SoftControl

Service Center 4.3.10

Administrator guide

Dear user!

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

COPYRIGHT

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

All the names used throughout this document are trademarks of it's respective owners.

LIABILITY LIMIT

Contents of the document may change without notice. SAFE ‘N SEC Corporation doesn't bear responsibility for inaccuracies and/or errors in this document, and possible damage associated with it.

SAFE ‘N SEC Corporation, 2017

Postal address:

127106 Russia, Moscow

Altufyevskoe shosse, 5/2

SAFE ‘N SEC Corporation

Tel:

+7 (495) 967-14-51

Fax:

+ 7 (495) 967-14-52

E-mails:

Customer service: sns@safensoft.com

Sales team: sales@safensoft.com

Website: http://www.safensoft.com

Contents

1. Introduction

1.1. Purpose

SoftControl 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.

- 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.

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

Notation example	Description
Appendix 5	Links to internal resources (document sections) with a specific page number, 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;
- **LAN** – local area network;
- **OS** – operating system;
- **RAM** – random access memory.

1.2.3. Glossary

Table 2. Glossary

Term	Description
Proactive protection	A series of measures to prevent harmful effects on the basis of prevention techniques.
Prevention techniques	The advanced data protection technologies 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, SoftControl Service Center does not require the bases of malicious code and their updates, which are necessary for traditional protections.
Control policy	A set of rules to monitor the application activity, analyze the applications, and to decide whether an application is malicious. It is the policy that determines what actions and sequence of actions should be considered as dangerous.

Term	Description
Activity control rule	A set of conditions that determine the application activity, and the actions that SoftControl Service Center performs with respect to the application with such an activity. The conditions of a rule specify the control area and refine it (by specifying the object of the control, operation on the object, the application that performs the operation, etc.).
System profile	A collection of check sums of a portable executable modules (see 'The Portable Executable (PE) format') and paths to them in the system. It is a result of the automatic setup (profile gathering).
Installer flag	A special token that gives particular privileges for process to launch (see 'installation mode')
Installation mode	A process launch mode without restrictions, when the process and all its child processes are moved to the system profile if they are not there yet.
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.
Role	An aggregate of access rights to the computer system objects.
The Portable Executable (PE) format	A file format for executables, object code and DLLs that is used in 32-bit and 64-bit versions of Microsoft® Windows® operating systems.
Host	A computer device (workstation / server / self-service terminal) that is connected to the local area network or wide area network.

2. Hardware and software requirements

2.1. SoftControl Server system requirements

Table 3. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10	3GHz	4GB	100MB + extra 4GB (for embedded DBMS installation)

Additional software:

- Microsoft® .NET Framework 4.5;
- Microsoft® SQL Server® 2008 / SQL Server® 2012 / / SQL Server® 2014 Express SP1.

2.2. SoftControl Admin Console system requirements

Table 4. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10	3GHz	4GB	100MB

Additional software:

- Microsoft® .NET Framework 4.5.

3. Installing and setting up SoftControl Service Center components

This section describes how to install[9] the SoftControl Server ('the server') and the SoftControl Admin Console components, set up[19] SoftControl Server when running[23] SoftControl Admin Console for the first time, and also gives instructions on how to register client applications[22].

3.1. Installing SoftControl Server and SoftControl Admin Console

There are the following ways to deploy SoftControl Service Center.

- typical[9]: install product components without the embedded DBMS;
- complete[12]: install product components including the embedded DBMS;
- custom[16]: 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[152].

Complete installation is the fastest way to deploy and configure. This way, all the essential operations including DBMS installation and database creation 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[9]).

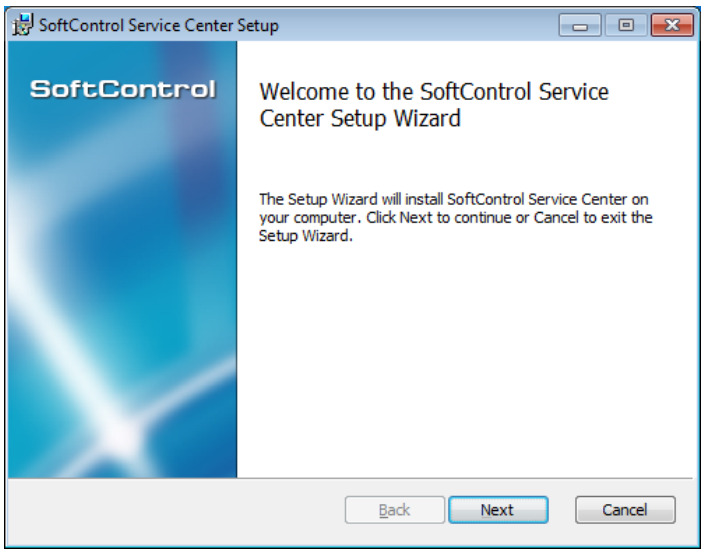

Figure 1. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement 10).

Figure 2. License agreement

4) Click **Typical** to select standard installation type (fig. Installation types 10).

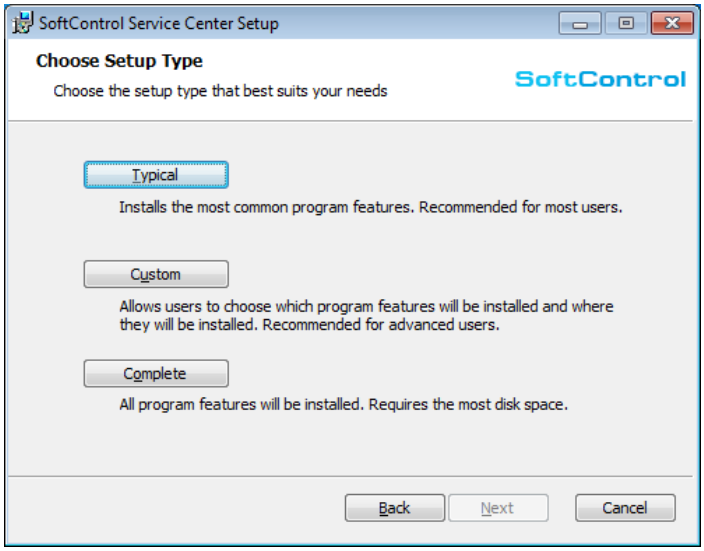

Figure 3. Installation types

5) Click **Install** (fig. Ready to install [11]).

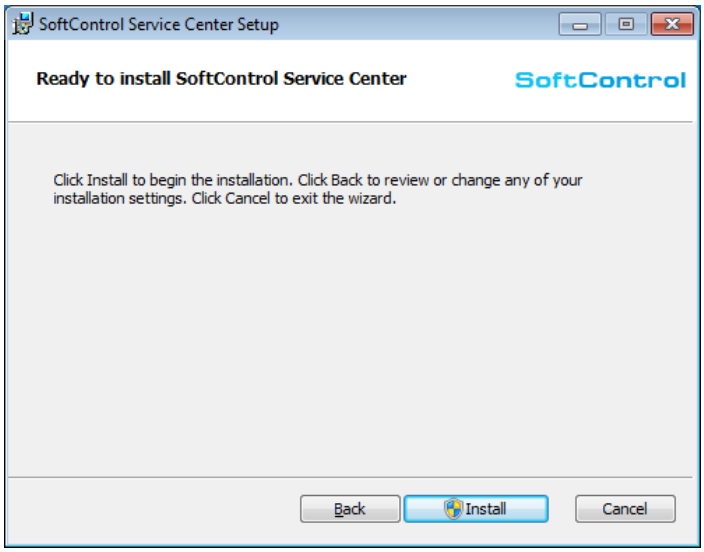

Figure 4. Ready to install

6) Wait until installation is complete (fig. Installation progress [11]).

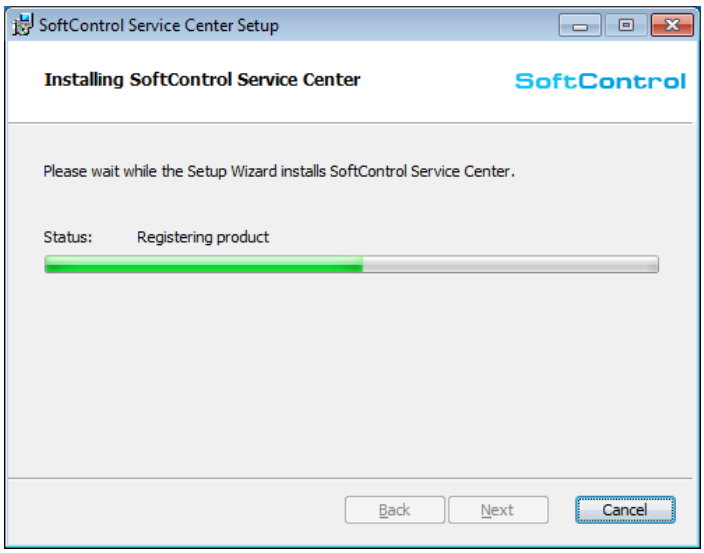

Figure 5. Installation progress

7) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Installation is complete 12).

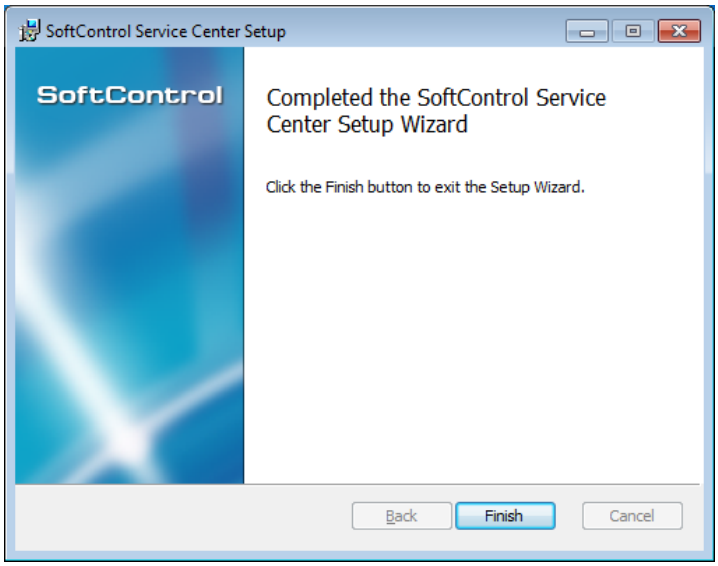

Figure 6. Installation is complete

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 12).

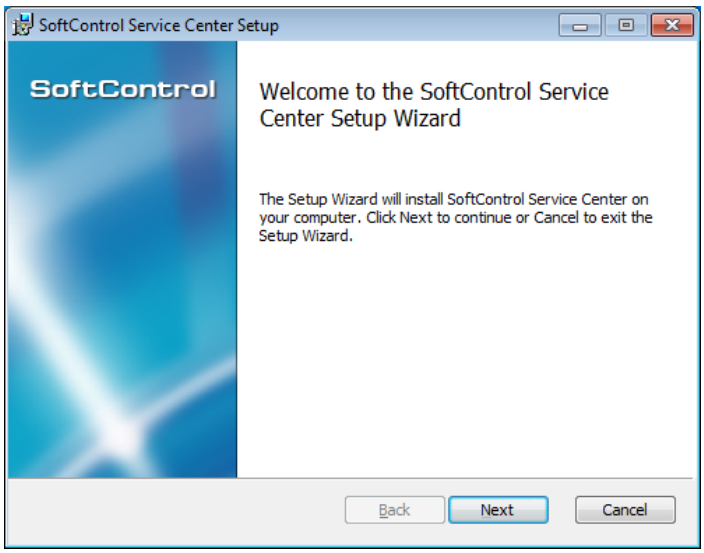

Figure 7. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement 13).

Figure 8. License agreement

4) Click **Complete** to select full installation type (fig. Installation types 13).

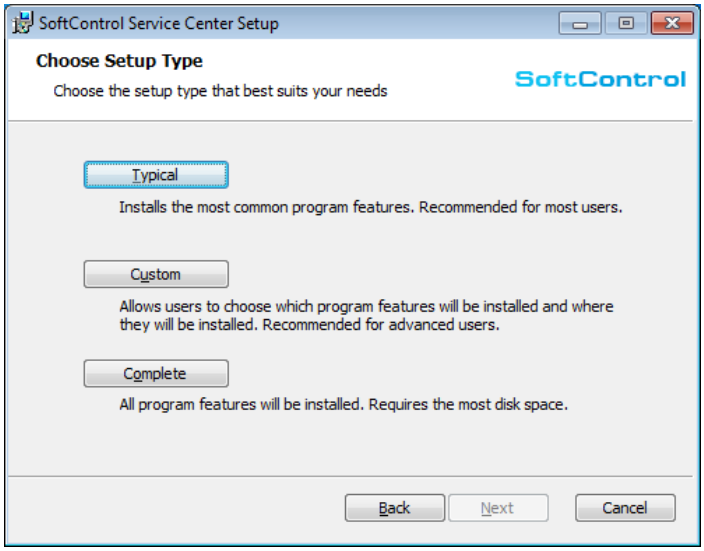

Figure 9. Installation types

5) Click **Install** (fig. Ready to install [14]).

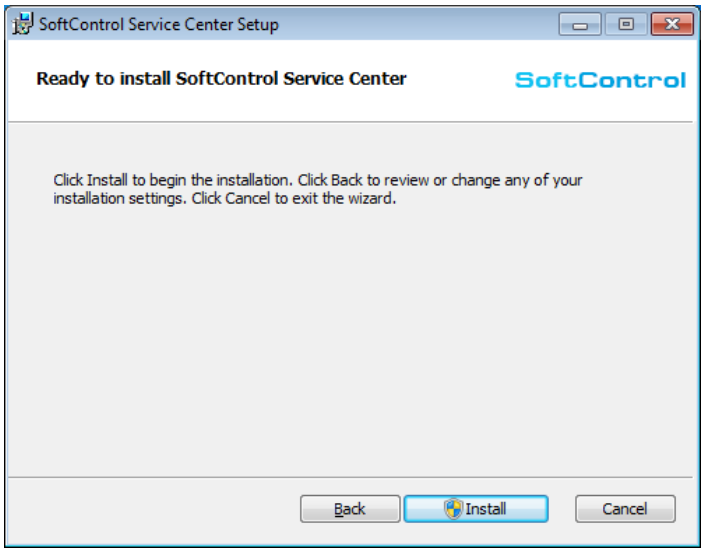

Figure 10. Ready to install

6) Wait until installation is complete (fig. Installation progress [14]).

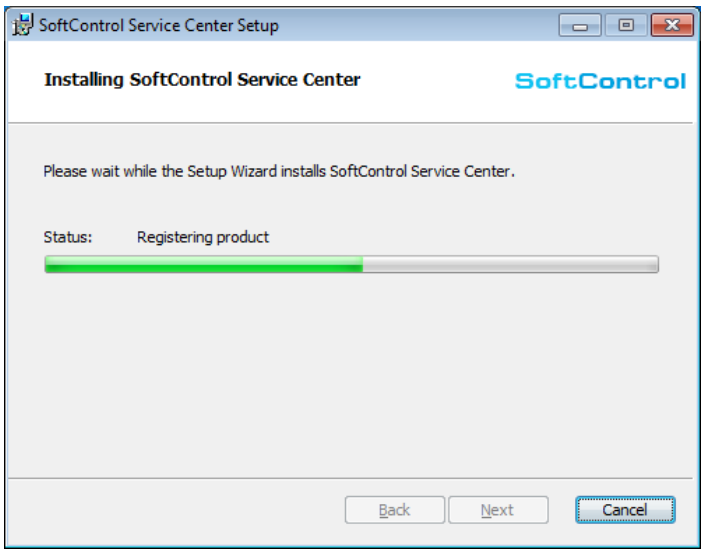

Figure 11. Installation progress

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 [15]).

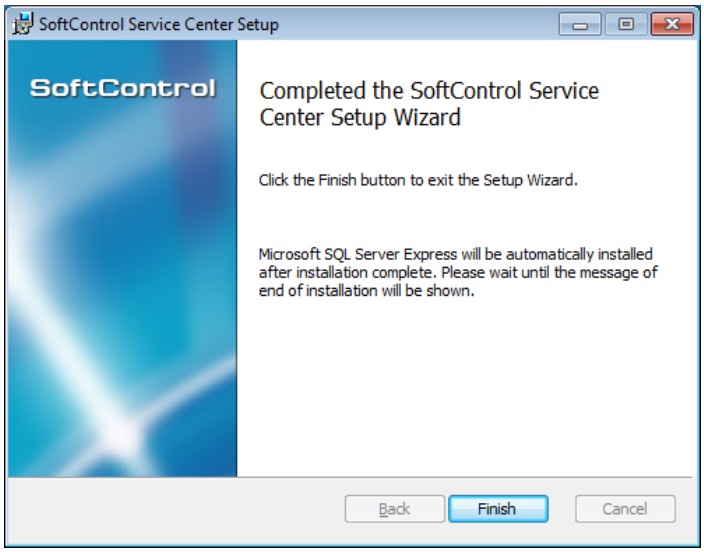

Figure 12. SoftControl Service Center installation is complete

8) Wait until Microsoft® SQL Server® 2014 Express SP1 installation is complete and then click **OK** (fig. Installation is complete [15]).

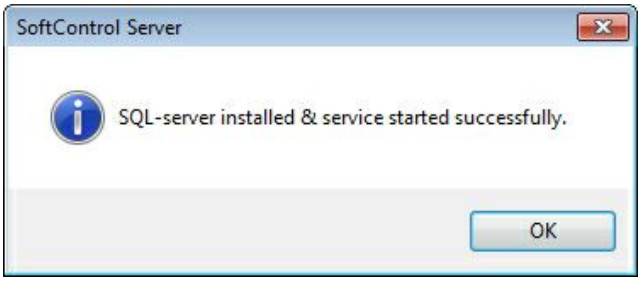

Figure 13. Installation is complete

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 16).

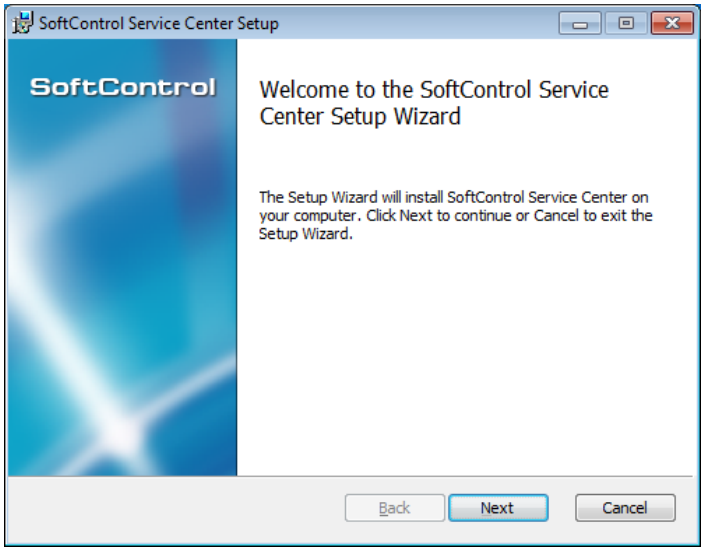

Figure 14. Running the installation program

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement 16).

Figure 15. License agreement

4) Click **Complete** to select complete installation type (fig. Installation types [17]).

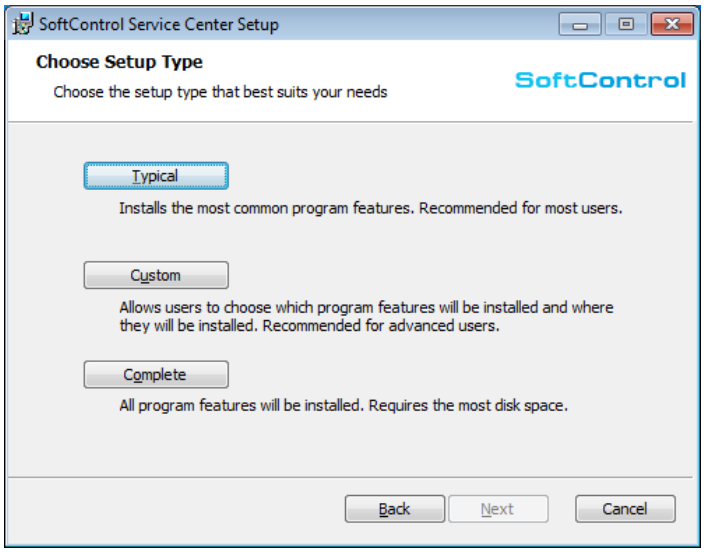

Figure 16. Installation types

5) Configure the component installation (fig. Component installation configuration [17]).Click the icon of the component that shouldn't been installed and select the **Entire feature will be unavailable** option from the drop-down menu (fig. Component installation options [18]. The **Will be installed on local hard drive** option should been selected for the component to install (fig. Component installation options [18]). 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.

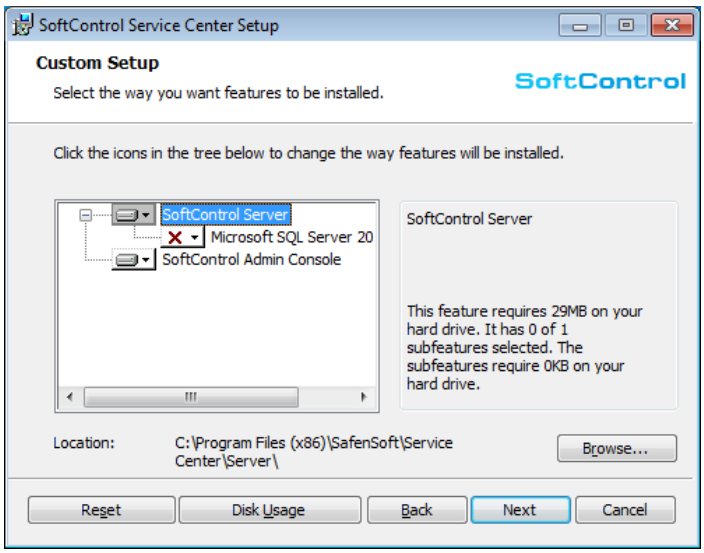

Figure 17. Component installation configuration

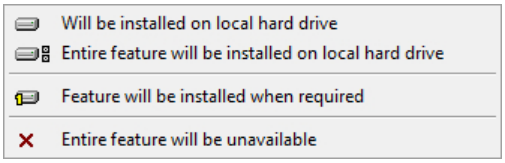

Figure 18. Component installation options

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 18). Otherwise, you should perform this operation manually (by default, port *8080* is used). To continue installation, click **Next**.

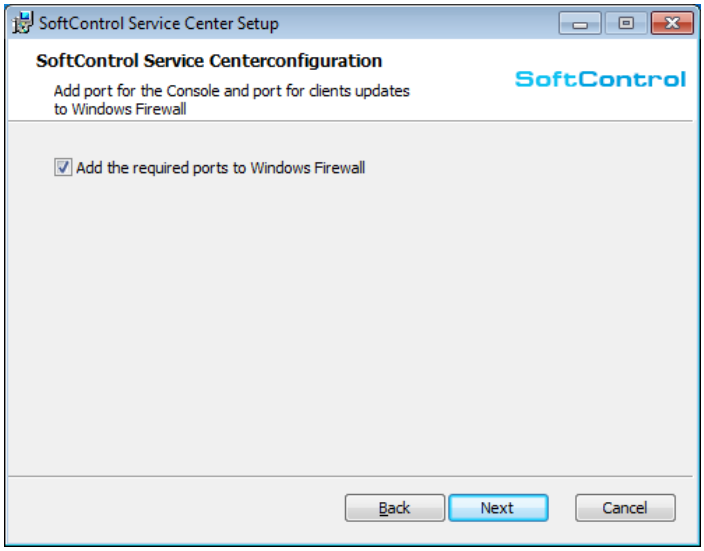

Figure 19. 'Adding a port to the firewall exceptions' option

7) If you have chosen SoftControl Admin Console and/or SoftControl Server without embedded DBMS installation, repeat actions 5-7 for typical installation[11]. If you have chosen SoftControl Server with the *Microsoft® SQL Server® 2014 Express SP1* component, repeat actions 5-8 for complete installation[14].

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. The first start of SoftControl Admin Console[19]).

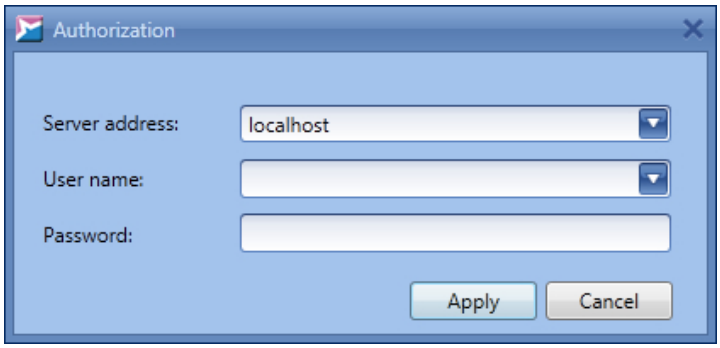

Figure 20. The first start of SoftControl Admin Console

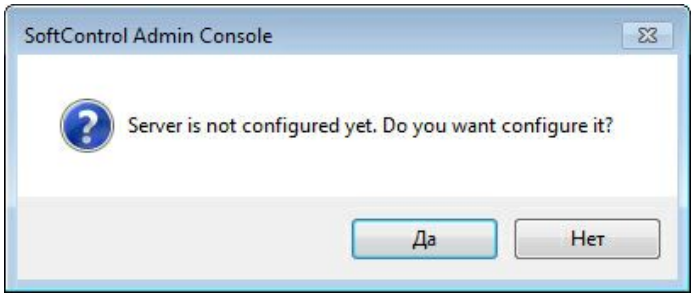

Figure 21. Suggestion to run server configuration wizard

Click **Yes** in the dialog box with the suggestion to create initial server configuration (fig. Suggestion to run server configuration wizard[19]).

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[20]):

- **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*).

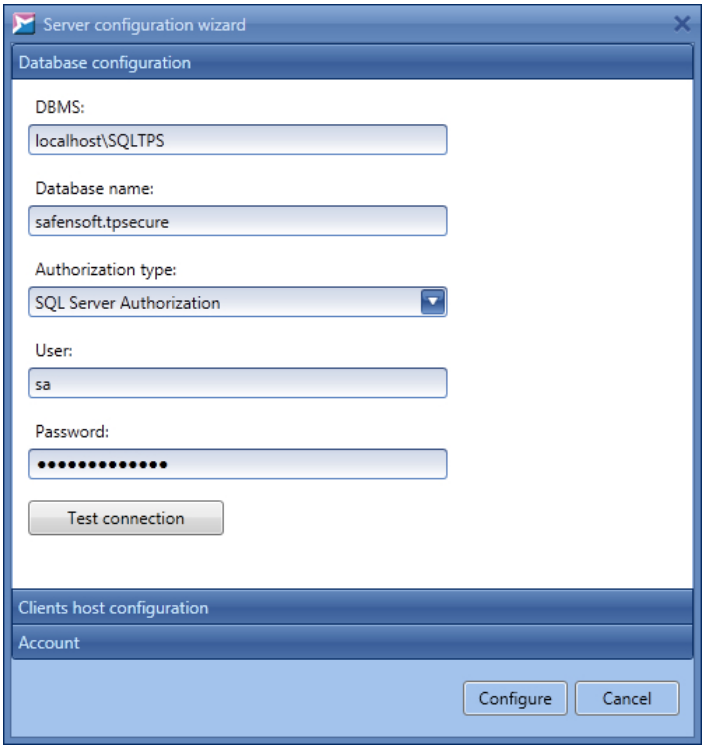

Figure 22. Setting up the connection to the DBMS

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 will be created on the DBMS server when the configuration wizard completes its operation.

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[21]). 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 NetBIOS names 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 [23]). 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 NetBIOS 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 [144].

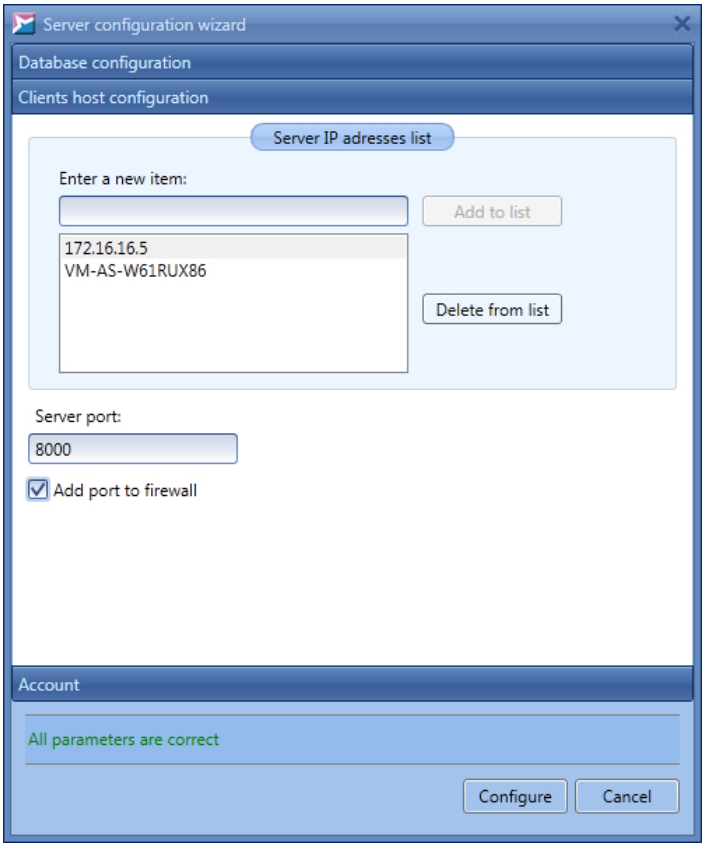

Figure 23. Setting up connection between client components and the server

Create the first user account by specifying **Account name**, **Password** and **Confirm password** in the **Account** section (fig. Creating a user [22]). 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 [33]).

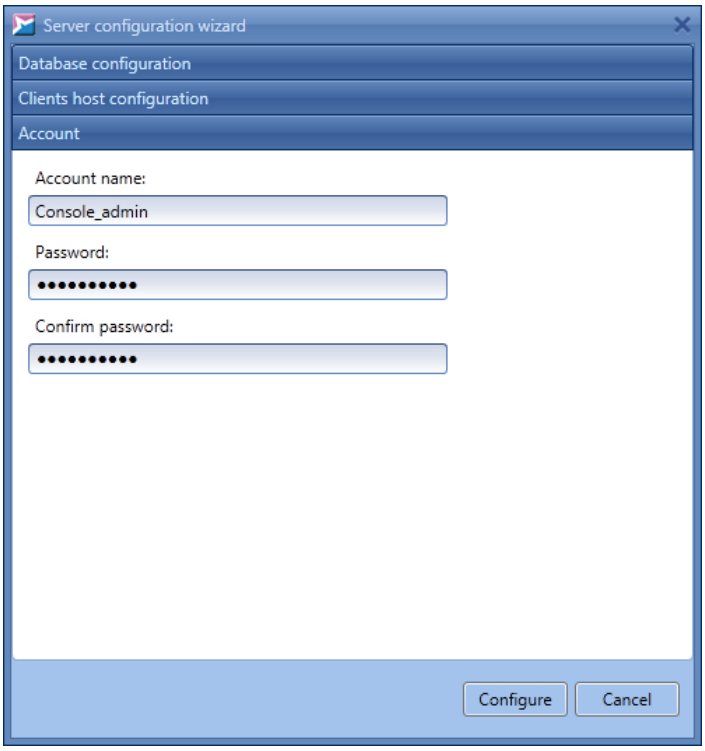

Figure 24. Creating a user

When all settings are specified, click **Configure**. If the configuration is created successfully, the corresponding message is displayed (fig. Configuration is created successfully [22]).

