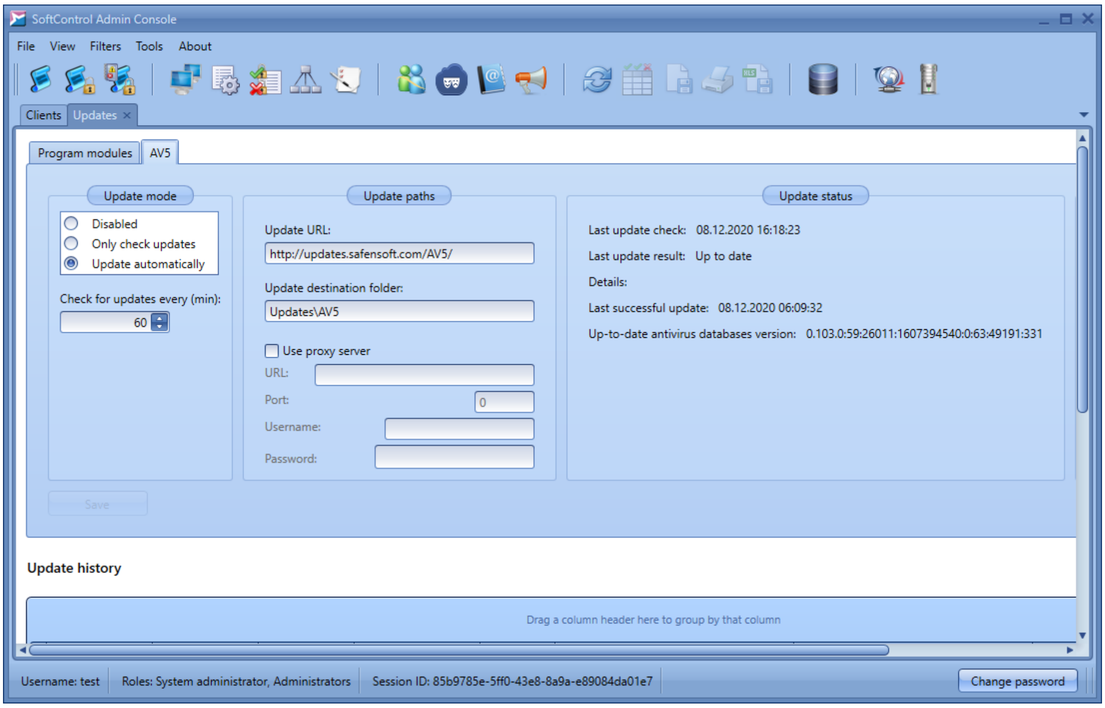
SoftControl Server and SoftControl Admin Console settings and SoftControl Admin Console user filters are saved after the software modules are updated. The accumulated events are stored in the database and are therefore not affected during the update.

The **Update status** section displays information about the current version and the last update check and installation.

To apply the modified settings, click **Save**.

5.2 Setting up updates for antivirus bases

This category of settings allows you to set up and manage the forwarding of SoftControl SysWatch antivirus bases from the external (Internet) servers (fig. The 'Updates' tab for antivirus bases[172]).



○ Disabled
○ Only check updates
● Update automatically

Check for updates every (min): 60

Update URL: http://updates.safensoft.com/AV5/

Update destination folder: Updates\AV5

□ Use proxy server

URL:

Port: 0

Username:

Password:

Last update check: 08.12.2020 16:18:23

Last update result: Up to date

Details:

Last successful update: 08.12.2020 06:09:32

Up-to-date antivirus databases version: 0.103.0:59:26011:1607394540:0:63:49191:331

Username: test | Roles: System administrator, Administrators | Session ID: 85b9785e-5ff0-43e8-8a9a-e89084da01e7

Figure 164. The 'Updates' tab for antivirus bases

Setting up the update mode

You can select three working modes in the **Update mode** section:

□**Disabled**:

Update in automatic mode is disabled.

□**Only check updates**:

SoftControl Service Center automatically checks for updates on the external servers with the frequency specified in the **Check for updates every (min)** counter but does not download them.

□**Update automatically**:

SoftControl Service Center automatically checks for updates on the external servers with the frequency specified in the **Check for updates every (min)** counter and forwards the update bases to the server if versions newer than the installed ones are found. Antivirus bases are updated as a part of the SoftControl SysWatch component update[176], from the created local 'mirror'.

Setting up the update paths and proxy server parameters

The following parameters are specified in the **Update paths** section:

- **Update url**:

  Link to the external server. SoftControl Service Center uses the link to check for updates. Links for different antivirus bases are given in table 38.

  Table 38. URLs to update the antivirus bases

Name	URL	Destination folder
AV4 antivirus bases	http://updates.safensoft.com/<license_number>/av4/	Updates\AV4
AV5 antivirus bases	http://updates.safensoft.com/<license_number>/av5/	Updates\AV5

  Note. You should specify your license number manually.

- **Update destination folder**:

  The path to save the update packages from the external servers, relative to the following directory: `C:\ProgramData\SoftControl`. Folders for different antivirus bases are given in table 38.

Tick off the **Use proxy server** checkbox if it is required to connect to the external servers through a proxy server. In this case, specify the parameters of the proxy server:

- **URL**:

  IP address or name of the proxy server host.

- **Port**:

  Port number to connect to the proxy server (if not specified, port *80* is used by default).

- **Username**:

  Login for authentication on the proxy server.

- **Password**:

  Password for authentication on the proxy server.

Basic authorization type is supported. If authentication on the proxy server is not required, you should leave the **Username** and **Password** fields empty.

Checking and updating on demand

Operations on demand can be performed in the **Available updates** section with the help of the following buttons:

- **Check for updates**:

Check for updates for the antivirus bases. If any updates are found, **Update version** and **Update size** (in bytes) are displayed.

- **Install updates**:

  Check for updates for the antivirus bases. If any updates are found, forward the antivirus bases from the external servers.

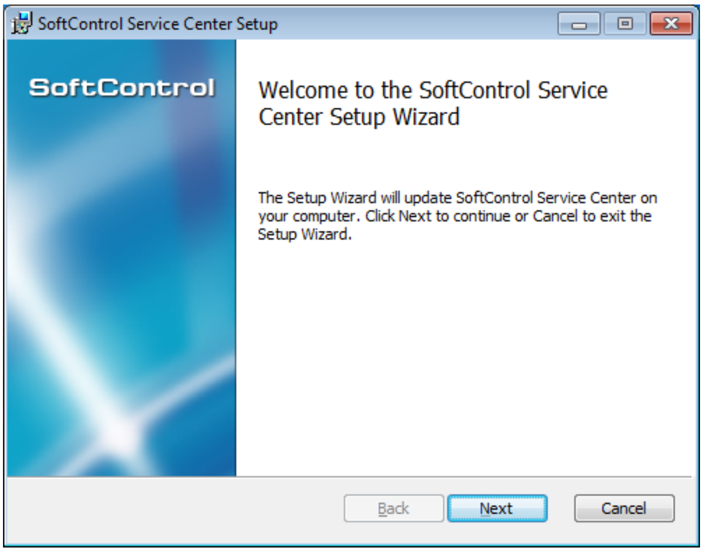
The **Update status** section displays information about the current version and the last update check and installation.

To apply the modified settings, click **Save**.

5.3 Updating SoftControl Server and SoftControl Admin Console manually

1) Run the *Service.Center.msi* installation package of the version you want to update to.

2) Click **Next** in the **SoftControl Service Center Setup** window (fig. Running the update[174]).

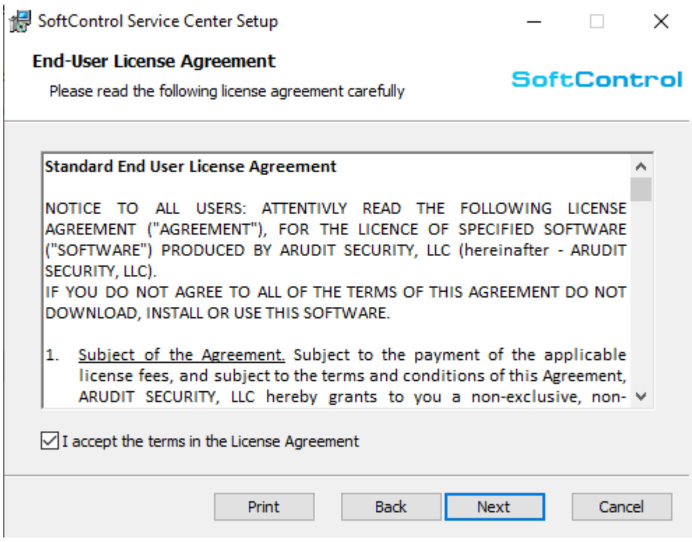


Welcome to the SoftControl Service Center Setup Wizard

The Setup Wizard will update SoftControl Service Center on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 165. Running the update

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement[174]).



SoftControl Service Center Setup

End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

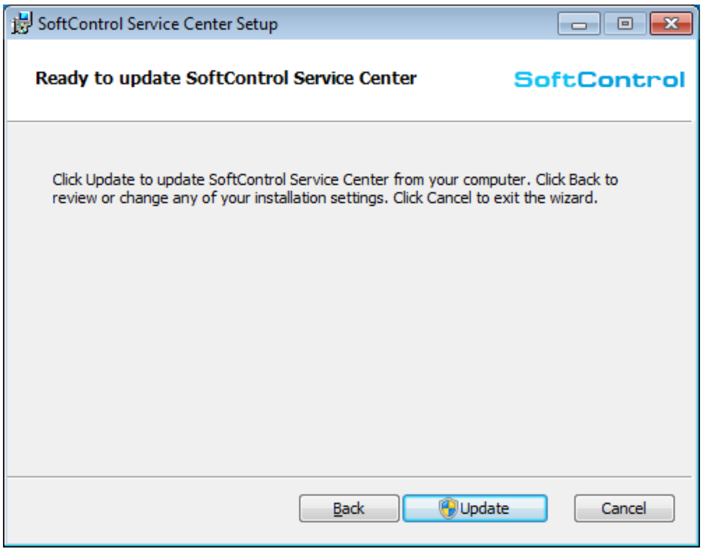
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

Figure 166. License agreement

4) Click **Update** (fig. Ready to update 175).



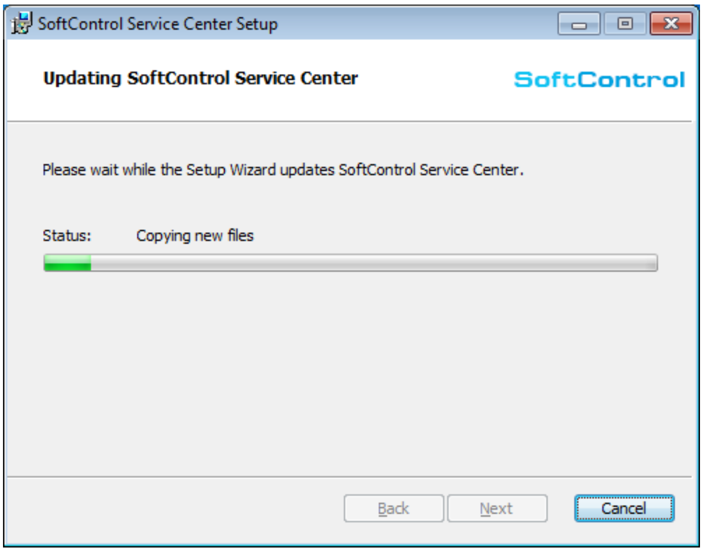
SoftControl Service Center Setup

Ready to update SoftControl Service Center

Click Update to update SoftControl Service Center from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 167. Ready to update

5) Wait until the update completes (fig. Updating progress 175).


SoftControl Service Center Setup

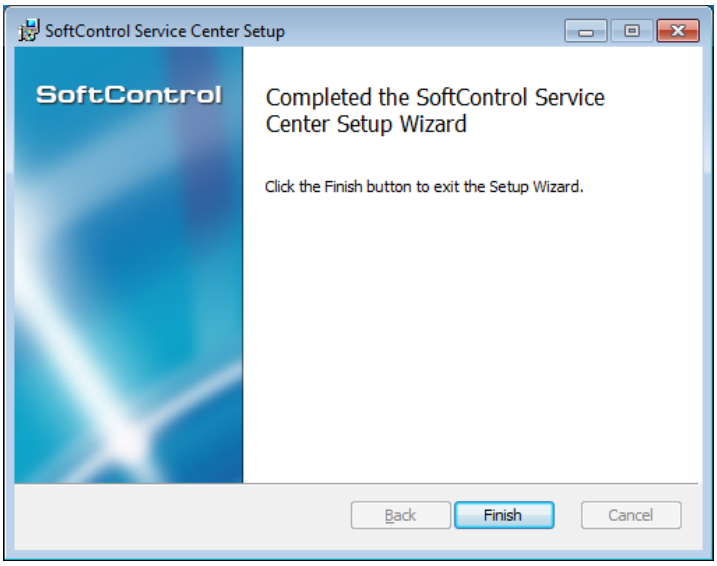
Updating SoftControl Service Center

Please wait while the Setup Wizard updates SoftControl Service Center.

Status: Copying new files

Figure 168. Updating progress

6) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Finishing the update[176]).


SoftControl Service Center Setup

Completed the SoftControl Service Center Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 169. Finishing the update

5.4 Updating client components

After forwarding the updates from the external servers, the client components can be updated from SoftControl Service Center in the following ways.

- ❑ When connected to SoftControl Service Center, SoftControl SysWatch, SoftControl SysCmd and SoftControl DLP Client automatically switch to the updates through the Service Center. The components are updated on demand by creating the corresponding task[121], or on schedule if the latter is set up for SoftControl SysWatch[71] / SoftControl DLP Client[111] / SoftControl SysCmd[112] .

- ❑ When offline, SoftControl SysWatch can also be updated from SoftControl Service Center. To do so, replace the predefined addresses in the SoftControl SysWatch internet update settings with the local addresses for the required components, as specified in table 39. Server connection port is *8088* by default. After the above-mentioned settings are applied, you can run the update on demand through GUI.

Table 39. Addresses for update from SoftControl Service Center

Component	Description	Address
Core	Program modules	http://<server IP address>:<server connection port>/api/updates/SNS
AV-AV4	AV4 Antivirus bases	http://<server IP address>:<server connection port>/api/updates/AV4
AV-AV5	AV5 Antivirus bases	http://<server IP address>:<server connection port>/api/updates/AV5

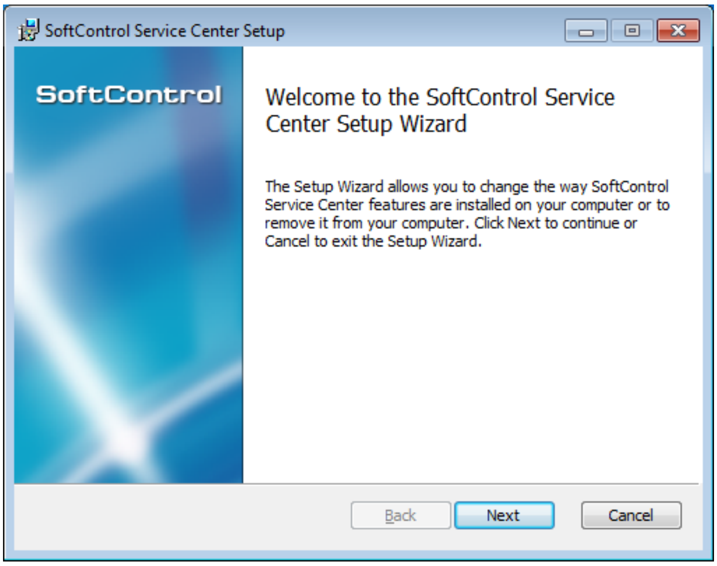
6. Removing SoftControl Service Center components

Removing SoftControl Server and SoftControl Admin Console: go to Windows Control Panel → **Programs** → **Programs and Features**, select *SoftControl Service Center* and click **Uninstall**.

Removing one of the components:

1) Go to Windows Control Panel → **Programs** → **Programs and Features**, select *SoftControl Service Center* and click **Change**.

2) Click **Next** in the **SoftControl Service Center Setup** window (fig. Running uninstallation[178]).



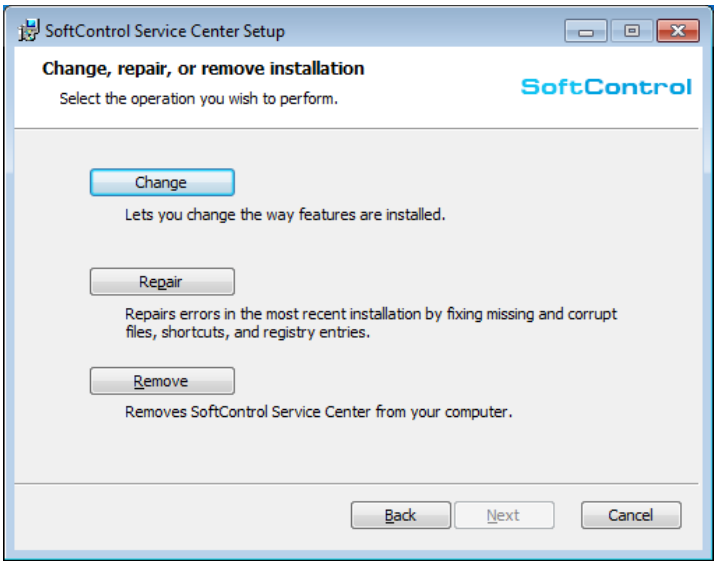
Welcome to the SoftControl Service Center Setup Wizard

The Setup Wizard allows you to change the way SoftControl Service Center features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 170. Running uninstallation

3) Click **Change** (fig. Types of operations[178]).

4) Select the component to remove (fig. Selecting components to remove[179]): click the icon of the component and select the **Entire feature will be unavailable** option from the drop-down menu (fig. Component installation options[179]). Click **Next** when all settings are specified.



SoftControl Service Center Setup

Change, repair, or remove installation

Select the operation you wish to perform.

Change

Lets you change the way features are installed.

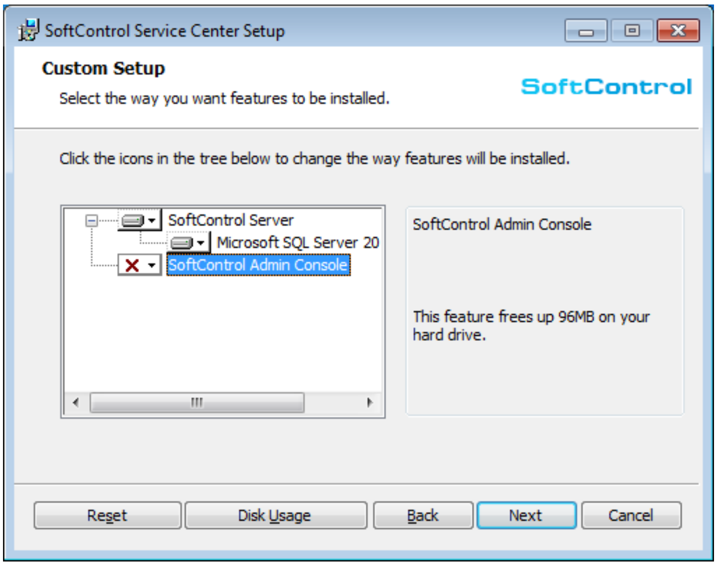
Repair

Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.

Remove

Removes SoftControl Service Center from your computer.

Figure 171. Types of operations



SoftControl Service Center Setup

Custom Setup

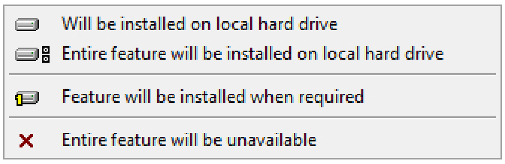
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

SoftControl Admin Console

This feature frees up 96MB on your hard drive.

Figure 172. Selecting components to remove



Will be installed on local hard drive

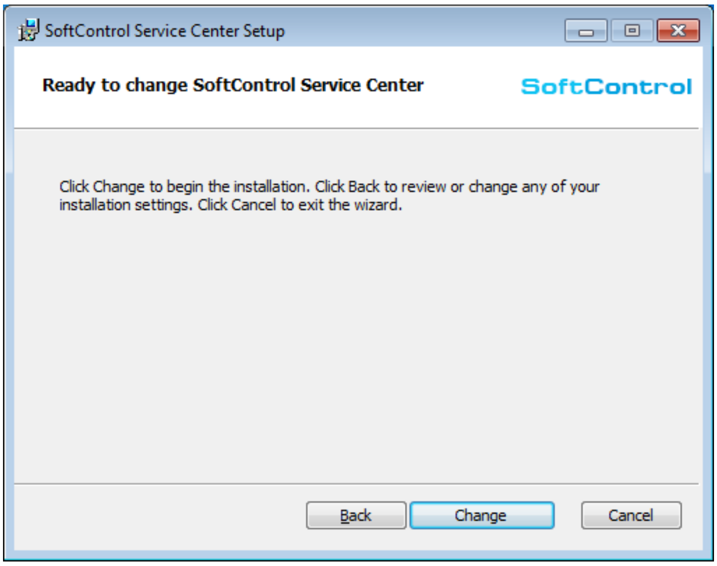
Entire feature will be installed on local hard drive

Feature will be installed when required

✗ Entire feature will be unavailable

Figure 173. Component installation options

5) Click **Change** (fig. Ready to uninstall[179]).



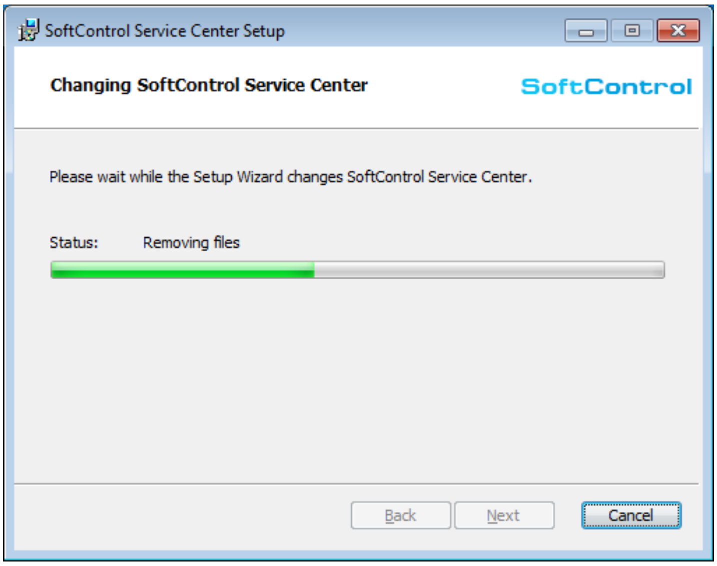
SoftControl Service Center Setup

Ready to change SoftControl Service Center

Click Change to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 174. Ready to uninstall

6) Wait until uninstallation completes (fig. Uninstallation progress [180]).



SoftControl Service Center Setup

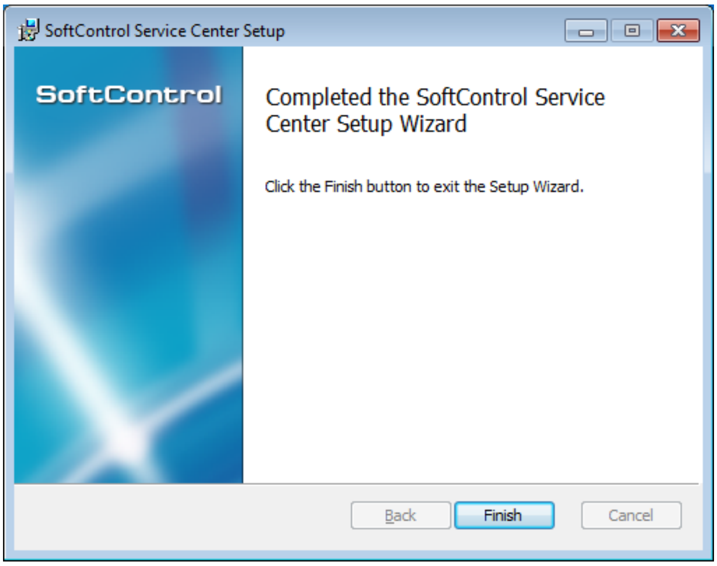
Changing SoftControl Service Center

Please wait while the Setup Wizard changes SoftControl Service Center.

Status: Removing files

Figure 175. Uninstallation progress

7) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Finishing uninstallation [180]).



SoftControl Service Center Setup

Completed the SoftControl Service Center Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 176. Finishing uninstallation

If SoftControl Server has been installed with the embedded DBMS (for example, Complete installation[14] has been performed), you should remove Microsoft® SQL Server® 2014 Express SP1 DBMS manually. To do so, delete the following components by using standard Windows tools:

- *Microsoft SQL Server 2014*;
- *Microsoft SQL Server 2012 Native Client*;
- *Microsoft SQL Server 2014 Setup (English)*;
- *Microsoft SQL Server 2008 Setup Support Files*;
- *Microsoft SQL Server 2014 Transact-SQL ScriptDom*.

7. Troubleshooting

If problems occur when deploying and operating SoftControl Service Center, please check the **SafenSoft** log in the Windows® Event Viewer first. To do so, go to Windows® Control Panel → **System and Security** → **Administrative Tools** → **Event Viewer**. Expand the **Applications and Services Logs** category in the displayed window and select the **SafenSoft** log in it. When you analyze the errors, warnings and messages in the report, you can find out what caused a failure during the component installation, launch and connection. If you cannot find the reason by yourself, contact customer support[186] and attach the text logs of the components to the message. Table 40 lists the required files.

Table 40. SoftControl Service Center components text logs

Title	File name	Path	Brief description	Default log rotation	Log rotation management
Service Center logs					
Service Center log	`ServerDetailedLog.txt`	`C:\Program Files (x86)\SafenSoft\Service Center\Server\logs\`	Service Center log	Once the size of 209715200 is exceeded, a new file is created	Through `SafenSoft.Enterprise.Server.exe.nlog`
Update log	`checks.log`	`C:\Program Files\(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\`	Log of update checks	–	–
Update log	`sns.log`	`C:\Program Files\(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\`	Module update log	–	–
Update log	`[av_name].log`	`C:\Program Files\(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\`	Antivirus update log, antivirus name goes instead of av_name (av4, av5)	–	–
Update log	`root.log`	`C:\Program Files\(x86)\Safensoft\Service Center\Server\Tools\Updates\Reports\`	General log that duplicates `sns.log` and `[av_name].log`	–	–
Admin Console logs					
Admin Console log	`ConsoleDetailedLog.txt`	`C:\ProgramData\SafenSoft\`	Admin Console log	–	–
Local logs of SysWatch					
Security event reports	`system_[date]_[time].txt`	`C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)`	Security event reports	30 days	Through settings

Title	File name	Path	Brief description	Default log rotation	Log rotation management
Profile gathering reports	profile_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	Profile gathering log, list of checked objects, and results of profile gathering	30 days	Through settings
Antivirus check log	scan_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	Antivirus check log	30 days	Through settings
Update log	update_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	Update log	30 days	Through settings
List of infected files	threats.xml	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec	List of infected files	–	–
SysWatch common logs	safensec_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Output of messages and errors from safensec.exe processes	Once a file reaches 50,000 records, a new file is created (the number of records may be different from the number of lines)	–
SysWatch common logs	snsmcon_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Output of messages and errors from snsmcon.exe GUI	Once a file reaches 50,000 records, a new file is created (the number of records may be different from the number of lines)	–
SysWatch common logs	snsods_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Output of messages and errors from the antivirus scanner snsods.exe	Once a file reaches 50,000 records, a new file is created (the number of records may be different from the number of lines)	–
Service Center connection log	sw_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	Output of messages generated when connecting to Service Center	–	–
Local logs of DLP Client					
Service Center connection log	dlp_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows	Output of messages generated	–	–

Title	File name	Path	Brief description	Default log rotation	Log rotation management
		XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	when connecting to Service Center		
DLP Client update log	update_log.txt	C:\Program Files\SafenSoft\DLP Client	Output of messages and errors when starting an update	–	–
DLP Client update log	checks.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	Log of update checks	–	–
DLP Client update log	sns.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	Module update log	–	–
DLP Client update log	root.log	C:\Program Files\SafenSoft\DLP Client\Updater\Reports	General log that duplicates sns.log	–	–
Local logs of SysCmd					
SysCmd common logs	SysCmd_[date]_[time]_[foobar].txt	C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Common Logs\	Output of messages and errors from SysCmd.exe processes	Once a file reaches 50,000 records, a new file is created (the number of records may be different from the number of lines)	–
Service Center connection log	scmd_notify_[date]_[time].txt	C:\Documents and Settings\All Users\Application Data\ (Windows XP) or C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\ (Windows 7 and higher)	Output of messages generated when connecting to Service Center	–	–
SysCmd update log	update_log.txt	C:\Program Files\SoftControl\SysCmd	Output of messages and errors when starting an update	–	–
SysCmd update log	checks.log	C:\Program Files\SoftControl\SysCmd\Updater\Reports	Log of update checks	–	–
SysCmd update log	sns.log	C:\Program Files\SoftControl\SysCmd\Updater\Reports	Module update log	–	–
SysCmd update log	root.log	C:\Program Files\SoftControl\SysCmd\Updater\Reports	General log that duplicates sns.log	–	–
Local logs of DeCrypt					
Standard log file	DecryptLog.log	C:\Windows\	List of devices and event notifications	Once the size of 100MB is reached, DeCryptLog(rotated dd.mm.yyyy).log is created, w here dd.mm.yyyy is the date of file rotation	–

Title	File name	Path	Brief description	Default log rotation	Log rotation management
Detailed log file	`DeCrypt.log`	`C:\ProgramData\DeCrypt\`	Events of the encryption system, reasons of operation failures	Once the size of 100MB is reached, DeCrypt.log_old1 is created, then DeCrypt.log_old2, etc.	–

Note 1. The server component event log supports log rotation, which allows managing the size of the log files. Rotation allows the logs to be automatically divided into parts of the following type (all parts have identical parameters):

Log.000, ..., *Log.N*,

where the latest log has the maximum index. A new file is created each time the size of the main log file (*ServerDetailedLog.txt*) exceeds 200 MB.

Note 2. Table 40 lists the default logs. To learn about the logs that are not created by default, read this article: http://kb.safensoft.com/index.php/SoftControl_logs/en.

To understand messages from logs of SoftControl components, read this article: http://kb.safensoft.com/index.php/Understanding_messages_from_SoftControl_log_files/en.

8. Customer support

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

9. Appendix

9.1 Installing and setting up Microsoft® SQL Server®

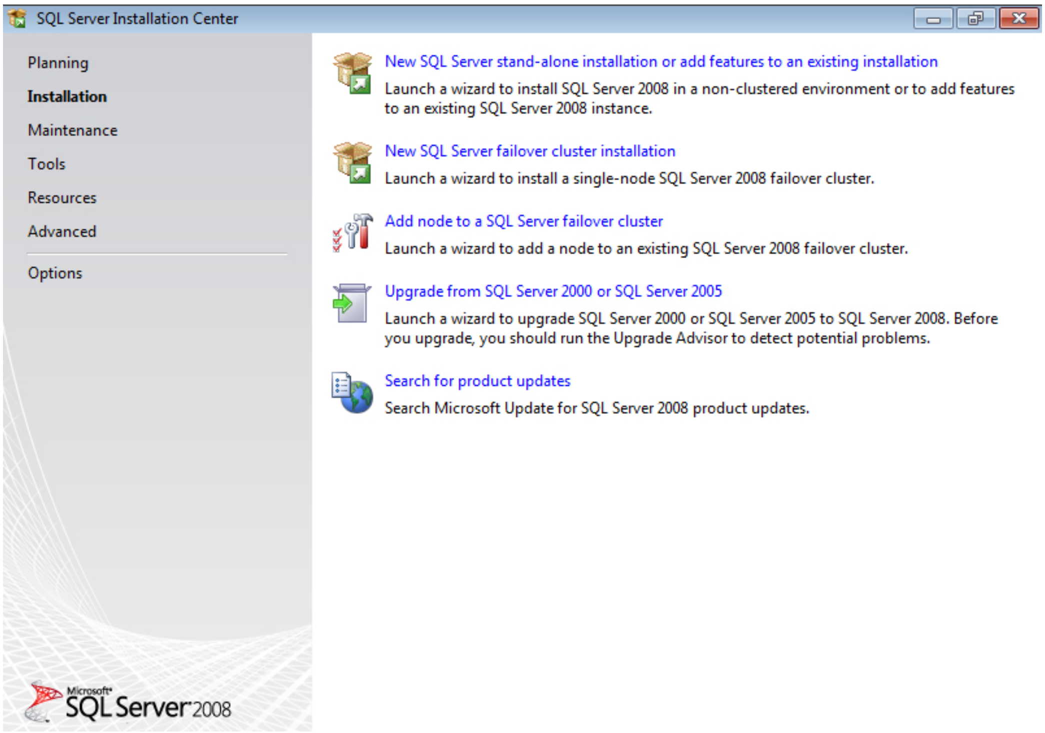
The SoftControl Service Center product can work with different versions of SQL servers: SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, SQL Server 2016, SQL Server 2017. This section describes how to install and set up the Microsoft® SQL Server® 2008 DBMS to use it along with SoftControl Service Center. Other versions of SQL servers are installed in the same way.

▿ Preparing to install Microsoft® SQL Server® 2008

Before installation, make sure that the system meets the minimal hardware and software requirements for installing Microsoft® SQL Server® 2008. Take the appropriate actions if the system does not meet the requirements.

▿ Installing Microsoft® SQL Server® 2008

1) Run Microsoft® SQL Server® 2008 installation package.
2) Open the **Installation** section and select **New SQL Server stand-alone installation or add features to an existing installation** in the **SQL Server Installation Server** window (fig. The 'Installation' section[187]).



New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2008 in a non-clustered environment or to add features to an existing SQL Server 2008 instance.

New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2008 failover cluster.

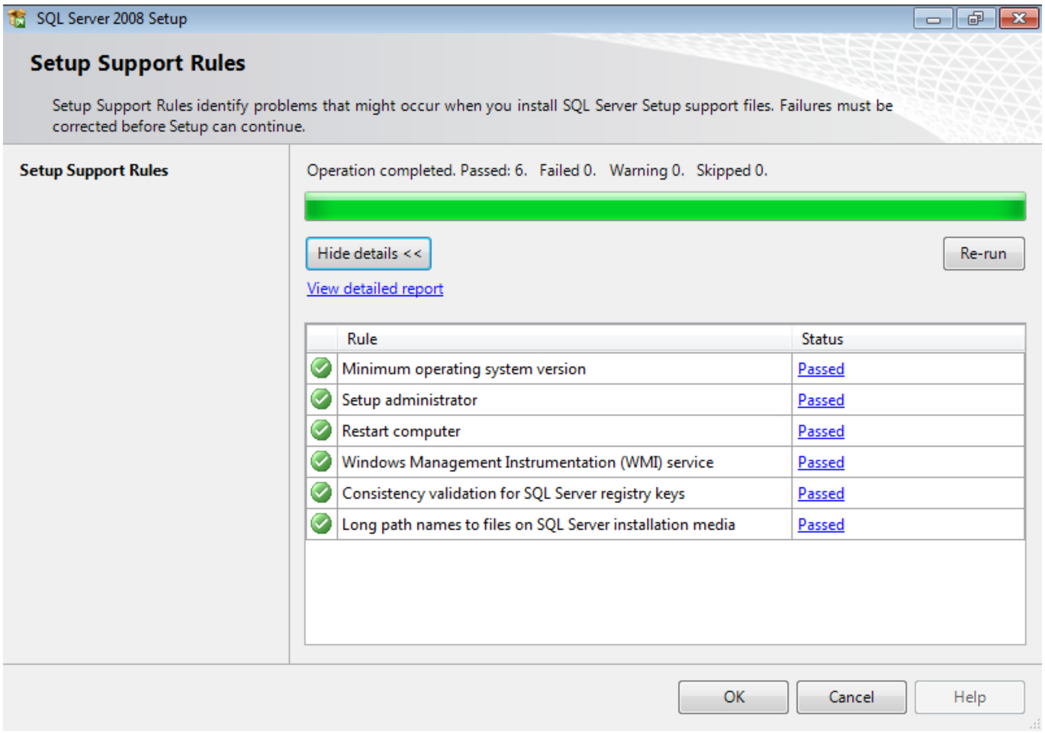
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2008 failover cluster.

Upgrade from SQL Server 2000 or SQL Server 2005
Launch a wizard to upgrade SQL Server 2000 or SQL Server 2005 to SQL Server 2008. Before you upgrade, you should run the Upgrade Advisor to detect potential problems.

Search for product updates
Search Microsoft Update for SQL Server 2008 product updates.

Figure 177. The 'Installation' section

3) The **Setup Support Rules** section checks for problems that might occur when installing auxiliary Microsoft® SQL Server® 2008 files (fig. Setup support rules check[188]). You should fix errors before continuing. If there are no problems, click **OK**.



SQL Server 2008 Setup

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Setup Support Rules

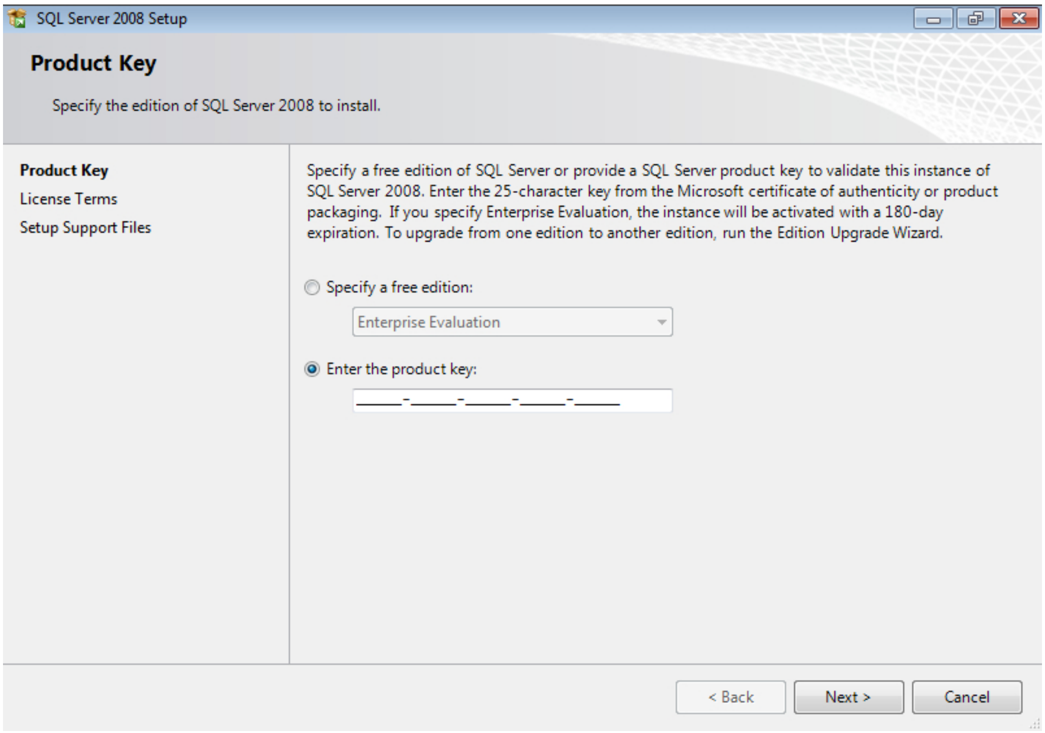
Operation completed. Passed: 6. Failed 0. Warning 0. Skipped 0.

View detailed report

	Rule	Status
✓	Minimum operating system version	Passed
✓	Setup administrator	Passed
✓	Restart computer	Passed
✓	Windows Management Instrumentation (WMI) service	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Long path names to files on SQL Server installation media	Passed

Figure 178. Setup support rules check

4) In the **Product Key** section, select **Enter the product key**, enter the license key for Microsoft SQL Server 2008 and click **Next** (fig. The 'Product Key' section[188]).