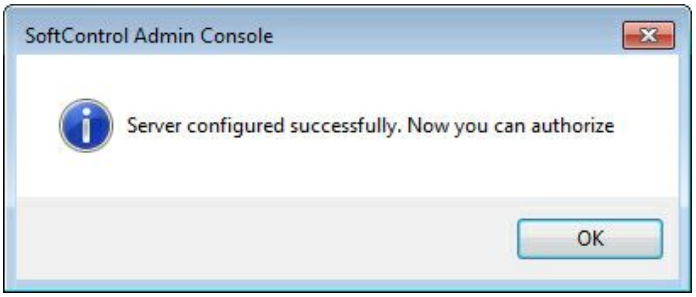

Figure 25. Configuration is created successfully

Use the created account to connect to SoftControl Server in the authorization window [23].

3.3. Registering client applications

After the initial setup [19] of the server, the encrypted configuration file is generated in the following path on the computer with the installed SoftControl Server:

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

The file contains server connection parameters for the client applications, as well as common client certificate [143] that is used to establish secure connection by default. To register with SoftControl Service Center, apply the above-mentioned file on the remote LAN nodes 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** [38].

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** in the **Authorization** window (fig. User authorization in SoftControl Admin Console [23]).

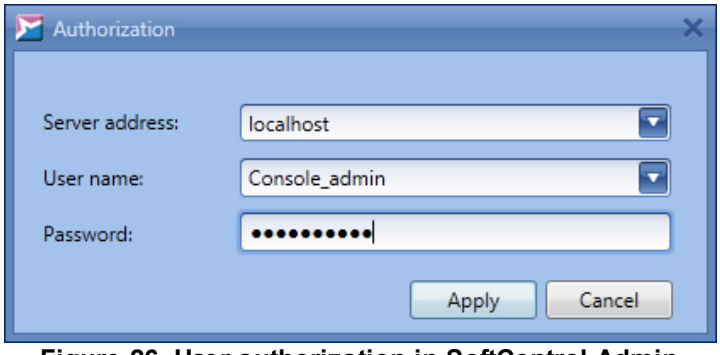

Figure 26. User authorization in SoftControl Admin Console

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\SoftControl\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\SoftControl\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>
```

Click **Apply** to connect to the SoftControl Server component and start the centralized ISS management[25].

4. Centralized ISS management

The SoftControl Admin Console management console enables remote centralized management of the SoftControl SysWatch and SoftControl DLP Client 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.

- Roles 29;
- Accounts 31;
- Security events 35;
- Client statuses 38;
- Organization units 44;
- Clients settings 49;
- Tasks 93;
- Log 100;
- Scanner 104;
- Changed settings 105;
- Notifications 118;
- Contacts 116;
- Updates 129;
- Configuration snapshots 123.

The upper part of the SoftControl Admin Console main window contains a row of graphical buttons under the program main menu. The buttons are use to perform basic operations in SoftControl Admin Console Besides, the Client statuses 38, Organization units 44, Clients settings 49, Tasks 93, Notifications 118 and Contacts 116 tabs have their own graphical buttons which apply only for these tabs. The general purpose buttons are described in table 5.

Table 5. The SoftControl Admin Console general purpose widgets

Button	Name	Description	Hot keys
	Server	Open the server connection settings.	
	Clients	Open the **Client statuses** tab.	F4
	Events log	Open the **Log** tab for the all devices.	
	Client settings	Open the **Client settings** tab.	
	Organization units	Open the **Organization units** tab.	
	Tasks	Open the **Tasks** tab.	
	Notifications	Open the **Notifications tab** tab.	
	Contacts	Open the **Contacts** tab.	
	Roles	Open the **Roles** tab.	
	Accounts	Open the **Accounts** tab.	
	Security events	Open the **Security events** tab.	
	Refresh	Refresh data in the current tab.	F5
	Choose columns	Modify how the fields in the table are arranged on the current tab.	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
	Export to Excel	Export the list of current devices or the selection of events to an *XLSX* (Microsoft® Excel®) file.	Ctrl + E
	Updates	Open the **Updates** tab.	
	Configuration snapshots	Opens the **Configuration snapshots** tab.	

Some of the functions that are called by the general purpose 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 his/her 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[23] 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[27]):

- **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[111] tab, in the **Events page size** field.

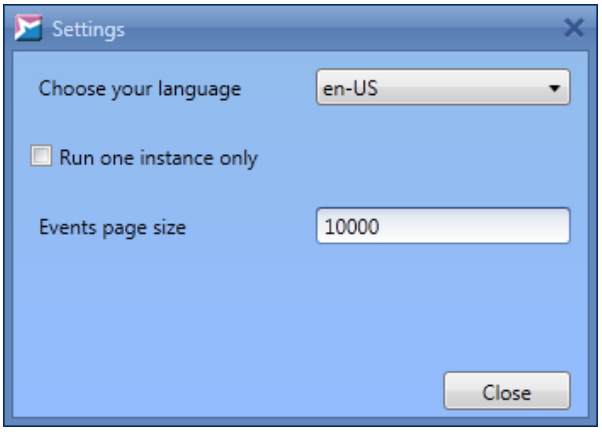

Figure 27. Interface settings

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 [23].
2) On the **Roles** tab, create additional roles [29] if necessary and assign the roles [29] with the specified permissions to the user accounts [31]. Supervise user actions [35] via management console with the help of the **Security events** tab.
3) We recommend that you additionally create at least one user account [31] with the 'operator' role in the **Accounts** tab, apart from the initial account with the 'administrator' role.
4) Approve [41] or reject [42] registration requests from the client components which are installed on LAN endpoints, on the **Clients setting** tab.
5) After you finish creating the workspace of the required devices, switch to the **Clients setting** tab and add configurations [50] that should apply to the client applications.
6) After you configure the client settings, switch to the **Organization units** tab and create organization units [46] (groups) by any principle to distribute the registered components on the client hosts. When you create units, bind them to certain configurations [46].
7) Switch to the **Client statuses** tab and move client components [43] to the created organizational units.
8) Create the required tasks [93] for client applications on the **Tasks** tab.
9) Switch to the **Log** tab and start viewing the reports from the client components [100].
10) Additionally, you can set up notifications [118] about the incidents.The notifications will be sent to the specified e-mails [116]. You also can export and print out [115] 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 the users' [31] access to different functions of SoftControl Server and SoftControl Admin Console on the basis of the their roles [29].

When the server authenticates the user, a session with unique ID is created. 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.

User actions are monitored through SoftControl Admin Console that registers the server security events [35].

4.3.1. Roles

The **Roles** tab allows you to manage the roles and set up the permissions for them (fig. The 'Roles' tab [29]).

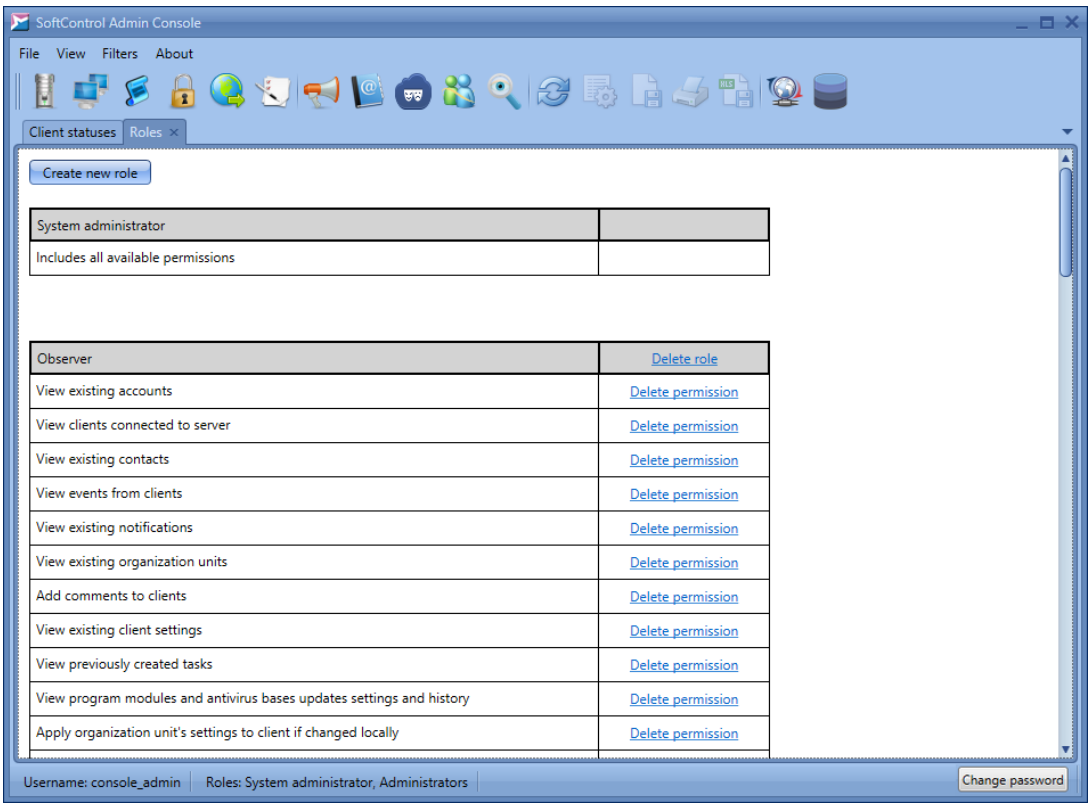

Figure 28. The 'Roles' tab

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 29). Specify the **Role name** in the displayed window and click **OK** (fig. Creating a new role 30).

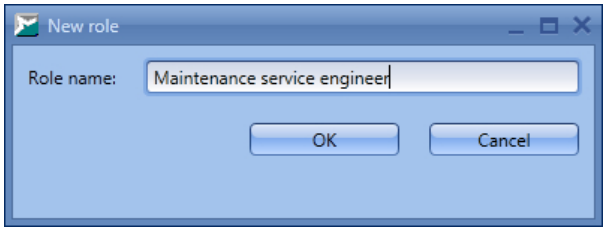

Figure 29. Creating a new role

The new role is added to the end of the role list. Set the permissions 30 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 30).

To delete a permission, click the **Delete permission** link in the corresponding row of the table with a role (fig. The 'Roles' tab 29).

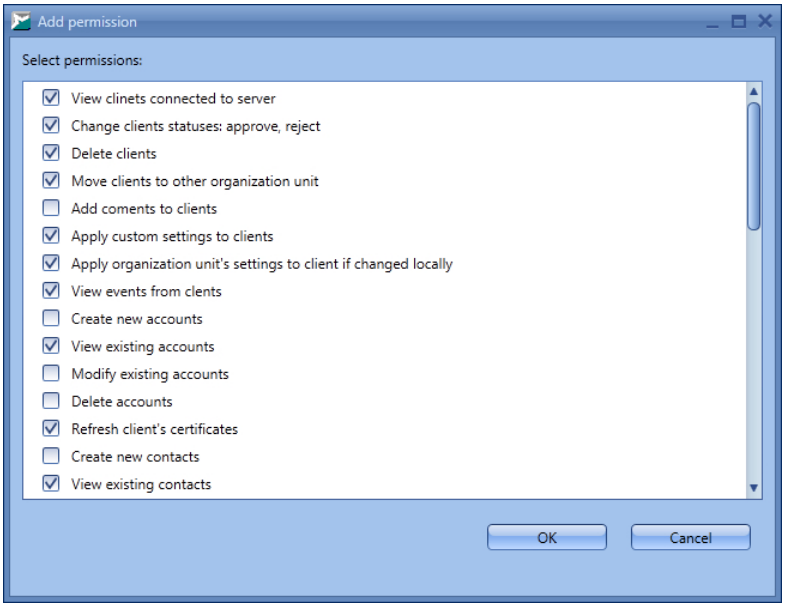

Figure 30. Adding permissions

Removing a role

To remove a role, click the **Delete role** link in the table row with the role name (fig. The 'Roles' tab 29) and confirm the removal in the dialog box.

4.3.2. Accounts

You can manage user accounts and assign the roles for them on the **Accounts** tab (fig. The 'Accounts' tab 31).

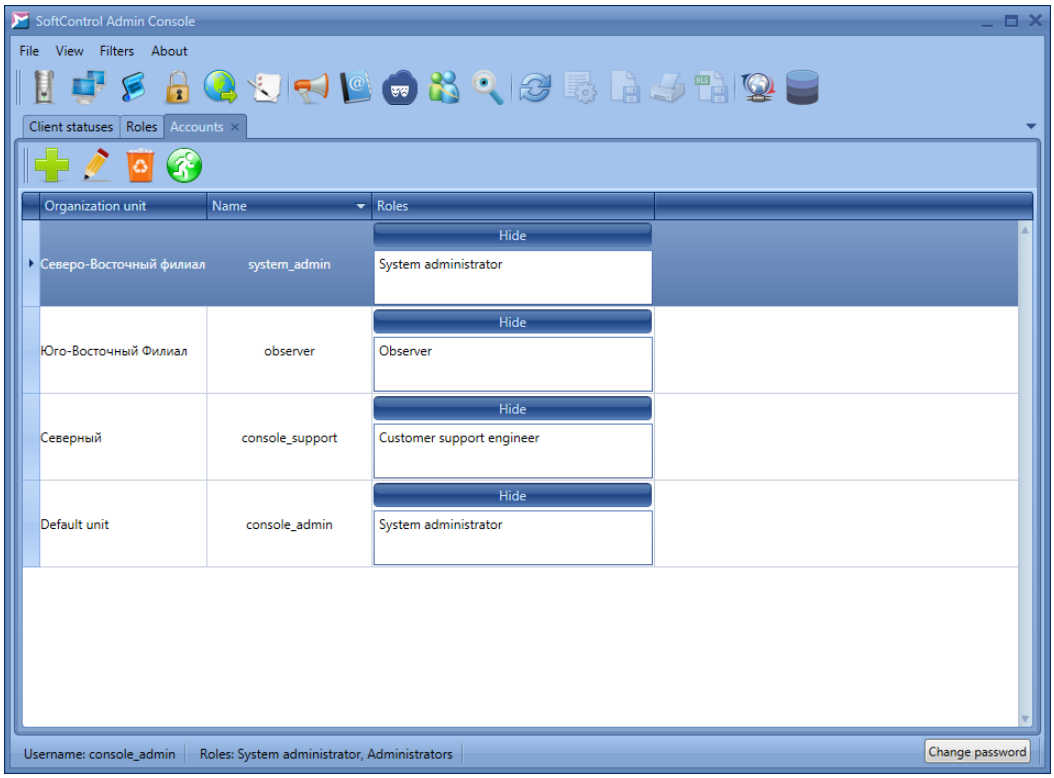

Figure 31. The 'Accounts' tab

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 31). Specify the user **Name**, enter **Password** and **Confirm** it (the password should be at least 7 characters long) in the displayed window. Select the required **Roles** for the user and then click **Apply** (fig. Creating an account 32).

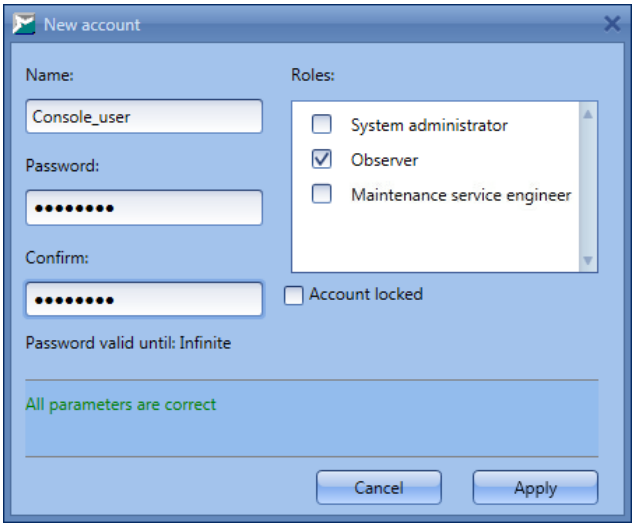

Figure 32. Creating an account

All new user accounts are automatically added to the **Default** organization units. You can move 34 the selected account to another unit.

Depending on his/her role 29, the user can access data in the current unit and all its subsidiary units, but cannot access any data in the parent units.

Modifying user account

To modify user account, click **Edit** (fig. The 'Accounts' tab 31).

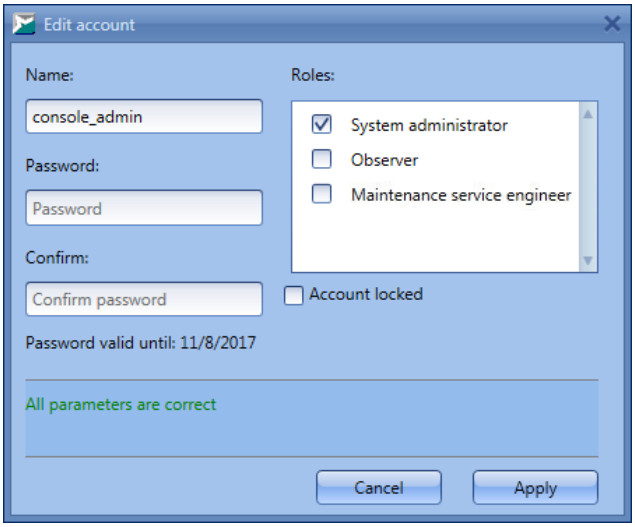

Figure 33. Modifying an account

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 32). 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 (the password should be at least 7 characters long).

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 31). The button is available on any tab.

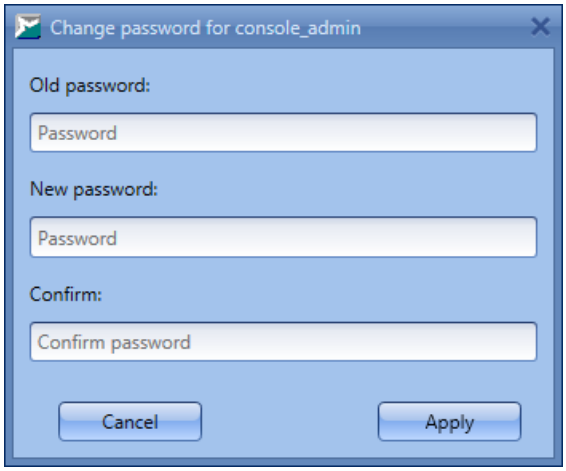

Figure 34. Changing user password

In this window, enter the old **Password**, the **New Password**, **Confirm** it (the password should be at least 6 characters long), 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\SoftControl\Server.Config.xml`). 0

means the lifetime is unlimited.

If you need to block the account, tick off **Account locked** (fig. Modifying an account 32).

Removing an account

To remove a user account, select it, press **Delete** (fig. The 'Accounts' tab 31) and confirm the removal in the dialog box.

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 34).

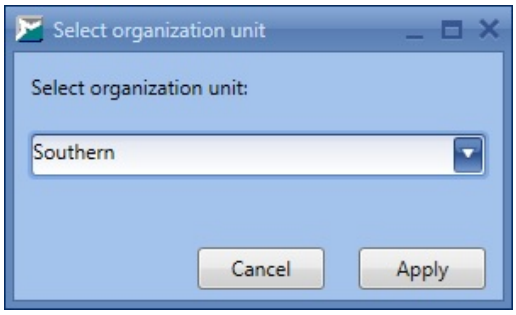

Figure 35. Moving an account

4.3.3. Server security events

Management console allows you to register user operations, so as to analyze them on the **Security events** tab (fig. The 'Security events' tab 35).

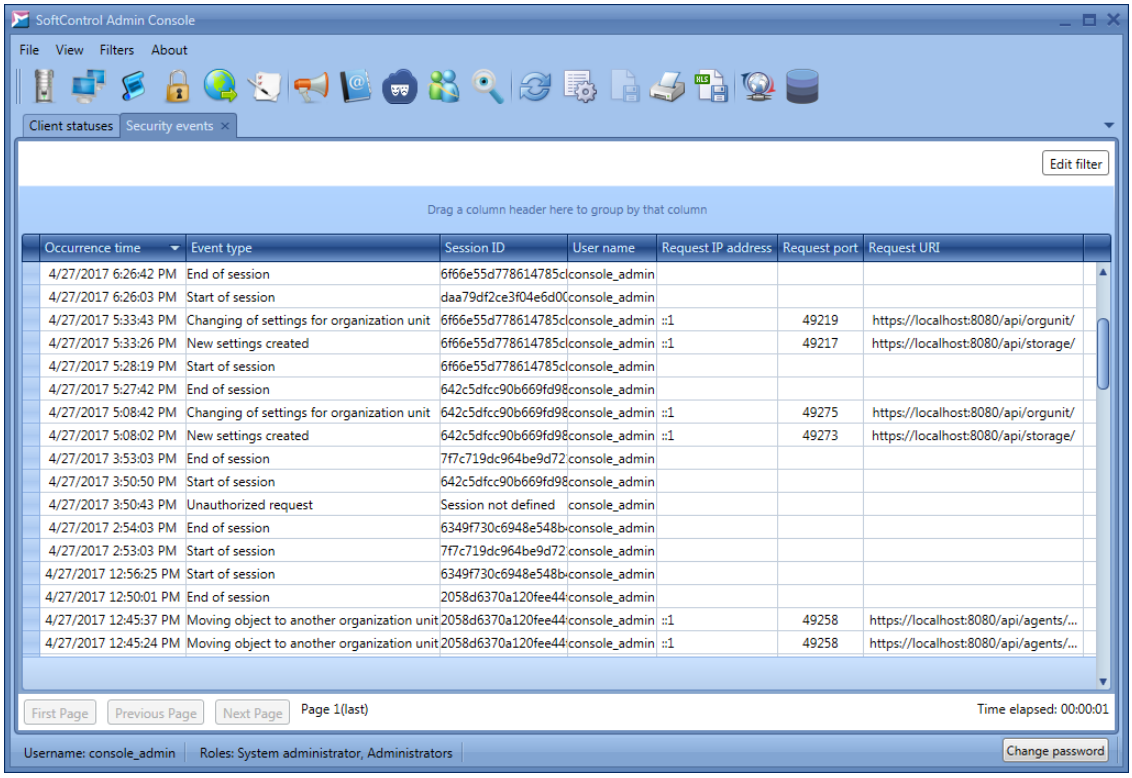

Figure 36. The 'Security events' tab

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

Table 8. The 'Security events' tab

Field	Description
Occurrence time	Date and time when the event occurred.
Event type	Type of the registered event: • **Start of session**; • **End of session**; • **Role created**; • **Role deleted**; • **Add permissions to role**; • **Role's permissions removed**; • **Account created**; • **Account changed**; • **Account deleted**; • **Approval of client**; • **Reject of client**; • **Deletion of client**; • **Attempt of change a client certificate**; • **New certificate assigned for client**;

Field	Description
	• **Moving object to another organization unit**; • **Created new organization unit**; • **Organization unit deleted**; • **New settings created**; • **Changing of settings for organization unit**; • **Assigned custom settings**; • **Settings deleted**; • **Task created**; • **Task cancelled**; • **Contact created**; • **Contact changed**; • **Contact deleted**; • **Notification created**; • **Notification changed**; • **Notification 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 created**, **Role deleted**, **Add permissions to role**, and **Role's permissions 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 removed** event type) role permissions.
Account name	User account name (only for the **Account was created**, **Account was changed**, and **Account was deleted** event types).
Client's Guid	Unique ID of the client application (only for the **Approval of client**, **Reject of client**, **Deletion of client**, and **Moving client to other organization unit** event types).
Client's name	NetBIOS name of a client host (only for the **Approval of client**, **Reject of client**, **Deletion of client**, **Attempt of change a client certificate**, **New certificate assigned for client**, and **Moving client to other organization unit** event types).
Organization unit	Organization unit which the installed client component is moved to (only for the **Moving client to other organization unit**, **Created new organization unit**, and **Organization unit was deleted** event types).
Settings	The name of the client application configuration (only for the **The creation of new settings**, **Changing of settings for organization unit**, and **Storage was deleted** event types).
Settings creation time	Time when the client application configuration is created on the server (only for the **The creation of new settings** event type).
Task ID	Task sequence number (only for the **Task created** and **Task cancelled** event types).
Task type	Task type (only for the **Task created** and **Task cancelled** event types).
Contact name	The name of the notification recipient (only for the **Contact was created**, **Contact was changed**, and **Contact was deleted** event types).

Field	Description
Notification name	Notification name (only for the **Notification was created**, **Notification was changed**, and **Notification was deleted** event types).
Request's 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).

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 37) to the required place in the table header.

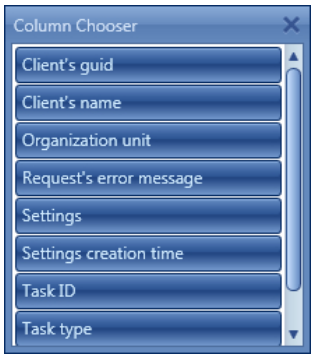

Figure 37. Selecting columns

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 37). If you group by several fields, category priority (nesting) decreases from left to right depending on the location on the panel.

4.4. Client statuses

The **Client statuses** 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 'Client statuses' tab 38).

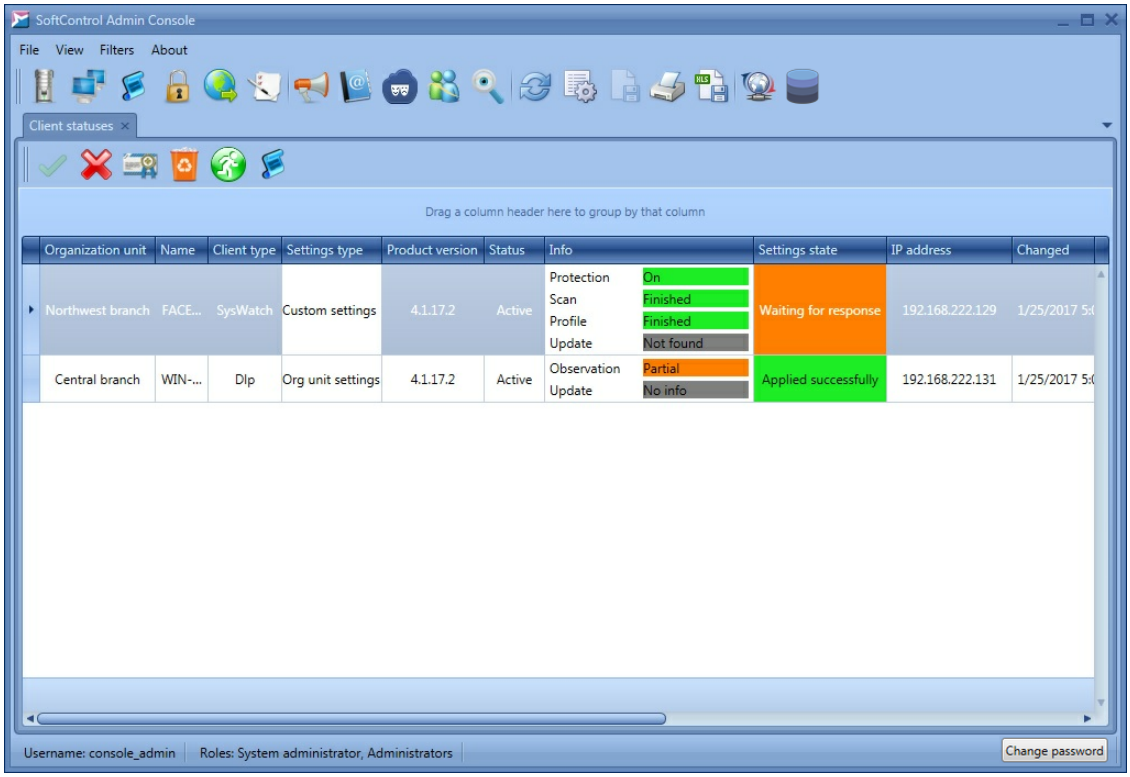

Figure 38. The 'Client statuses' tab

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 'Client statuses' 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.	
	Events log	Open the **Log** tab for the selected components.	

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

Table 10. The 'Client statuses' tab fields

Field	Description
Organization unit	The organization unit which the client component belongs to.
Name	NetBIOS 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).
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 53. • **Inactive**: a registered client component has not sent a connection request to the server for the double heartbeat period 53.
Info	Additional information on a client component state. 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; – **Need 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.

Field	Description
	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**; • **apply error**; • **local settings**; • **no info**.
Certificate expire date	Expiration date of the client component's specific certificate.
User comment	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 server.

Basic operations on this tab are:

- managing the registration process [41];
- moving to the organization units [43];
- managing the list of files that are allowed to run [43].

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 comment** fields (categories). To do so, drag the column header to the panel between the table header and group of the tab buttons (fig. The 'Client statuses' tab 38). If you group by several fields, category priority (nesting) decreases from left to right depending on the location on the panel.

Viewing reports

To open the Log 100 tab with the events list, select the required components and perform one of the following operations:

- click **Events log** in the group of buttons on the tab (fig. The 'Client statuses' tab 38);
- invoke the context menu by right-clicking the list of components and select the **Show Log** command.

When you open the list of events, the header of the Log 100 tab displays the number of the selected components (fig. The 'Client statuses' tab 38).

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 'Client statuses' tab 38).

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 143 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 'Client statuses' tab 38).

The **Status** field switches to the **Rejected** state as soon as the registration is rejected.

When switched to this state, the client's certificate is moved to the black list and interaction 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 143.

Updating client's certificate

Select the required client components that are in the **Active** or the **Inactive** state and click **Refresh** (fig. The 'Client statuses' tab 38).

The **Certificate expire date** field updates when the client component with the new specific certificate 143 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 'Client statuses' tab 38). The specific certificate 143 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 143 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 43).

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

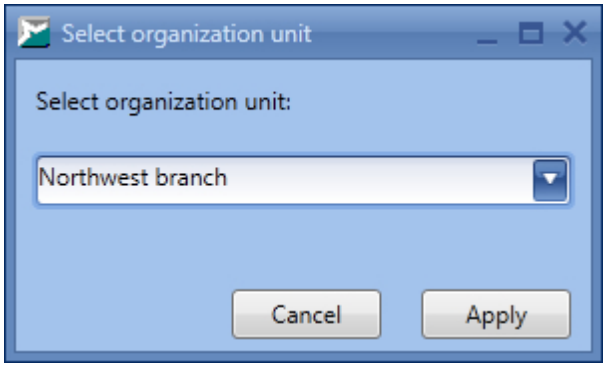

Figure 39. Selecting an organization unit to move the component to

4.4.3. Managing the list of allowed files

In SoftControl Admin Console, you can obtain the list of files that are allowed to 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 43). 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, and the size of the file.

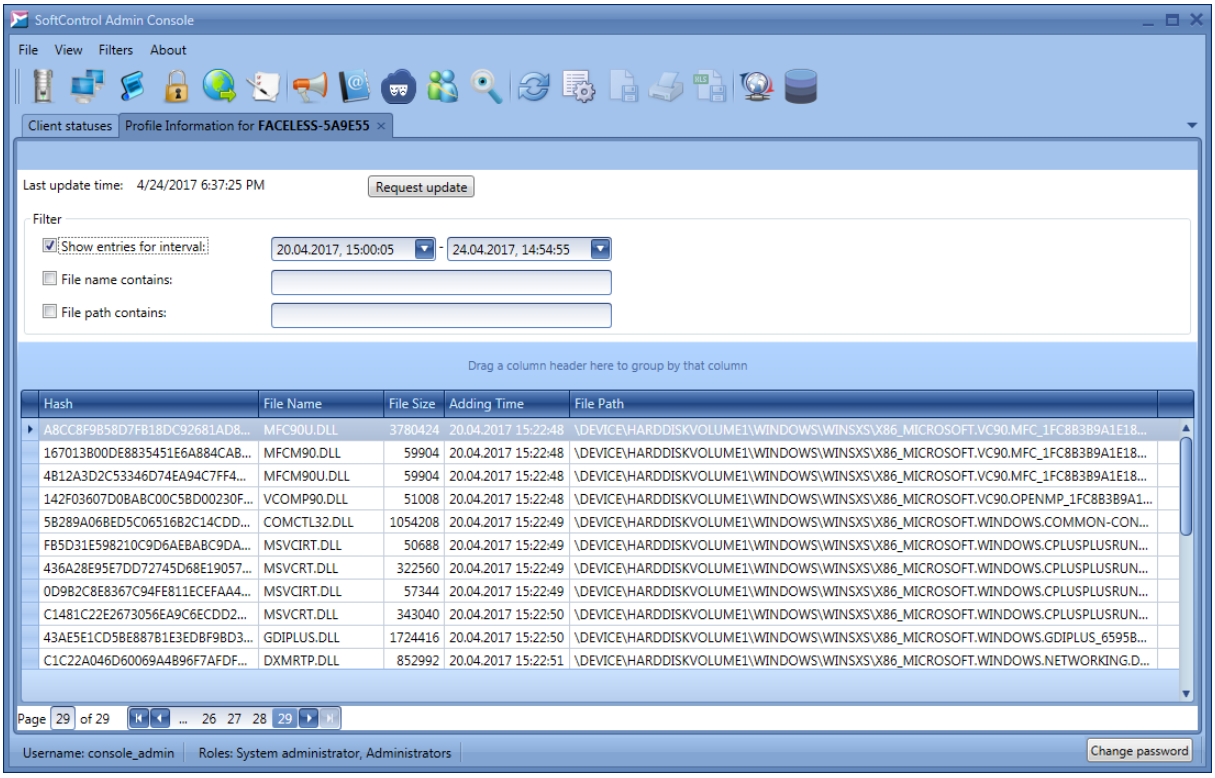

Figure40. The 'Profile information for...' tab

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 44). Besides, you can bind organization units to the configurations and generate one-time passwords on this tab.

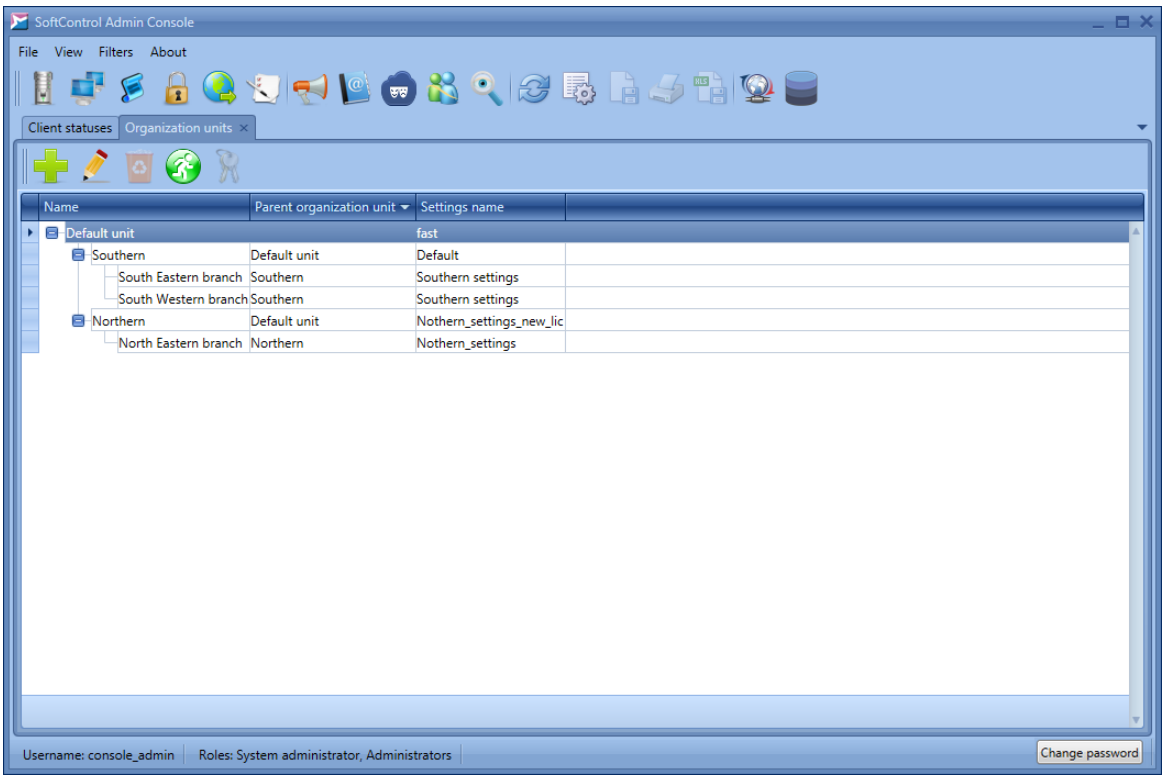

Figure 41. The 'Organization units' tab

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	Open the one-time password generator window.

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 [46];
- generating one-time passwords [48].

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 [44]).

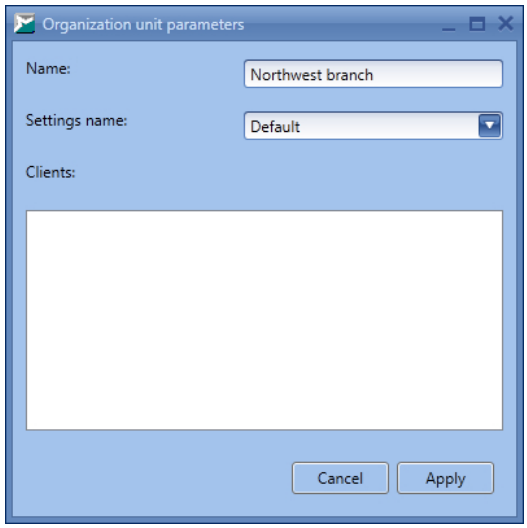

Figure 42. Creating an organization unit

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 [46]).

Modifying an organization unit properties

To modify an organization unit properties, click **Edit** (fig. The 'Organization units' tab [44]).

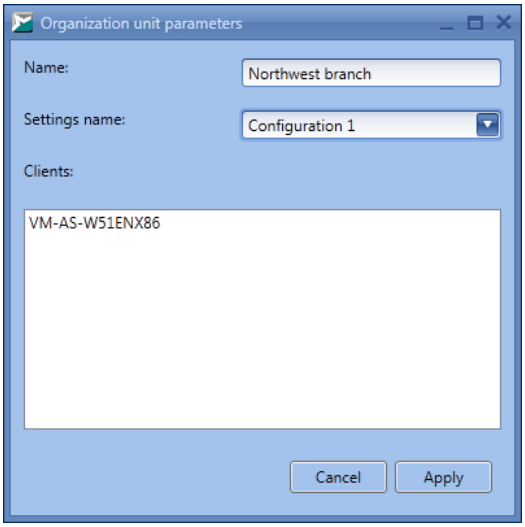

Figure 43. Organization unit properties

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 46). If the organization unit contains components, they are displayed in the **Clients** list.

Removing an organization unit

To remove an organization unit, select it, click **Delete** (fig. The 'Organization units' tab 44) and confirm the removal in the dialog box.

> 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 47).

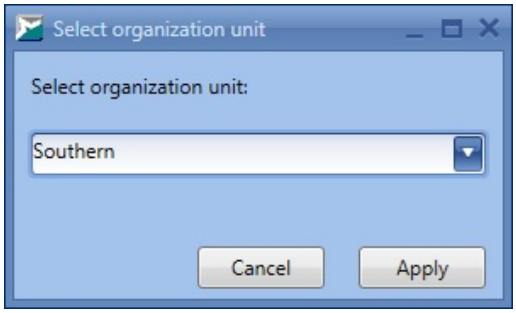

Figure 44. Moving an organization unit

> 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

%SC%> 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 single access to SoftControl SysWatch without disclosing the main password).
You should enable and set up the corresponding option[64] in the organization unit configuration to start working with the one-time password generator.

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** (fig. The 'Organization units' tab[44]). The displayed window contains the **Current password** and its **Time left** in the *dd:hh:mm:ss* format (fig. The generator window[48]). The **Current password** updates after its lifetime expires.

I) One-time passwords 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[60] 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.

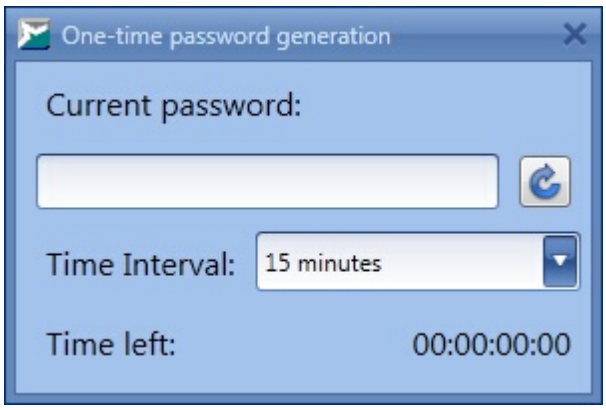

Figure 45. The generator window

4.6. Setting up client components

The **Clients settings** tab contains the list of the client application configurations (settings) (fig. The 'Clients settings' tab 49).

SoftControl Admin Console has the following types of configurations:

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

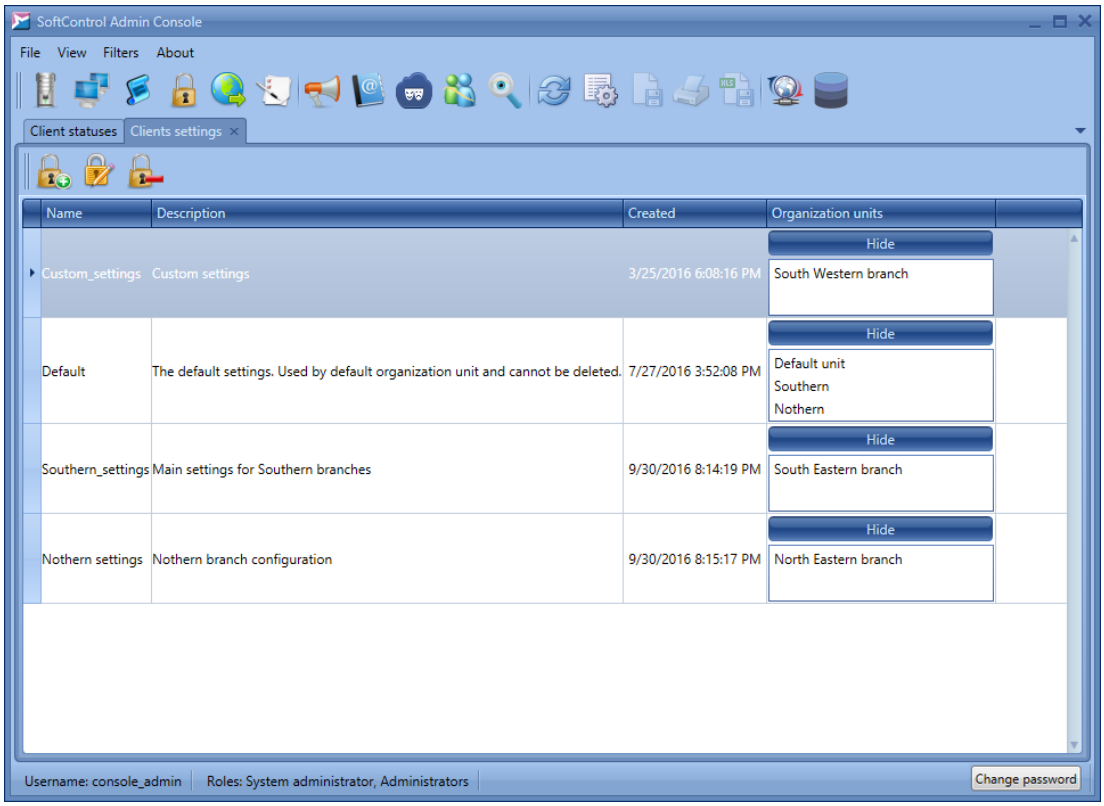

Figure 46. The 'Clients settings' tab

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 (51).

Basic operations with the configurations are performed via the tab's graphical buttons that are described in table 13.

Table 13. The 'Clients settings' tab widgets

Button	Name	Description
	New	Create a new client component configuration.
	Edit	Modify the selected configuration.
	Delete	Remove the selected configuration(s).

The list of the tab fields is given in table 14.

Table 14. The 'Clients 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 (52);
- SoftControl SysWatch settings (55);
- SoftControl DLP Client settings (83).

Basic operations on this tab are:

Creating a configuration

To add a new configuration, click **New** (fig. The 'Clients settings' tab (49)). Specify the configuration parameters in the **Clients settings editor** window (see figures from The 'Name' section (53) to Update schedule settings (91)). If the **All parameters are correct** status is displayed in the lower part of the window, click **Apply** to add the created configuration;

otherwise, modifyinvalid 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 'Clients settings' tab 49);
- double-click the configuration.

In the the **Clients 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 53 to Update schedule settings 91). 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.

Changing settings type

To change the type of the client component settings, go to the Client statuses 38 tab, invoke the context menu by right-clicking right 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 Client statuses 38 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 51).

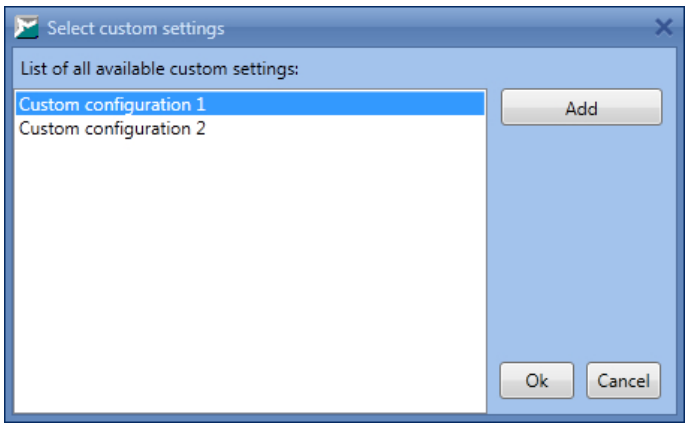

Figure 47. Managing custom settings

Specify the configuration parameters in the **Clients settings editor** window (see figures from The 'Name' section 53 to Update schedule settings 91). 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. 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 'Clients settings' tab 49) 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 53).

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

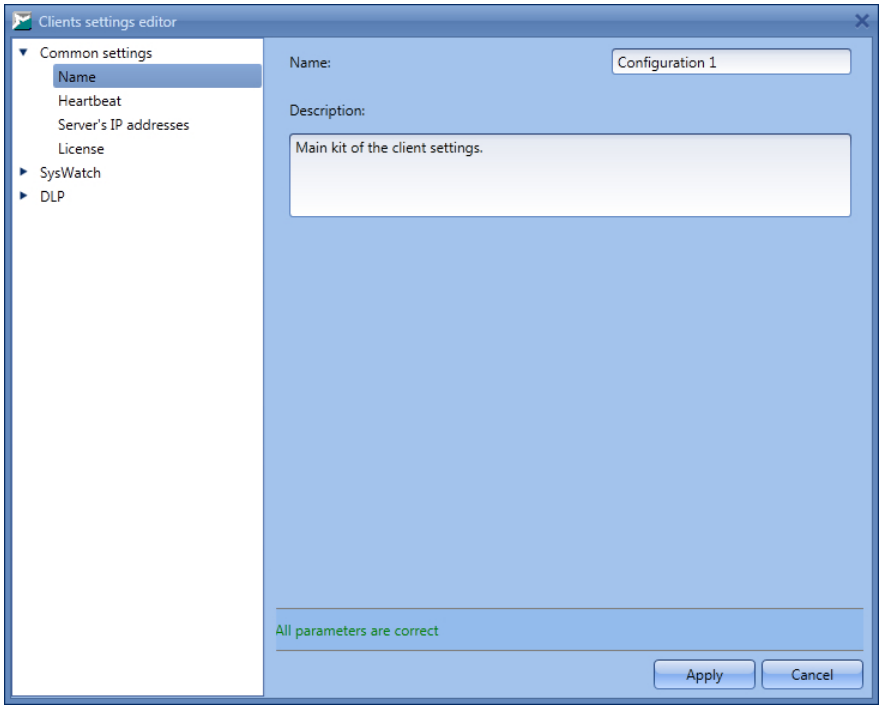

Figure 48. The 'Name' section

Heartbeat

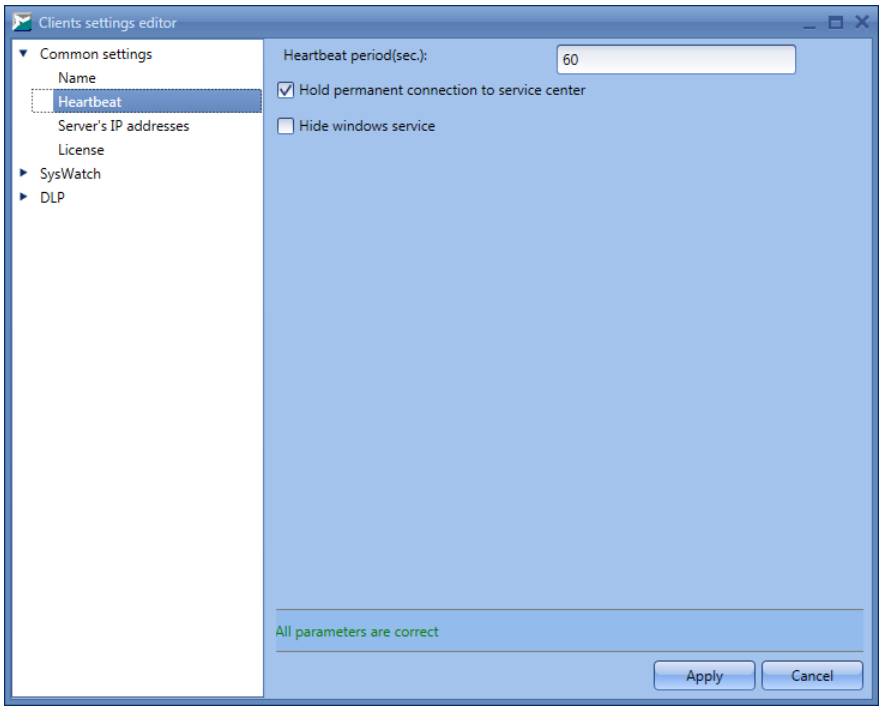

Figure 49. The 'Heartbeat' section

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 53).

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 90.

Tick off **Hide windows service** if the SoftControl SysWatch and SoftControl DLP Client system services (*safensec.exe* and *eventsvc.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.

Specifying the server IP addresses

You can specify the server addresses that the client components can access, in the server configuration wizard 20.

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 54).

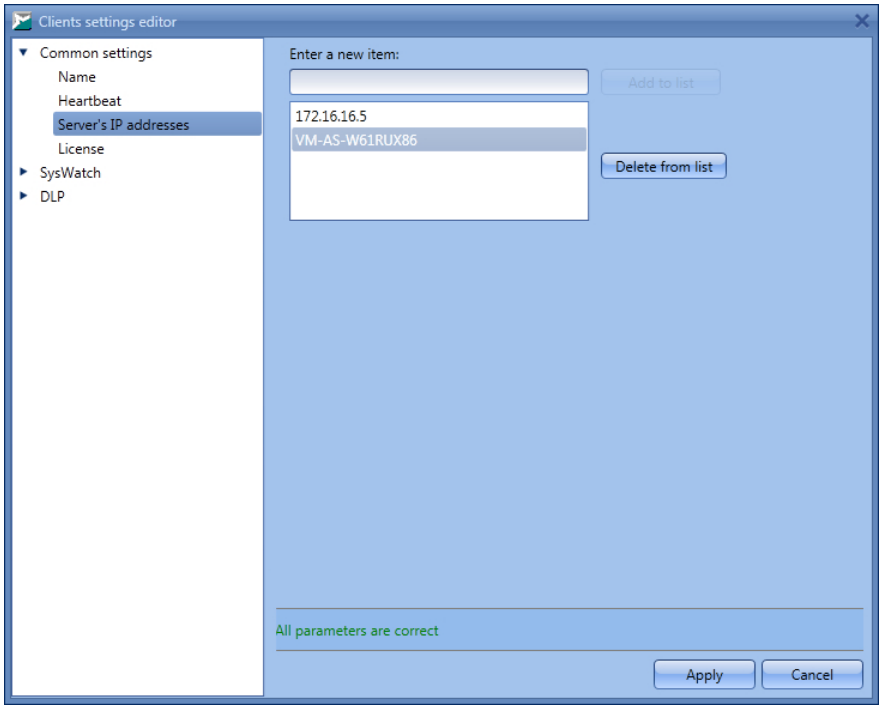

Figure 50. The 'Server's IP addresses' section

To add an address to the list, enter a new value of an IP address or a NetBIOS 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**), 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 55).

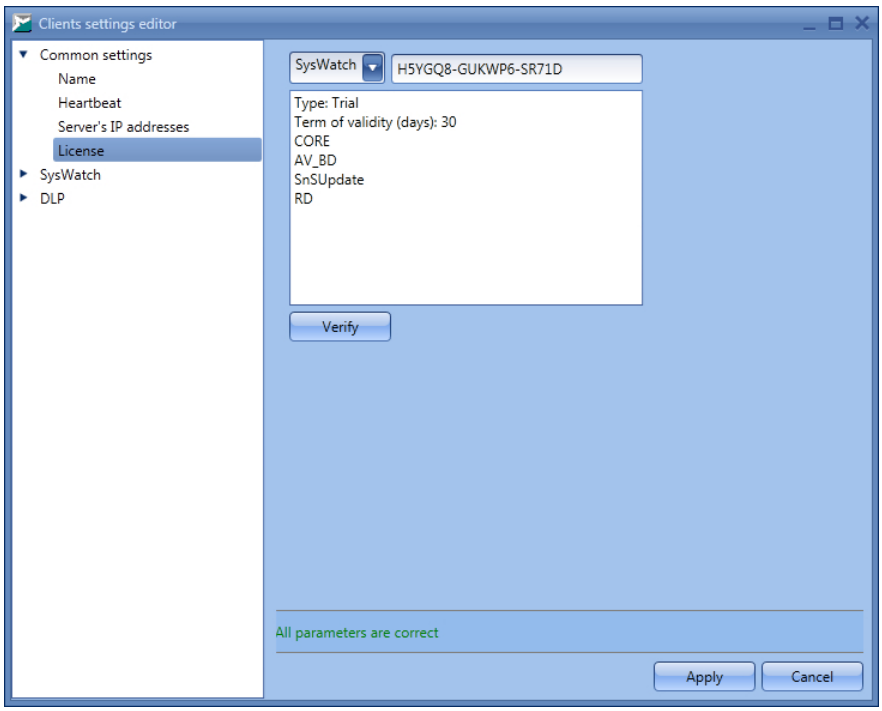

Figure 51. The 'License' section

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 [57]):

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

Select the required additional options of the activity control below:

- **Disable service external management**:

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

- **Global installation mode**:

  execute all processes in installation mode.

  When this mode is active, all processes run with the installer flag 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 of unknown applications on the first run**:

  automatically activate the option of recording the activity history for all new untrusted processes.