SQL Server 2008 Setup

Product Key

Specify the edition of SQL Server 2008 to install.

Specify a free edition of SQL Server or provide a SQL Server product key to validate this instance of SQL Server 2008. Enter the 25-character key from the Microsoft certificate of authenticity or product packaging. If you specify Enterprise Evaluation, the instance will be activated with a 180-day expiration. To upgrade from one edition to another edition, run the Edition Upgrade Wizard.

○ Specify a free edition:

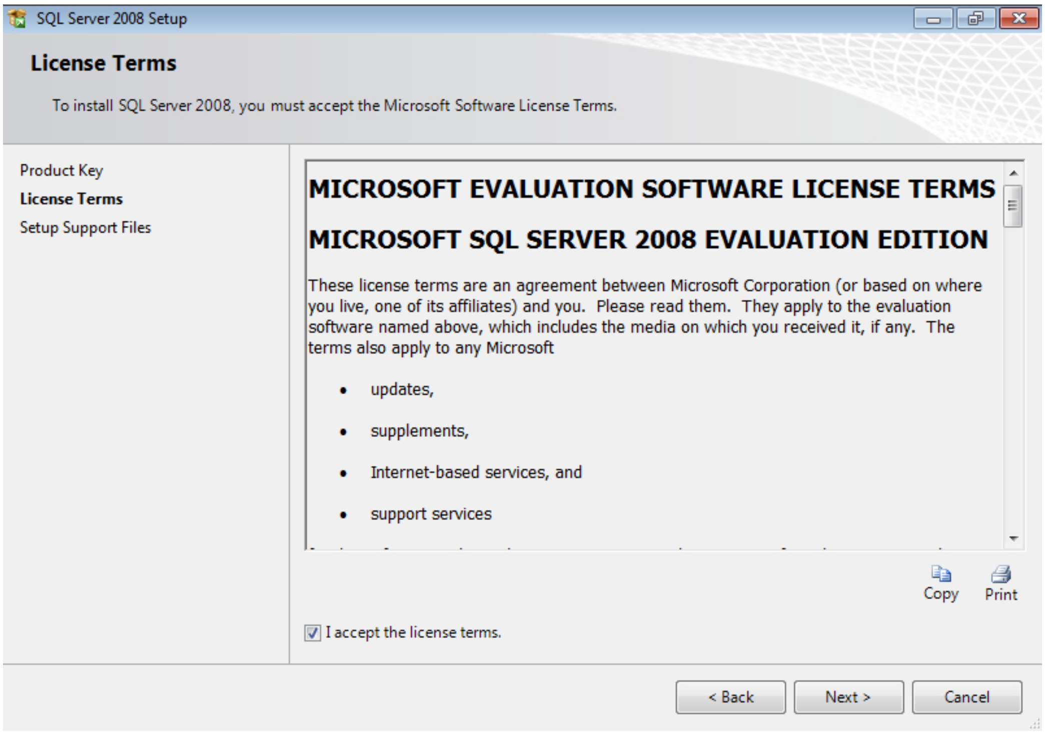
Enterprise Evaluation

● Enter the product key:

_____-_____-_____-_____-_____

Figure 179. The 'Product Key' section

5) Read the **License Terms**. If you accept the terms, select **I Accept the license terms** and click **Next** (fig. The 'License Terms'[189]).



SQL Server 2008 Setup

License Terms

To install SQL Server 2008, you must accept the Microsoft Software License Terms.

MICROSOFT EVALUATION SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2008 EVALUATION EDITION

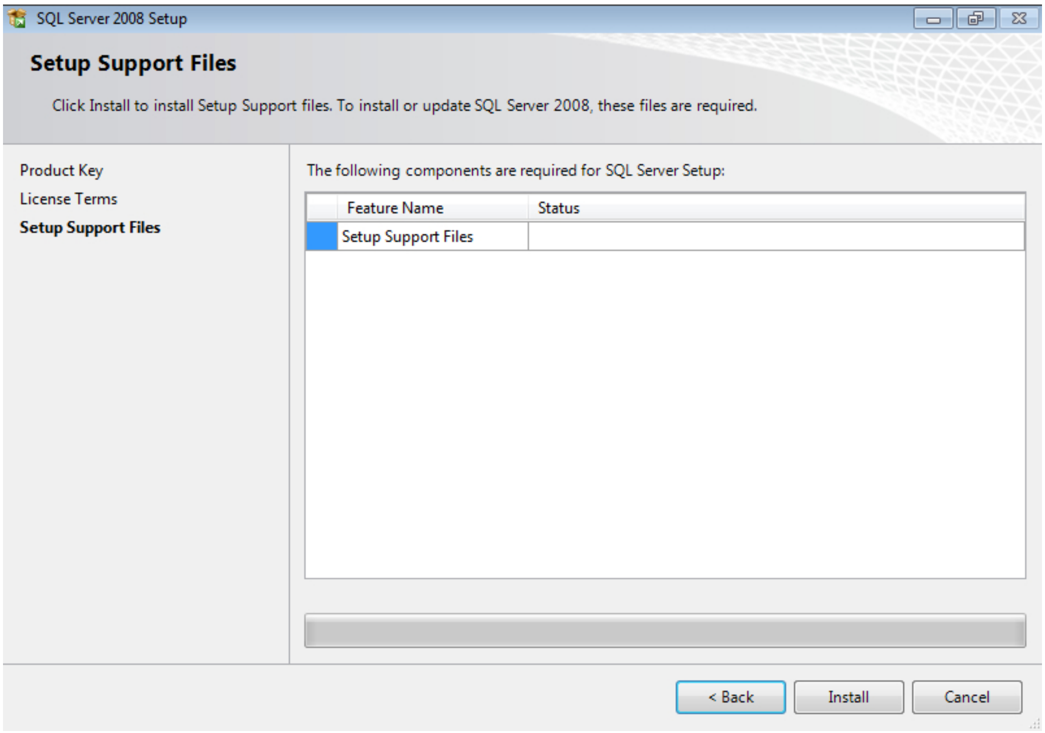
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the evaluation software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

☑ I accept the license terms.

Figure 180. The 'License Terms'

6) Click **Install** in section **Setup Support Files** (fig. The 'Setup Support Files' section[189]).



Setup Support Files

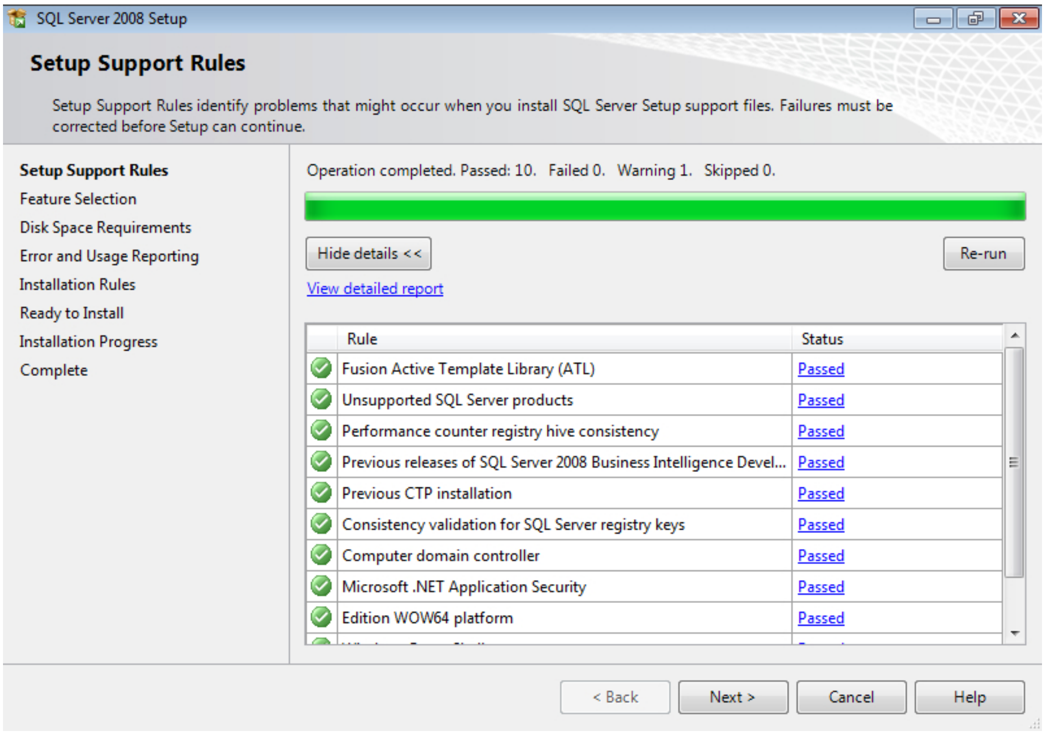
Click Install to install Setup Support files. To install or update SQL Server 2008, these files are required.

The following components are required for SQL Server Setup:

Feature Name	Status
Setup Support Files	

Figure 181. The 'Setup Support Files' section

7) The **Setup Support Rules** section checks for problems that might occur when installing auxiliary Microsoft® SQL Server® 2008 files (fig. The 'Setup Support Rules' section. Details[190]). You should fix errors before continuing. If there are no problems, click **Next**.



Setup Support Rules

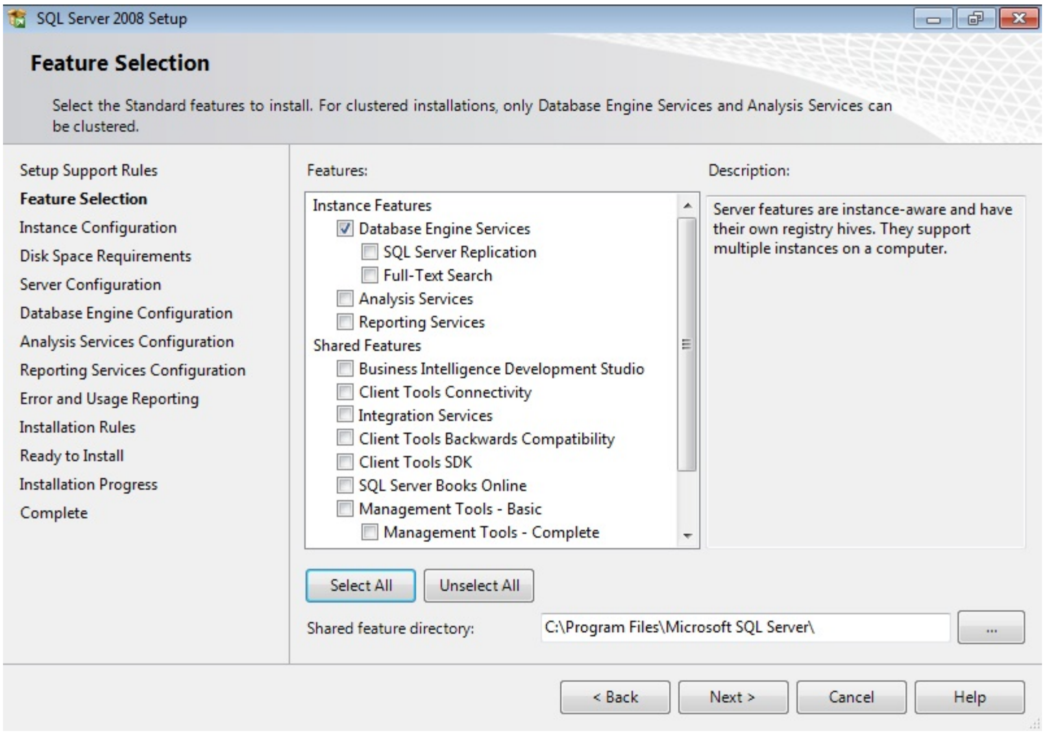
Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 10. Failed 0. Warning 1. Skipped 0.

Rule	Status
Fusion Active Template Library (ATL)	Passed
Unsupported SQL Server products	Passed
Performance counter registry hive consistency	Passed
Previous releases of SQL Server 2008 Business Intelligence Devel...	Passed
Previous CTP installation	Passed
Consistency validation for SQL Server registry keys	Passed
Computer domain controller	Passed
Microsoft .NET Application Security	Passed
Edition WOW64 platform	Passed

Figure 182. The 'Setup Support Rules' section. Details

8) In the **Feature Selection** section, check **Database Engine Services**, specify the installation path in the **Shared feature directory** field and click **Next** (fig. The 'Feature Selection' section 191).



SQL Server 2008 Setup

Feature Selection

Select the Standard features to install. For clustered installations, only Database Engine Services and Analysis Services can be clustered.

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication
  - □ Full-Text Search
- □ Analysis Services
- □ Reporting Services

Shared Features
- □ Business Intelligence Development Studio
- □ Client Tools Connectivity
- □ Integration Services
- □ Client Tools Backwards Compatibility
- □ Client Tools SDK
- □ SQL Server Books Online
- □ Management Tools - Basic
  - □ Management Tools - Complete

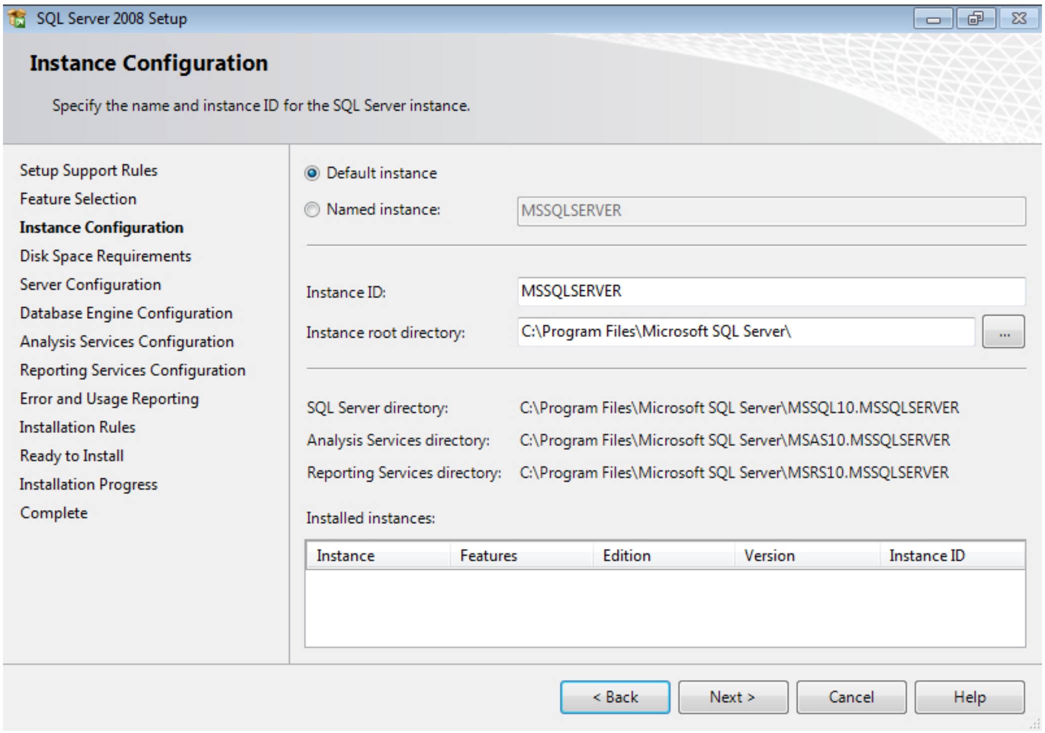
Description:

Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Figure 183. The 'Feature Selection' section

9) Select **Default Instance** and click **Next** in the **Instant Configuration** section (fig. The 'Instance Configuration' section 191).



SQL Server 2008 Setup

Instance Configuration

Specify the name and instance ID for the SQL Server instance.

● Default instance

○ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER

Analysis Services directory: C:\Program Files\Microsoft SQL Server\MSAS10.MSSQLSERVER

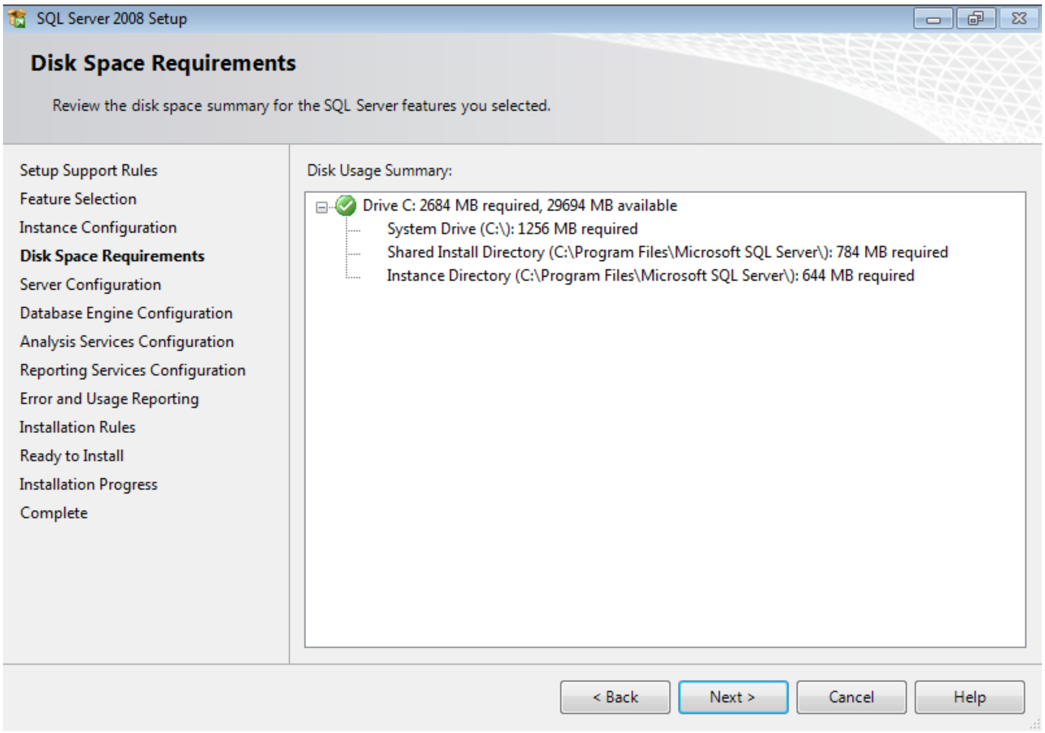
Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS10.MSSQLSERVER

Installed instances:

Instance	Features	Edition	Version	Instance ID

Figure 184. The 'Instance Configuration' section

10) Click **Next** in the **Disc Space Requirements** section (fig. The 'Disc Space Requirements' section[192]).



SQL Server 2008 Setup

Disk Space Requirements

Review the disk space summary for the SQL Server features you selected.

Disk Usage Summary:

Drive C: 2684 MB required, 29694 MB available
- System Drive (C:\): 1256 MB required
- Shared Install Directory (C:\Program Files\Microsoft SQL Server\): 784 MB required
- Instance Directory (C:\Program Files\Microsoft SQL Server\): 644 MB required

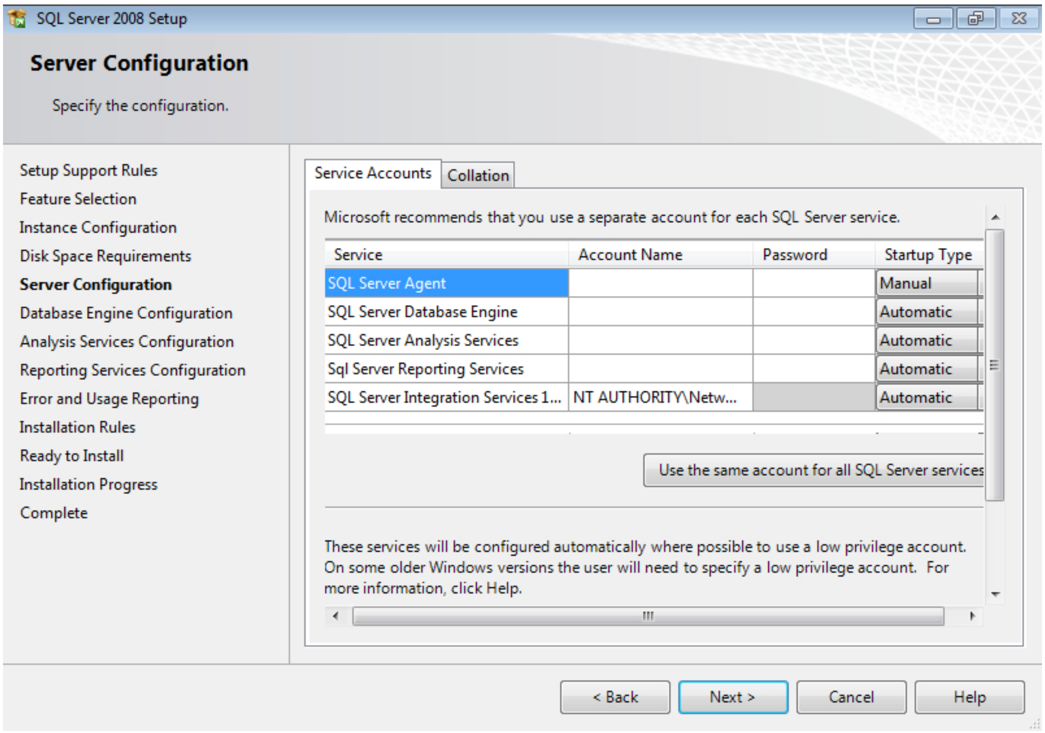
Figure 185. The 'Disc Space Requirements' section

11) Click **Use the same account for all SQL Server services** in the **Service Accounts** tab of

the **Server Configuration** section (fig. The 'Service Accounts' tab of the 'Server Configuration' section[193]).