- **Disable script engine**:

  do not allow the interpreters to run untrusted scripts (except for the scripts that are signed by a valid digital signature or by a digital signature from the white list of certificates). The following processes are blocked:

  - wscript.exe (Microsoft ® Windows Based Script Host);
  - cscript.exe (Microsoft ® Console Based Script Host);
  - java.exe (Java(TM) Platform SE binary);
  - javaw.exe (Java(TM) Platform SE binary);
  - javaws.exe (Java(TM) Web Start Launcher).

  In order to block specific processes, we recommend that you create the appropriate Control policy rules [68].

❑ **Enable dll modules control**:

activate the integrity control of the dynamic link libraries (DLL) that are used by the executable components.

Dll module control works as follows. When an exe file tries to load a dll library, SoftControl SysWatch checks whether the library is signed by 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 is not signed, 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: libraries that do not have an entry point (resource-only libraries without executable code) cannot be blocked.

❑ **Disable modification of portable executable files (except for installers)**:

do not allow the untrusted processes (the processes without the installer flag) to modify PE files.

This option prevents any processes that are not trusted installers from modifying dll and exe files.

❑ **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.

❑ **Service delay time start value (minutes)**:

specify the delay of the SoftControl SysWatch system service start.

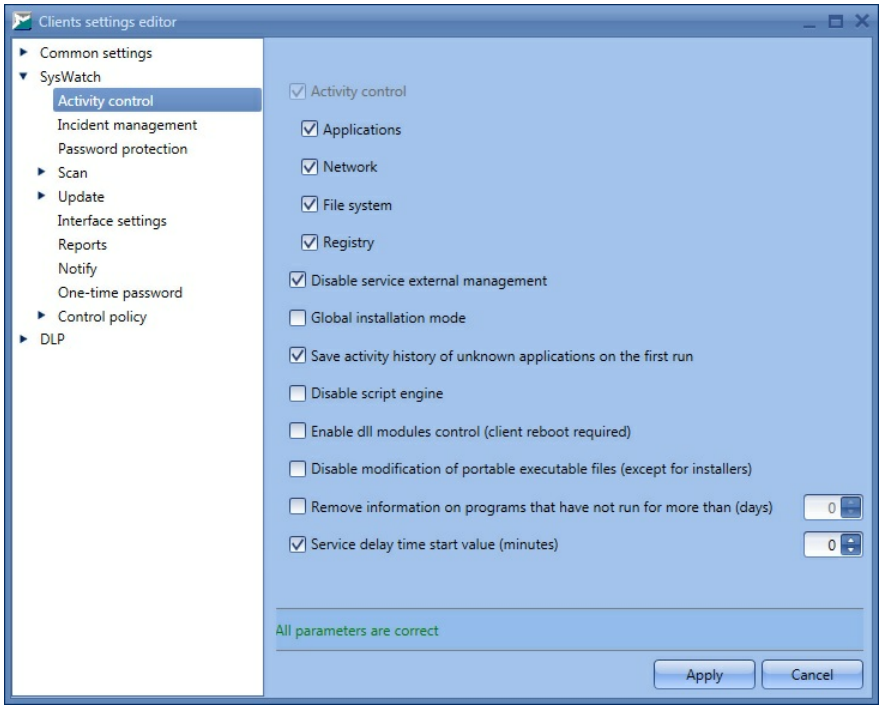

Figure 52. Activity control settings

Incident management

Tick off the **Enable automatic processing of incidents** 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 15 (fig. Incident processing settings 58).

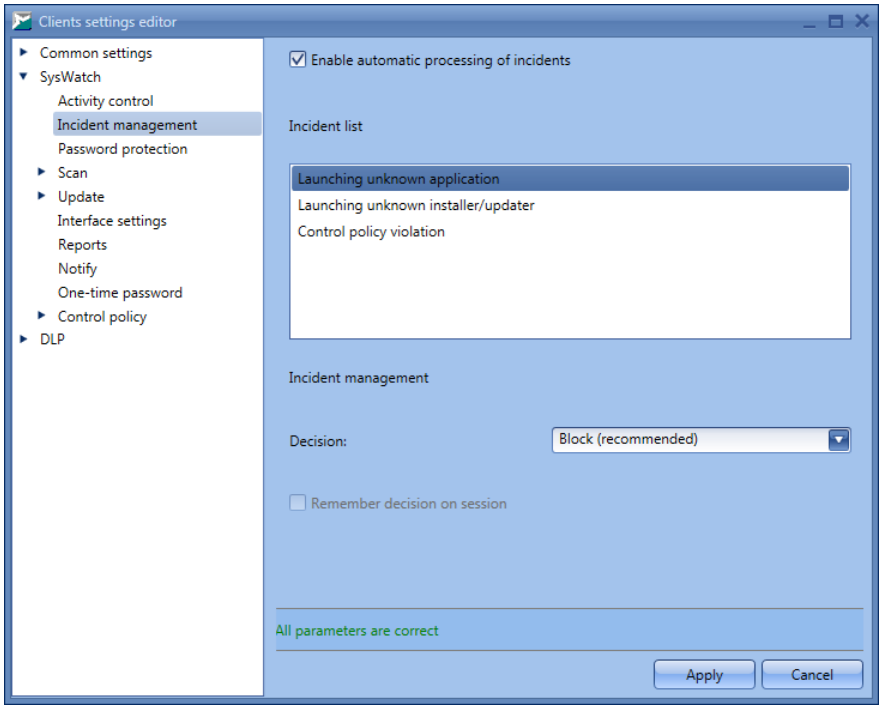

Figure 53. Incident processing settings

Table 15. Possible actions on incidents

Incident	Actions
Unknown application launching	• **Execute in a limited mode** The application runs under current user account or in the isolated environment ('sandbox') under the 'V.I.P.O.' user account with restricted rights. The application is not added to the system profile but is moved to the restricted zone instead. The application can download additional modules that are not added to the system profile either. Even if this application is harmful and it installs some extra components, the system prevents them from loading. • **Scan and execute in a limited mode after** The application runs in limited mode, if no malicious code has been found during the antivirus scanning. Otherwise,the application is blocked. • **Execute in install mode** The application runs under current user account without restrictions or with reduced privileges. The application and all its child modules are moved to the system profile and the trusted zone. • **Scan and execute in install mode after** The application runs in installation mode, if no malicious code has been found during the antivirus scanning. Otherwise,the application is blocked. • **Block (recommended)** (default) The application is blocked and moved to the blocked zone.
Unknown installer launching	• **Install** The installer runs under current user account without restrictions or with reduced privileges. The application and all its child modules are moved to the system profile and the trusted zone after installation. • **Scan and install after** The installer runs in installation mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Install in a limited mode** The installer runs under current user account or in the isolated environment

Incident	Actions
	(«sandbox») under the 'V.I.P.O.' user account with restricted rights. The installer is not added to the system profile. The application and all its child modules are moved to the restricted zone after installation. • **Scan and install in a limited mode after** The installer runs in limited mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Block (recommended)** (default) The installer is blocked and moved to the blocked zone.
Control policy violation	• **Allow** Allow a process to perform an action that meets the conditions of the specified control policy rule. • **Scan and allow after** Allow a process to perform an action that meets the conditions of the specified control policy rule, 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. When **Remember decision on session** checkbox is ticked off, the above-mentioned actions are repeated during the session; otherwise, the actions are only performed once.

To delegate the authorities to handle the incidents to a local SoftControl SysWatch user, deselect the **Enable automatic processing of incidents** 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 60). Enter a **Password** and its **Confirmation**, and select the **Scope**:

- **Settings changing**:
  request the password when accessing SoftControl SysWatch GUI.
- **Program uninstalling**:
  request the password when uninstalling SoftControl SysWatch.

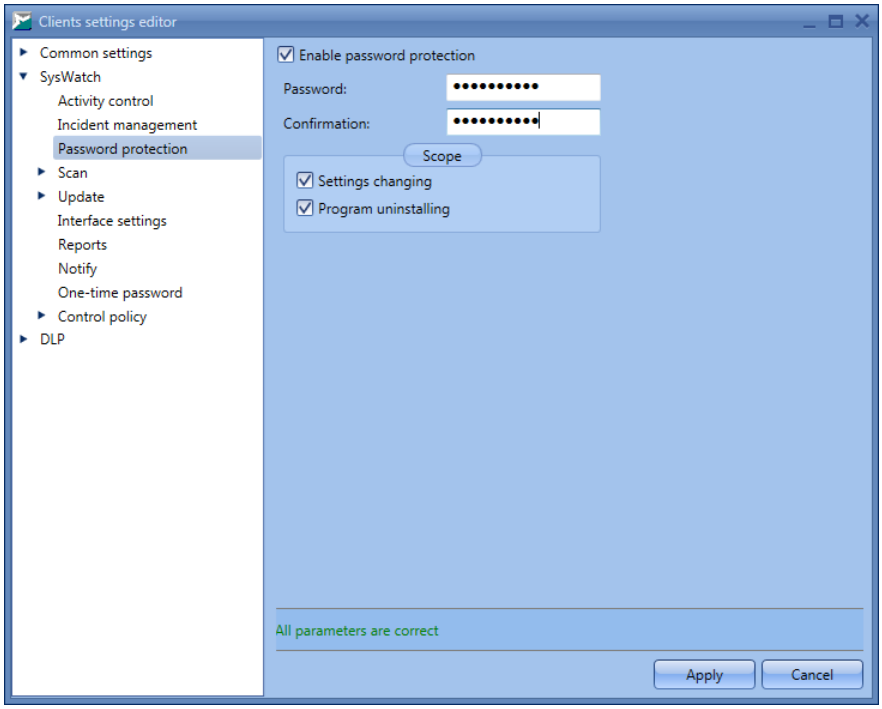

Figure 54. Password protection settings

Scan settings

Specify the antivirus check parameters in the **Scan** → **Scan common settings** section of the **SysWatch** category (fig. Common scan settings 61).

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

- **Selecting actions automatically**:

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

- **Choice of 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.

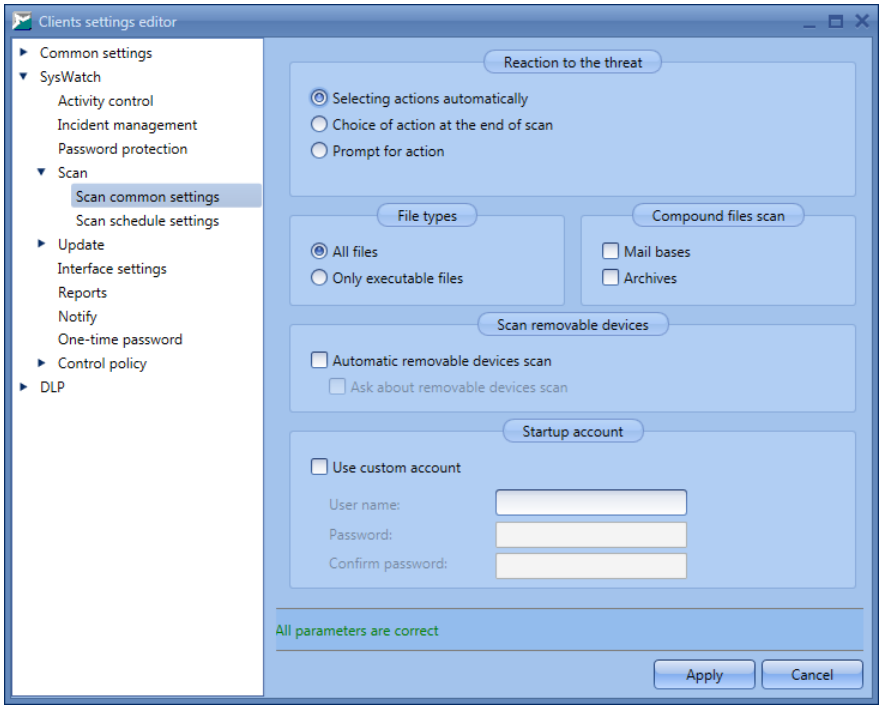

Figure 55. Common scan settings

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 **Automatic removable devices scan** 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 removable devices scan** to show the dialog box with the scan suggestion on a client host.

Tick off **Use custom account** in the **Startup 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 62). Specify frequency of the scanning task in the **Days frequency** counter, and the time of the task start in *hh:mm:ss* format in the **Invoke time** field.

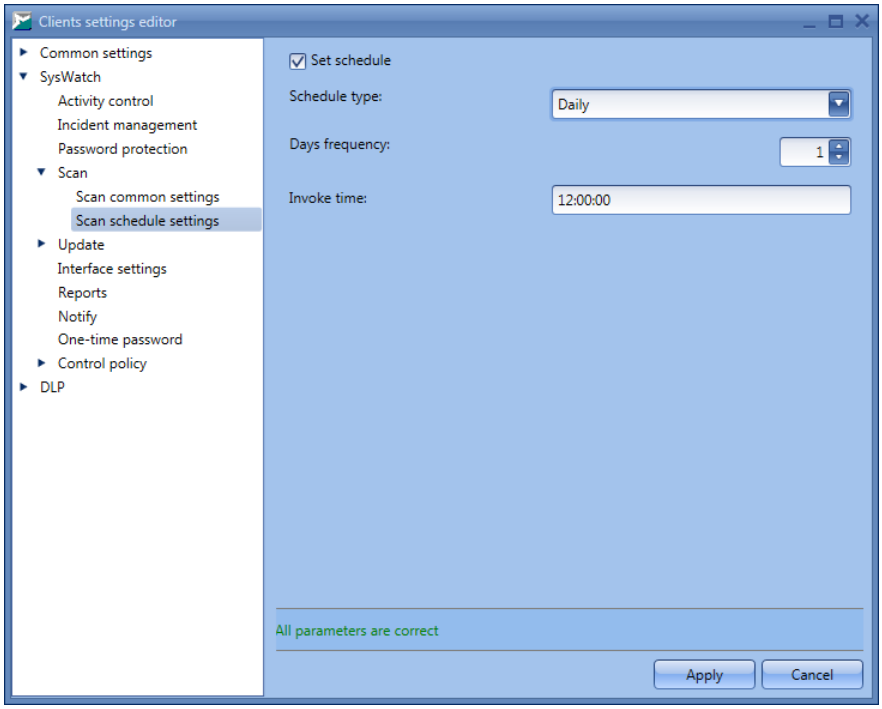

Figure 56. Scan schedule settings

Update settings

Specify the update parameters in the **Update** → **Update settings** section of the **SysWatch** category (fig. Common update settings 63).

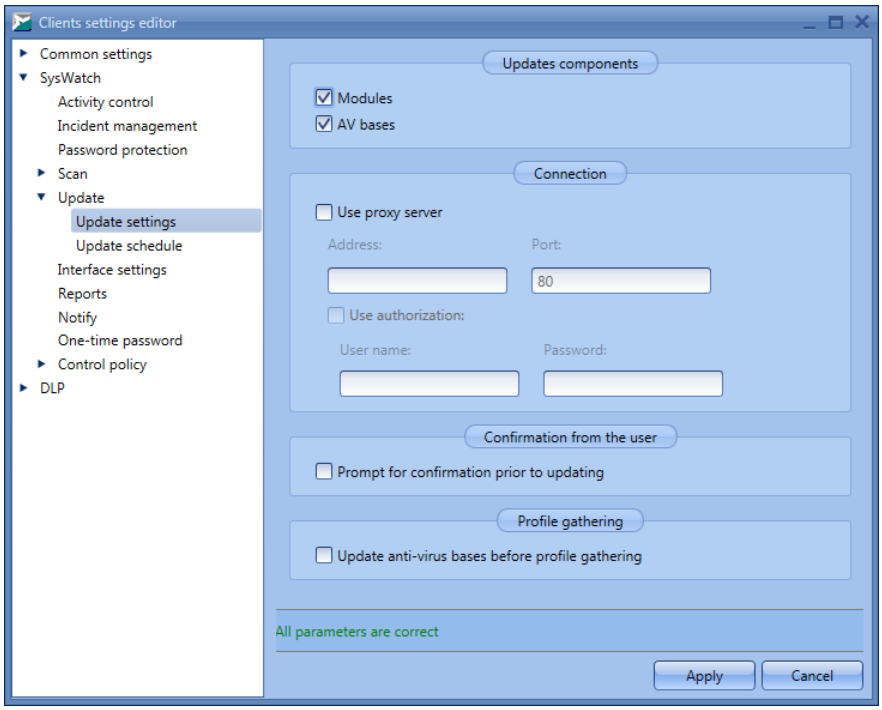

Figure 57. Common update settings

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 prior to 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 anti-virus 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 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 64). 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.

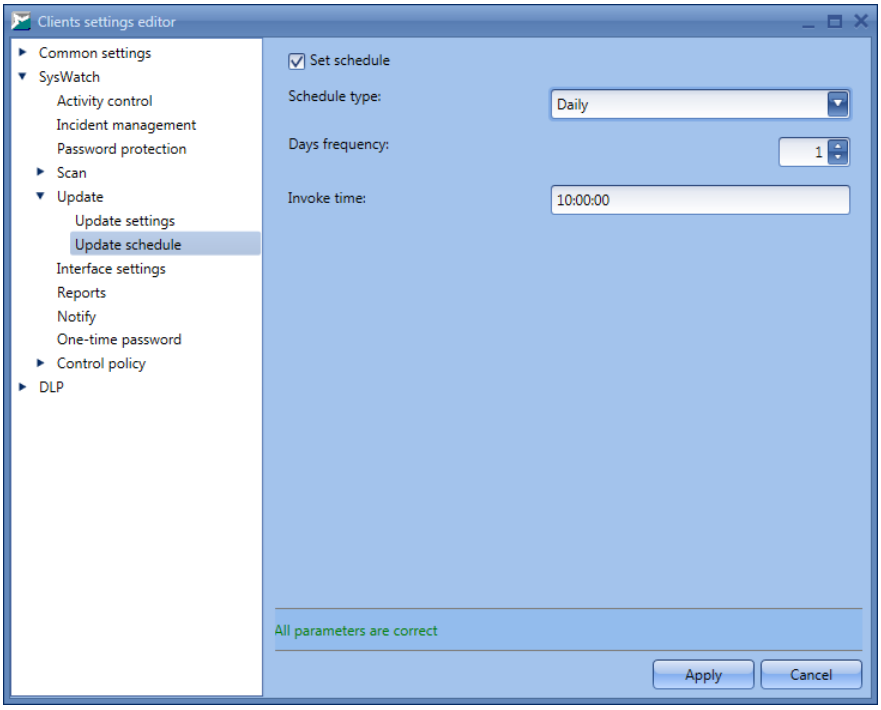

Figure 58. Update schedule settings

One-time password

Tick off **Enable one-time passwords** in the **One-time password** 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 65).

Generating a new key makes all the previous passwords invalid.

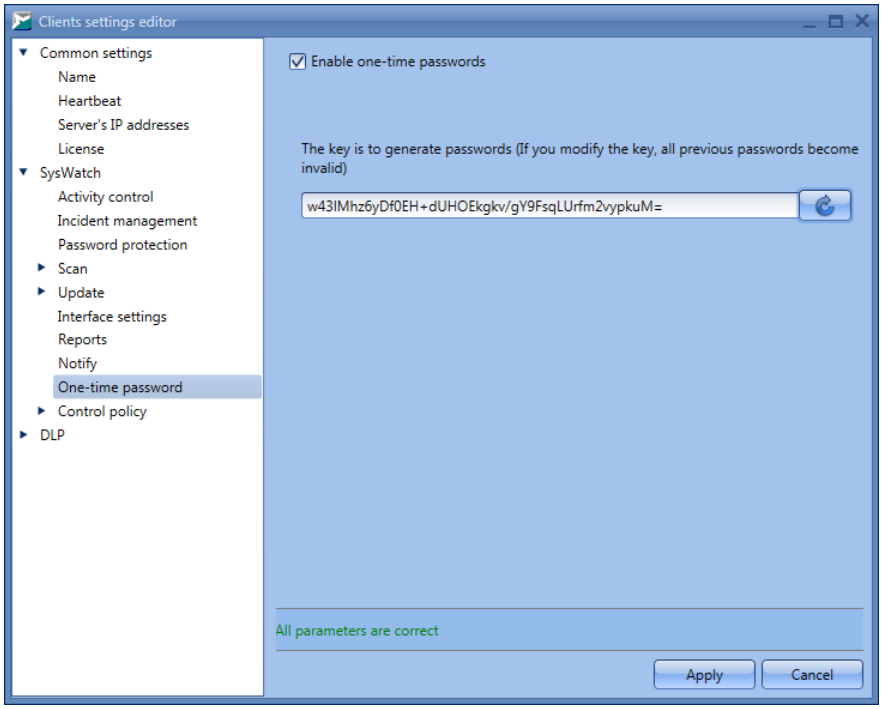

Figure 59. One-time password settings

You can generate one-time passwords on the Organization units 48 tab.

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 65).

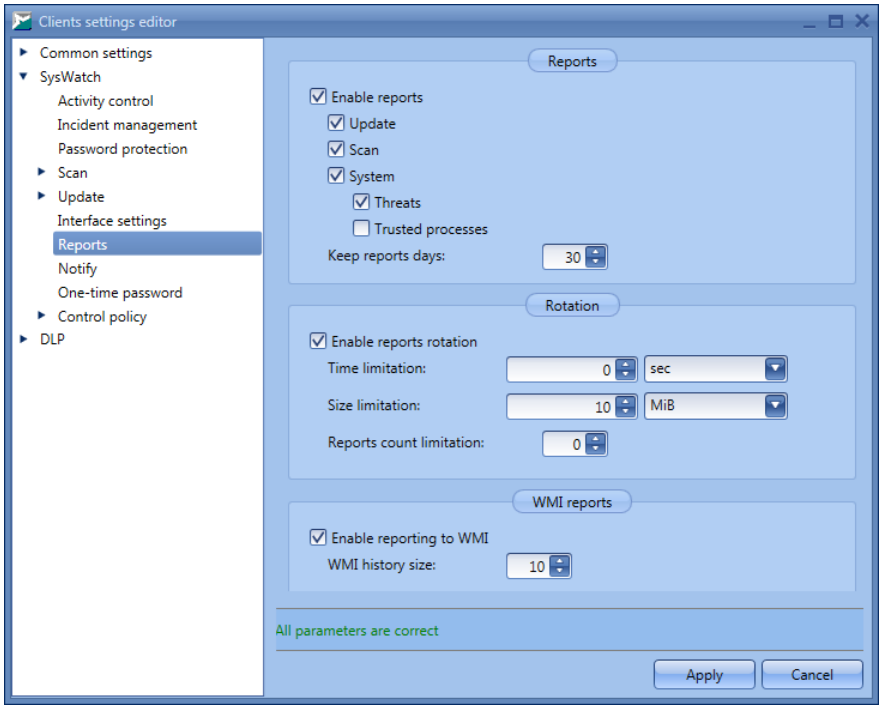

Figure 60. Report settings

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**;
  - ❑ **Trusted processes**.

Tick off **Trusted processes** 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 **Keep reports days** counter.

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

- **Time limitation**:

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

- **Size limitation**:

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

- **Reports count limitation**:

  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.

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 67):

❑ **Show icon in tray**:

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

❑ **Enable sounds**:

enable sound notifications about the incidents.

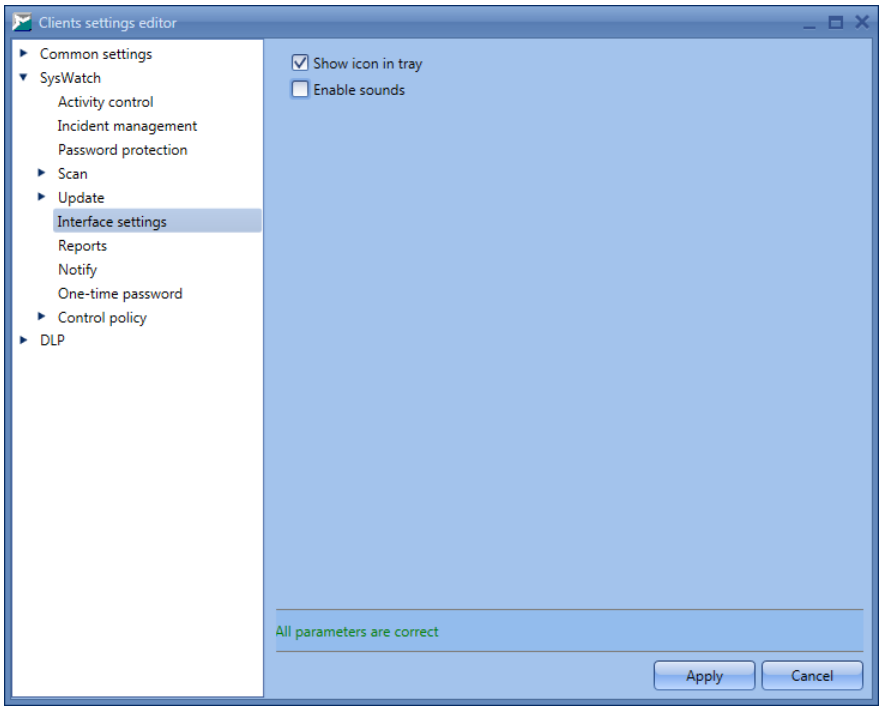

Figure 61. Interface settings

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 68):

- ❑ **Protection status**;
- ❑ **Update**;
- ❑ **Scan for malware**;
- ❑ **Reports**;
- ❑ **Licensing**;
- ❑ **Application installation (uninstallation)**;
- ❑ **Program modules blocking**;
- ❑ **Restricting applications**.

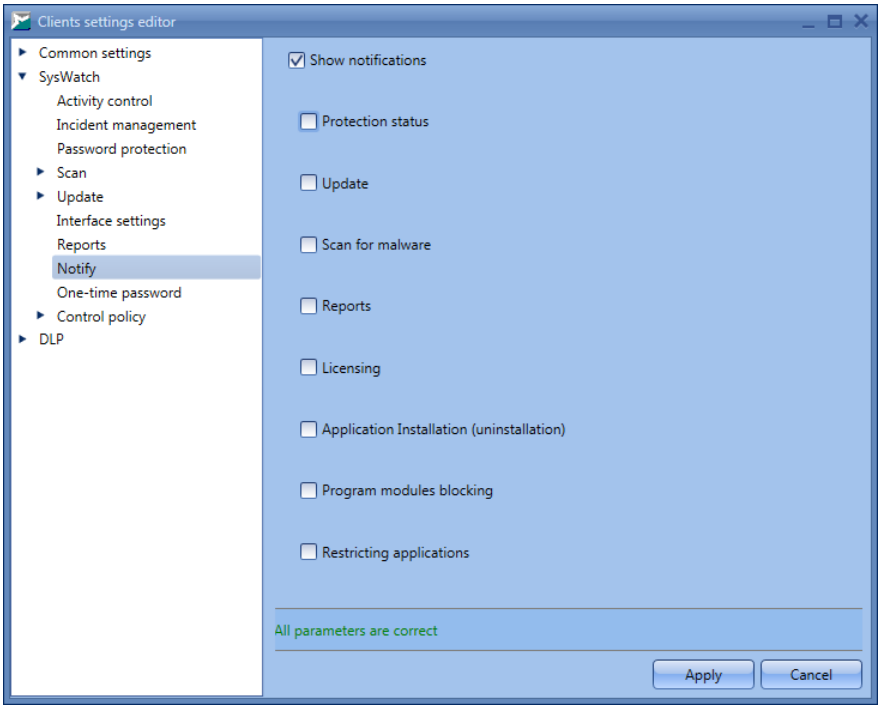

Figure 62. Local notification settings

Control policy: File system

Specify the application permissions to access the file system objects on the client hosts, in the **Control policy** → **Filesystem** section of the **SysWatch** category (fig. File system control policy 69):

- 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.

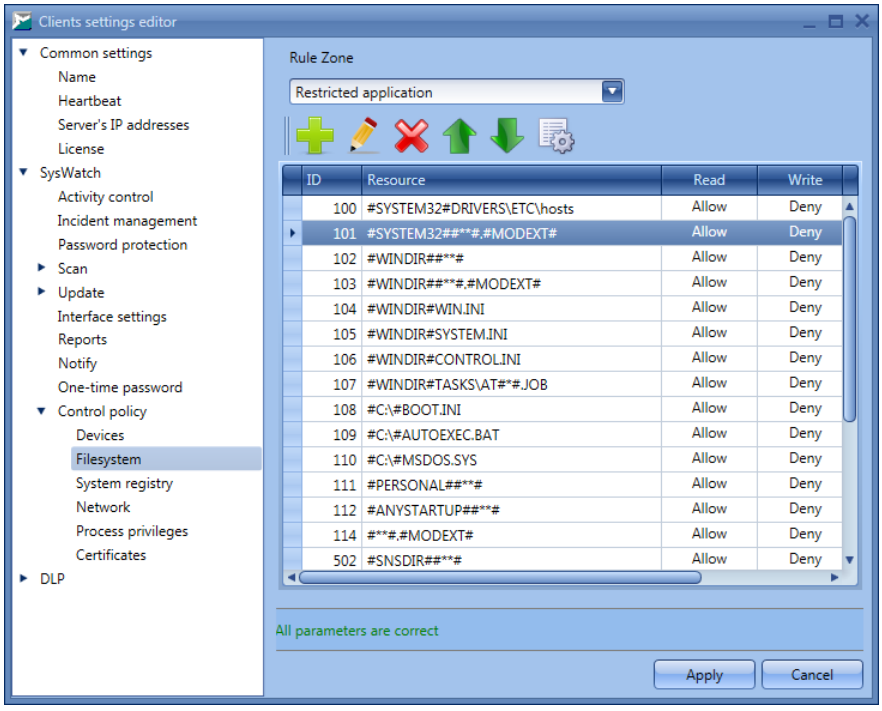

Figure 63. File system control policy

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 70).

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 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;
- **Confirm** – display the request when the operation with the object matches the rule condition.

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

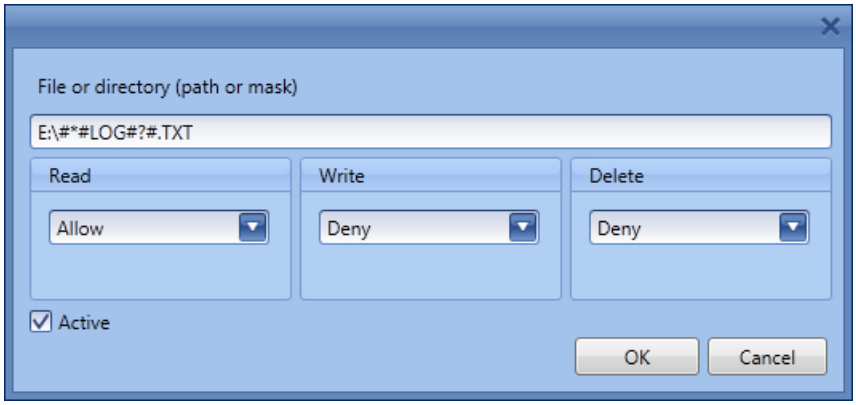

Figure 64. Creating a rule for the file system object

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 it applies to, click (**Additionally**). In the displayed window, set the time intervals and add users with the help of the **Add** button (fig. Adding users and intervals for the rule 71). To confirm changes, click **Apply**.

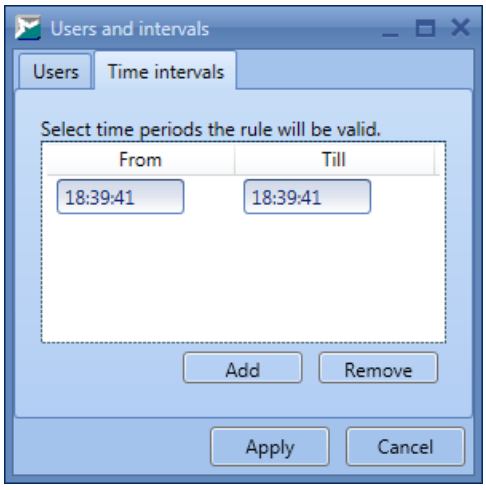

Figure 65. Adding users and intervals for the rule

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

SoftControl SysWatch contains the preset rules that apply to the system folders and the objects in the folders of the product components. Changing or deleting the 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 72):

- 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.

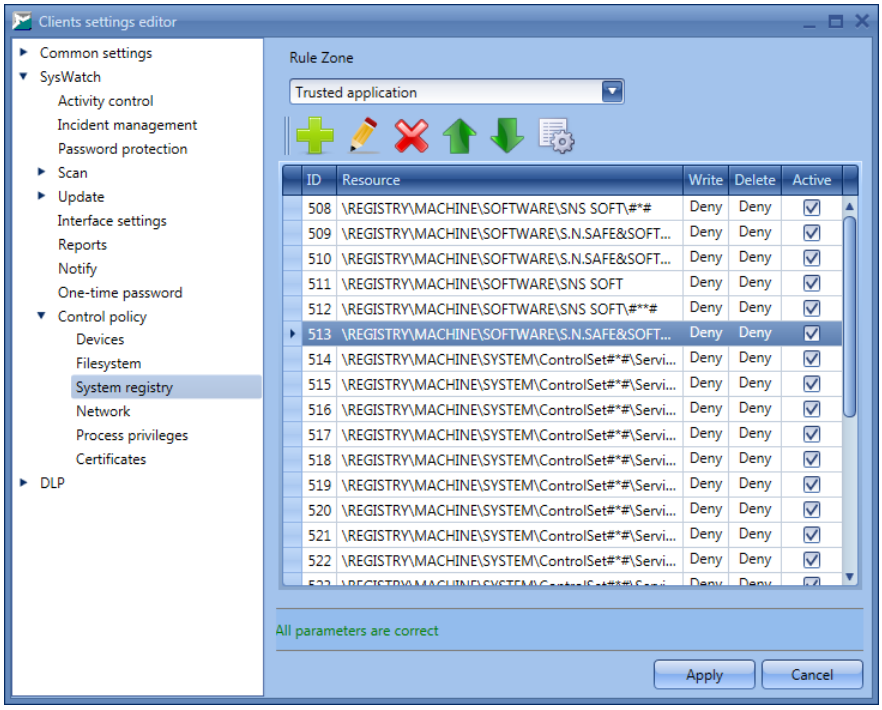

Figure 66. System registry policy

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 73). 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 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;
- **Confirm** – display the request when the operation with the object matches the rule condition.

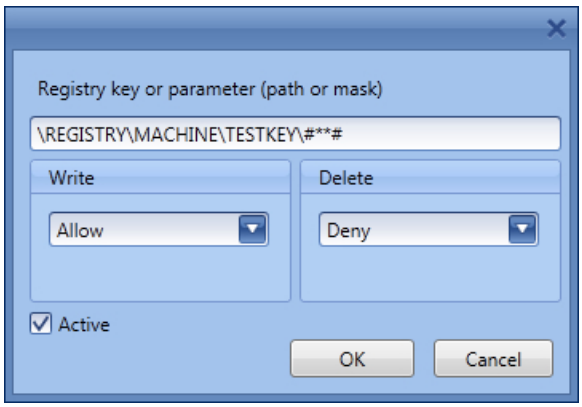

Figure 67. Creating a rule for the system registry object

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 it applies to, click (**Additionally**). In the displayed window, set the time intervals and add users with the help of the **Add** button (fig. Adding users and intervals for the rule 74). To confirm changes, click **Apply**.

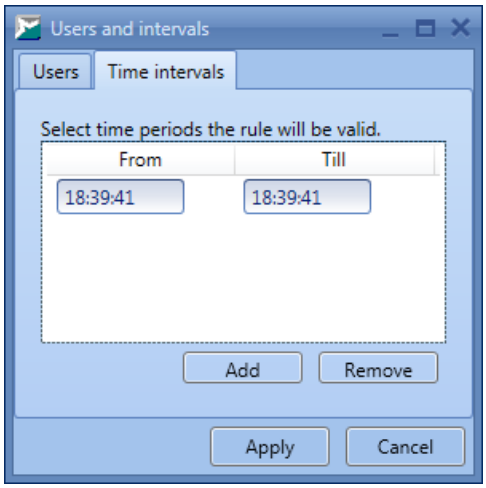

Figure 68. Adding users and intervals for the rule

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

%SW%> contains the 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 the preset rules may cause violation of the system integrity protection.

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 74):

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

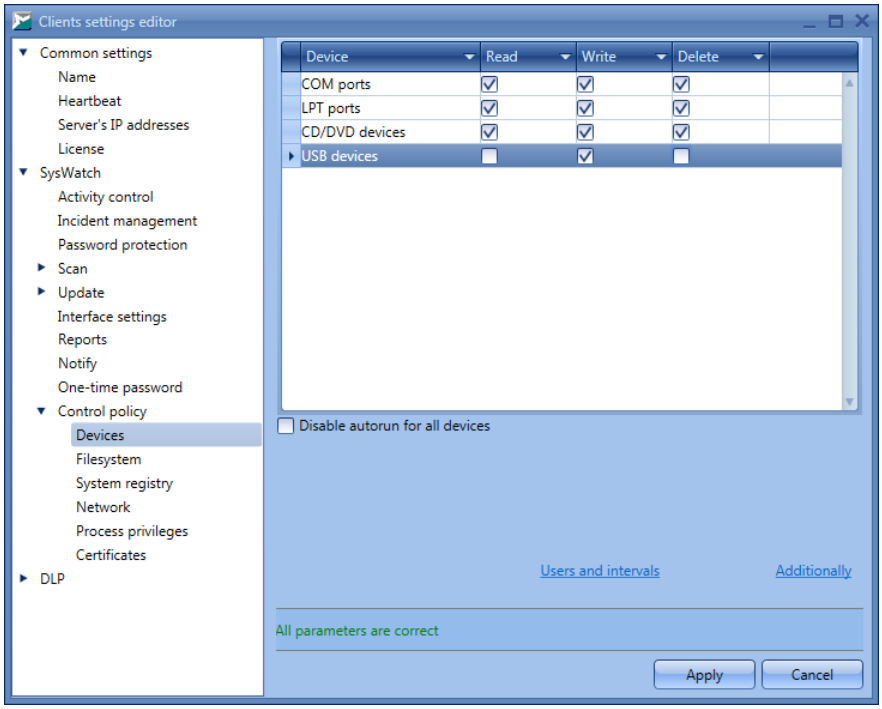

Figure 69. Device control policy