Select the **NETWORK SERVICE** account in the displayed window and click **OK** (fig. Account[193]).

Specify the **SQL_Latin1_General_CP1_CI_AS** parameter for the **Database Engine** component and the **Latin1_General_CI_AS** parameter for the **Analysis Services** component, in the **Collation** tab of the **Server Configuration** section (fig. The 'Collation' tab of the 'Server Configuration' section[193]).



Server Configuration

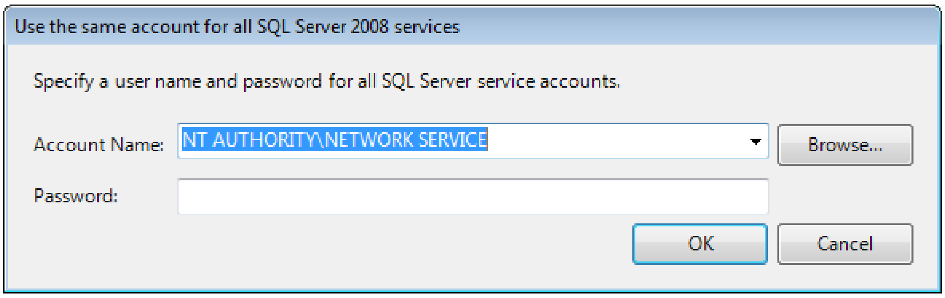
Specify the configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent			Manual
SQL Server Database Engine			Automatic
SQL Server Analysis Services			Automatic
Sql Server Reporting Services			Automatic
SQL Server Integration Services 1...	NT AUTHORITY\Netw...		Automatic

These services will be configured automatically where possible to use a low privilege account. On some older Windows versions the user will need to specify a low privilege account. For more information, click Help.

Figure 186. The 'Service Accounts' tab of the 'Server Configuration' section



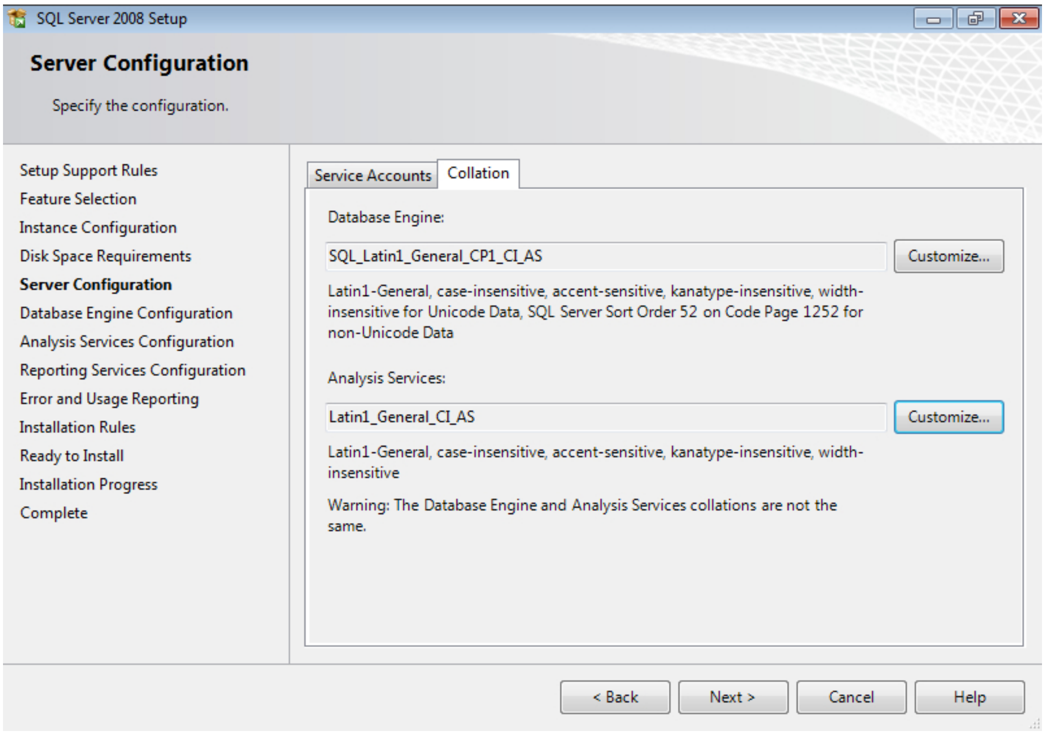
Use the same account for all SQL Server 2008 services

Specify a user name and password for all SQL Server service accounts.

Account Name: NT AUTHORITY\NETWORK SERVICE

Password:

Figure 187. Account



SQL Server 2008 Setup

Server Configuration

Specify the configuration.

Database Engine:

SQL_Latin1_General_CP1_CI_AS [Customize...]

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data

Analysis Services:

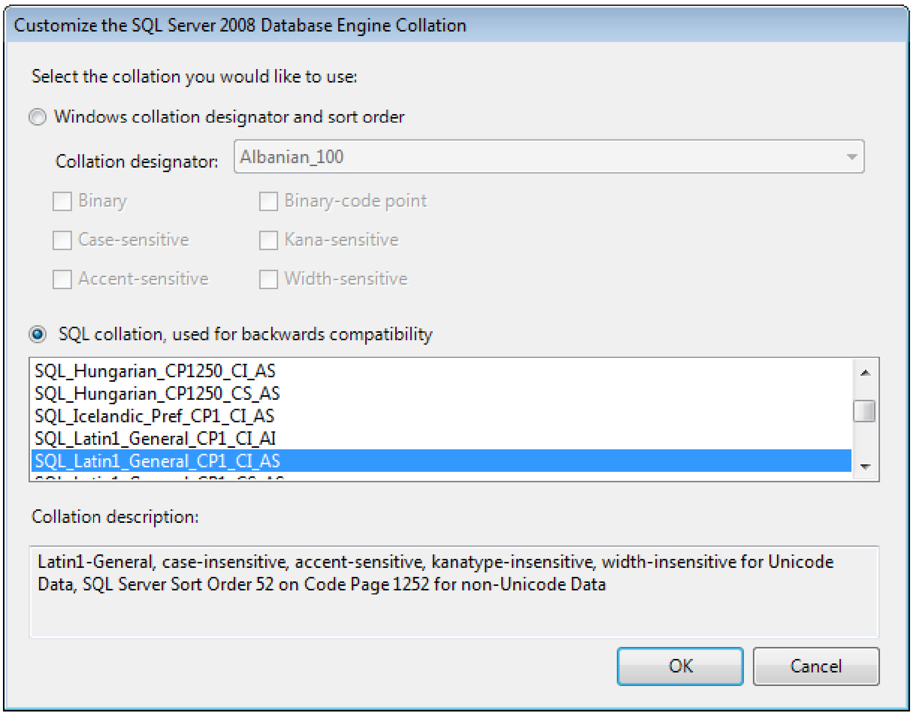
Latin1_General_CI_AS [Customize...]

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive

Warning: The Database Engine and Analysis Services collations are not the same.

Figure 188. The 'Collation' tab of the 'Server Configuration' section

To do so, click **Customize** for the **Database Engine** component, select **SQL collation, used for backwards compatibility**, select **SQL_Latin1_General_CP1_CI_AS** from the list and click **OK** (fig. Specifying the collation parameters for the Database Engine component 194).



Customize the SQL Server 2008 Database Engine Collation

Select the collation you would like to use:

○ Windows collation designator and sort order

Collation designator: Albanian_100

□ Binary □ Binary-code point

□ Case-sensitive □ Kana-sensitive

□ Accent-sensitive □ Width-sensitive

● SQL collation, used for backwards compatibility

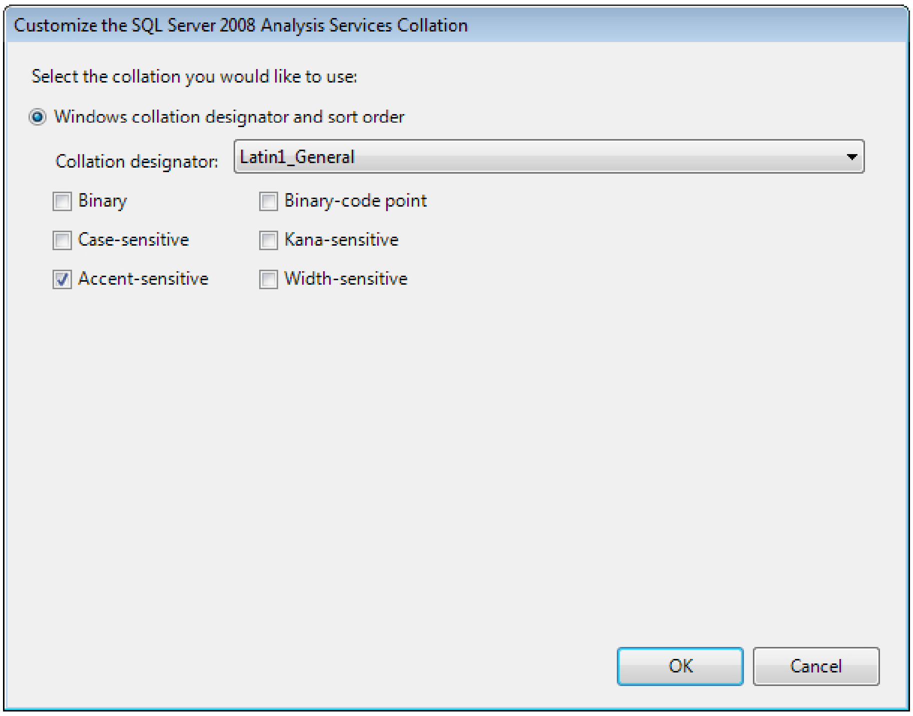
SQL_Hungarian_CP1250_CI_AS
SQL_Hungarian_CP1250_CS_AS
SQL_Icelandic_Pref_CP1_CI_AS
SQL_Latin1_General_CP1_CI_AI
SQL_Latin1_General_CP1_CI_AS

Collation description:

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data

Figure 189. Specifying the collation parameters for the Database Engine component

Click **Customize** for the **Analysis Services** component, select **Latin1_General** in the **Collation designator** drop-down list, tick off the **Accent-sensitive** checkbox and click **OK** (fig. Specifying the collation parameters for the Analysis Services component[195]).



Customize the SQL Server 2008 Analysis Services Collation

Select the collation you would like to use:

● Windows collation designator and sort order

Collation designator: Latin1_General

□ Binary □ Binary-code point

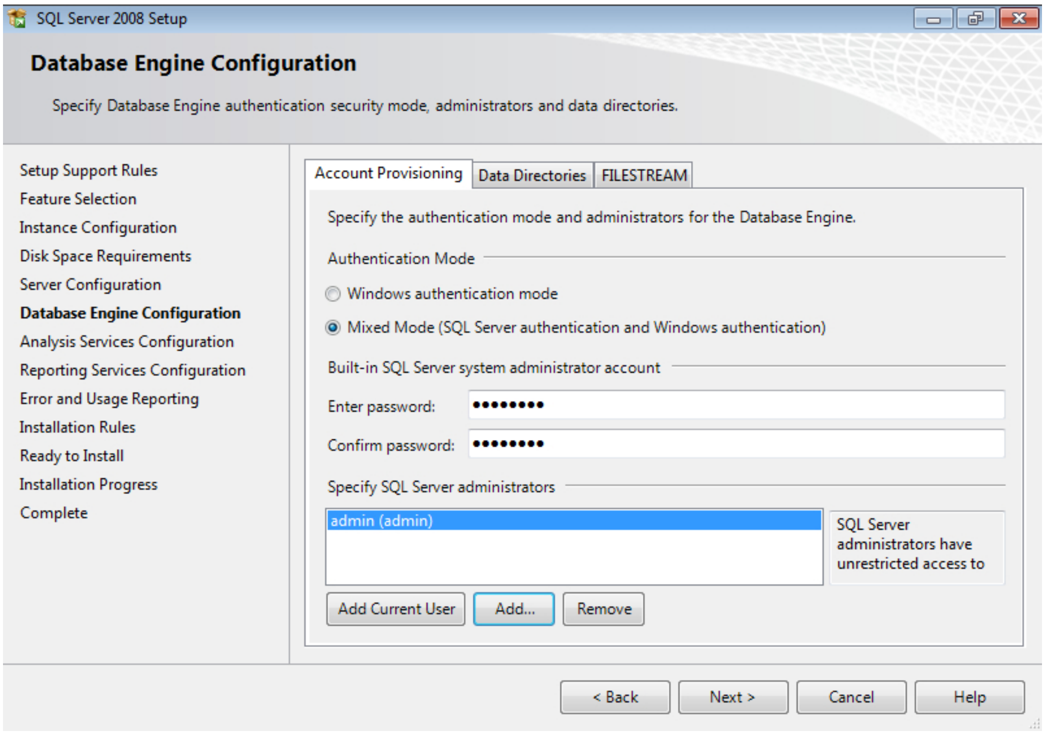
□ Case-sensitive □ Kana-sensitive

☑ Accent-sensitive □ Width-sensitive

Figure 190. Specifying the collation parameters for the Analysis Services component

Click **Next** in the **Server Configuration** section to continue installation.

12) Select **Mixed Mode** in the **Database Engine Configuration** section, specify the **Built-in SQL Server system administrator account** password in the **Enter password** field and confirm it in the **Confirm password** field (fig. The 'Database Engine Configuration' section[195]). Click **Add Current User** and make sure that the current system account is displayed in the **Specify SQL Server administrators** list; then click **Next**.



SQL Server 2008 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password: ••••••••

Confirm password: ••••••••

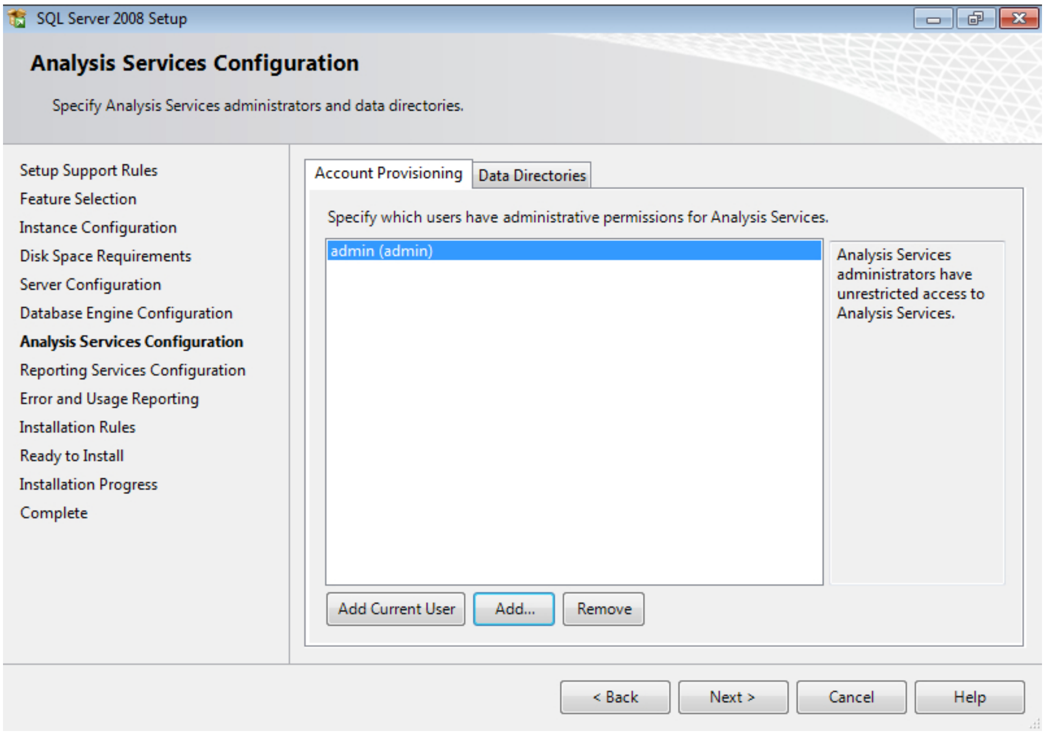
Specify SQL Server administrators

admin (admin)

SQL Server administrators have unrestricted access to

Figure 191. The 'Database Engine Configuration' section

13) Click **Add Current User** and make sure that the current system account is displayed in the **Specify which users have administrative permissions for Analysis Services** list on the **Account Provisioning** tab of the **Analysis Services Configuration** section; then click **Next** (fig. The 'Analysis Services Configuration' section 196).



SQL Server 2008 Setup

Analysis Services Configuration

Specify Analysis Services administrators and data directories.

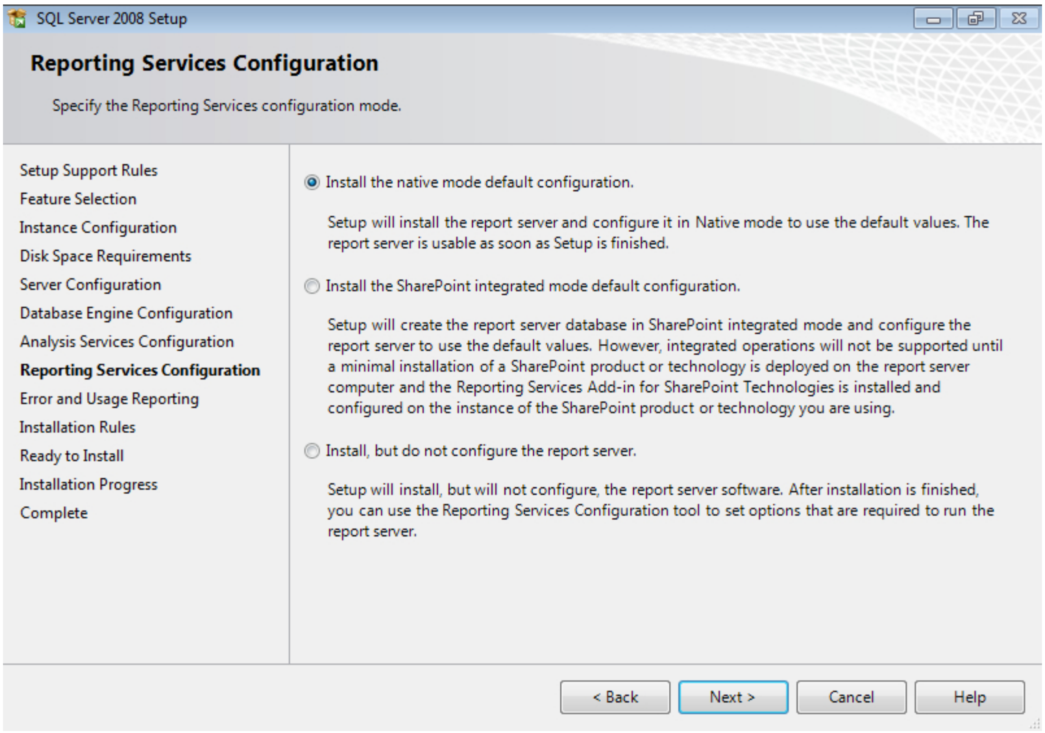
Specify which users have administrative permissions for Analysis Services.

admin (admin)

Analysis Services administrators have unrestricted access to Analysis Services.