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 white list'). To do so, click on the **Additionally** link and click ✚ (**Add**) in the displayed window (fig. Exceptions for USB storage devices 75).

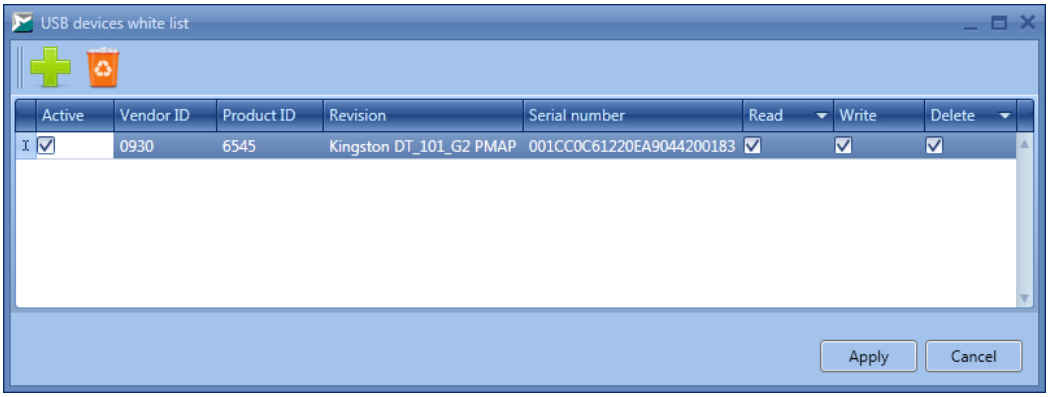

Figure 70. Exceptions for USB storage devices

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-clickthe 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 the time intervals and the users the selected access rights apply to. To do so, click **Users and intervals** link. In the displayed window, set the time intervals and add users with the help of the **Add** button (fig. Adding users and intervals for the rule 76). To confirm changes, click **Apply**.

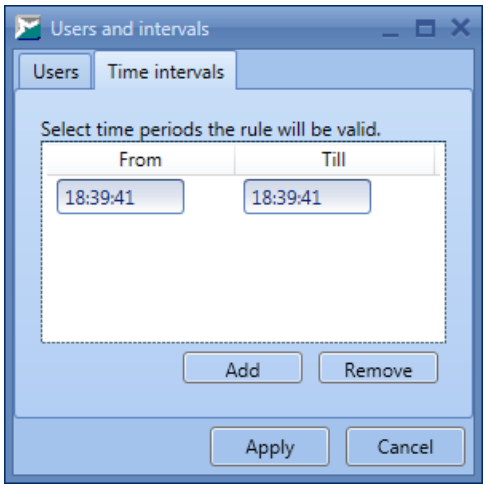

Figure 71. Adding users and intervals for the rule

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: 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 77):

- 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.

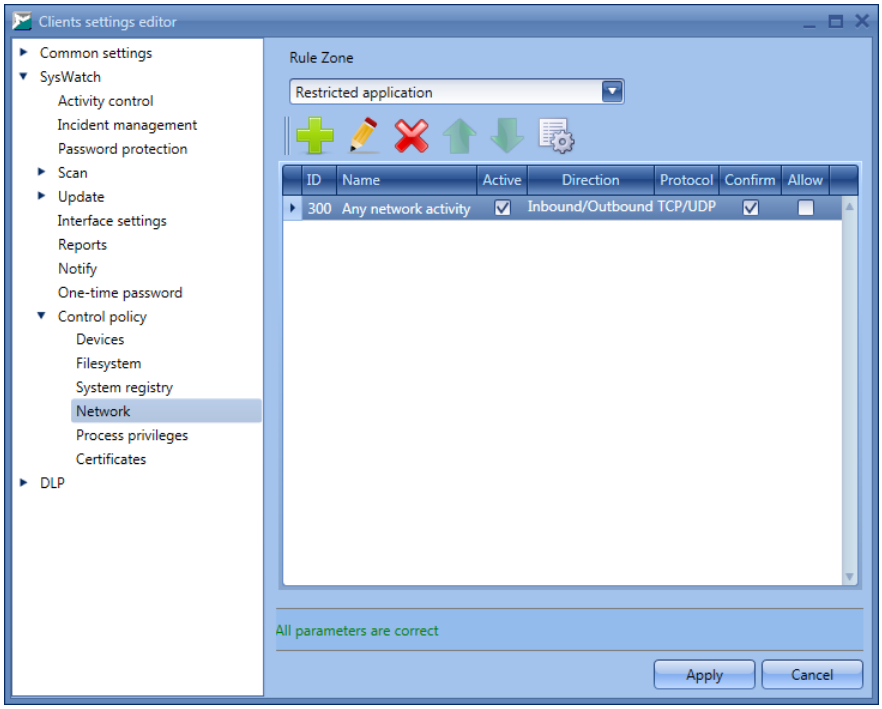

Figure 72. Network activity control policy

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 occurred) 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 79):

- **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**.

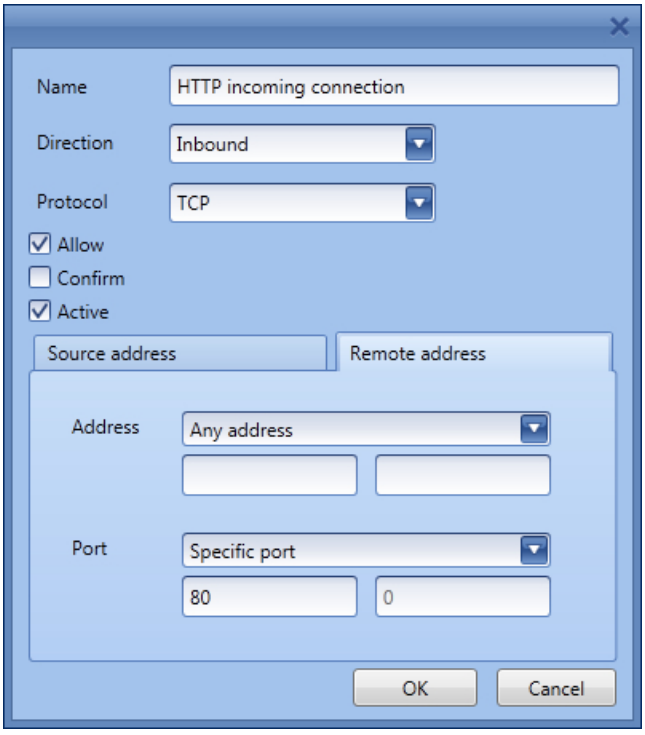

Figure 73. Creating a network activity rule

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[58] should be disabled).

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 rule creation.

To specify when the rule is valid and the users it applies to, click (**Additionally**). In the displayed window, set the time intervals and add users with the help of the **Add** button (fig. Adding users and intervals for the rule[80]). To confirm changes, click **Apply**.

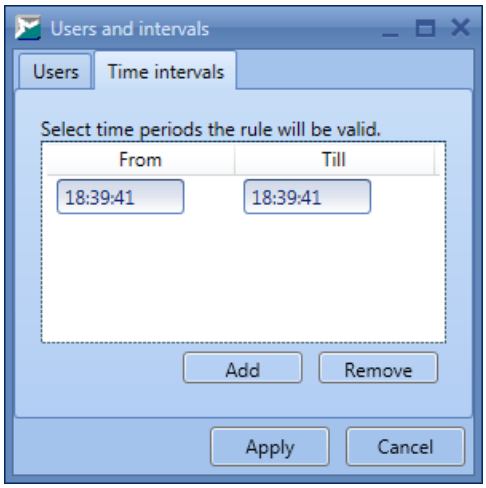

Figure 74. Adding users and intervals for the rule

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

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[81]):

- Back up files and directories;
- Bypass traverse checking;
- Create global objects;
- Create a pagefile;
- 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.

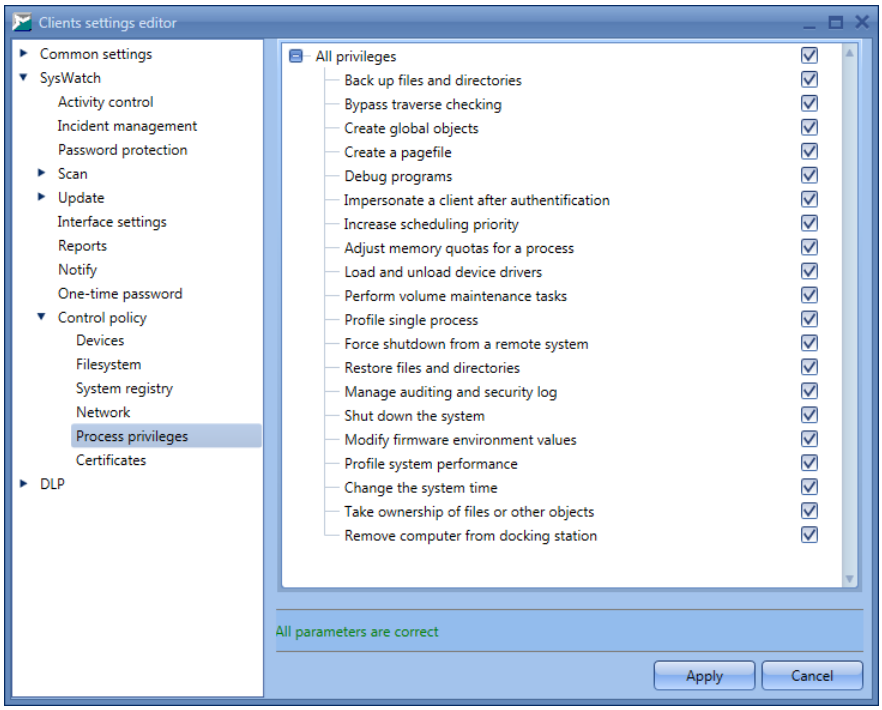

Figure 75. Process privileges control policy

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 147.

Control policy: Certificates

Specify the white list of certificates for additional process activity control on client hosts, in the **Control policy** → **Certificates** section of the **SysWatch** category (fig. The white list of certificates 82).

When a process runs, SoftControl SysWatch heuristically determines whether it is an installer or a script. By default, if the process has a valid digital signature, it gets the installer flag. Besides, it is possible to check whether a digital signature certificate is in the white list. To do so, tick off the **Enable certificate white list** and create the list.

Initially, SoftControl SysWatch contains the basic list of the certificates by trusted vendors, including two 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 82). Tick off the box in the **Trust** column for the added certificates (fig. The white list of certificates 82).

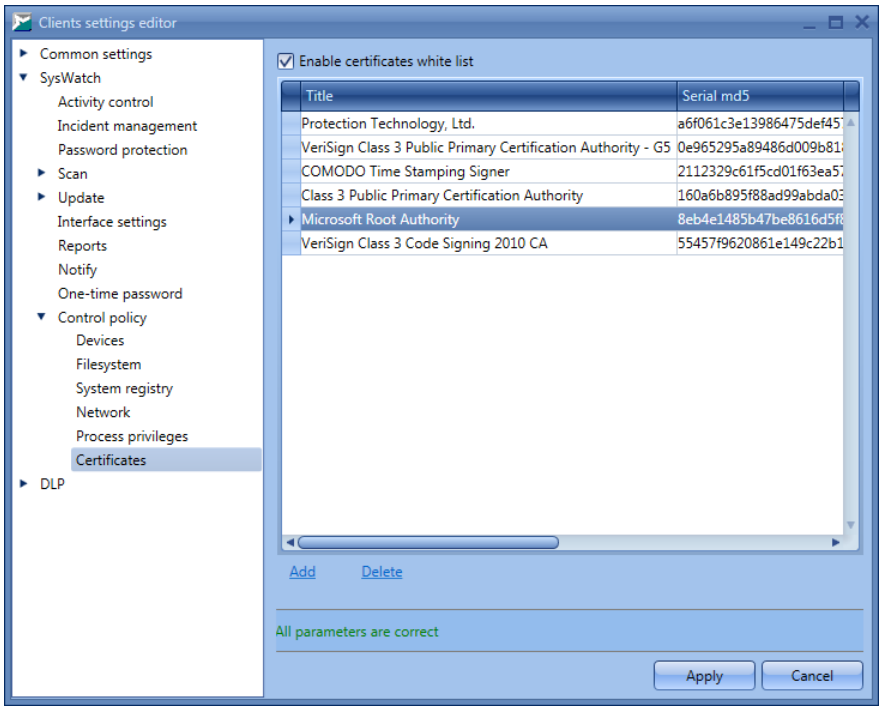

Figure 76. The white list of certificates

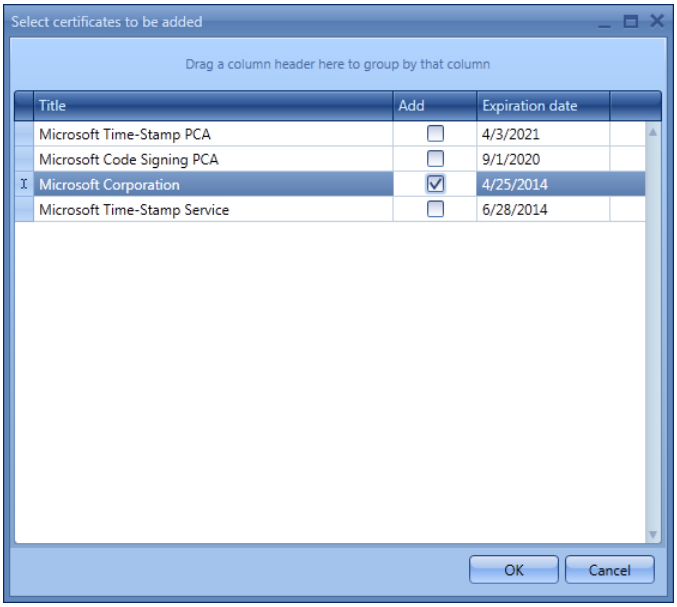

Figure 77. Selecting certificates to add

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 white list of certificates 82).

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 83):

- ❑ **Applications work time**;
- ❑ **USB control**;
- ❑ **Document printing control**;
- ❑ **Control document setting by email**;
- ❑ **Enable key logger**.

Observation over file system 85, system registry 87 and network traffic 88 is active if **Collect data** is checked and the rules are added to the corresponding subsections in the **Observation** section.

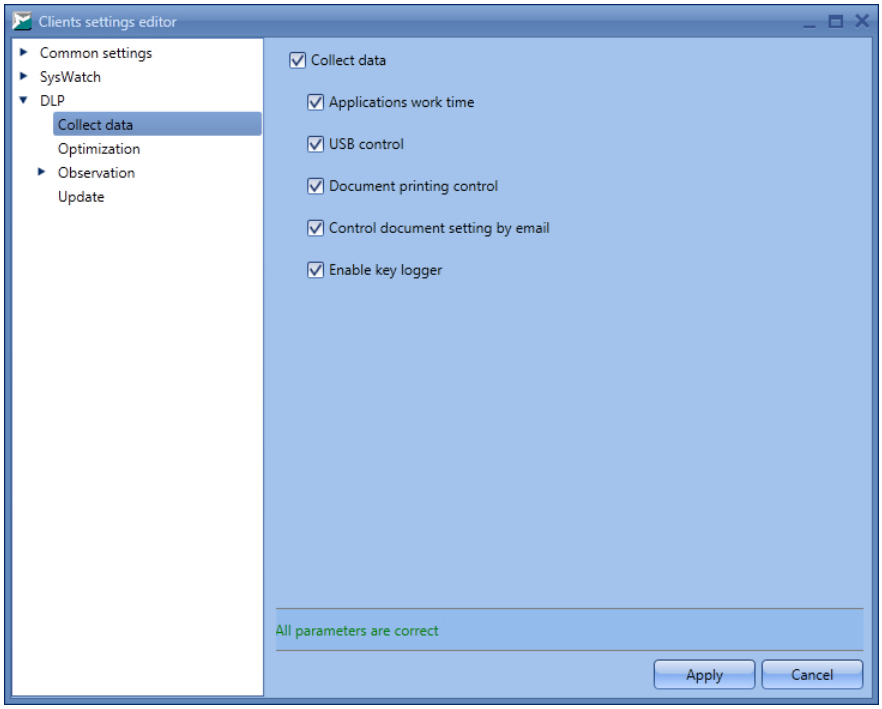

Figure 78. Data collection settings

Optimization

Time parameters of the event registration are specified in the **Optimization** section of the **DLP** category (fig. Optimization settings 84).

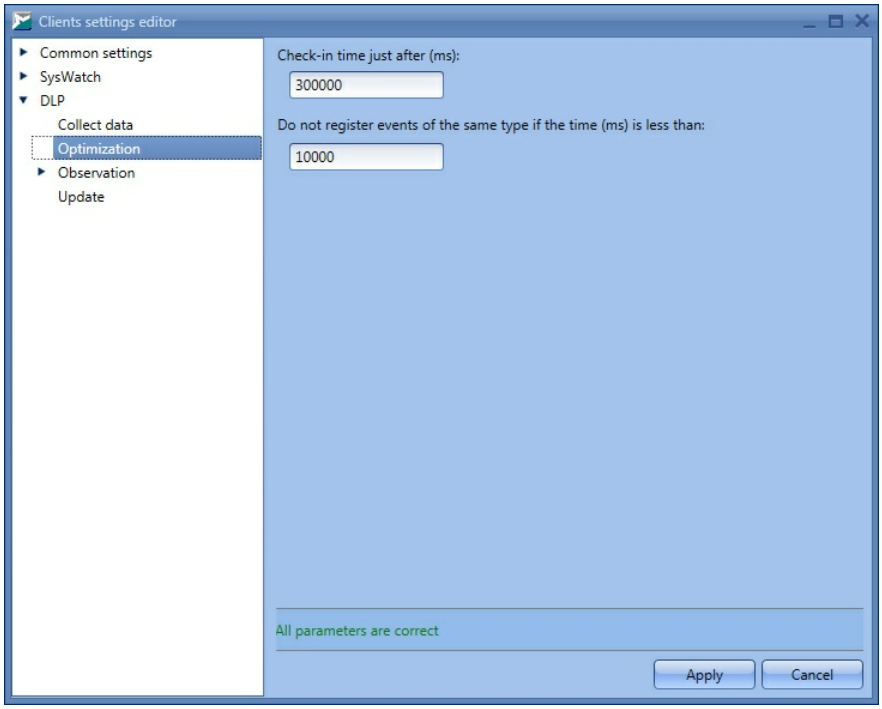

Figure 79. Optimization settings

Enter the **Check-in time just after (ms)** and **Do not register events of the same type if**

the time (ms) is less than 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 **Check-in time just after (ms)** option works when the **Applications work time** option is enabled (see fig. Data collection settings 83) 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 85).

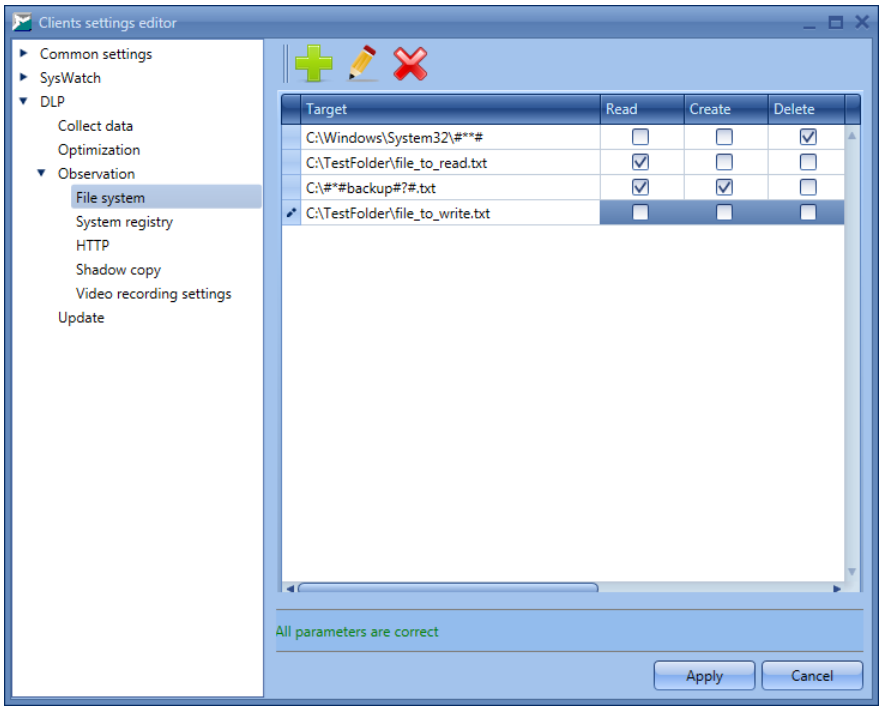

Figure 80. File system monitoring settings

To add an object to monitor, click ✚ (**Add**) and enter the full path to it in the displayed window (fig. Object under observation 86).

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.

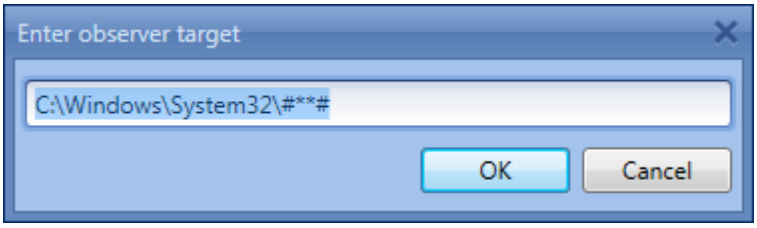

Figure 81. Object under observation

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**;
- ❑ **Create**;
- ❑ **Delete**;
- ❑ **Rename**;
- ❑ **Change**.

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

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 89 global option is enabled

and **Delete** or **Create** fields are ticked off. If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters[90] 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[87]).

To add an object to monitor, click ✚ (**Add**) and enter the full path to it in the displayed window (fig. Object under observation[88]). 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.

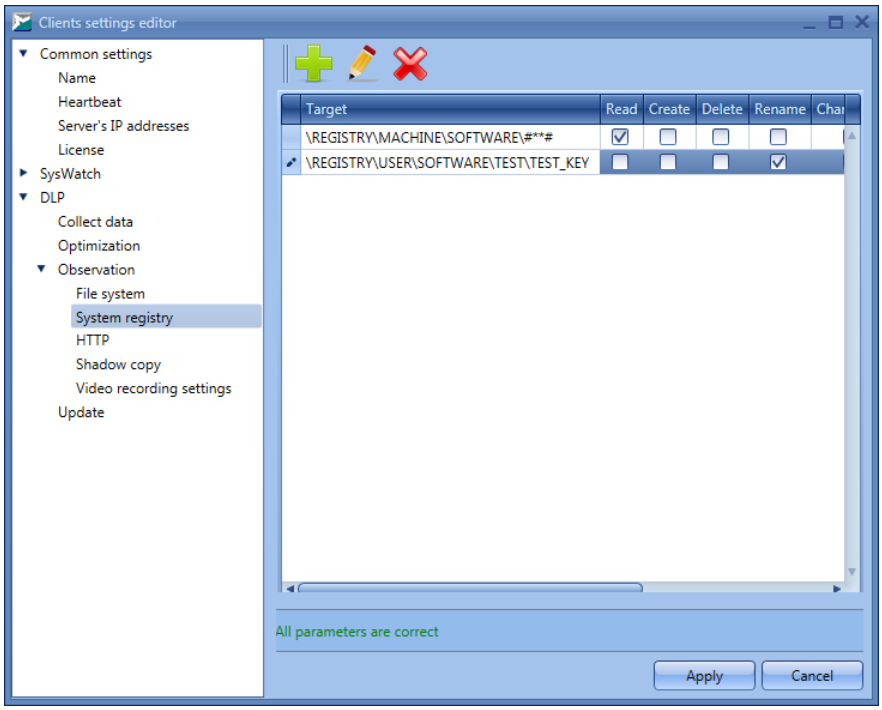

Figure 82. System registry monitoring settings

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.

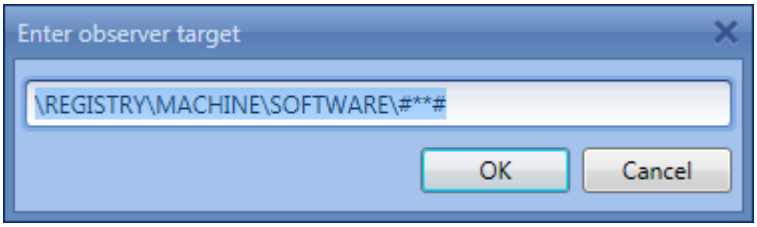

Figure 83. Object under observation

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**;
- ❑ **Create**;
- ❑ **Delete**;
- ❑ **Rename**;
- ❑ **Change**.

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

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 89 global option is enabled and **Delete** or **Create** fields are ticked off. If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters 90 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 88).

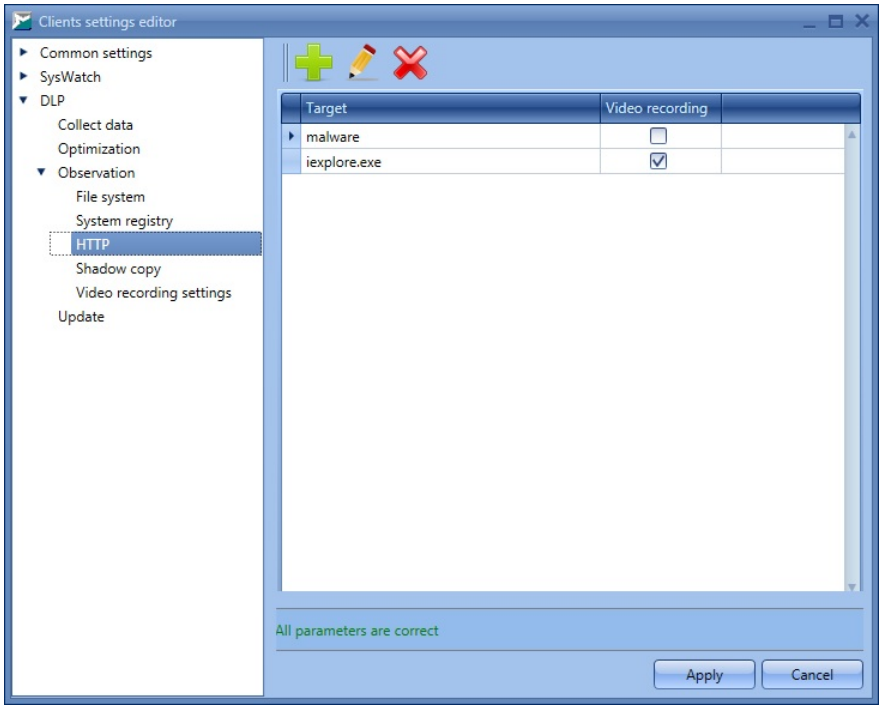

Figure 84. Network traffic monitoring settings

To add data to monitor, click the **Add** link and enter a string in the displayed window (fig. Object under observation[89]). 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.

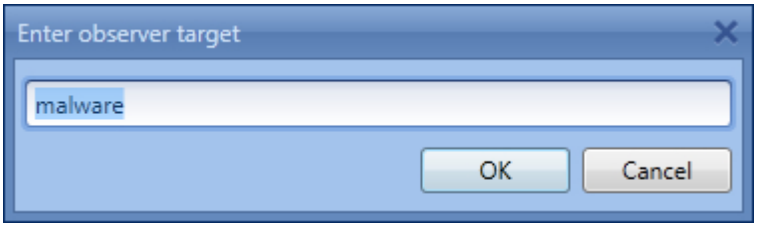

Figure 85. Object under observation

To change the traced text, select a string from the list and click the **Edit** link. To delete a text from observation, select a string and click the **Delete** link.

If the **Video recording** option is selected, the screen shots of the client host are saved with the specified parameters[90] 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[89]).

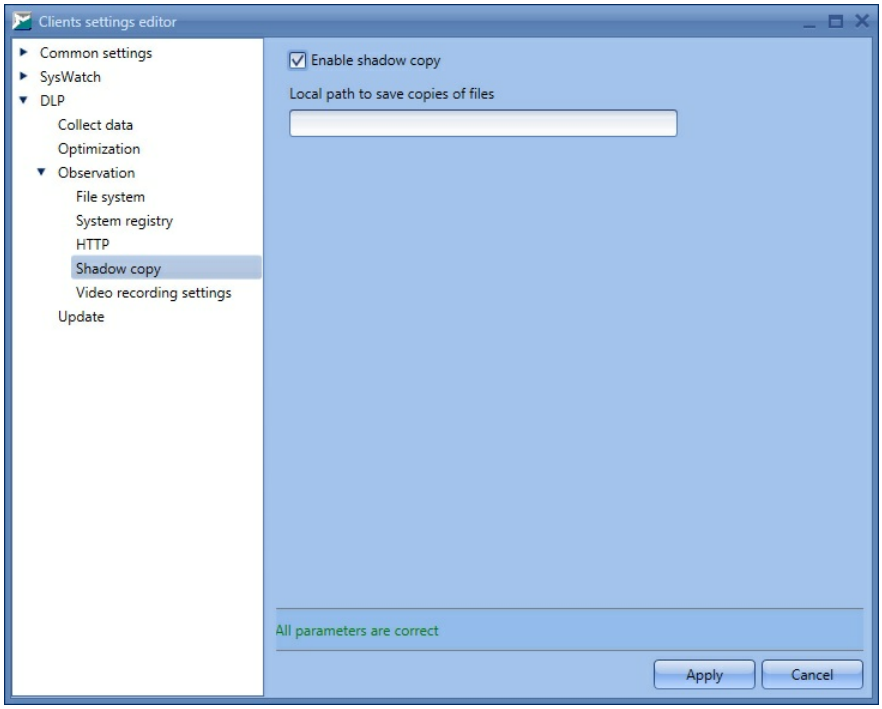

Figure 86. Shadow copying settings

Tick off the **Enable shadow copy** checkbox to enable the backups of the file system[85] and system registry[87] objects under observation, when the objects are modified (fig. Shadow copying settings[89]). 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[90]). 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).

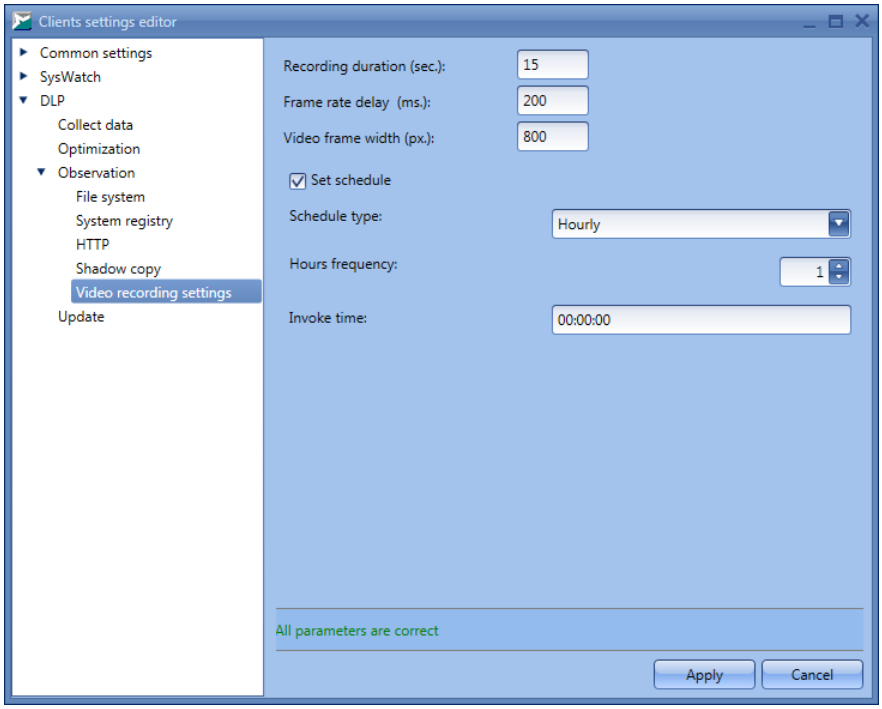

Figure 87. Video recording settings

To start recoding the video in real time, right-click the required SoftControl DLP Client component on the Client statuses 38 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;
- **Days frequency/Hours frequency** – 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 91).

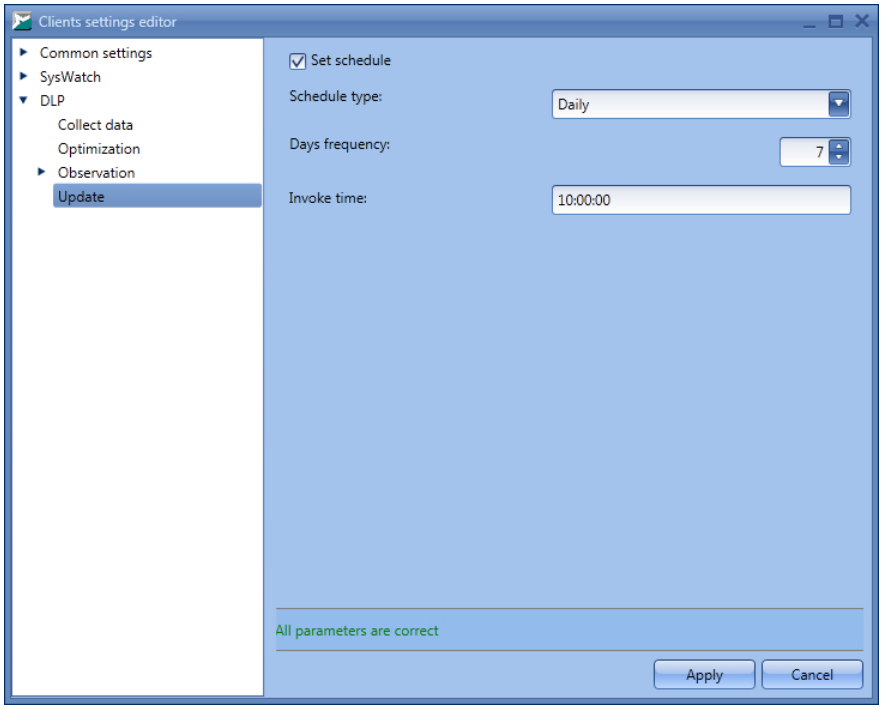

Figure 88. Update schedule settings

Select the schedule type (**Daily** or **Hourly**), specify the frequency of the task in the **Days frequency** counter, and the start time in *hh:mm:ss* format in the **Invoke time** field.

4.7. Tasks

The **Tasks** tab allows you to create tasks for client applications and watch the details of their execution (fig. The 'Tasks' tab 93).

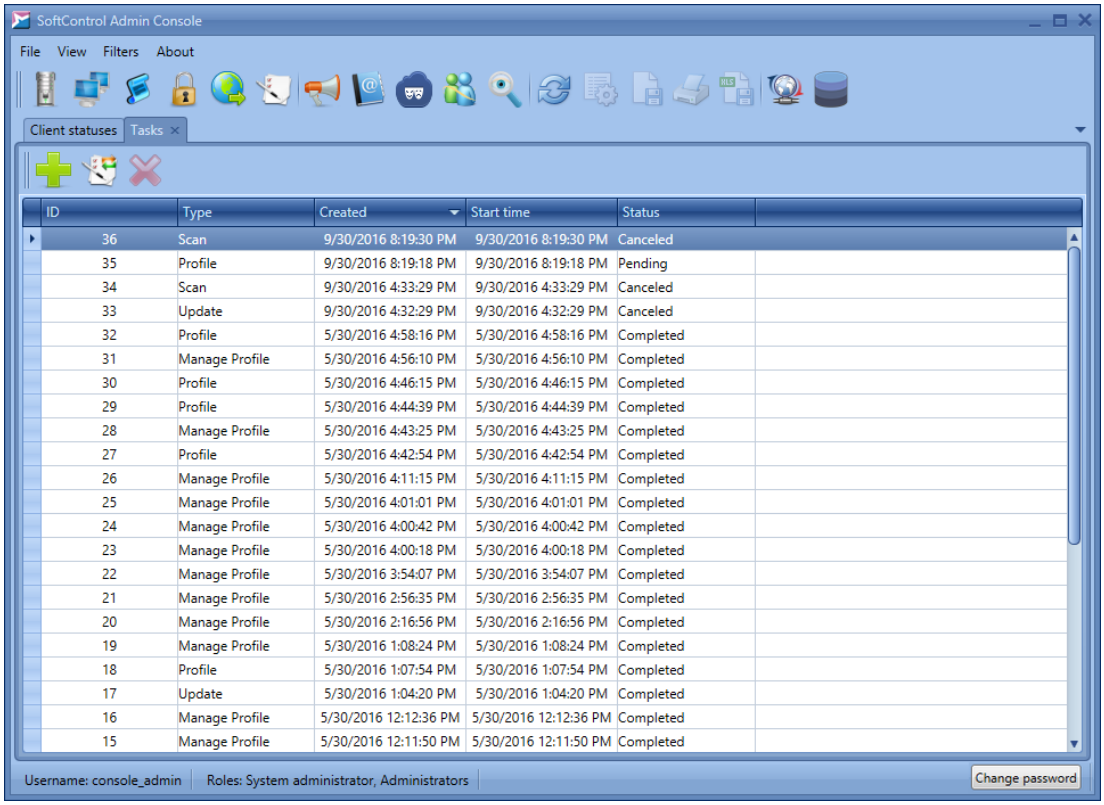

Figure 89. The 'Tasks' tab

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 16.

Table 16. The 'Tasks' tab widgets

Button	Name	Description
	New	Create a new task for the client components.
	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 17.

Table 17. The 'Tasks' tab fields

Field	Description
ID	Task order number.
Type	Task type: • **profile**; • **scan**; • **update**.
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 [93]). Specify the task parameters depending on its type, in the **New task** window (see figures from The 'Task type' section [96] to The 'Clients' section [99] in section Updating [98]).

- profile gathering [96];
- antivirus scanning [97];
- updating [98].

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 [93]);
- 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 [95]). Besides the main information (table 17) and the task parameters, the tab displays the **Status of task on clients** table. Description of its fields is given in table 18.

Table 18. The 'Status of task on clients' table fields

Field	Description
Organization unit	The organization unit which the client component belongs to.
Client name	NetBIOS 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** – client component couldn't started task execution; • **in process** – the task is in execution by the client component; • **process error** – an error occurred during task execution; • **canceled** – the task has been canceled; • **completed** – task execution has been finished; • **complete error** – an error occurred during task completion.
End time	The time of task completion on the client host.

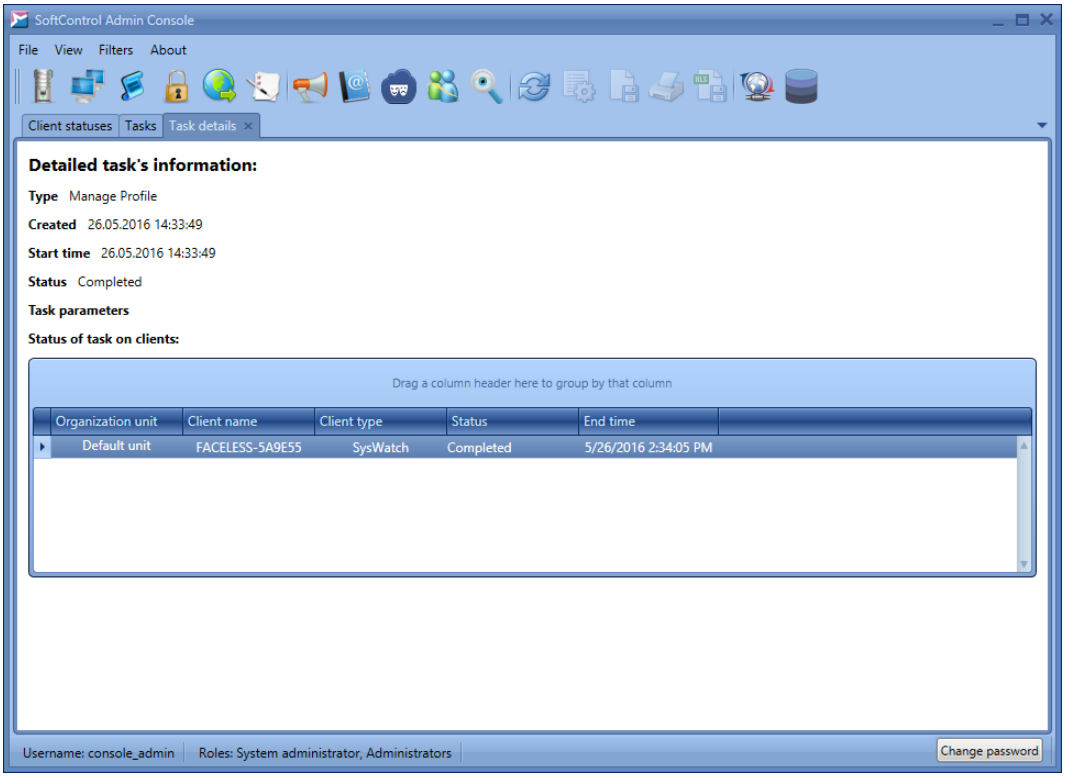

Figure 90. Task execution details

To view the report on the completed operations, go to the **Log** tab and apply filters [112] to the required types of operations.

4.7.1. Profile gathering

1) Select **Profile** from the drop-down list in the **Task type** section and click **Next** (fig. The 'Task type' section 96).

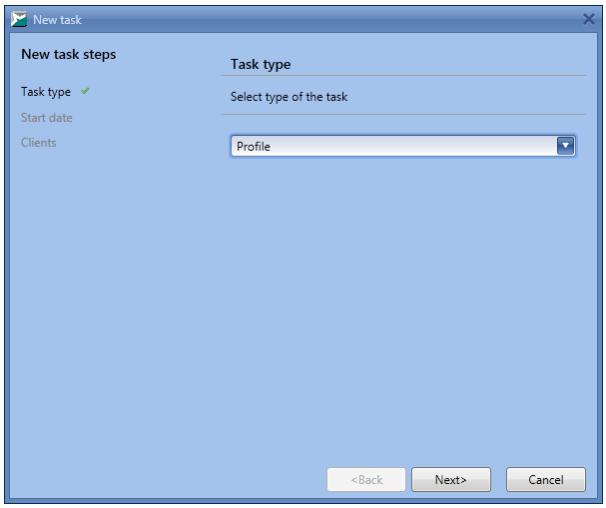

Figure 91. The 'Task type' section

2) Select the **Immediately** option in the **Start date** 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 96). Click **Next** to continue.

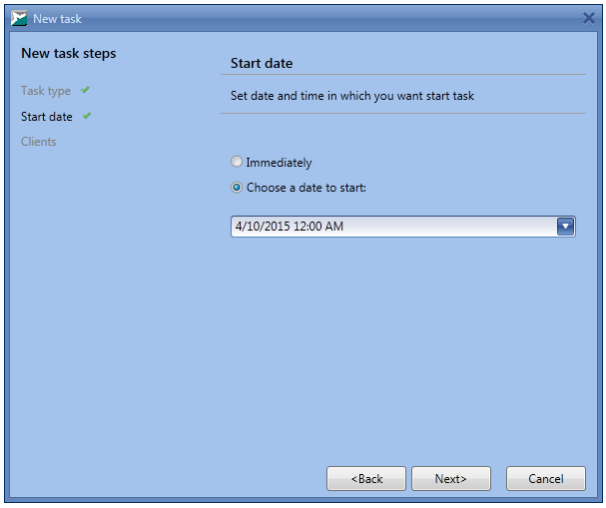

Figure 92. The 'Start date' section

3) In the **Clients** section, tick off the client components which you want to create the task for (fig. The 'Clients' section 96). 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.

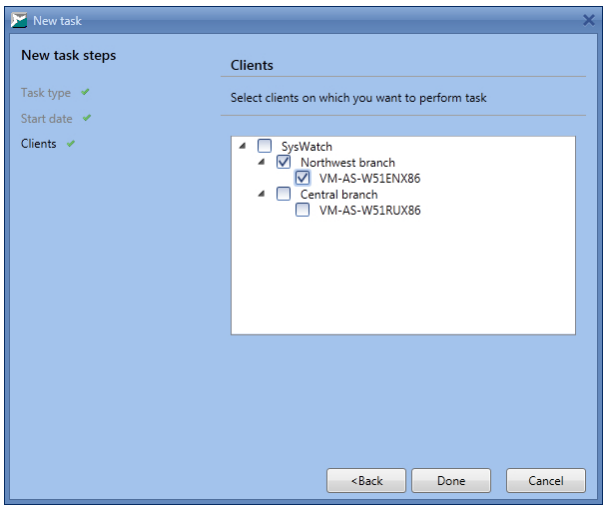

Figure 93. The 'Clients' section

4.7.2. 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 97):

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

Click **Next** to continue.

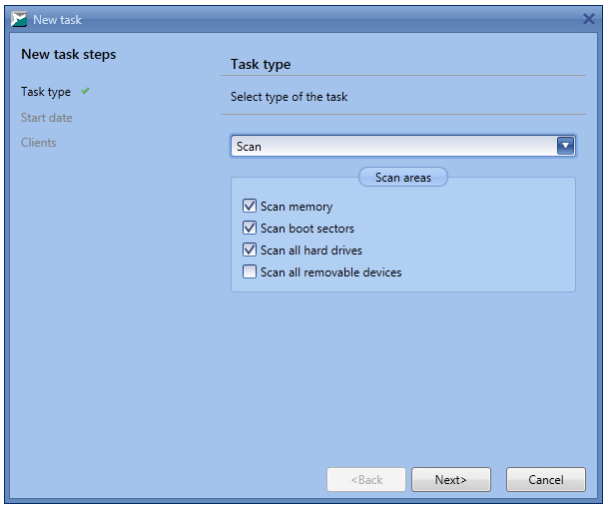

Figure 94. The 'Task type' section

2) Select the **Immediately** option in the **Start date** 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[98]). Click **Next** to continue.

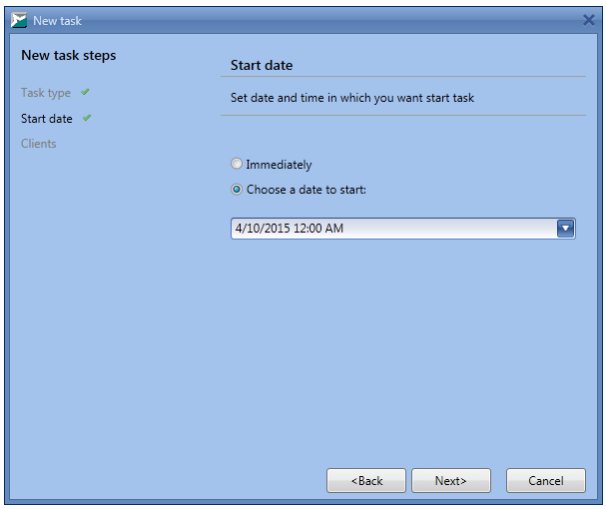

Figure 95. The 'Start date' section

3) In the **Clients** section, tick off the client components which you want to create a task for step (fig. The 'Clients' section[98]).

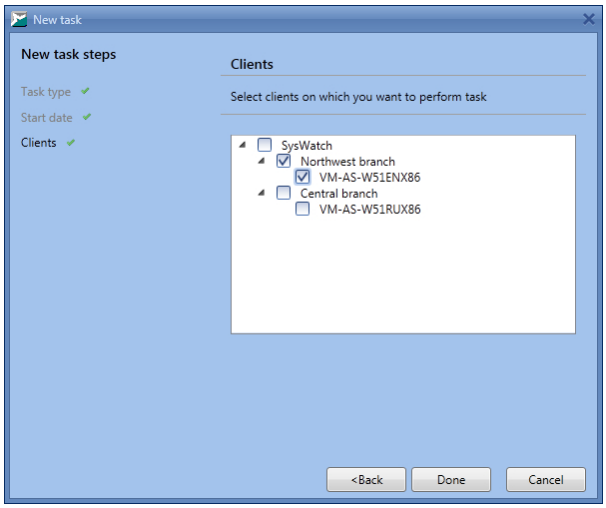

Figure 96. The 'Clients' section

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.

4.7.3. 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[99]):

- ❑ **Program updates**: update SysWatch and DLP 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, which is displayed in the update status of the component in the Client statuses[38] tab and in the update events in logs[100].

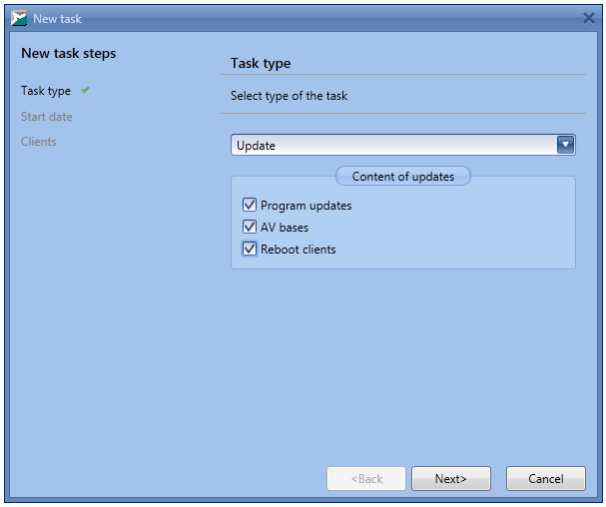

Figure 97. The 'Task type' section

Click **Next** to continue.

2) Select the **Immediately** option in the **Start date** 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[99]). Click **Next** to continue.

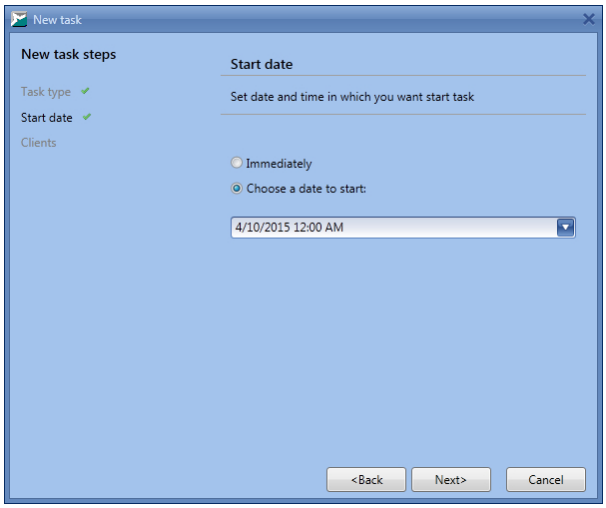

Figure 98. The 'Start date' section

3) In the **Clients** section, tick off the client components which you want to create the task for (fig. The 'Clients' section[99]).

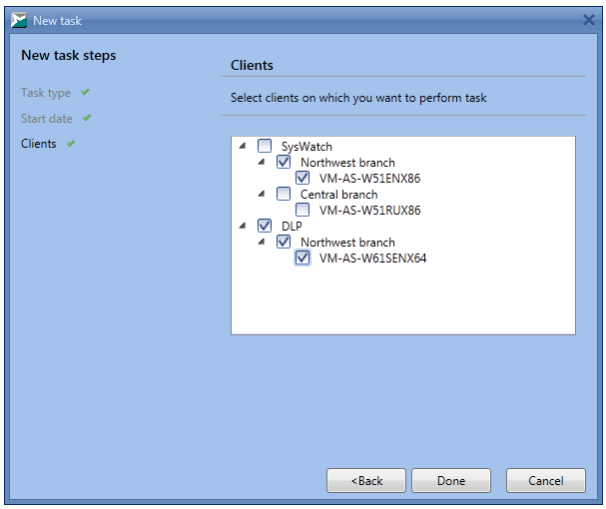

Figure 99. The 'Clients' section

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. Viewing reports

The **Log** tab is designed to view the consolidated reports from the client applications in SoftControl Admin Console. The tab enables tracing the events on several client hosts simultaneously in real time, and sampling the required data with the help of flexible filtering[111]. On the tab, the administrator can access the following data in a convenient format.

- SoftControl SysWatch logs[100];
- SoftControl DLP Client logs[107].

The obtained reports can be printed or exported to a file[115].

4.8.1. SoftControl SysWatch logs

The **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[100]).

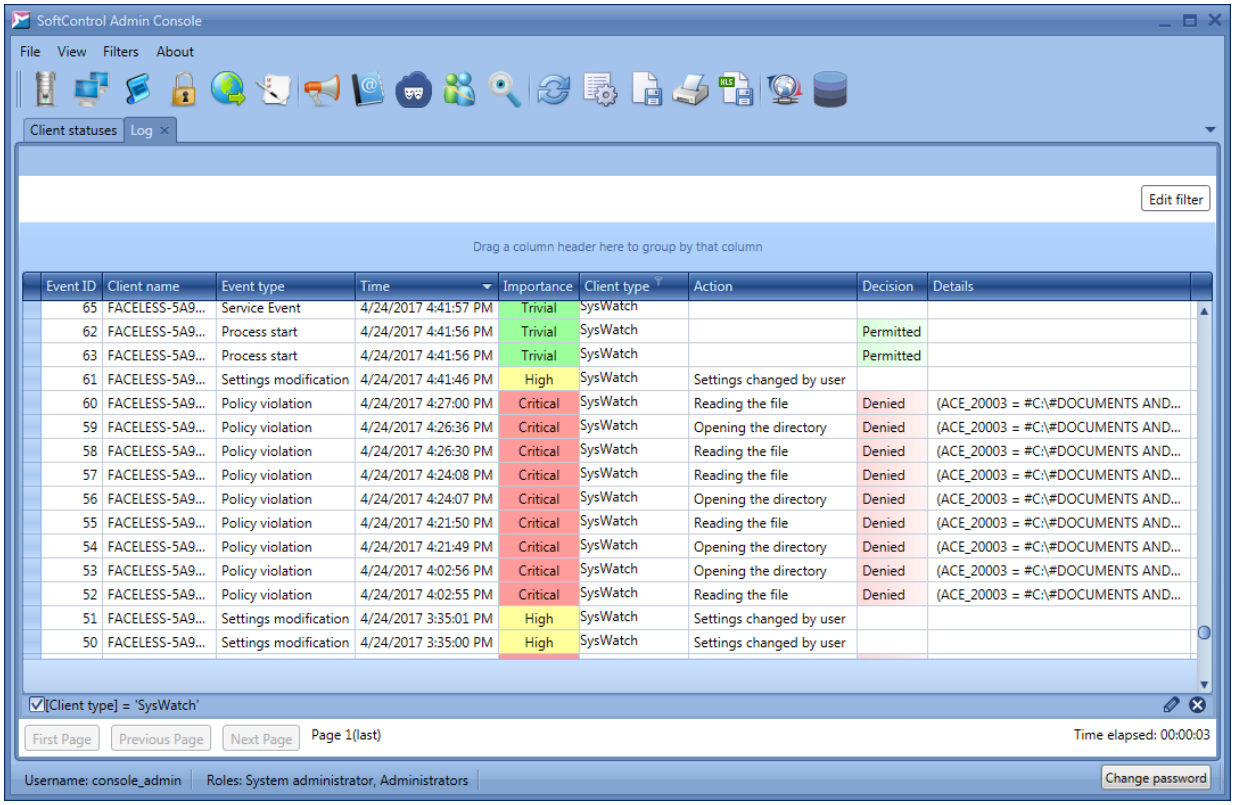

Figure 100. The 'Log' tab for the SoftControl SysWatch component

The full list of the tab fields for the SoftControl SysWatch component is given in table 19.

Table 19. The 'Log' tab fields for SoftControl SysWatch

Field	Description
Client name	NetBIOS 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 150. 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 updating**; • **process launch**; • **virus scan**; • **changing settings**; • **status**; • **user logon**; • **user logoff**.
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

Field	Description
	security: • trivial; • high; • critical. Each priority level has the corresponding cell color.
Action	Action if a policy violation event occurs: • **file read**; • **file change**; • **file rename**; • **file delete**; • **directory open**; • **directory delete**; • **registry key open**; • **registry key create**; • **registry key delete**; • **registry value change**; • **registry value delete**; • **loading of dll module**; • **invalid password entered**. Action if a **process launch** event occurs: • **application launch**; • **signed application launch**; • **unknown application launch**; • **unknown signed application launch**; • **installer launch**; • **signed installer launch**; • **signed installer launch out of `White list`**; • **unknown installer launch**; • **unknown signed installer launch**; • **unknown signed installer launch out of `White list`**. Action if a **virus scan** event occurs: • **scanner launch**; • **building profile begins**; • **scanner finish**; • **building profile done**; • **scan object**. Action if a **client updating** event occurs: • **refresh started**; • **refresh finished**. Action if a **changing settings** event occurs: • **settings changed by user**; • **settings changed by server**.
Action status	Action status if a **virus scan** event occurs: • **scanner launched**; • **scanner launch error**; • **scanner was stopped**; • **success**; • **fail**.

Field	Description
	Action status if a **client updating** event occurs: • **updating started**; • **refresh start error**; • **new updates not found**; • **updating interrupt by user**; • **refreshes successfully installed**; • **need system reboot**; • **refresh finished with errors**.
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 causes the events of the **policy violation** or the **process launch** types.
Command line	– Command that causes the **process launch** type event. – File system/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 launch** or the **changing settings** types has occurred.
Zone	Application execution zone: • **trusted**; • **default**; • **blocked**.
PID	Unique process identifier in the OS for the event of the **process launch** type.
Parent PID	Unique parent process identifier in the OS for the event of the **process launch** type.
Parent process	The name of the parent process for the event of the **process launch** 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:

Field	Description
	• **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.
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 antivirus scanning [97] of the client hosts.

Open the event list on the Log [100] tab for the SoftControl SysWatch component and select an event of the **Virus scan** type with the **Scanner finish** 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 scan 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 [105]).

The full list of the tab fields is given in table 20.

Table 20. 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: • **Clean**; • **Infected**; • **Suspected**; • **Error**; • **Disinfect error**; • **Move error**; • **Delete error**.
Scan action	Action that is performed for the object during the antivirus scanning: • **Disinfected**; • **Moved**; • **Skipped**; • **Deleted**; • **No action**.

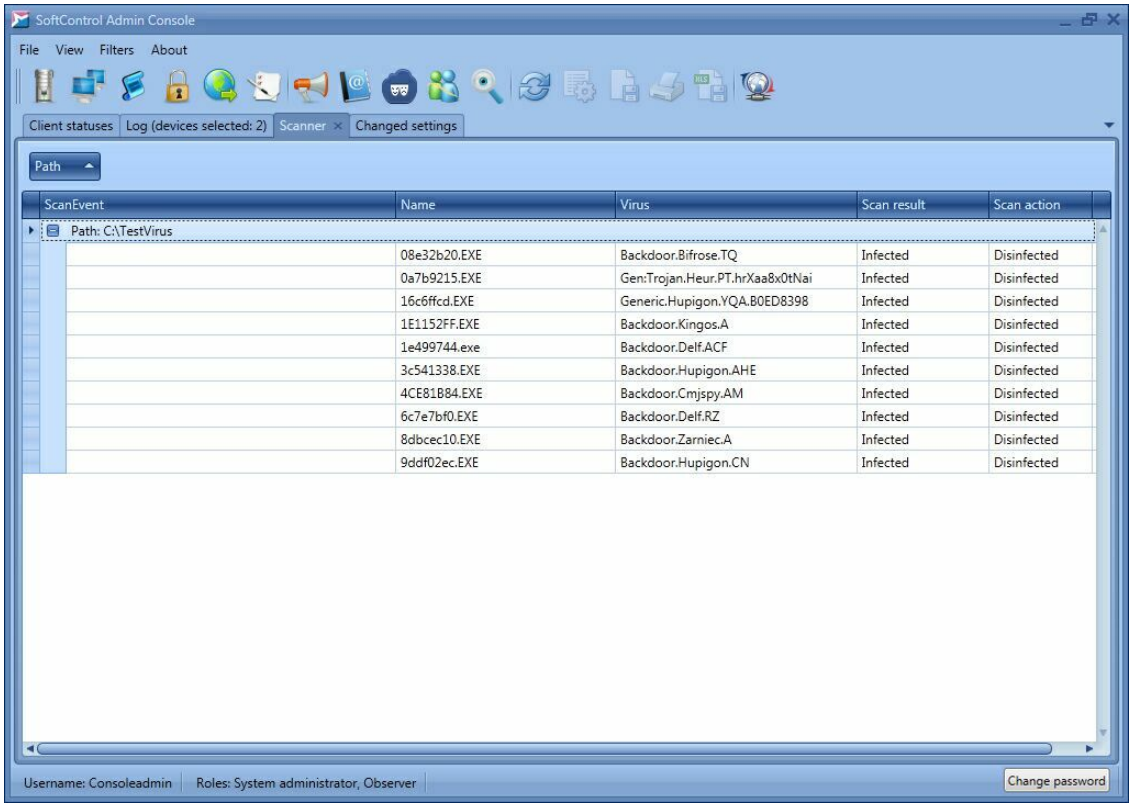

Figure 101. Antivirus check results on the 'Scanner' tab

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 [55];
- by the local user with the help of:
  – the program GUI;
  – the configuration file.

Open the list of events on the **Log** tab for the SoftControl SysWatch component and select an event of the **Changing settings** 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 changing settings event** command.

The displayed **Changed settings** tab contains the list of the SoftControl SysWatch settings and their new status (fig. The 'Changed settings' tab [106]).

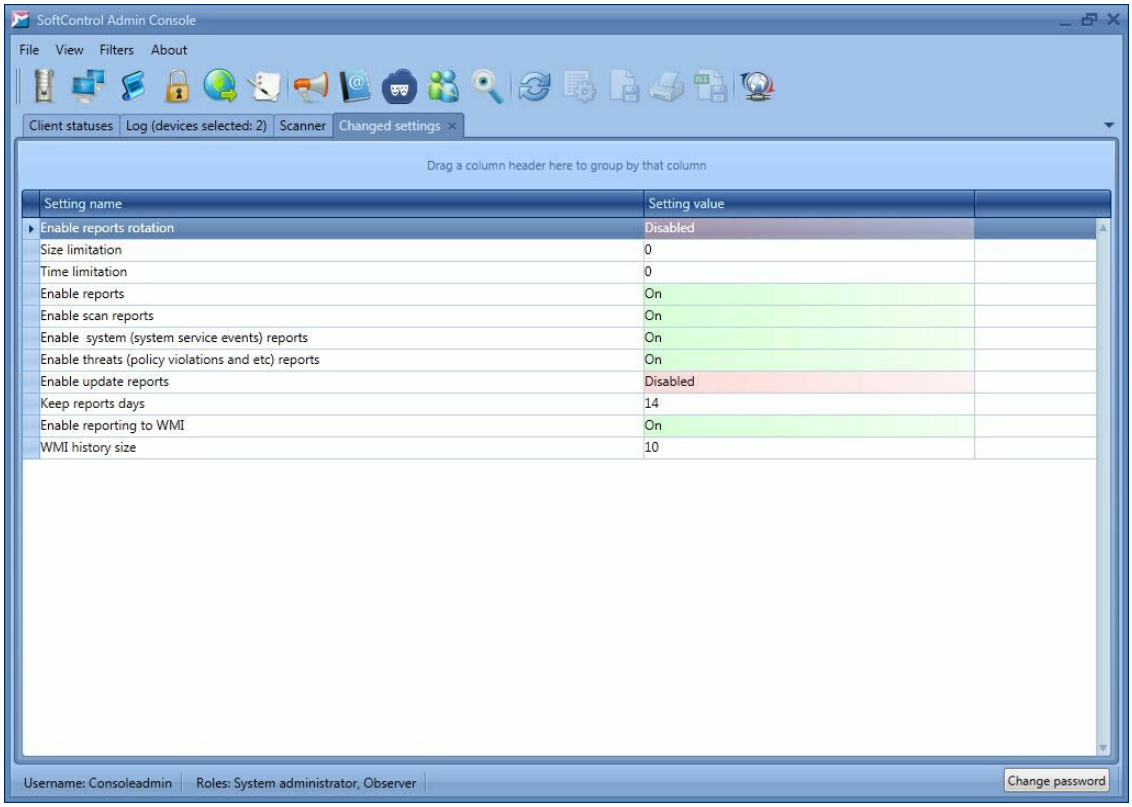

Figure 102. The 'Changed settings' tab

The full list of the tab fields is given in table 21.

Table 21. 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.

4.8.2. SoftControl DLP Client logs

The **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 107).

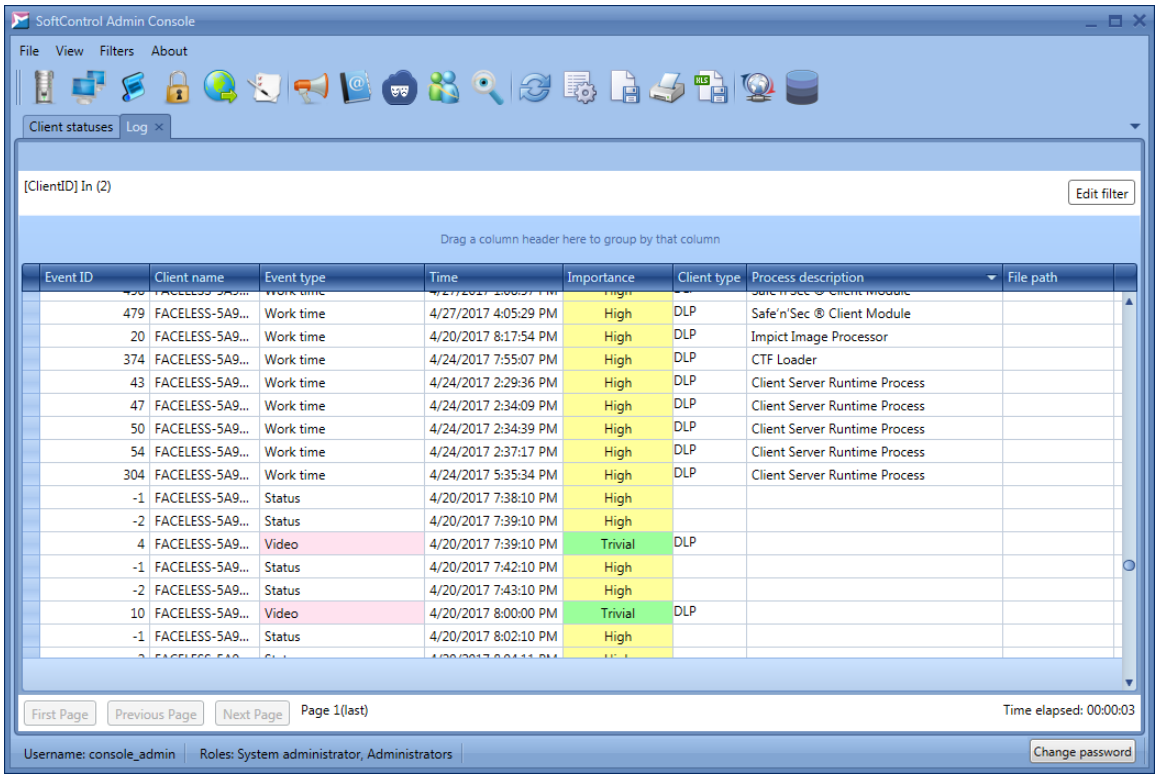

Figure 103. The 'Log' tab for the SoftControl DLP Client component

The full list of the tab fields for the SoftControl DLP Client component is given in table 22.

Table 22. The 'Log' tab fields for SoftControl DLP Client

Field	Description
Client name	NetBIOS 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 150. 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.

Field	Description
Event type	Type of the data collection event: • **hardware added**; • **attach**; • **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. 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 causes the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, **printer**, **attach** types.
Process description	Description of the process that causes the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, **printer**, **attach** types.
User name	User account that is used to run the process that causes the event of the **file**, **registry**, **HTTP**, **keylogger**, **work time**, **printer**, **attach** 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**, **HTTP** types.
Attachment path	The path to the attached file in the Microsoft® Outlook® 2003 mail client, for the event of the **attach** type.
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**.

Field	Description
Registry path	The path to the monitored registry key or registry key value, for the event of the **registry** type.
Key logger time	The date when the keyboard input has been recorded, for the event of the **keylogger** type.
Key logger 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).

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 109).

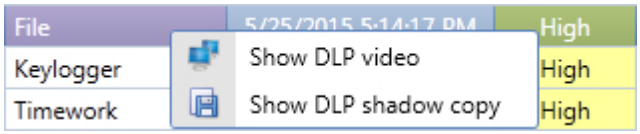

Figure 104. Context menu of the event with additional data

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 109).

Click **Load** in the displayed video player window and manage the playback with the help buttons (fig. SoftControl DLP Client video player 110) that are described in table 23.

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[168].

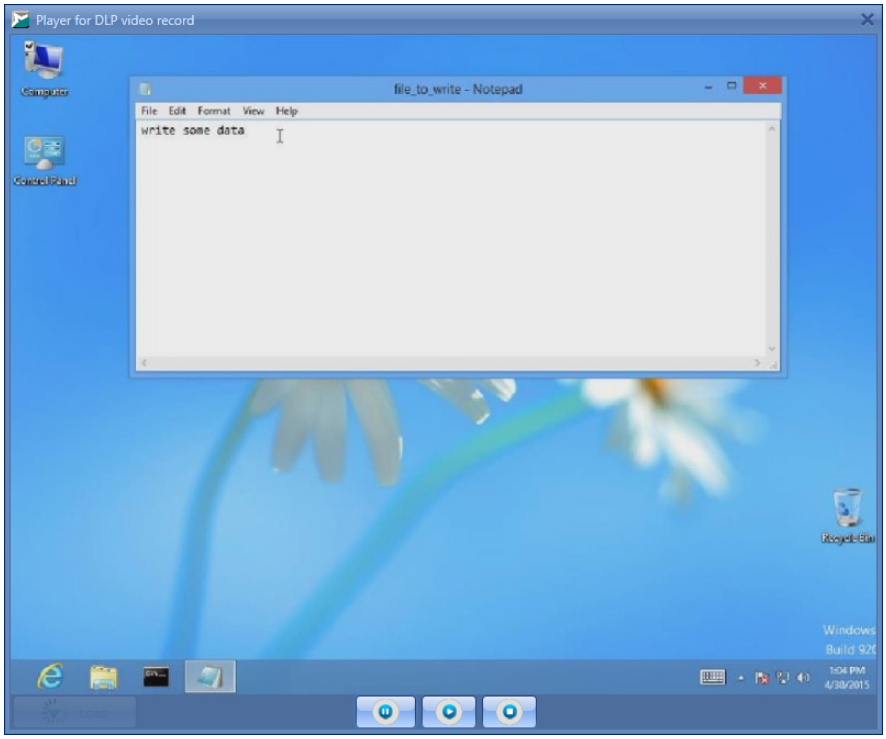

Figure 105. SoftControl DLP Client video player

Table 23. 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[109]) and click **Open** in the displayed **Preview DLP shadow copy** window to view the saved copy of the specified object under observation (fig. Shadow copy of the monitored object[110]).

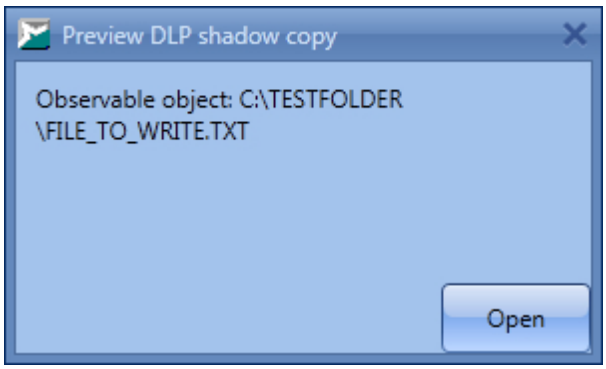

Figure 106. Shadow copy of the monitored object

4.8.3. Filtering the events

Page representation

Information on the **Log** tab is displayed page by page. The maximum number of events per page is specified in the SoftControl Admin Console interface settings[27] (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 inchronological order, i.e. the page with the largest number corresponds the last chunk of events. When you open the **Log** tab, the first page loads. To navigate between pages, use the corresponding buttons in the lower part of the tab (fig. Page navigation[111]). You can only switch to the previous/next page.

Figure 107. Page navigation

Data grouping

For the convenience, information on the **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[107] to Shadow copy of the monitored object[110] in section above[107]). 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 Launch**;
- **Virus Scan**;
- **Changing settings**;
- **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**;
- **Attach**;
- **File**;
- **HTTP**;
- **Keylogger**;
- **Printer**;
- **Registry**;
- **Hardware removed**;
- **Work time**.

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.

Filtering by user 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 113) 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.

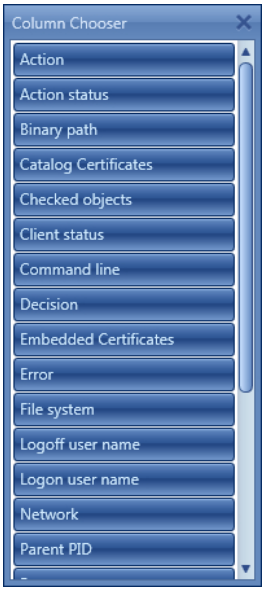

Figure 108. Choosing the columns

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 113).

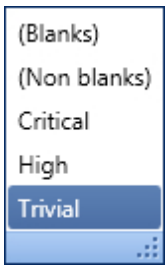

Figure 109. Filter by field

You can filter the selection by several fields simultaneously. The key icon is displayed permanently in the filtered field headers.

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.

To open the editor, click **Edit Filter** on the right-hand part of the string with the parameters. The editor window is shown in fig. Filter editor 114.

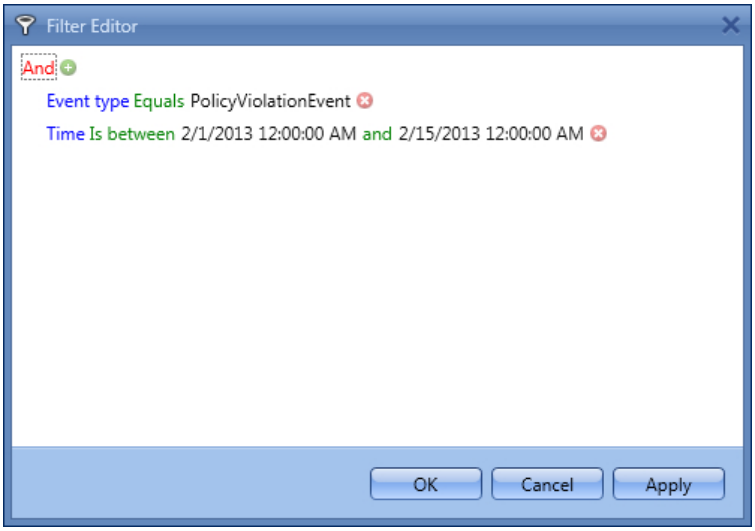

Figure 110. Filter editor

The first string of the editor 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, select the **Add Condition** menu item or click the plus icon near the logical operation. To add a filter parameter that contains several parameters with the same logical operator, select the **Add Group** menu item. Working with group elements is similar to working with the elements of the common list. You can create nested groups. To clear the filter, select the **Clear All** menu item. 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 115).