Figure 192. The 'Analysis Services Configuration' section

14) Select **Install the native mode default configuration** and click **Next** in the **Reporting Services Configuration** section (fig. The 'Reporting Services Configuration' section 197).



Reporting Services Configuration

Specify the Reporting Services configuration mode.

● Install the native mode default configuration.

Setup will install the report server and configure it in Native mode to use the default values. The report server is usable as soon as Setup is finished.

○ Install the SharePoint integrated mode default configuration.

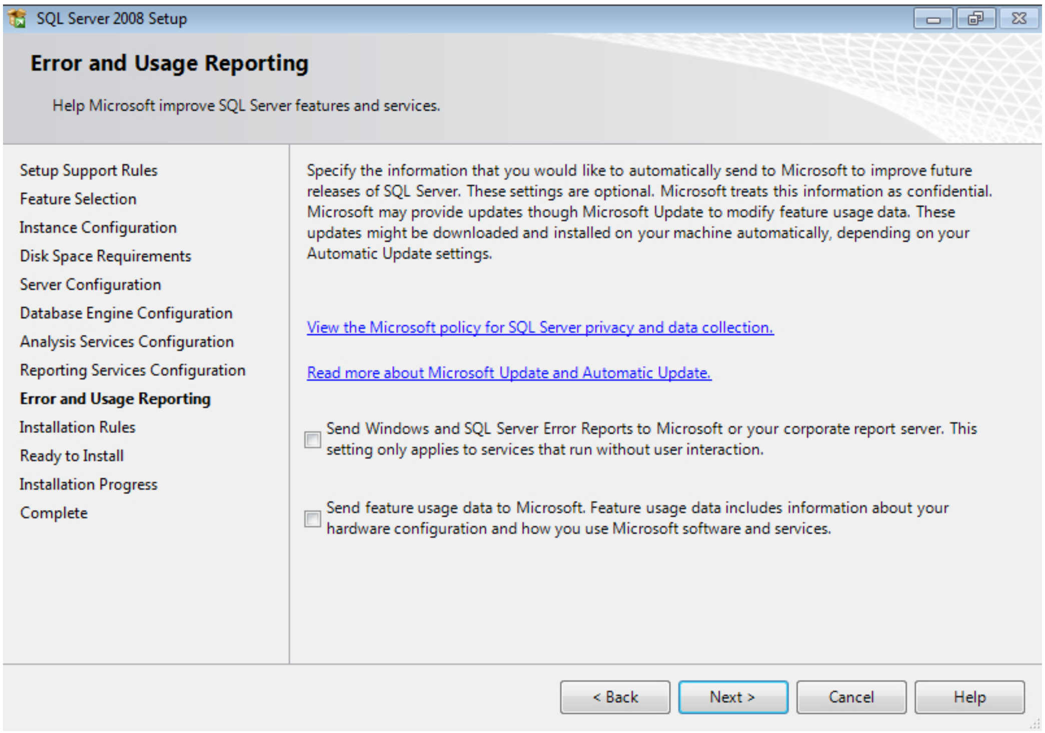
Setup will create the report server database in SharePoint integrated mode and configure the report server to use the default values. However, integrated operations will not be supported until a minimal installation of a SharePoint product or technology is deployed on the report server computer and the Reporting Services Add-in for SharePoint Technologies is installed and configured on the instance of the SharePoint product or technology you are using.

○ Install, but do not configure the report server.

Setup will install, but will not configure, the report server software. After installation is finished, you can use the Reporting Services Configuration tool to set options that are required to run the report server.

Figure 193. The 'Reporting Services Configuration' section

15) Click **Next** in the **Error and Usage Reporting** secton (fig. The 'Error and Usage Reporting' section 197).



SQL Server 2008 Setup

Error and Usage Reporting

Help Microsoft improve SQL Server features and services.

Setup Support Rules
Feature Selection
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Reporting Services Configuration
Error and Usage Reporting
Installation Rules
Ready to Install
Installation Progress
Complete

Specify the information that you would like to automatically send to Microsoft to improve future releases of SQL Server. These settings are optional. Microsoft treats this information as confidential. Microsoft may provide updates though Microsoft Update to modify feature usage data. These updates might be downloaded and installed on your machine automatically, depending on your Automatic Update settings.

View the Microsoft policy for SQL Server privacy and data collection.

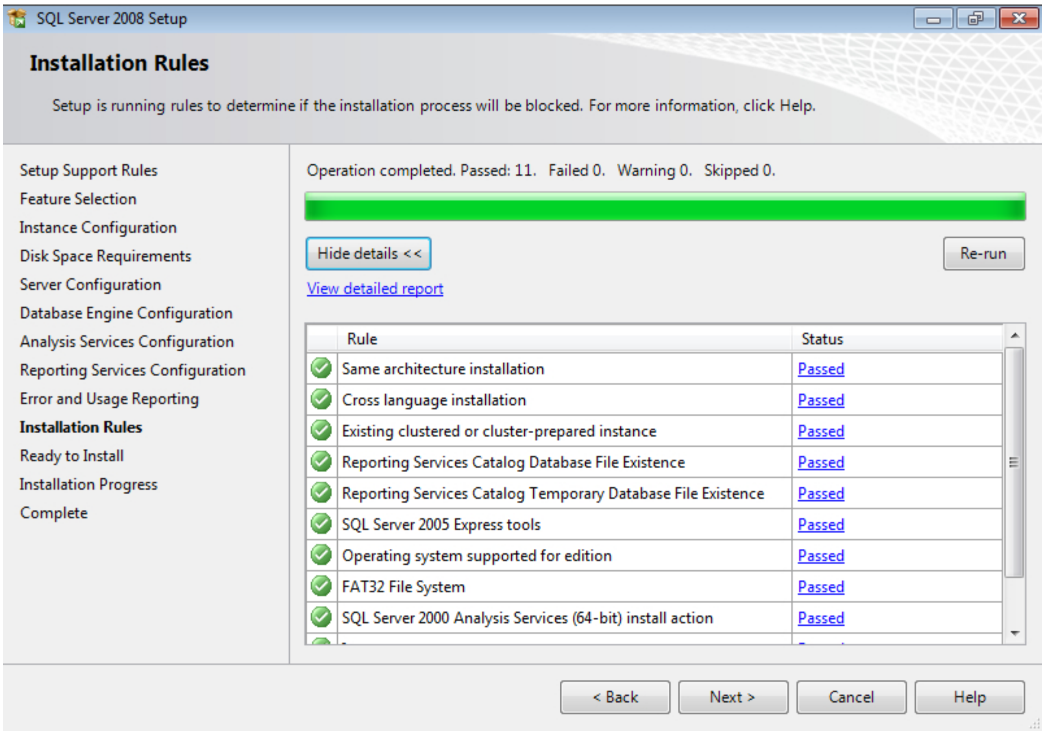
Read more about Microsoft Update and Automatic Update.

□ Send Windows and SQL Server Error Reports to Microsoft or your corporate report server. This setting only applies to services that run without user interaction.

□ Send feature usage data to Microsoft. Feature usage data includes information about your hardware configuration and how you use Microsoft software and services.

Figure 194. The 'Error and Usage Reporting' section

16) The **Installation Rules** section checks for problems that might occur when installing Microsoft® SQL Server® 2008 (fig. The 'Installation Rules' section[198]). If there are no problems, click **Next**.



SQL Server 2008 Setup

Installation Rules

Setup is running rules to determine if the installation process will be blocked. For more information, click Help.

Setup Support Rules
Feature Selection
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Reporting Services Configuration
Error and Usage Reporting
Installation Rules
Ready to Install
Installation Progress
Complete

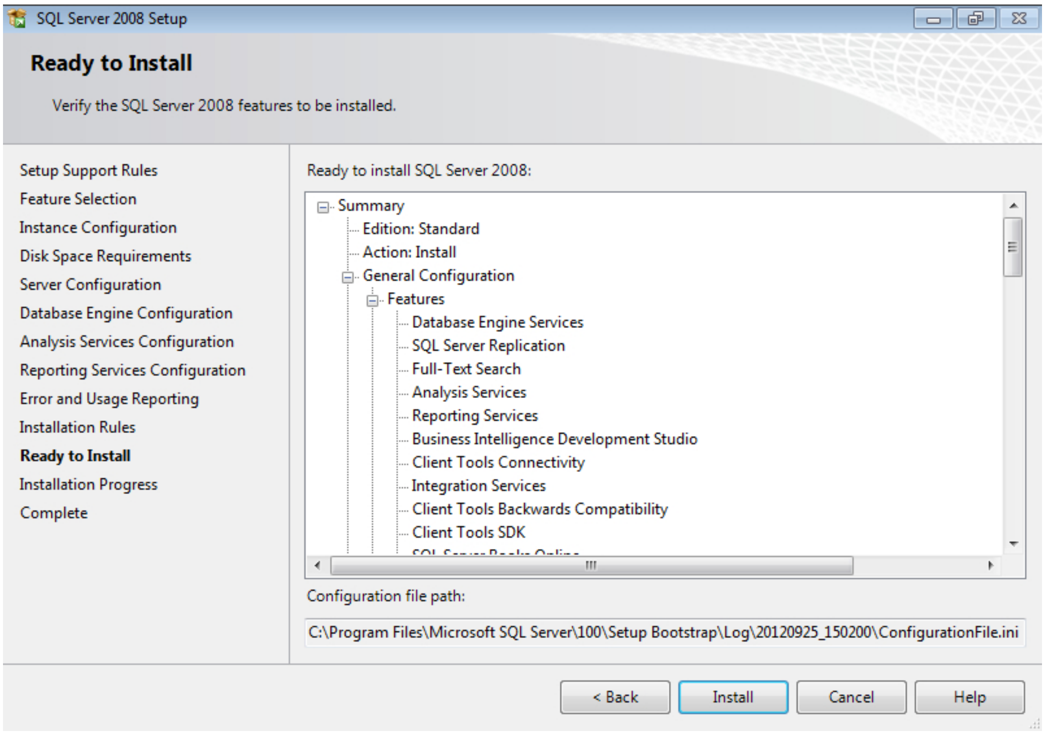
Operation completed. Passed: 11. Failed 0. Warning 0. Skipped 0.

View detailed report

Rule	Status
✓ Same architecture installation	Passed
✓ Cross language installation	Passed
✓ Existing clustered or cluster-prepared instance	Passed
✓ Reporting Services Catalog Database File Existence	Passed
✓ Reporting Services Catalog Temporary Database File Existence	Passed
✓ SQL Server 2005 Express tools	Passed
✓ Operating system supported for edition	Passed
✓ FAT32 File System	Passed
✓ SQL Server 2000 Analysis Services (64-bit) install action	Passed

Figure 195. The 'Installation Rules' section

17) Check the list of the components to be installed and click **Install** in the **Ready to Install** section (fig. The 'Ready to Install' section[199]).



Ready to Install

Verify the SQL Server 2008 features to be installed.

Ready to install SQL Server 2008:

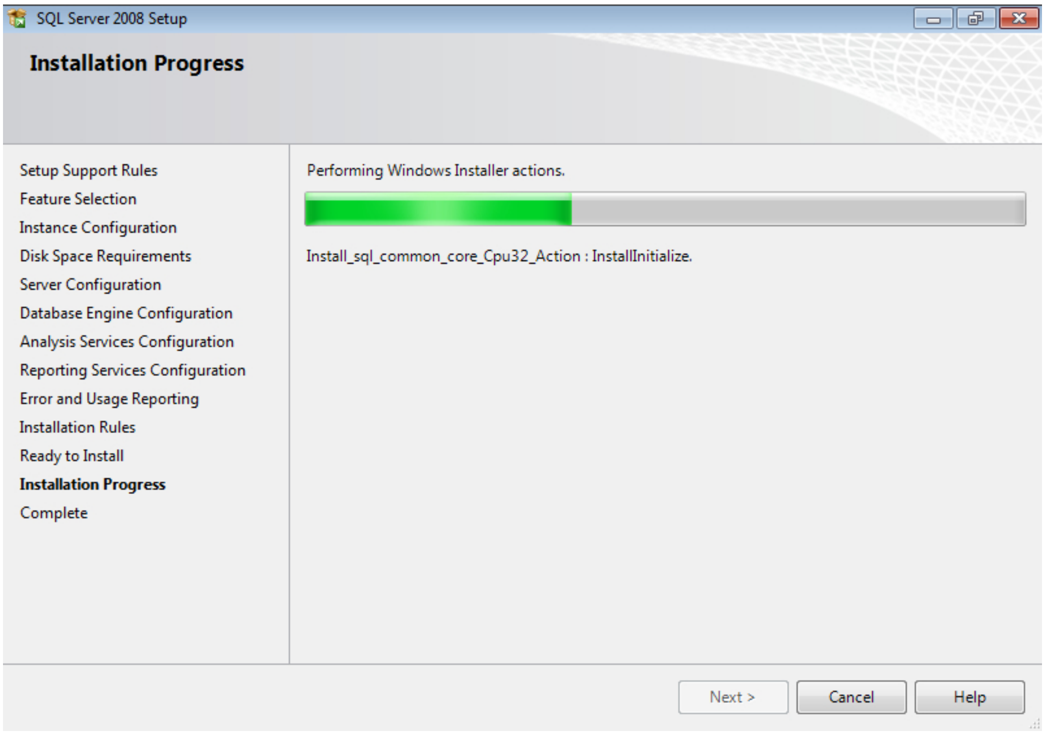
```
Summary
  Edition: Standard
  Action: Install
  General Configuration
    Features
      Database Engine Services
      SQL Server Replication
      Full-Text Search
      Analysis Services
      Reporting Services
      Business Intelligence Development Studio
      Client Tools Connectivity
      Integration Services
      Client Tools Backwards Compatibility
      Client Tools SDK
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20120925_150200\ConfigurationFile.ini

Figure 196. The 'Ready to Install' section

18) The **Installation Progress** section displays the progress of installing the Microsoft SQL Server 2008 components (fig. The 'Installation Progress' section[199]).



Installation Progress

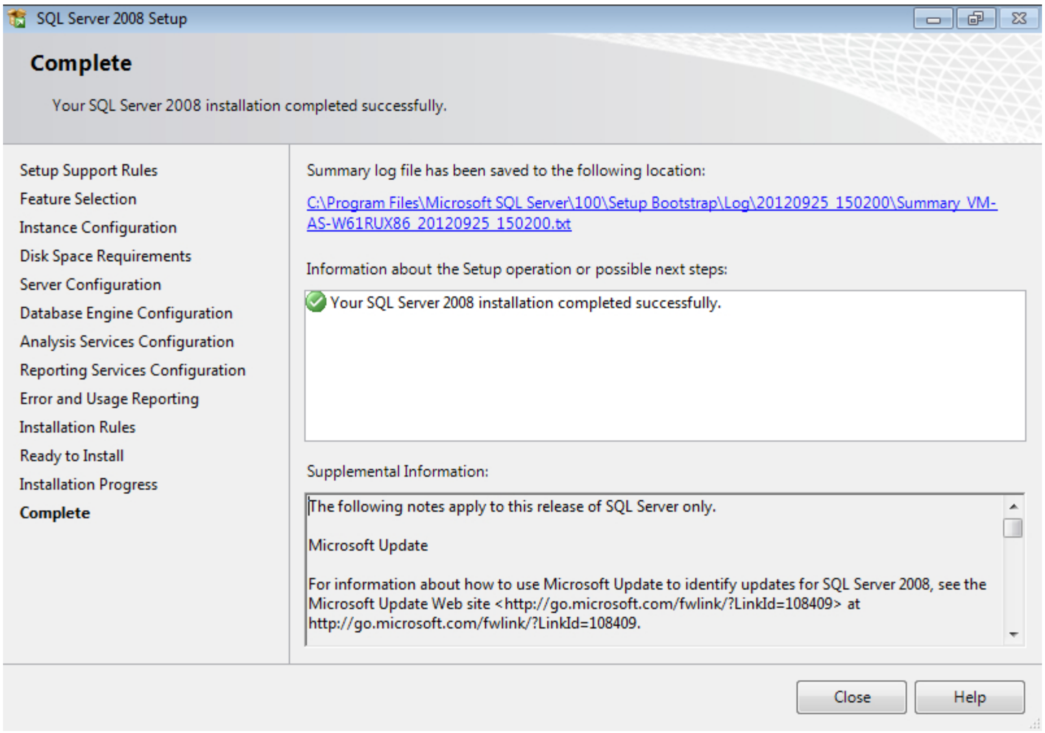
Performing Windows Installer actions.

Install_sql_common_core_Cpu32_Action : InstallInitialize.

Figure 197. The 'Installation Progress' section

Click **Next** when the installation completes.

Click **Close** in the **Complete** section to complete the installation (fig. The 'Complete' section[200]).



Your SQL Server 2008 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20120925_150200\Summary_VM-AS-W61RUX86_20120925_150200.txt

Information about the Setup operation or possible next steps:

✓ Your SQL Server 2008 installation completed successfully.

Supplemental Information:

The following notes apply to this release of SQL Server only.

Microsoft Update

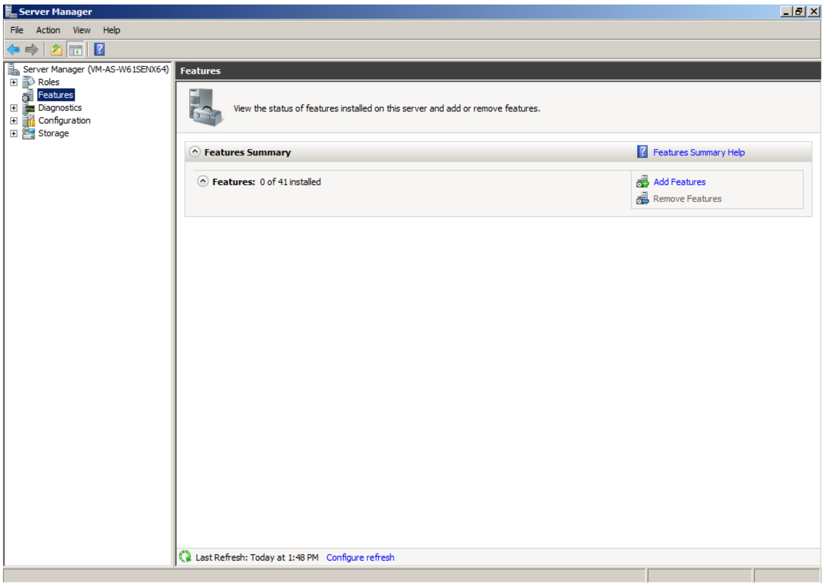
For information about how to use Microsoft Update to identify updates for SQL Server 2008, see the Microsoft Update Web site <http://go.microsoft.com/fwlink/?LinkId=108409> at http://go.microsoft.com/fwlink/?LinkId=108409.

Figure 198. The 'Complete' section

9.2 Adding the Desktop Experience component

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. Go to the **Features** section and click **Add Features** in the **Features Summary** area (fig. The Server Manager snap-in[200]).



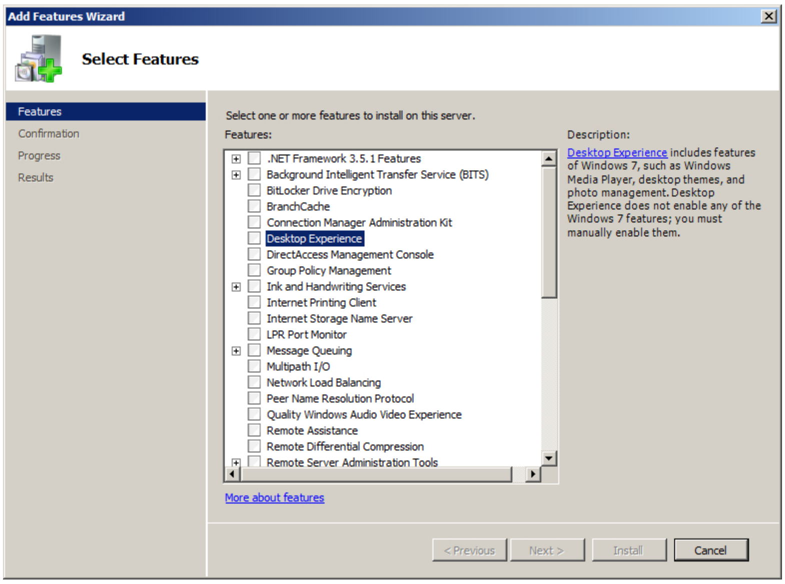
View the status of features installed on this server and add or remove features.

Features: 0 of 41 installed

Last Refresh: Today at 1:48 PM

Figure 199. The Server Manager snap-in

2) Tick off **Desktop Experience** in the displayed **Add Features Wizard** window (fig. Selecting components to add[201]) (for Microsoft® Windows® Server 2012 / 2012 R2: **User Interfaces and Infrastructure** → **Desktop Experience**).



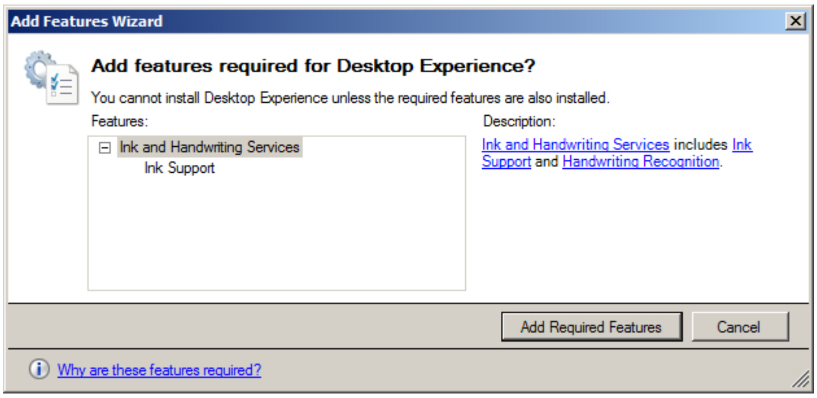
Select one or more features to install on this server.

- ☐ .NET Framework 3.5.1 Features
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BranchCache
- ☐ Connection Manager Administration Kit
- ☐ Desktop Experience
- ☐ DirectAccess Management Console
- ☐ Group Policy Management
- ☐ Ink and Handwriting Services
- ☐ Internet Printing Client
- ☐ Internet Storage Name Server
- ☐ LPR Port Monitor
- ☐ Message Queuing
- ☐ Multipath I/O
- ☐ Network Load Balancing
- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ☐ Remote Server Administration Tools

Desktop Experience includes features of Windows 7, such as Windows Media Player, desktop themes, and photo management. Desktop Experience does not enable any of the Windows 7 features; you must manually enable them.

Figure 200. Selecting components to add

3) When the dialog box with information about required components appears, click **Add Required Features** (fig. Requesting to add the required components[201]).



Add Features Wizard

Add features required for Desktop Experience?

You cannot install Desktop Experience unless the required features are also installed.

Features:

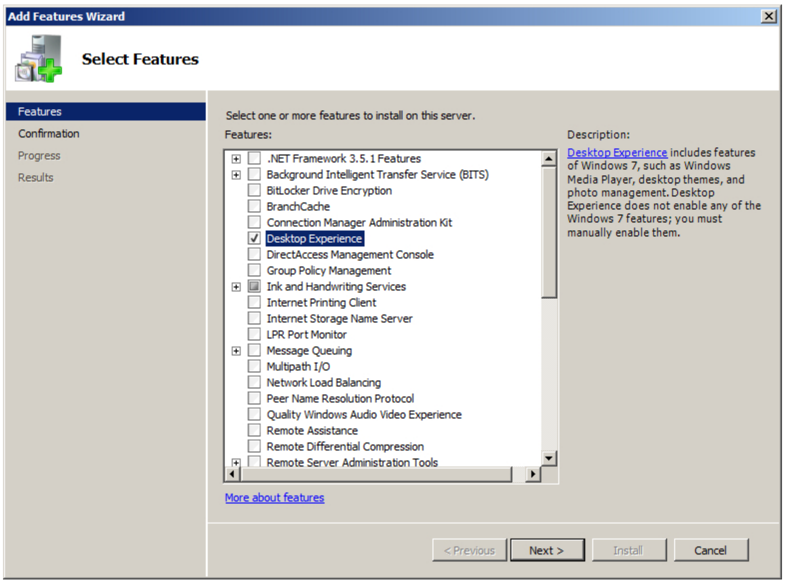
- Ink and Handwriting Services
  - Ink Support

Description:

Ink and Handwriting Services includes Ink Support and Handwriting Recognition.

Figure 201. Requesting to add the required components

4) Make sure that the **Desktop Experience** component is selected and click **Next** (fig. Selecting components to add[202]).



Add Features Wizard

Select Features

Select one or more features to install on this server.

Features:

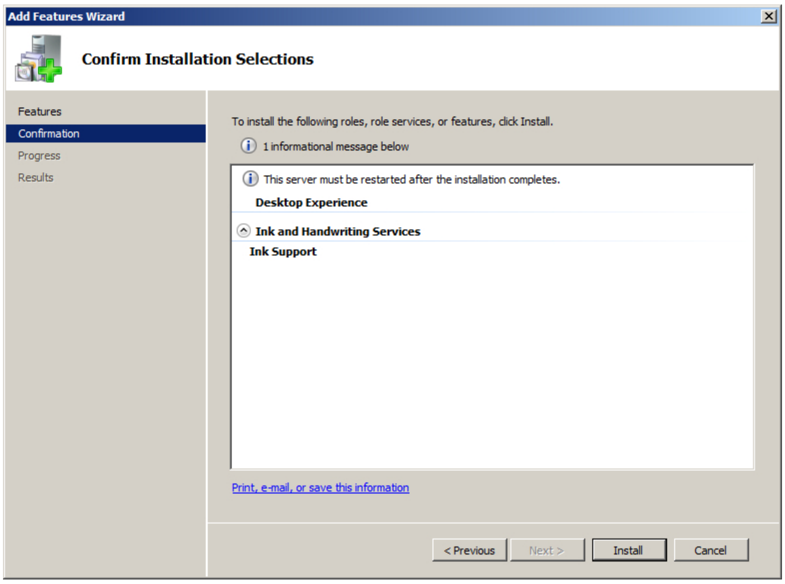
- □ .NET Framework 3.5.1 Features
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BranchCache
- □ Connection Manager Administration Kit
- ☑ Desktop Experience
- □ DirectAccess Management Console
- □ Group Policy Management
- ▣ Ink and Handwriting Services
- □ Internet Printing Client
- □ Internet Storage Name Server
- □ LPR Port Monitor
- □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ Remote Assistance
- □ Remote Differential Compression
- □ Remote Server Administration Tools

Description:

Desktop Experience includes features of Windows 7, such as Windows Media Player, desktop themes, and photo management. Desktop Experience does not enable any of the Windows 7 features; you must manually enable them.

Figure 202. Selecting components to add

5) Click **Next** in the **Confirmation** step (fig. Confirming installation selection[202]).



Add Features Wizard

Confirm Installation Selections

To install the following roles, role services, or features, click Install.

1 informational message below

This server must be restarted after the installation completes.

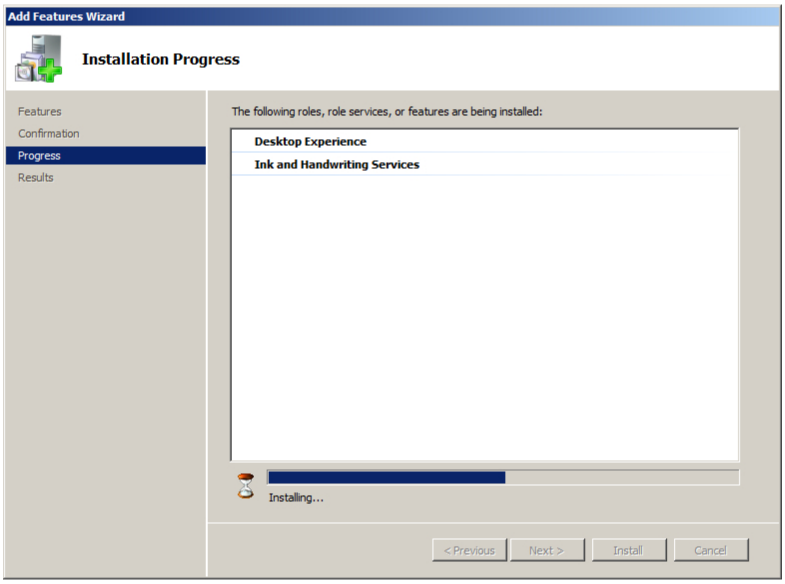
Desktop Experience

Ink and Handwriting Services

Ink Support

Figure 203. Confirming installation selection

6) Wait until the installation completes (fig. Installation progress[203]).



Add Features Wizard

Installation Progress

The following roles, role services, or features are being installed:

Desktop Experience

Ink and Handwriting Services

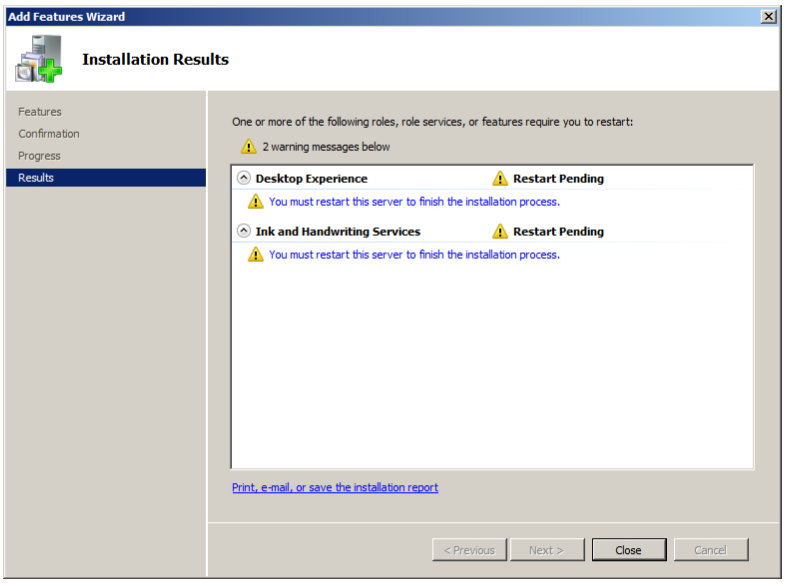
Installing...

Figure 204. Installation progress

7) Click **Close** in the **Results** step (fig. Finished adding the components[203]).

8) Select **Yes** in the dialog box that suggests system restart. The system is then restarted to complete the installation (fig. Requesting system restart[204]).

9) After the system reboots, make sure that all the required components are installed successfully (**Installation succeeded**), in the displayed **Resume Configuration Wizard** displayed window. Click **Close** (fig. The result of adding the components[204]).



Installation Results

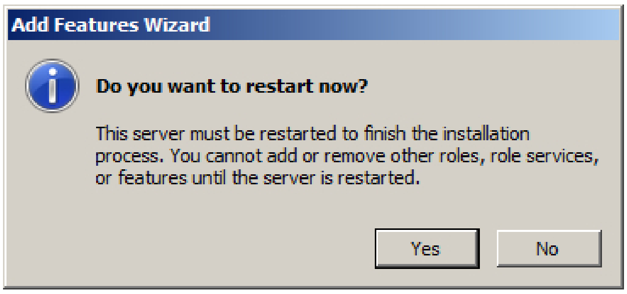
One or more of the following roles, role services, or features require you to restart:

⚠ 2 warning messages below

Desktop Experience	⚠ Restart Pending
⚠ You must restart this server to finish the installation process.	
Ink and Handwriting Services	⚠ Restart Pending
⚠ You must restart this server to finish the installation process.	

Print, e-mail, or save the installation report

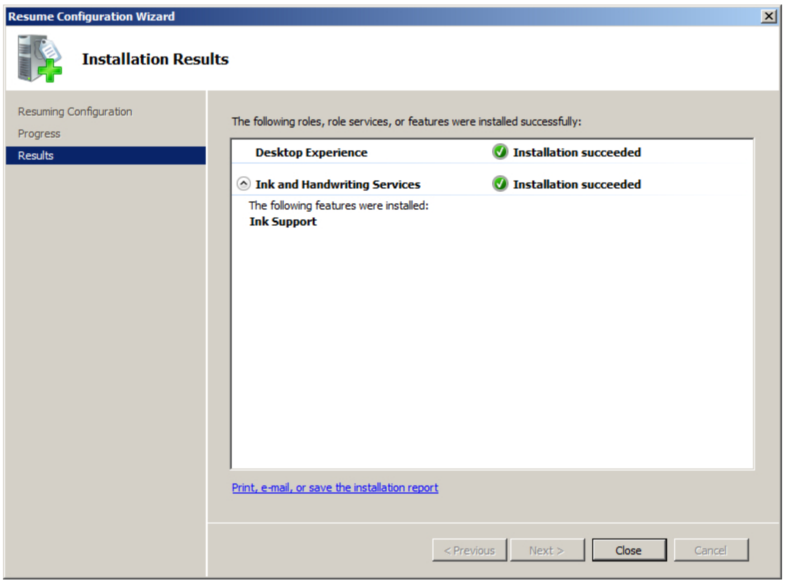
Figure 205. Finished adding the components



Do you want to restart now?

This server must be restarted to finish the installation process. You cannot add or remove other roles, role services, or features until the server is restarted.

Figure 206. Requesting system restart



Installation Results

The following roles, role services, or features were installed successfully:

Desktop Experience	✓ Installation succeeded
Ink and Handwriting Services	✓ Installation succeeded

The following features were installed:
Ink Support

Print, e-mail, or save the installation report

Figure 207. The result of adding the components

10. Supplemental information

10.1 About certificates

This section describes the most important aspects of cryptographic protection of the communication channel between SoftControl Service Center and client applications (hereafter referred to as 'clients').

The HTTPS communication protocol is used in SoftControl Service Center for interaction between the SoftControl Server component and the clients. All data between the server and an endpoint are sent in an encrypted form through a secure channel. X.509 standard certificates are used for client authorization.

SoftControl Server generates the following kinds of certificates during its operation:

- **CA certificate** is a self-signed root certificate of the certification authority (CA) within a SoftControl ISS. SoftControl Server generates this certificate at the time of configuring and places the CA certificate in the Windows storage. All the other certificates are signed with the CA certificate, which is a validity criterion.
- **Server certificate** is a certificate signed with the CA certificate and used by the server to establish a protected SSL/TLS connection with clients. SoftControl Server generates this certificate at the time of configuring and places the CA certificate in the Windows storage on the server computer.
- **Common client certificate** is a certificate signed with the CA certificate and used by a client to establish a protected SSL/TLS connection with SoftControl Server when it connects to SoftControl Server for the first time. This certificate is common for all new clients and it is only used for sending their first request to the server. The common client certificate is integrated into the encrypted client configuration file 26 that is applied to the client at an endpoint. The common client certificate is generated by the server at the time of configuring and is stored on the server computer at the following path:

  ```
  C:\ProgramData\SafenSoft\Client.pem
  ```

- **Specific client certificate** is a certificate signed with the CA certificate and used by a client to establish a protected SSL/TLS connection with SoftControl Server after registration confirmation 46 by the administrator via SoftControl Admin Console. This certificate is unique for each client, which makes unauthorized access to the communication channel impossible even if violators have a stolen specific certificate of another client or a common certificate. If a specific certificate is considered invalid for some reason or is expired, it is possible to revoke it (rejecting the registration[47]) or issue another certificate (updating[47]).

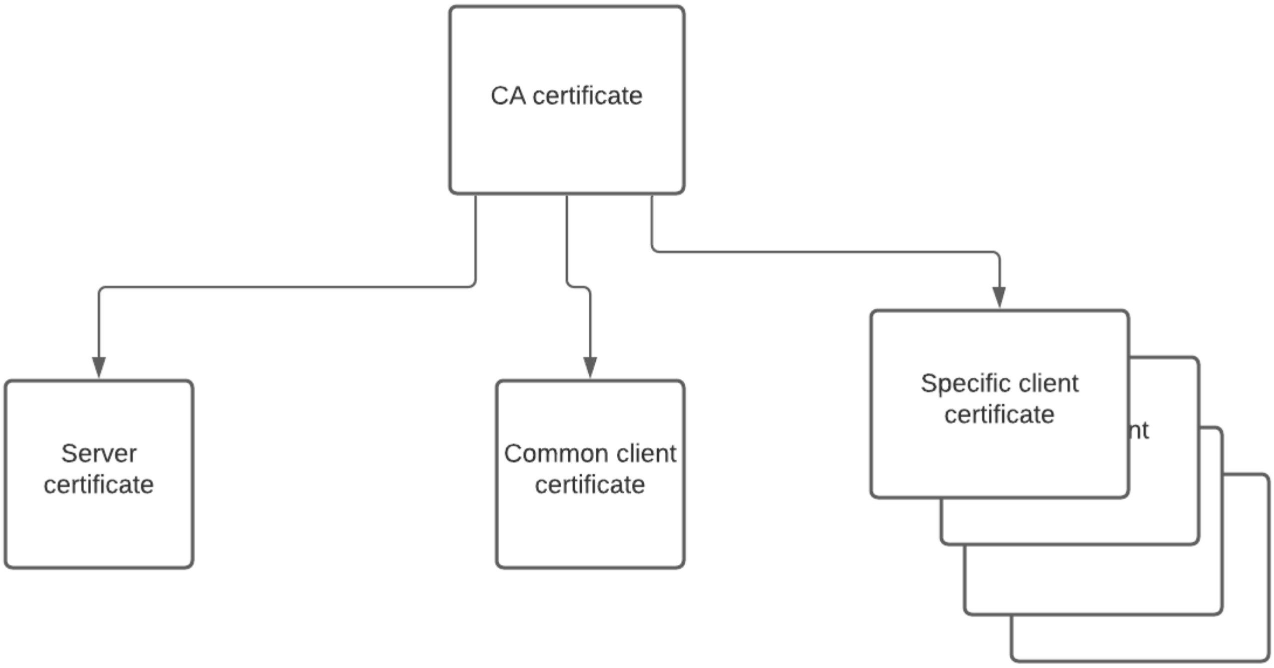
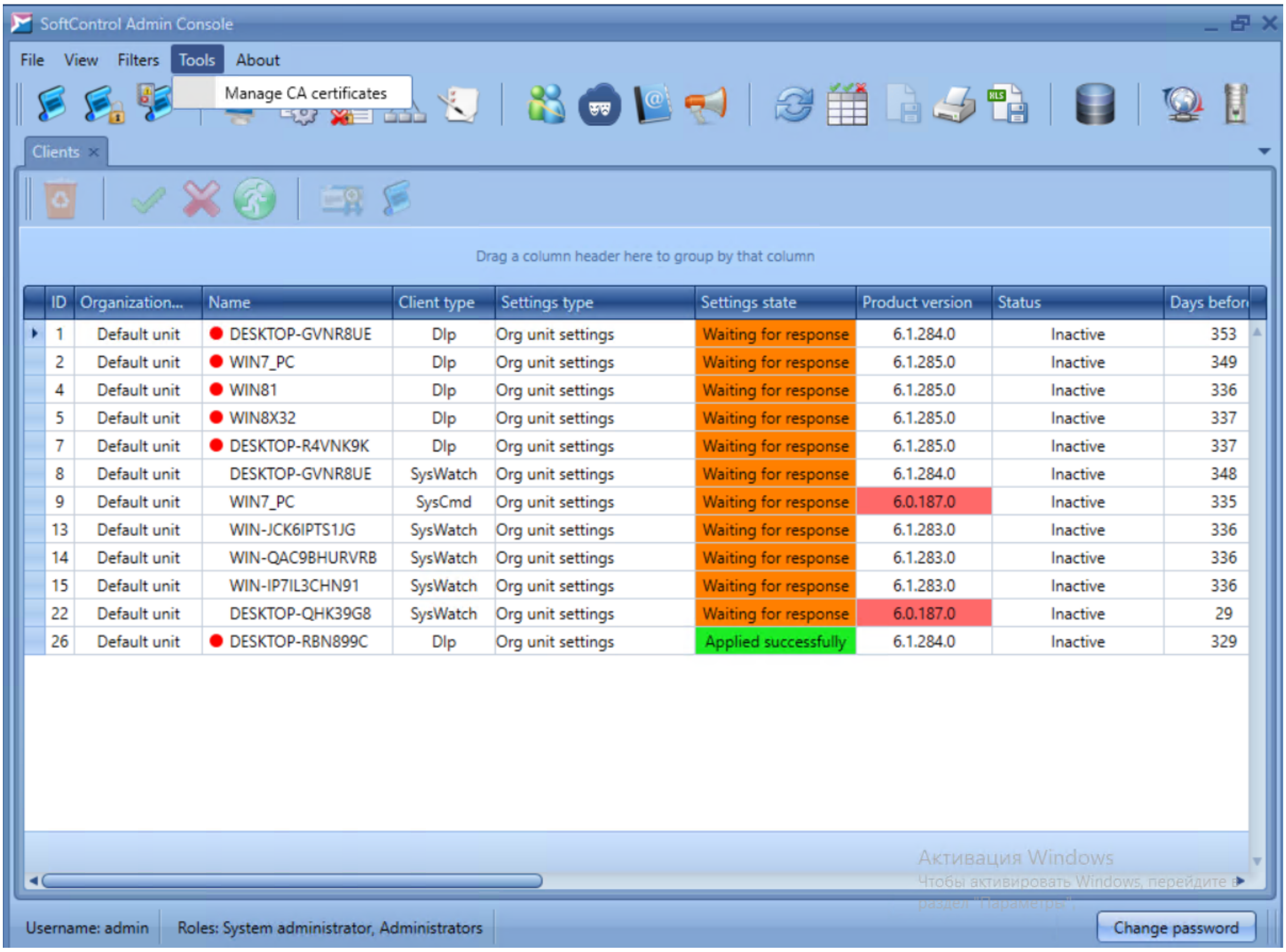


Figure 208. Certificates in a SoftControl ISS

10.2 Managing certificates

Open **Tools** → **Manage CA certificates** to generate and apply new CA (certification authority) certificates.


SoftControl Admin Console
File
View
Filters
Tools
About
Manage CA certificates
Clients
Drag a column header here to group by that column

ID	Organization...	Name	Client type	Settings type	Settings state	Product version	Status	Days befor
1	Default unit	● DESKTOP-GVNR8UE	Dlp	Org unit settings	Waiting for response	6.1.284.0	Inactive	353
2	Default unit	● WIN7_PC	Dlp	Org unit settings	Waiting for response	6.1.285.0	Inactive	349
4	Default unit	● WIN81	Dlp	Org unit settings	Waiting for response	6.1.285.0	Inactive	336
5	Default unit	● WIN8X32	Dlp	Org unit settings	Waiting for response	6.1.285.0	Inactive	337
7	Default unit	● DESKTOP-R4VNK9K	Dlp	Org unit settings	Waiting for response	6.1.285.0	Inactive	337
8	Default unit	DESKTOP-GVNR8UE	SysWatch	Org unit settings	Waiting for response	6.1.284.0	Inactive	348
9	Default unit	WIN7_PC	SysCmd	Org unit settings	Waiting for response	6.0.187.0	Inactive	335
13	Default unit	WIN-JCK6IPTS1JG	SysWatch	Org unit settings	Waiting for response	6.1.283.0	Inactive	336
14	Default unit	WIN-QAC9BHURVRB	SysWatch	Org unit settings	Waiting for response	6.1.283.0	Inactive	336
15	Default unit	WIN-IP7IL3CHN91	SysWatch	Org unit settings	Waiting for response	6.1.283.0	Inactive	336
22	Default unit	DESKTOP-QHK39G8	SysWatch	Org unit settings	Waiting for response	6.0.187.0	Inactive	29
26	Default unit	● DESKTOP-RBN899C	Dlp	Org unit settings	Applied successfully	6.1.284.0	Inactive	329

Username: admin

Roles: System administrator, Administrators

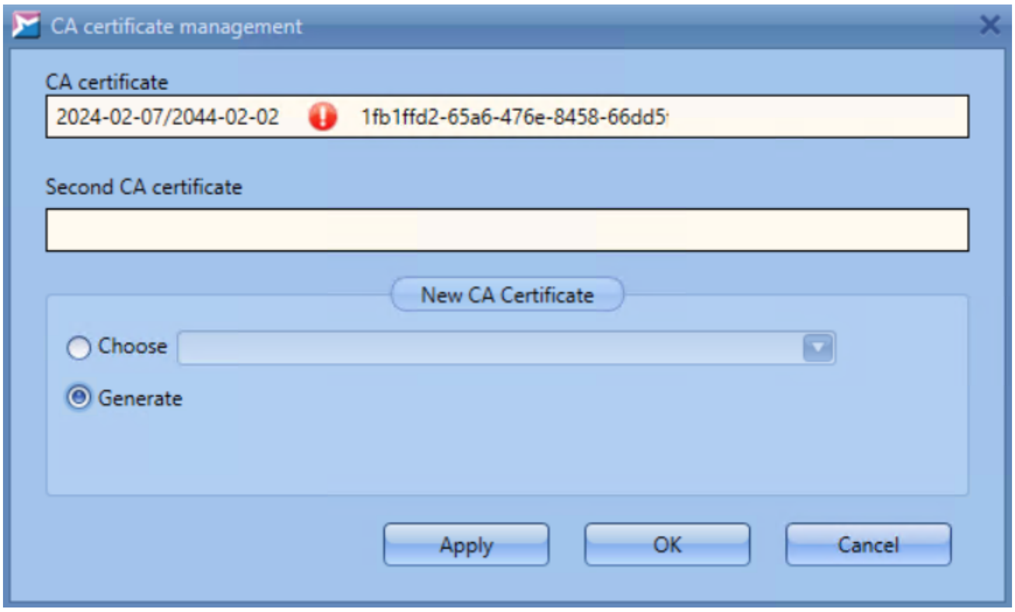
Figure 209. Managing CA certificates

The **CA certificate** and **Second CA certificate** fields show information about the currently used CA certificate and the certificate that will be used when the current one expires. A new CA certificate is generated automatically three years prior to expiration of the currently used CA certificate. You might need a new certificate sooner if you update SoftControl software to version 6.0 or later (from versions under 6.0). Clients that are already connected to SoftControl Server will continue to operate, but if you wish to register new clients, you will have to update your CA certificate.

To do this, you can **Choose** a previously generated certificate or **Generate** a new one. To generate a new CA certificate, select **Generate** and click

Apply or **OK**, confirm your intention by clicking **Yes** in the pop-up window.

After applying the certificate in the **CA certificate** field as the currently active CA certificate and the certificate in the **New CA certificate** as the next CA certificate in line. Learn more about updating certificates for version 6.0 and newer versions in the article http://kb.safensoft.com/index.php/Updating_SoftControl_5_to_SoftControl_6.



CA certificate management

CA certificate: 2024-02-07/2044-02-02 1fb1ffd2-65a6-476e-8458-66dd5

Second CA certificate:

New CA Certificate

○ Choose

● Generate

Figure 210. Window for managing CA certificates

CA certificate details have the following format: **<generation_date>/<expiration_date><EKU_-flag_if_present><certificate_name>**.

10.3 Recovering connection with the server

In the system of the client-server interaction (in the context of an ISS on the basis of SoftControl Service Center), IP address of the server can change automatically, for example, when entering the network after a reboot. In this case, client applications with configurations that only contain IP addresses of the computer with the installed SoftControl Server, but not the computer's network name, lose connection with the server. In order not to edit IP addresses manually and locally in the settings of each client component, rescue recovery server is provided. To activate it, take the following steps:

1) Open the server configuration file that is located by the following path:

```
C:\ProgramData\SafenSoft\Server.Config.xml
```

2) Set the *Active* flag value to *True* in the *RescueSettings* element.

3) Add subitems of the following type to the *RescueSettings* element:

```
<Address Uri="<server new IP address or name>" Port="<connection port>" />
```

4) Save changes in the configuration file.

5) Change the name of the computer with the installed SoftControl Server to *screstore*.

6) Reboot the computer with the installed SoftControl Server to apply new settings and change the host's network name.

7) The *8888* port for rescue connection is added to the Windows firewall automatically after the SoftControl Server system service runs.

8) After 10 failed attempts to connect the addresses specified in the settings, client components attempt to connect to the rescue server with the name *screstore* on port *8888* (by default). After successful connection to this address, a new list of server addresses specified in the settings is transferred to the clients, and the old list of addresses is replaced with the new one in the settings. After connection with all clients connected to SoftControl Service Center is recovered, the server's network name can be changed to the original one.

10.4 SoftControl Service Center backup

In some cases, you might need to create a backup copy[209] of the SoftControl Service Center components, so as to restore[210] a fully functional configuration without losing connection with the client applications on the remote hosts. The cases that these operations apply to are as follows.

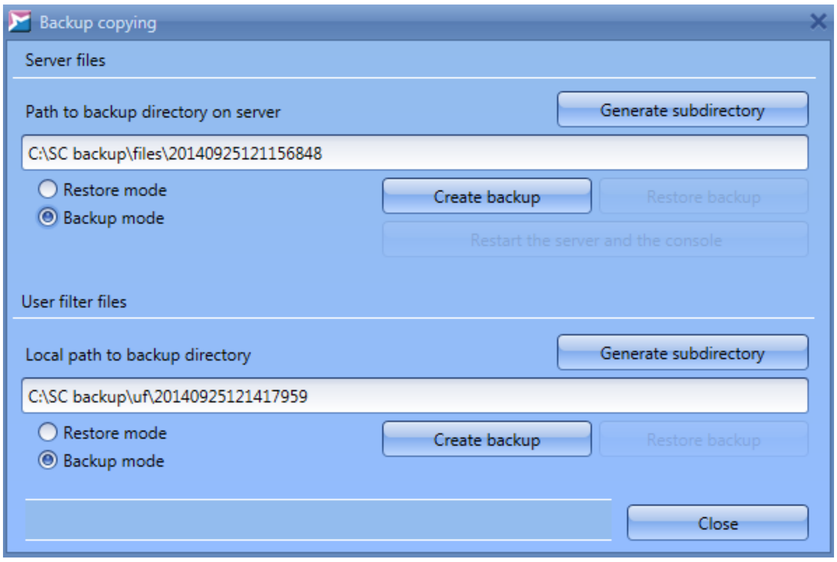
- you need to reinstall the OS on the computer with the SoftControl Service Center components;
- you need to transfer SoftControl Service Center to another computer.

10.4.1 Creating the backup copy

A backup copy of the SoftControl Service Center files includes the SoftControl Server configuration files and certificates[205] that are necessary for restoring. SoftControl Admin Console user filters[146] can also be saved (optional). To create a backup copy, perform the following operations.

1) Select **View** → **Backup copying** in the SoftControl Admin Console main menu.

2) Select **Create mode** in the **Server files** area in the displayed window (fig. Creating a backup copy[209]).



Path to backup directory on server: C:\SC backup\files\20140925121156848

○ Restore mode
● Backup mode

Local path to backup directory: C:\SC backup\uf\20140925121417959

○ Restore mode
● Backup mode

Figure 211. Creating a backup copy

Enter the path to the folder to save backup files in the corresponding field. If you need to create a subfolder with the unique identifier by the specified path, click **Generate subdirectory**. If you click the button when the input field is empty, the subfolder is placed to the following directory by default:

```
C:\Windows\System32
```

Click **Create backup** to create backup files by the specified path. Action status is displayed in the lower part of the window.

3) To save user filters, repeat operations in the previous item for the **User filter files** area in the **Backup copying** window (fig. Creating a backup copy[209]).

If you click **Generate subdirectory** when the input field is empty, the subfolder is placed to the SoftControl Admin Console installation directory by default.

4) If SoftControl Service Center database is located on an external server (that differs from the computer with the installed SoftControl Service Center components), you do not need to save its copy. Otherwise, create a backup copy of the current database with the help of Microsoft® SQL Server® tools.

10.4.2 Restoring from the backup copy

To restore SoftControl Service Center from a backup copy, perform the following operations.

1) Make sure the time settings on the computer are valid.

2) Install[11] SoftControl Service Center of the same version as on the computer that the

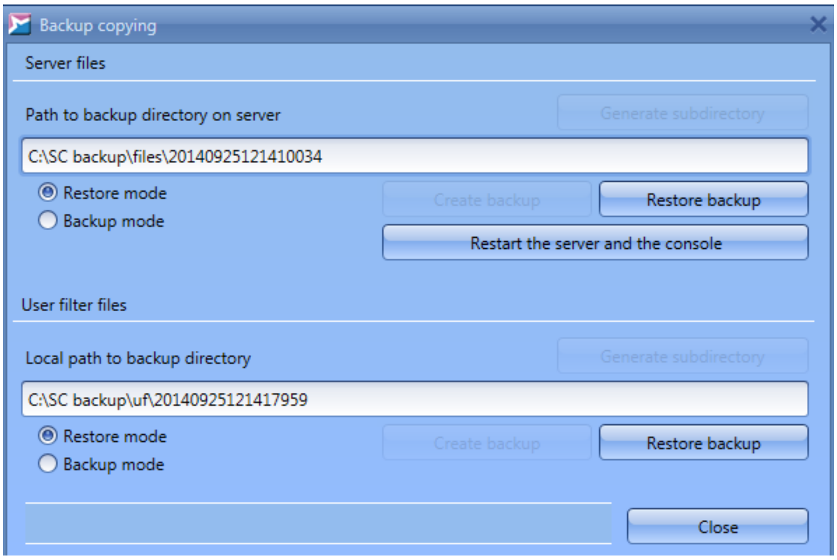
backup copy has been created on.

3) Restore the previously saved database. Skip this step if the database has been on another computer and has not been deleted.

4) Set up[21] SoftControl Service Center. Specify a new **Database name** that differs from the name of the old database, so as not to damage the settings of the old database. After restoring SoftControl Service Center from a backup copy, the server switches to the old database automatically.

5) Select **View** → **Backup copying** in the SoftControl Admin Console main menu.

6) Select **Restore mode** in the **Server files** area in the displayed window (fig. Restoring from a backup copy[211]).



Server files

Path to backup directory on server

C:\SC backup\files\20140925121410034

● Restore mode
○ Backup mode

User filter files

Local path to backup directory

C:\SC backup\uf\20140925121417959

● Restore mode
○ Backup mode

Figure 212. Restoring from a backup copy

Enter the path to the folder with the previously saved backup files in the corresponding field and click **Restore backup**. Action status is displayed in the lower part of the window.

7) If you need to restore user filters, repeat the operations of step 6[211] for the **User filter files** area in the **Backup copying** window (fig. Restoring from a backup copy[211]).

8) Click **Restart server and console** to restart the SoftControl Server system service and apply the restored configuration.

Note: you may need to restart the computer for some OS.

9) Remove the temporary database you created during step 4[211].

10) Log in[26] to SoftControl Admin Console. Make sure all the components work.

10.5 Process privileges

Table 41 describes Windows privileges that the processes use (see also https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716(v=vs.85).aspx and https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4704).

Table 41. Process privileges

Privilege	Description
Manage auditing and security log	Required to generate audit-log entries. With this privilege, the user can add entries to the security log.
Back up files and directories	Required to perform backup operations. This privilege causes the system to grant all read access control to any file, regardless of the access control list (ACL) specified for the file. Any access request other than read is still evaluated with the ACL. With this privilege, the user can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system.
Restore files and directories	Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL. With this privilege, the user can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories. Additionally, this privilege enables you to set any valid user or group SID as the owner of a file.
Change the system time	Required to modify the system time. With this privilege, the user can change the time and date on the internal clock of the computer. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.
Shut down the system	Required to shut down a local system.
Force shutdown from a remote computer	Required to shut down a system using a network request.
Take ownership of files or other objects	Required to take ownership of an object without being granted discretionary access. With this privilege, the user can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.
Debug programs	Required to debug and adjust the memory of a process owned by another account. With this privilege, the user can attach a debugger to any process or to the kernel. Developers who are debugging their own applications do not need this user right. Developers who are debugging new system components need this user right. This user right provides complete access to sensitive and critical operating system components.
Modify firmware environment values	Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
Profile the system performance	Required to gather profiling information for the entire system. With this privilege, the user can use performance monitoring tools to monitor the performance of system processes.
Profile single process	Required to gather profiling information for a single process.

Privilege	Description
	With this privilege, the user can use performance monitoring tools to monitor the performance of non-system processes.
Increase scheduling priority	Required to increase the base priority of a process. With this privilege, the user can use a process with Write property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.
Load and unload device drivers	Required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers.
Create a pagefile	Required to create a paging file. With this privilege, the user can create and change the size of a pagefile.
Adjust memory quotas for a process	Required to increase the quota assigned to a process.
Bypass traverse checking	Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. It is enabled by default for all users.
Remove a computer from the docking station	Required to undock a laptop. With this privilege, the user can undock a portable computer from its docking station without logging on.
Perform volume maintenance tasks	Enables volume management privileges. Required to run maintenance tasks on a volume, such as remote defragmentation.
Impersonate a client after authentication	Required to impersonate. With this privilege, the user can impersonate other accounts.
Create global objects	Required to create named file mapping objects in the global namespace during Terminal Services sessions. This privilege is enabled by default for administrators, services, and the LocalSystem account.

10.6 SoftControl SysWatch traffic

There are three sources of SoftControl SysWatch traffic:

1) HTTPS overhead,

2) Logs from client device,

3) Updates (client module and antivirus bases).

HTTPS overhead

HTTPS overhead traffic amounts to 3.7 KB per heartbeat. (Heartbeat is the client component parameter that specifies the period when a client component connects to the SoftControl Server component.)

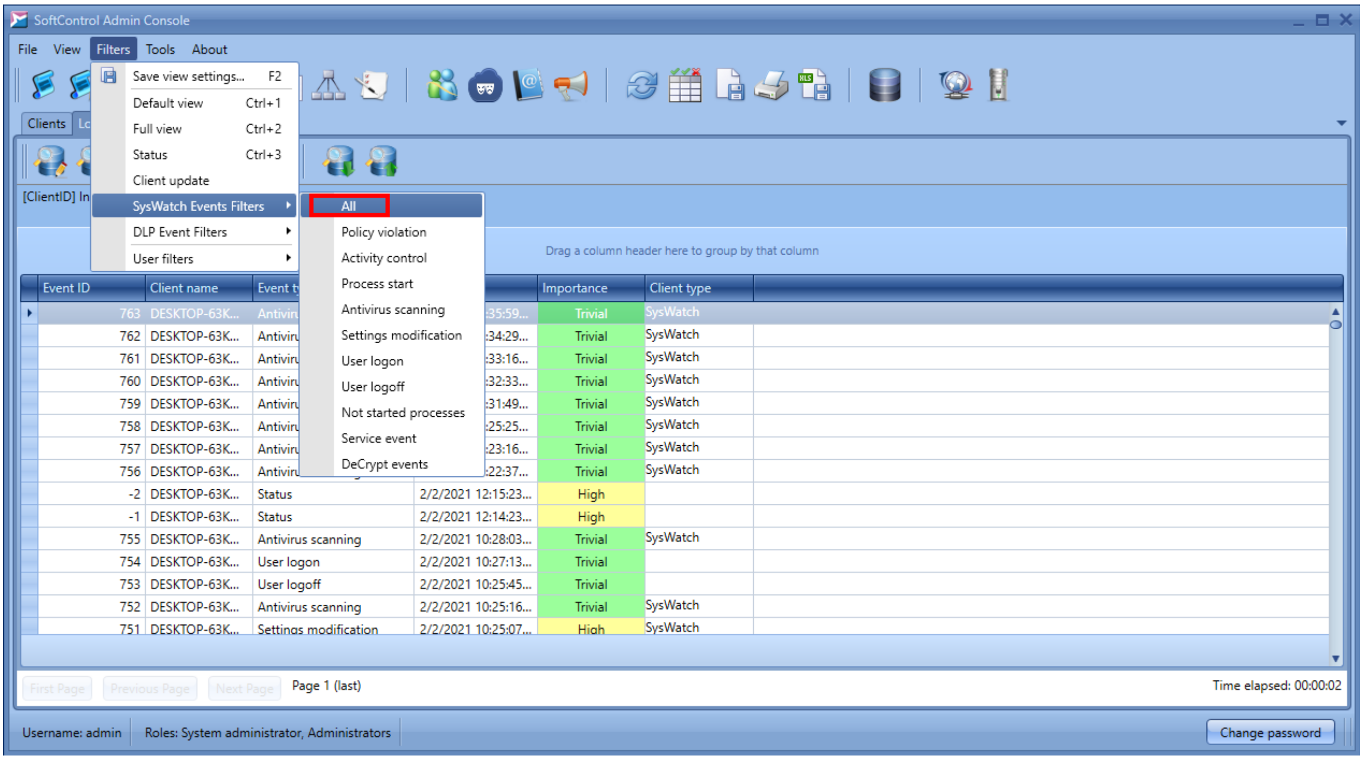
To estimate monthly traffic generated by HTTPS overhead, you can use the following formula: `T1=3.7*30*24*3600/heartbeat value [seconds]`. The result will be measured in KBs per month.

Logs from client device

Traffic generated for one event amounts to approximately 500 bytes. You can use the number of events to estimate the traffic amount generated by logs on a standard device within 24 hours, as well as the required database capacity.

Follow these steps to export event records of a standard device created within 24 hours:

1. Open the event log of the device in SoftControl Admin Console.
2. Select in the top menu panel **Filters –> SysWatch Events Filters –> All**.



Event ID	Client name	Event t		Importance	Client type
763	DESKTOP-63K...	Antiviru	:35:59...	Trivial	SysWatch
762	DESKTOP-63K...	Antiviru	:34:29...	Trivial	SysWatch
761	DESKTOP-63K...	Antiviru	:33:16...	Trivial	SysWatch
760	DESKTOP-63K...	Antiviru	:32:33...	Trivial	SysWatch
759	DESKTOP-63K...	Antiviru	:31:49...	Trivial	SysWatch
758	DESKTOP-63K...	Antiviru	:25:25...	Trivial	SysWatch
757	DESKTOP-63K...	Antiviru	:23:16...	Trivial	SysWatch
756	DESKTOP-63K...	Antiviru	:22:37...	Trivial	SysWatch
-2	DESKTOP-63K...	Status	2/2/2021 12:15:23...	High	
-1	DESKTOP-63K...	Status	2/2/2021 12:14:23...	High	
755	DESKTOP-63K...	Antivirus scanning	2/2/2021 10:28:03...	Trivial	SysWatch
754	DESKTOP-63K...	User logon	2/2/2021 10:27:13...	Trivial	
753	DESKTOP-63K...	User logoff	2/2/2021 10:25:45...	Trivial	
752	DESKTOP-63K...	Antivirus scanning	2/2/2021 10:25:16...	Trivial	SysWatch
751	DESKTOP-63K...	Settings modification	2/2/2021 10:25:07...	High	SysWatch

Page 1 (last)

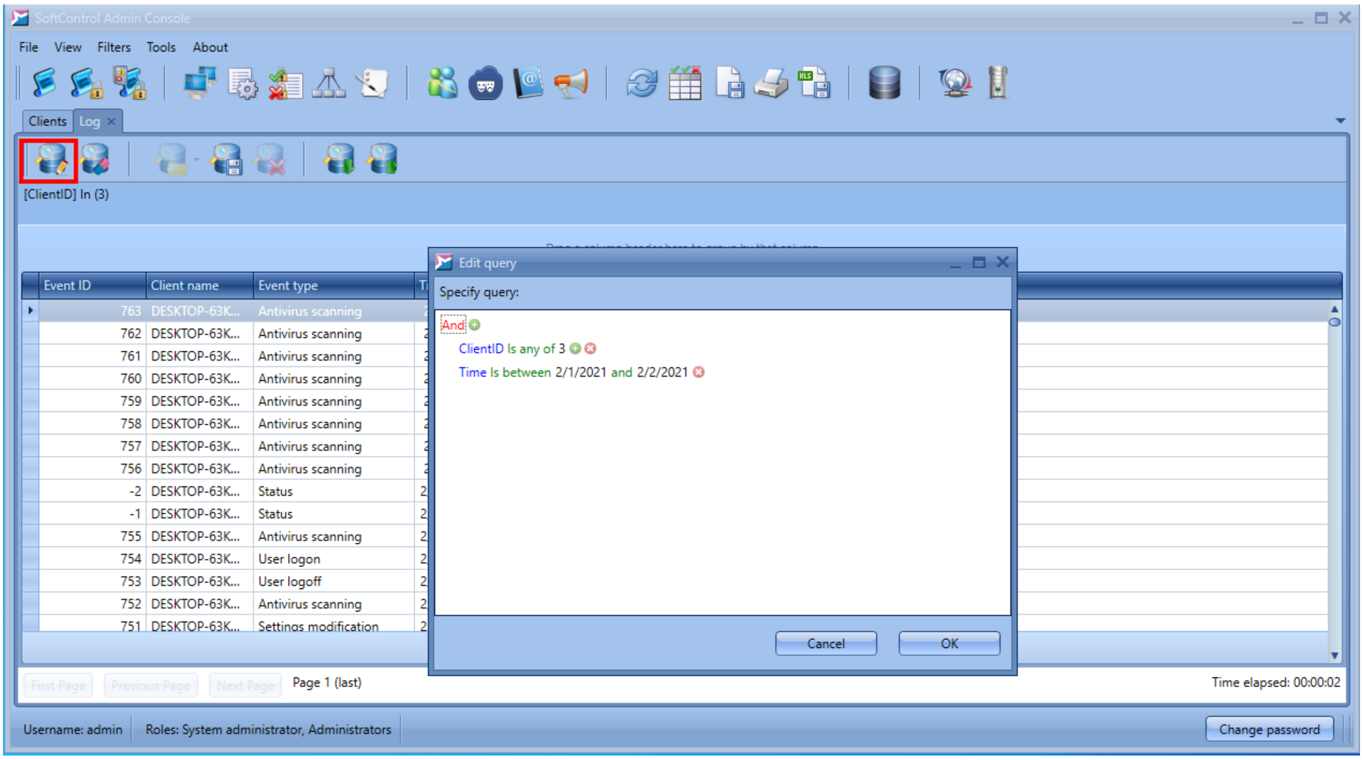
Time elapsed: 00:00:02

Username: admin

Roles: System administrator, Administrators

Figure 213. Set filter for event log

3. Click (**Edit query**). See Filtering the events[144] and Database queries[148] for details.
4. To add the time filter, click on the green circle with the plus sign, then select **Time**, **Is between**, and set a one-day interval.



[ClientID] In (3)

Specify query:

```
And
  ClientID Is any of 3
  Time Is between 2/1/2021 and 2/2/2021
```

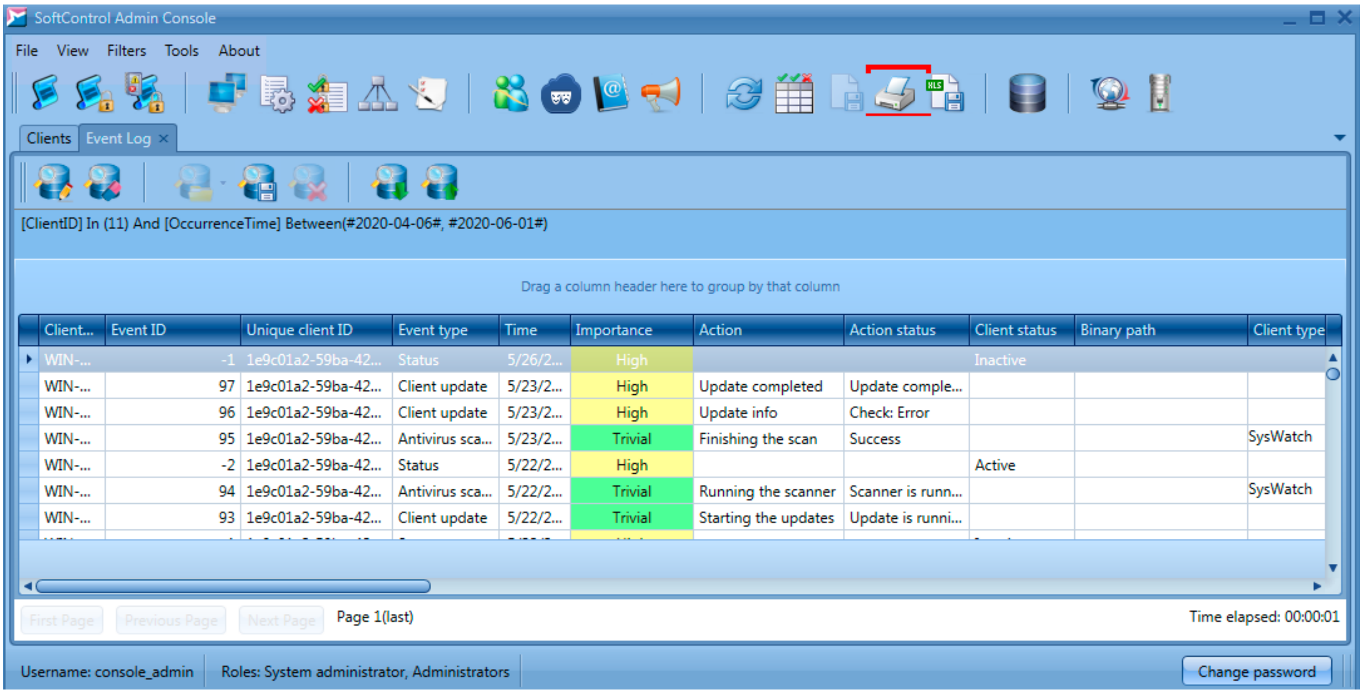
Event ID	Client name	Event type
763	DESKTOP-63K...	Antivirus scanning
762	DESKTOP-63K...	Antivirus scanning
761	DESKTOP-63K...	Antivirus scanning
760	DESKTOP-63K...	Antivirus scanning
759	DESKTOP-63K...	Antivirus scanning
758	DESKTOP-63K...	Antivirus scanning
757	DESKTOP-63K...	Antivirus scanning
756	DESKTOP-63K...	Antivirus scanning
-2	DESKTOP-63K...	Status
-1	DESKTOP-63K...	Status
755	DESKTOP-63K...	Antivirus scanning
754	DESKTOP-63K...	User logon
753	DESKTOP-63K...	User logoff
752	DESKTOP-63K...	Antivirus scanning
751	DESKTOP-63K...	Settings modification

Page 1 (last) Time elapsed: 00:00:02

Username: admin Roles: System administrator, Administrators

Figure 214. Edit database query. Set time

5. SoftControl Admin Console will show you records of events that pertain to the specified period. Click **Export to Excel** and choose the directory where you wish to save the event log.


SoftControl Admin Console
File View Filters Tools About
Clients Event Log ×
Drag a column header here to group by that column
First Page
Previous Page
Next Page
Change password

[ClientID] In (11) And [OccurrenceTime] Between(#2020-04-06#, #2020-06-01#)

Client...	Event ID	Unique client ID	Event type	Time	Importance	Action	Action status	Client status	Binary path	Client type
WIN-...	-1	1e9c01a2-59ba-42...	Status	5/26/2...	High			Inactive		
WIN-...	97	1e9c01a2-59ba-42...	Client update	5/23/2...	High	Update completed	Update comple...			
WIN-...	96	1e9c01a2-59ba-42...	Client update	5/23/2...	High	Update info	Check: Error			
WIN-...	95	1e9c01a2-59ba-42...	Antivirus sca...	5/23/2...	Trivial	Finishing the scan	Success			SysWatch
WIN-...	-2	1e9c01a2-59ba-42...	Status	5/22/2...	High			Active		
WIN-...	94	1e9c01a2-59ba-42...	Antivirus sca...	5/22/2...	Trivial	Running the scanner	Scanner is runn...			SysWatch
WIN-...	93	1e9c01a2-59ba-42...	Client update	5/22/2...	Trivial	Starting the updates	Update is runni...			

Page 1(last) Time elapsed: 00:00:01

Username: console_admin Roles: System administrator, Administrators

Figure 215. Export to XLSX

6. Count records in the exported file. Multiply this number by 500 bytes, and you will get approximate traffic amount generated within 24 hours by the device logs.

Updates

Client module updates

One update amounts to 30 MB. New updates are released 3–4 times a year.

Antivirus base updates

The first update after installation amounts to 60 MB. Following updates generate 400 to 1,300 KB daily (depending on new antivirus bases released).

10.7 Sources

Sources of supplemental information are presented in table 42.

Table 42. Supporting documentation

Name	Description
SoftControl ATM Client user's guide	Installing, setting up and working with the SoftControl ATM Client component
SoftControl Endpoint Client user's guide	Installing, setting up and working with the SoftControl Endpoint Client component
SoftControl SClient user's guide	Installing, setting up and working with the SoftControl SClient component
SoftControl DLP Client installation guide	Installing and setting up the SoftControl DLP Client component.

10.8 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 antivius bases on 32-bit Windows XP.

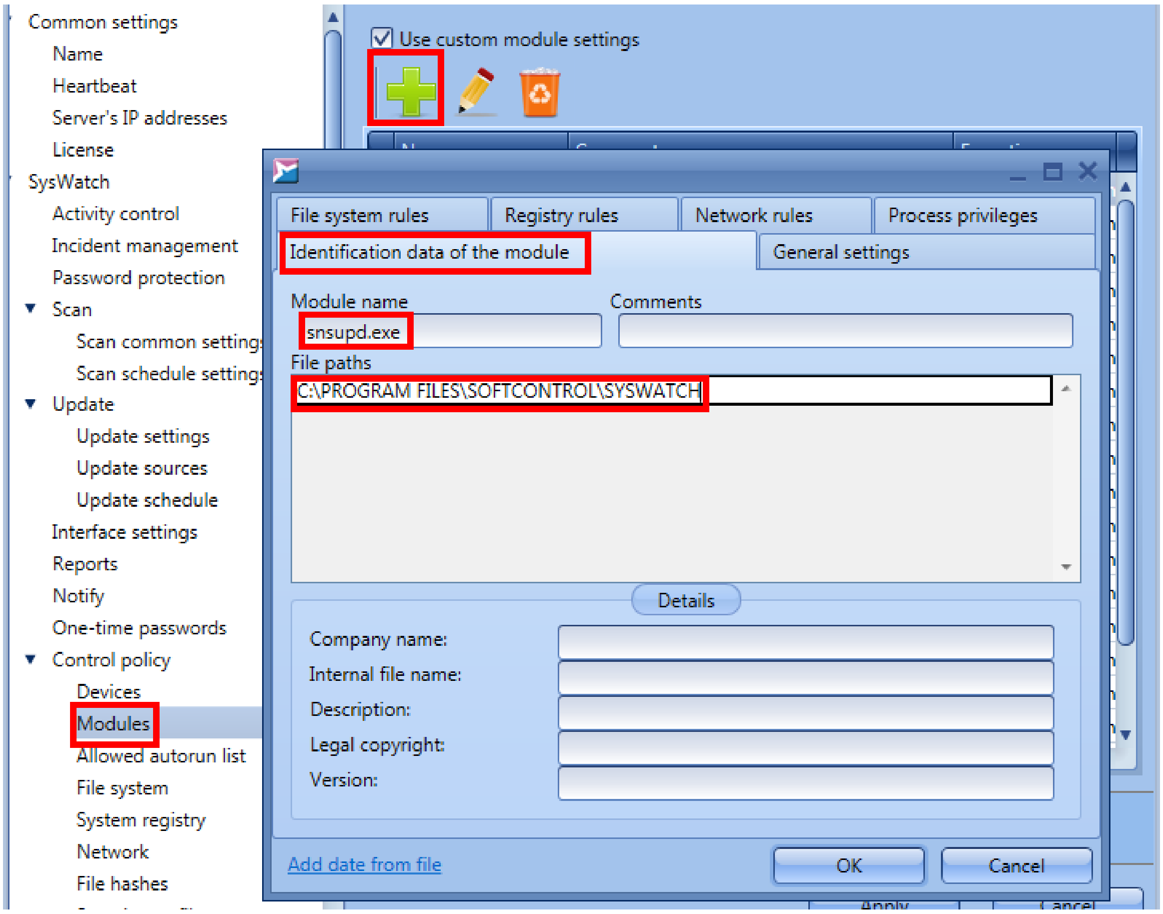
Note. If you install version 5.1.79 or later of SoftControl SysWatch and it is the first installation of the application on your computer, these actions are not required: all updates will be performed properly. For SoftControl DLP and SoftControl SysCmd, you do not need to perform instructions from this 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 43. 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



☑ Use custom module settings

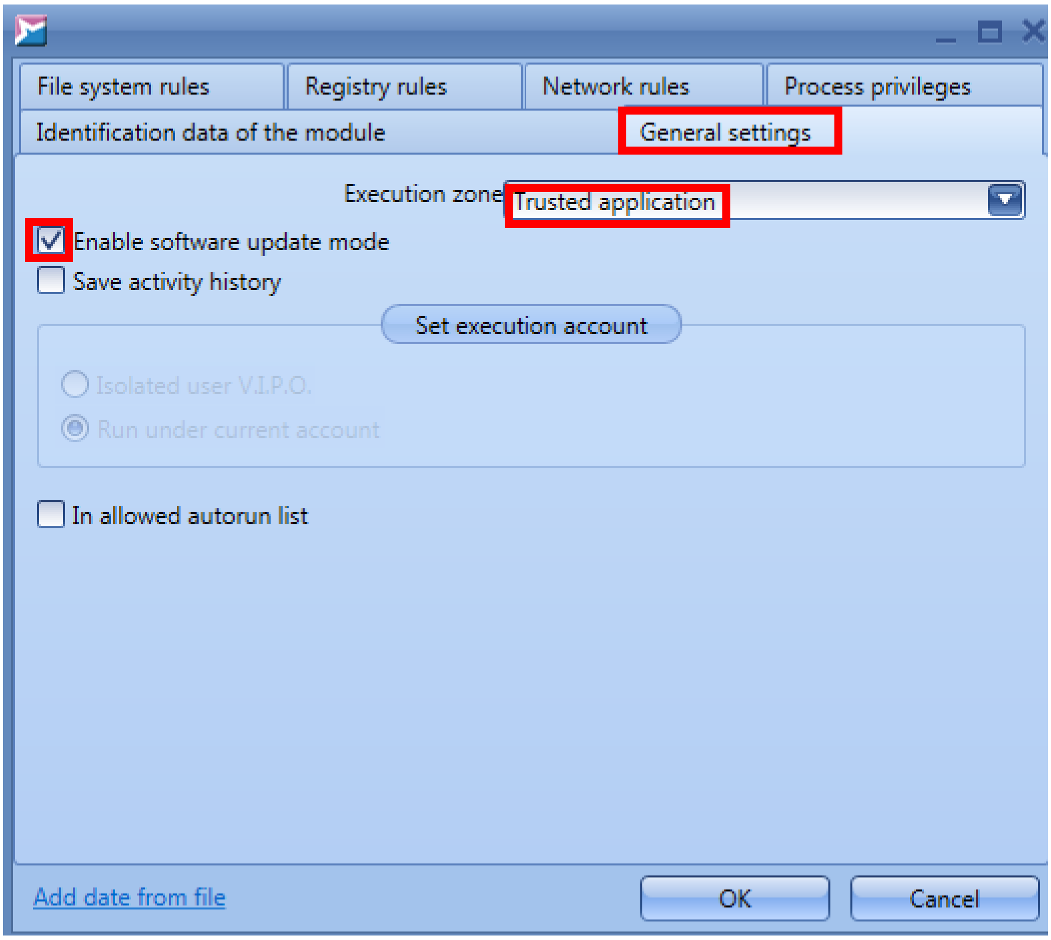
Module name: snsupd.exe

Comments:

File paths: C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH

Figure 216. Setting up an update module (for SoftControl SysWatch)

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



Execution zone: Trusted application

☑ Enable software update mode

□ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

□ In allowed autorun list

Figure 217. 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.