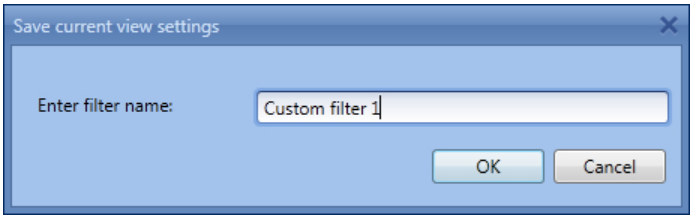

Figure 111. Saving the filter

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.

4.8.4. 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 111 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 116).

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[111] and click **Export to Excel**. Specify the path to save the report and the report name in the dialog box and click **Save**.

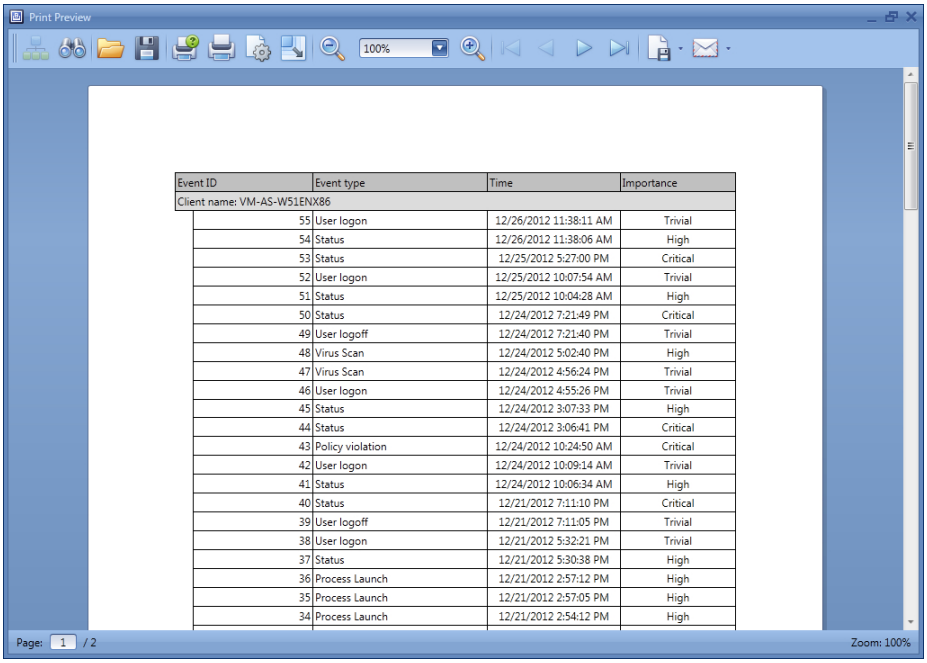

Figure 112. Print preview

4.9. 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 is not at a standard workstation with the installed SoftControl Admin Console.

First of all, you need to specify the contacts[116] of the notification recipients; then you should set up notification sending parameters[118].

4.9.1. Contacts

You can specify the recipients of notifications on the **Contacts** tab (fig. The 'Contacts' tab[117]).

Basic operations with the contacts are performed via the tab's graphical buttons that are described in table 24.

Table 24. The 'Contacts' tab widgets

Button	Name	Description
	New	Create a new contact.
	Edit	Modify the properties of the selected contact.

Button	Name	Description
	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 25.

Table 25. 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.

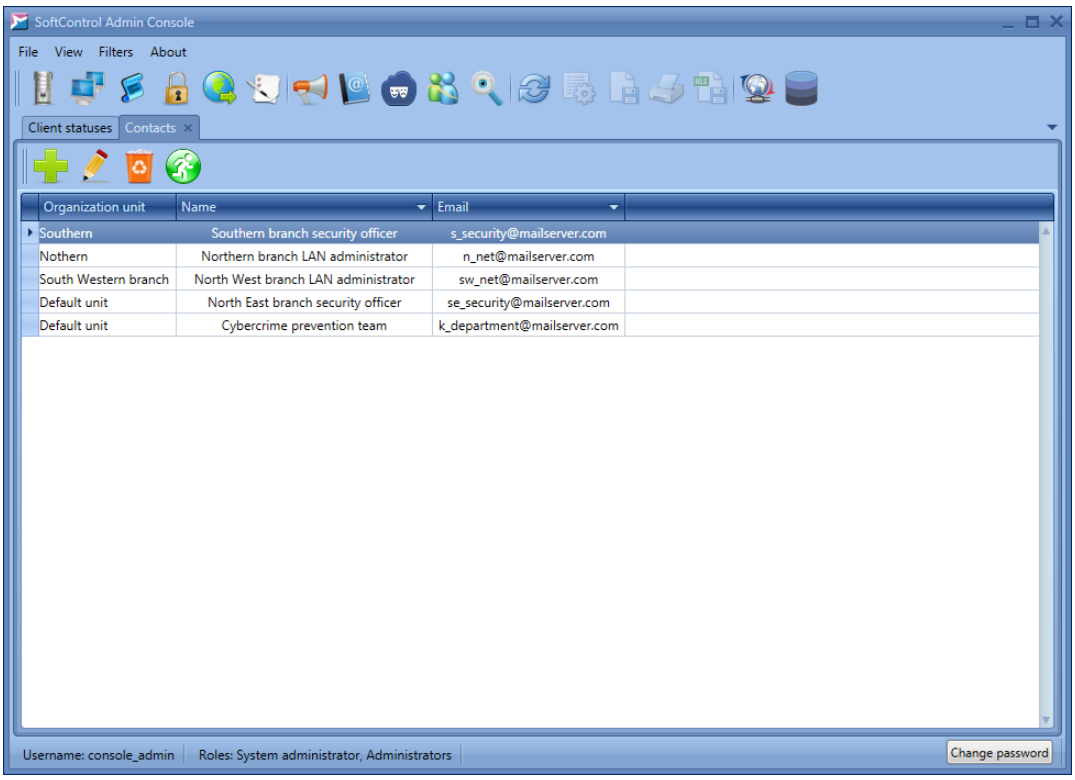

Figure 113. The 'Contacts' tab

To add a new recipient, click **New** (fig. The 'Contacts' tab 117). Specify the recipient data in the **Contact Name** and **Email fields** and then click **Apply** (fig. Adding a contact 117).

To modify and remove contacts, use the corresponding buttons.

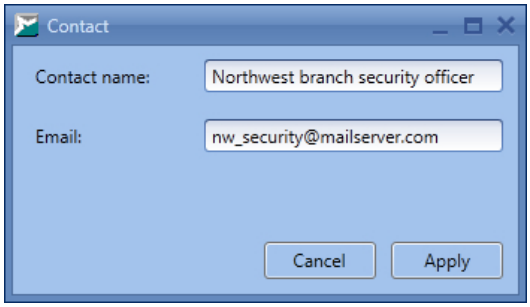

Figure 114. Adding a contact

4.9.2. Setting up notifications

The Notifications tab is designed to set up the options of sending event notifications via email (fig. The 'Notifications' tab 118).

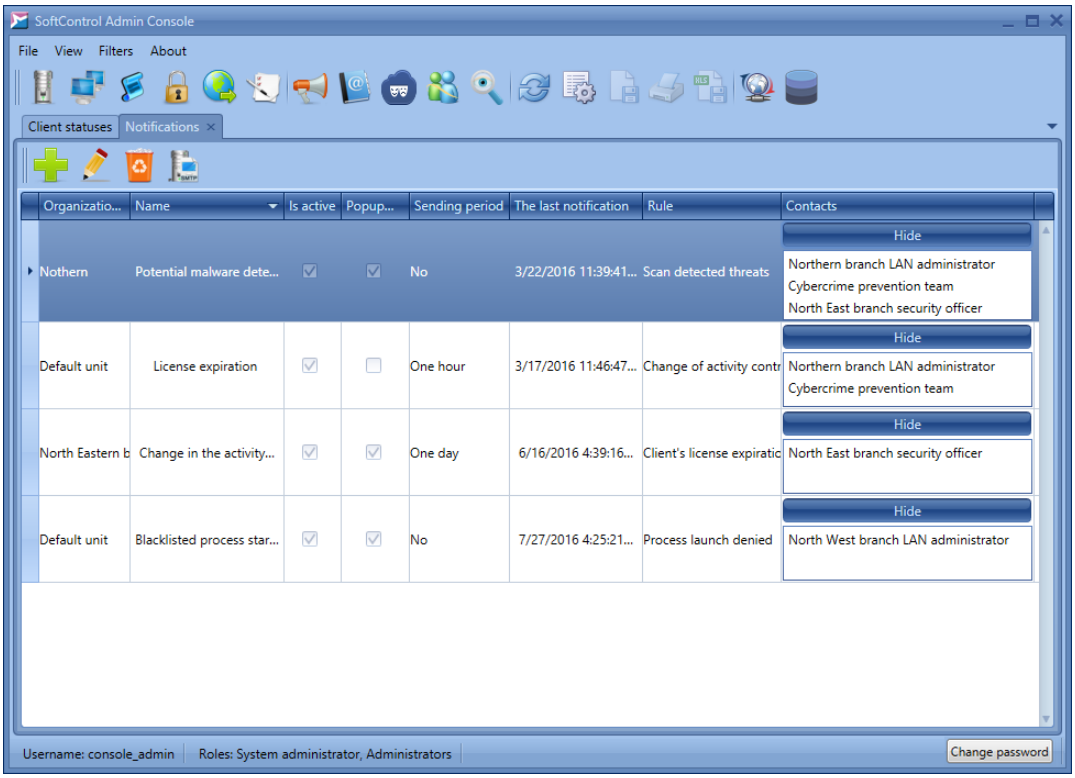

Figure 115. The 'Notifications' tab

Basic operations with the notifications are performed via the tab's graphical buttons that are described in table 26.

Table 26. 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	Set up the SMTP server.

The list of the tab fields is given in table 27.

Table 27. The 'Notifications' tab fields

Field	Description
Organization unit	The organization unit that the notification belongs to.
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 118).

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 119). 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 letter**.

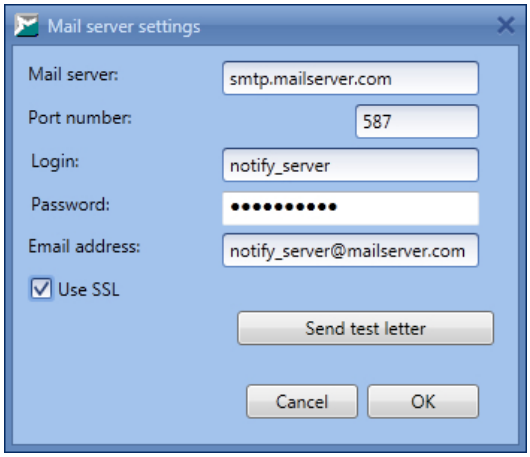

Figure 116. Mail server settings

Click **OK** to apply settings.

Creating a notification

To add a new notification, click **New** (fig. The 'Notifications' tab 118).

Specify the notification **Name** on the **General** tab of the displayed window, select minimum **Sending period** in the drop-down list, enter the **Theme** of the message and tick off the **Is active** checkbox (fig. General notification parameters 120).

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 120).

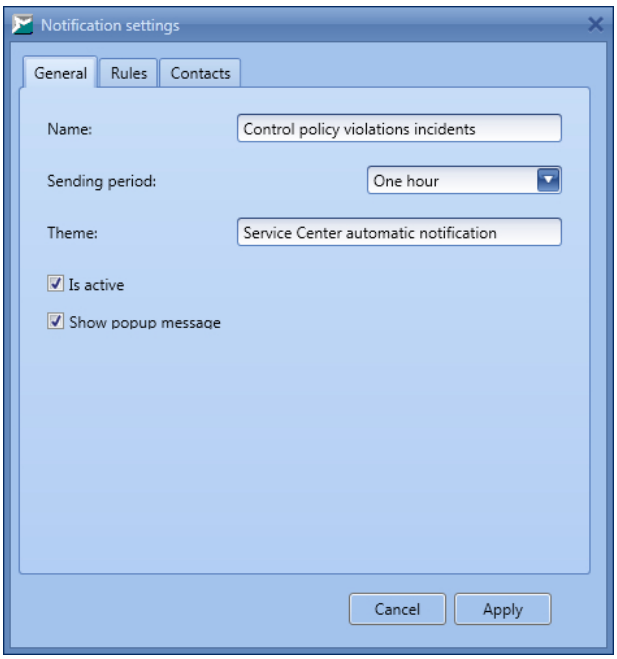

Figure 117. General notification parameters

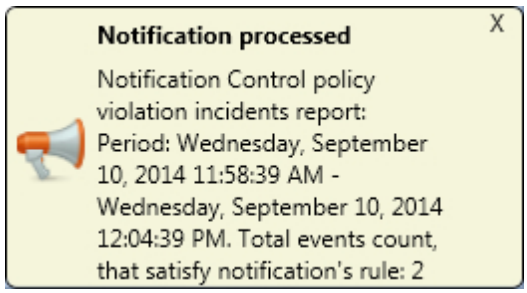

Figure 118. Pop-up message

On the **Rule** tab, select the condition that triggers the notification (fig. Conditions that trigger notification 121):

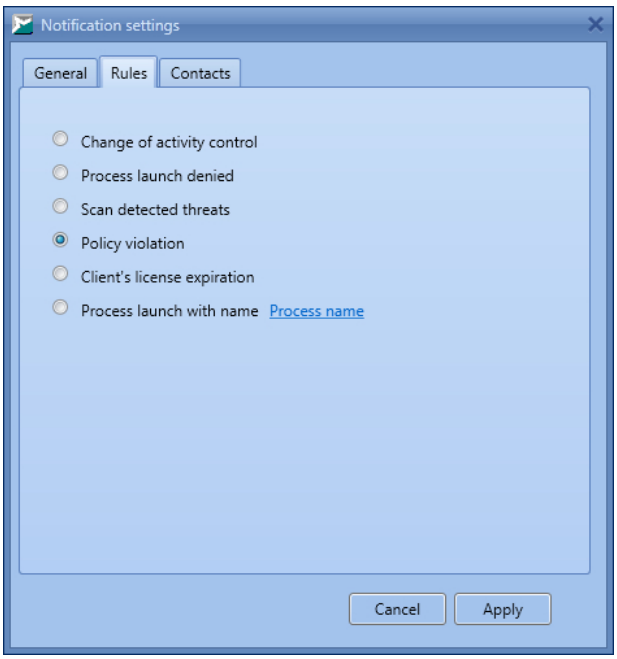

Figure 119. Conditions that trigger notification

- **Change of activity control**:

the SoftControl SysWatch activity control status for any area has changed.

- **Process launch denied**:

SoftControl SysWatch has registered the event of the 'process launch' type with the 'denied' decision.

- **Scan detected threats**:

SoftControl SysWatch has detected malicious code during antivirus check.

- **Policy violation**:

SoftControl SysWatch has detected the event of the 'policy violation' type.

- **Client's license expiration**:

a client component's license key expires in less than 10 days.

We strongly recommend that you set the **Sending period** parameter for this notification to at least 4 hours.

- **Process launch with name**:

  SoftControl SysWatch has registered the event of the 'process launch' type, with the specified **Process name**.

Switch to the **Contacts** tab and select the notification recipients (fig. Selecting notification recipients 122).

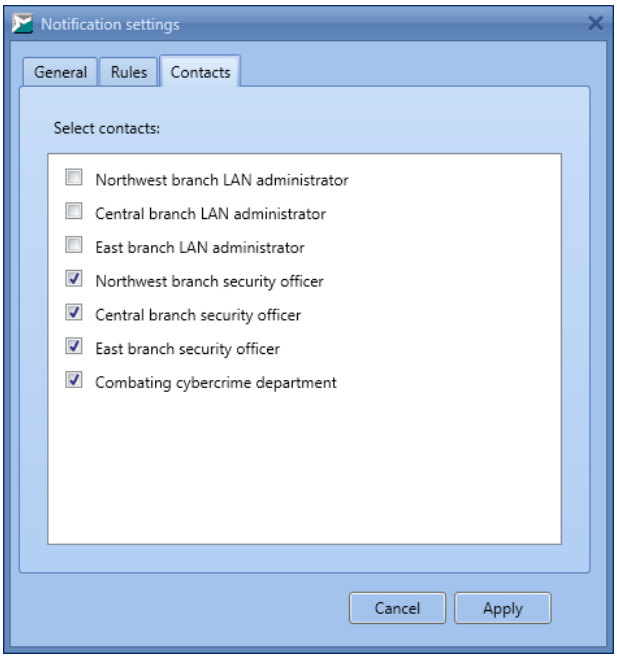

Figure 120. Selecting notification recipients

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 118);
- double-click the notification.

In the the displayed window, modify the required parameters, as you do with a new configuration (fig. General notification parameters 120, Conditions that trigger notification 121, Selecting notification recipients 122).

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 120).

To remove a notification, select it, press **Delete** (fig. The 'Notifications' tab 118) and confirm the removal in the dialog box.

4.10. 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.

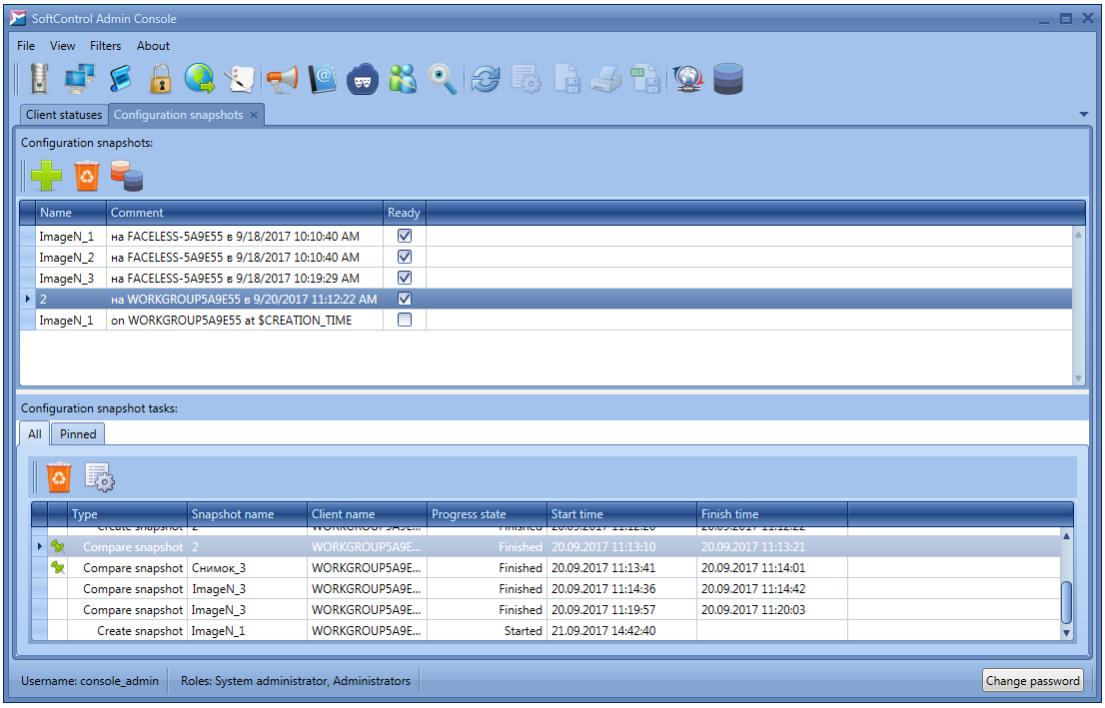

Figure 121. 'Configuration snapshots' tab

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 124;

- snapshot tasks[126].

4.10.1. Snapshots

Basic operations with the snapshots in the **Configuration snapshots** section are performed via the tab graphical buttons which are described in table 28.

Table 28. The 'Configuration snapshots' section widgets

Button	Name	Description
	Create 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 29.

Table 29. The 'Configuration snapshots' section fields

Field	Description
Name	The name of the task.
Comment	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  (**Create new**) (fig. 'Configuration snapshots' tab[123]). In the displayed window, specify the name of the snapshot, select a client host to snapshot and click **Apply** (fig. Creating a snapshot[124]). The snapshot creation task is then generated, and the corresponding entry appears in the table[127] in the **Configuration snapshot tasks** section.

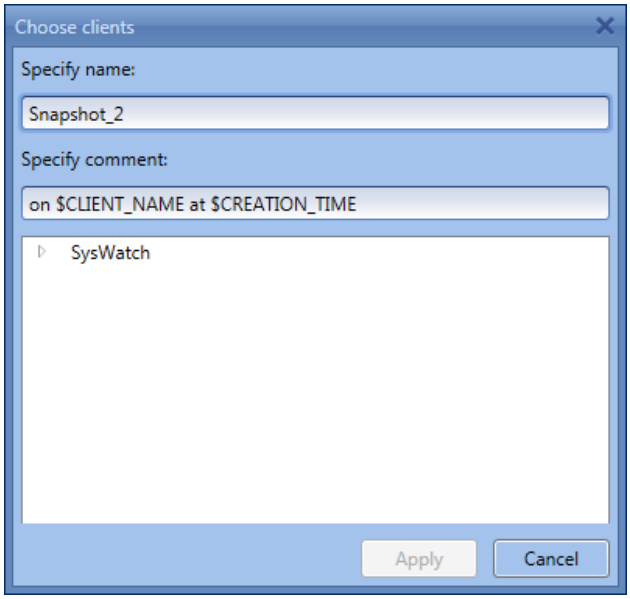

Figure 122. Creating a snapshot

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 **Configuration snapshot tasks** section (see below[127]) is **Started**. After the client host responds, the snapshot is marked as **Ready** (the corresponding column in the table[124] 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[123]). In the displayed window, select the client host (or several client hosts) and click **Apply** (fig. Selecting client hosts to compare[125]). If you select several client hosts to compare, a comparison task is created for each of them.

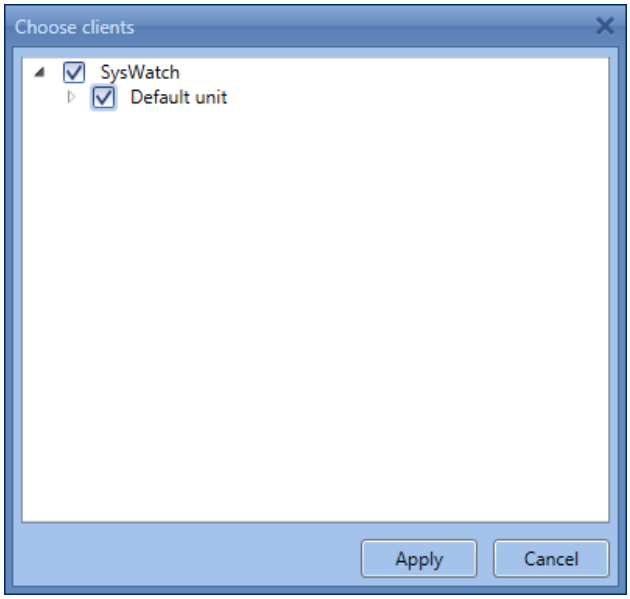

Figure 123. Selecting client hosts to compare

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 123) 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.

4.10.2. Snapshot tasks

The **Configuration snapshot tasks** section 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 30.

Table 30. The 'Configuration 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 31.

Table 31. The 'Configuration 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 **Configuration snapshots**.
Client name	The name of the client host.
Progress state	Task status: **Started**, **Finished**.
Start time	Date and time when the task was started.
Finish time	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 127). SoftControl Admin Console deletes the tasks that are not pinned 180 days after they are completed.

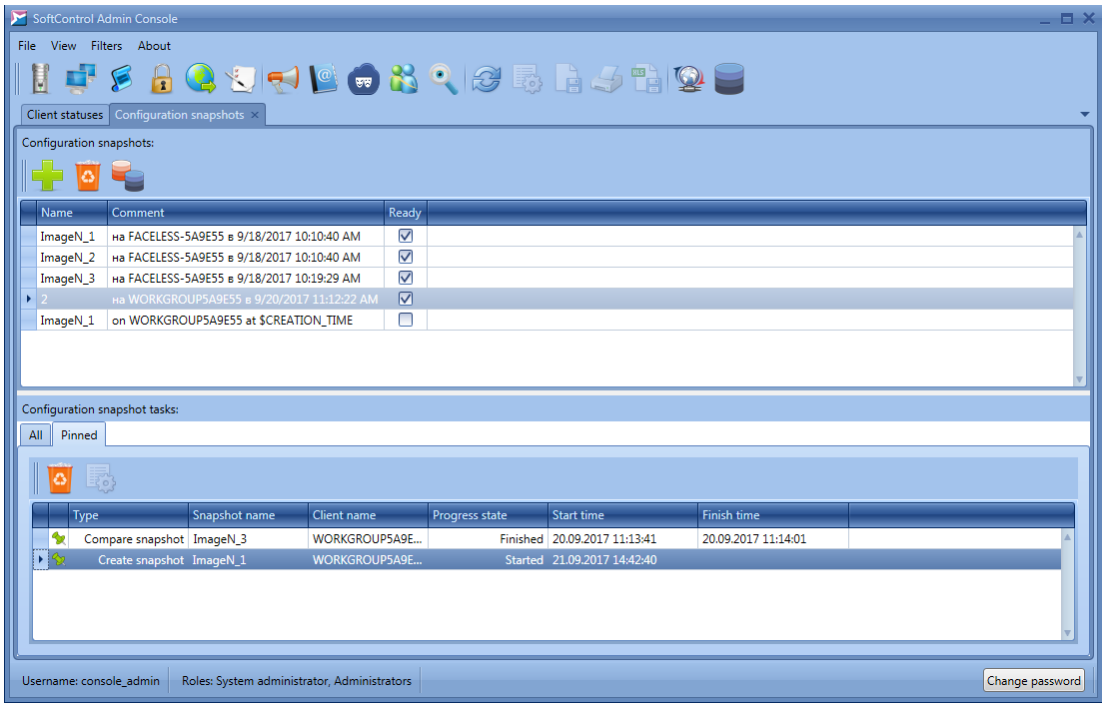

Figure 124. Pinned tasks

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 **Comparison results** tab that contains two fields, **Gone items** and **Appeared items** (fig. Comparing snapshots 127).

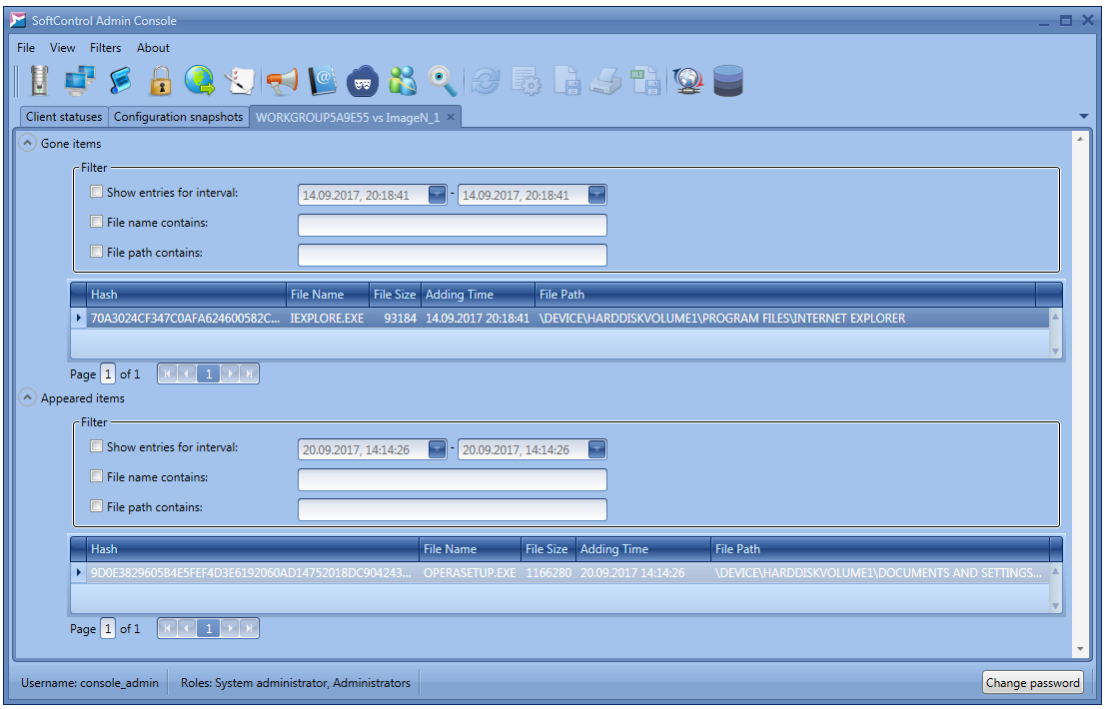

Figure 125. Comparing snapshots

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.

5. Updating ISS components

SoftControl Service Center allows centralized updates for all the system components from an automatically deployed local server. The **Updates** tab allows setting up and viewing the update history (fig. The 'Updates' tab for program modules 129, The 'Updates' tab for antivirus bases 133).

The upper part of the tab contains two categories of settings to update the corresponding components:

- Program modules 129;
- Antivirus bases 133.

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 32.

Table 32. Fields of the update history list

Field	Description
Last check date	Date and time of the last check for updates.
Last update data	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 relay of the SoftControl SysWatch and SoftControl DLP Client client components' modules, from the external (Internet) servers (fig. The 'Updates' tab for program modules 129).

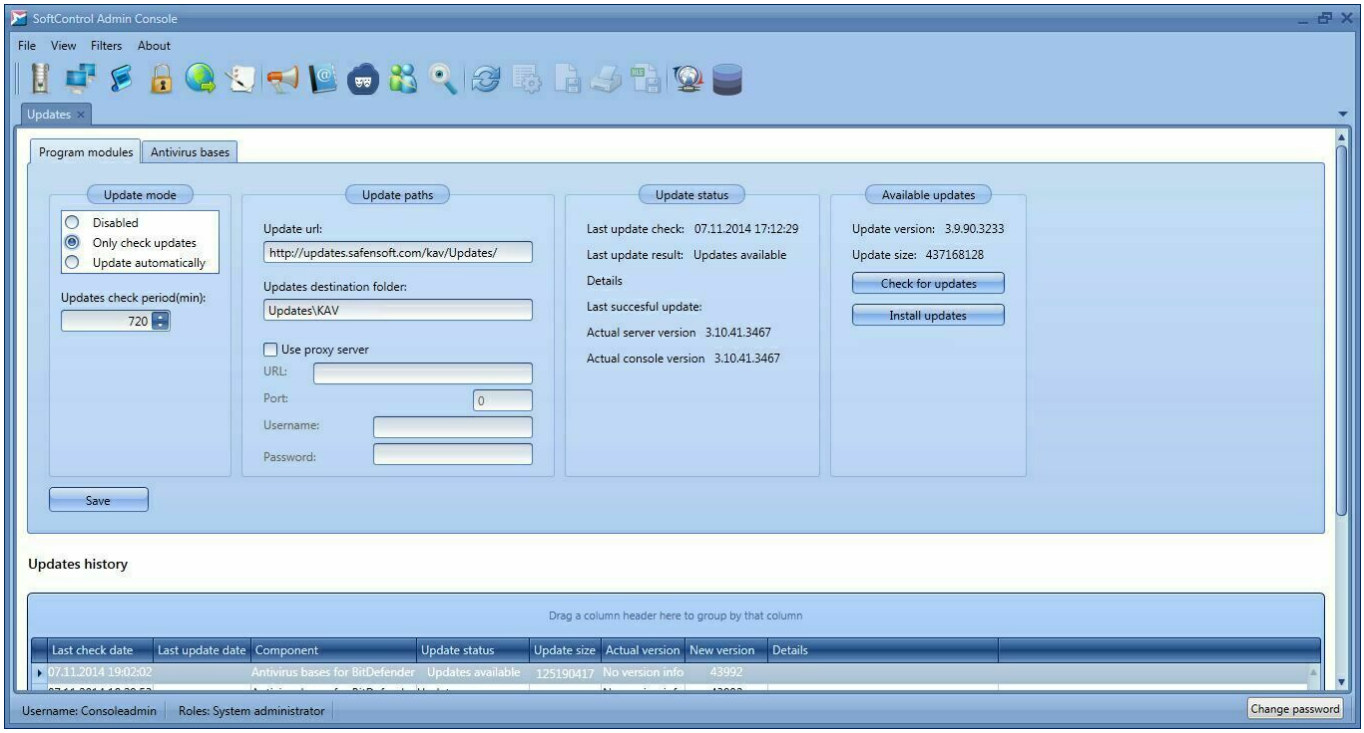

Figure 126. The 'Updates' tab for program modules

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 **Updates check period(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 **Updates check period(min.)** counter and relays 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 [137] 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 [135] 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.

- **Updates destination folder**:

  The path to save the update packages from the external servers, relative to the following directory: `C:\ProgramData\SoftControl`.

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 NetBIOS 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, relay 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, relay 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 relay of SoftControl SysWatch antivirus bases from the external (Internet) servers (fig. The 'Updates' tab for antivirus bases 133).

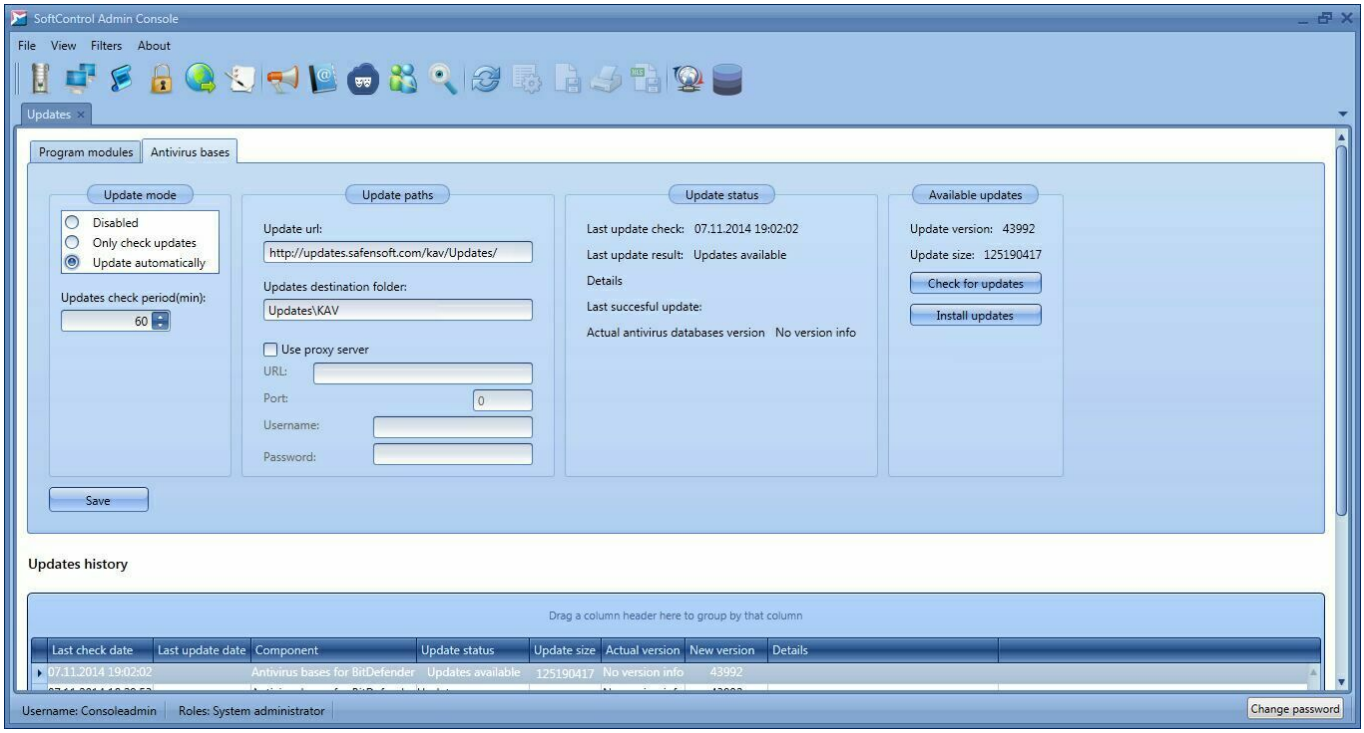

Figure 127. The 'Updates' tab for antivirus bases

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 **Updates check period(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 **Updates check period(min.)** counter and relays 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 137, 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 33.

  Table 33. URLs to update the anti-virus bases

Name	URL	Destination folder
Kaspersky antivirus bases	http://updates.safensoft.com/kav/<license_number>	Updates\KAV
Avira antivirus bases	http://updates.safensoft.com/av4/<license_number>	Updates\AV4

  Note. You should specify your license number manually.

- **Updates 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 33.

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 NetBIOS 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** (except for Kaspersky Antivirus bases):
  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, relay the antivirus bases from the external servers.

By default, trial license key for the Kaspersky Antivirus bases is included in SoftControl Service Center. After the trial key expires, you cannot update Kaspersky Antivirus bases. Therefore, you should buy a commercial KAV license and place the received license file with the *.key* extension to the following folder on the computer with installed SoftControl Server:

```
<SoftControl Server installation folder>\Tools\Updates\Plugins\KAV\
```

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 135).

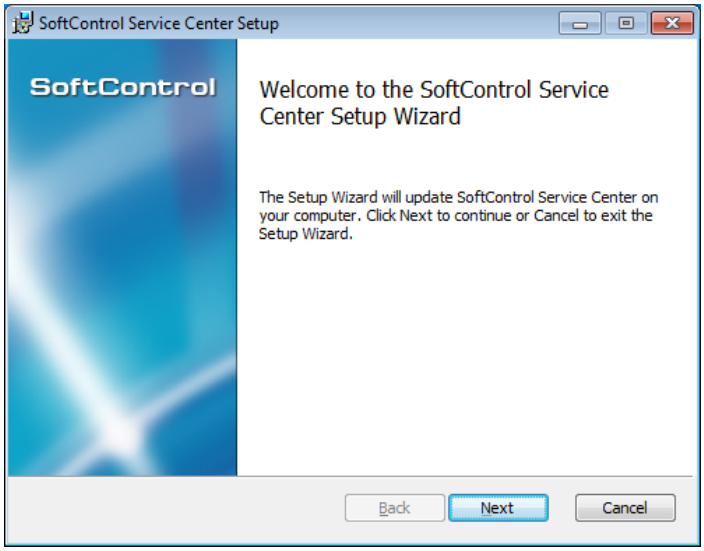

Figure 128. Running the update

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement[136]).

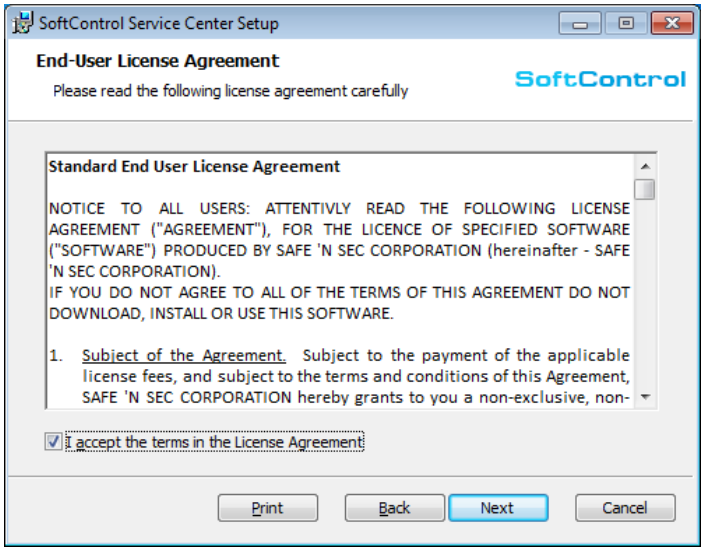

Figure 129. License agreement

4) Click **Update** (fig. Ready to update[136]).

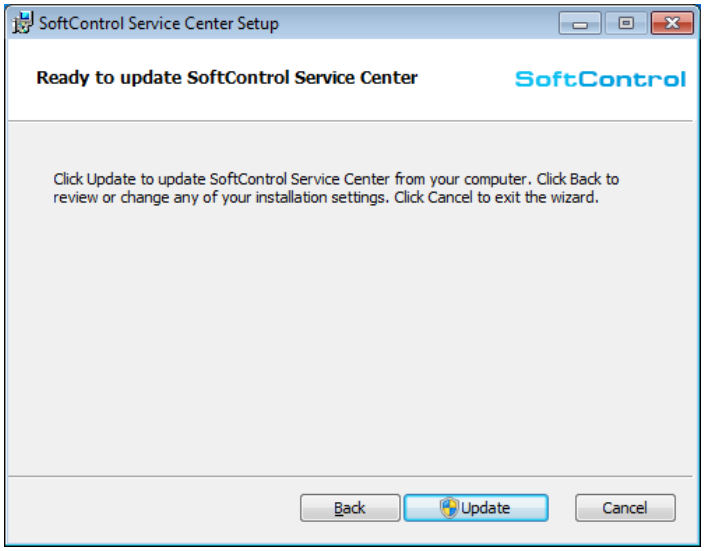

Figure 130. Ready to update

5) Wait until the update completes (fig. Updating progress[136]).

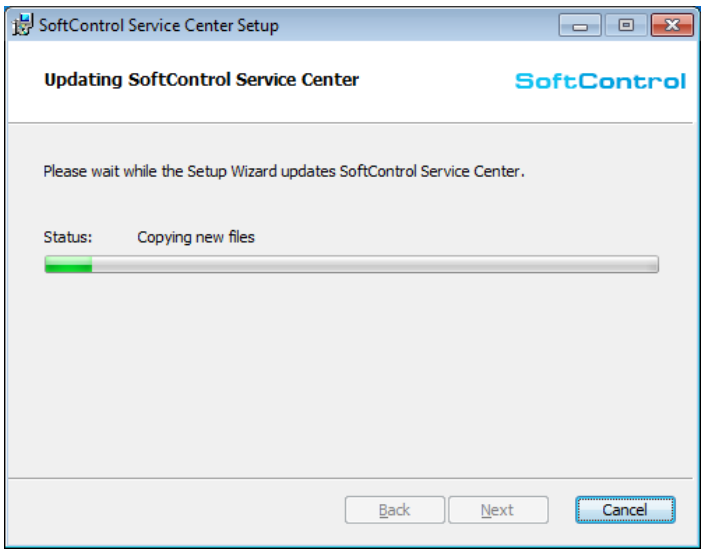

Figure 131. Updating progress

6) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Finishing the update [137]).

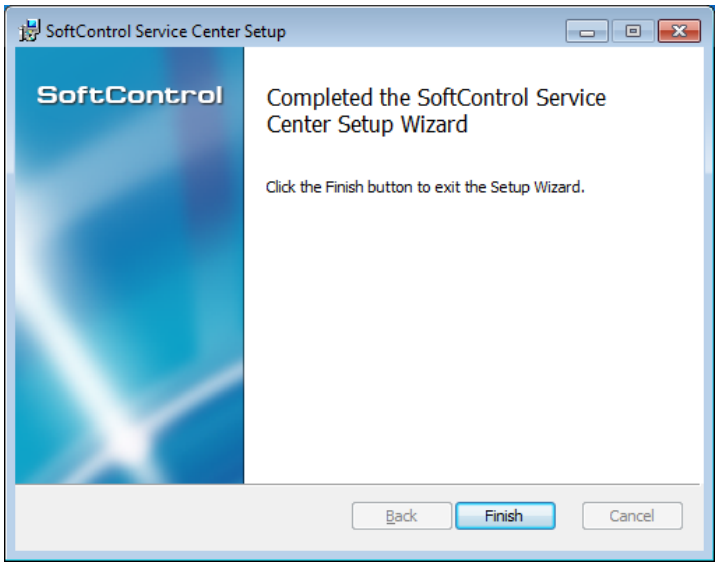

Figure 132. Finishing the update

5.4. Updating client components

After relaying 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 and SoftControl DLP Client automatically switch to the updates through the Service Center. The components are updated on demand by creating the corresponding task [98], or on schedule if the latter is set up for SoftControl SysWatch [63] / SoftControl DLP Client [91].

❑ When offline, %SW%> 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 34. Server connection port is *8088* by default. After the above-mentioned settings are applied, you can run the update on demand through GUI.

Table 34. Addresses for update from SoftControl Service Center

Component	Description	Address
Core	Program modules	http://<server IP address>:<server connection port>/api/updates/SNS
AV_KAV	Kaspersky Antivirus bases	http://<server IP address>:<server connection port>>/api/updates/KAV
AV-AV4	Avira Antivirus bases	http://<server IP address>:<server connection port>/api/updates/AV4

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 139).

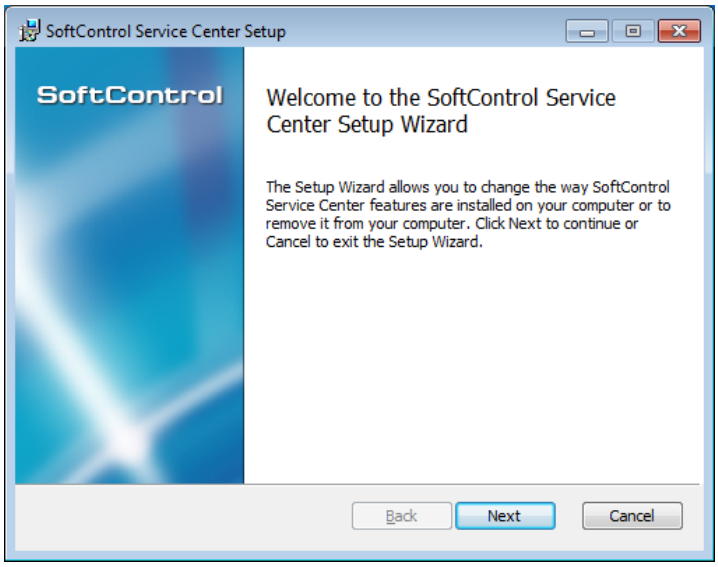

Figure 133. Running uninstallation

3) Click **Change** (fig. Types of operations 139).
4) Select the component to remove (fig. Selecting components to remove 140): click the icon of the component and select the **Entire feature will be unavailable** option from the drop-down menu (fig. Component installation options 140). Click **Next** when all settings are specified.

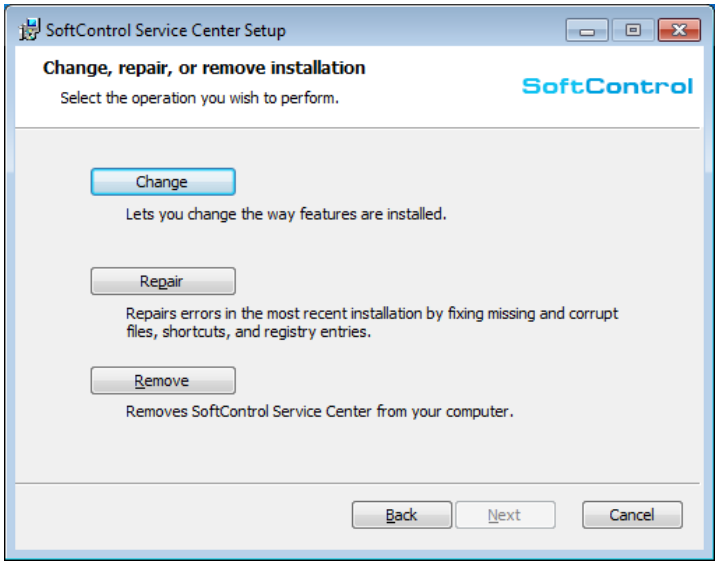

Figure 134. Types of operations

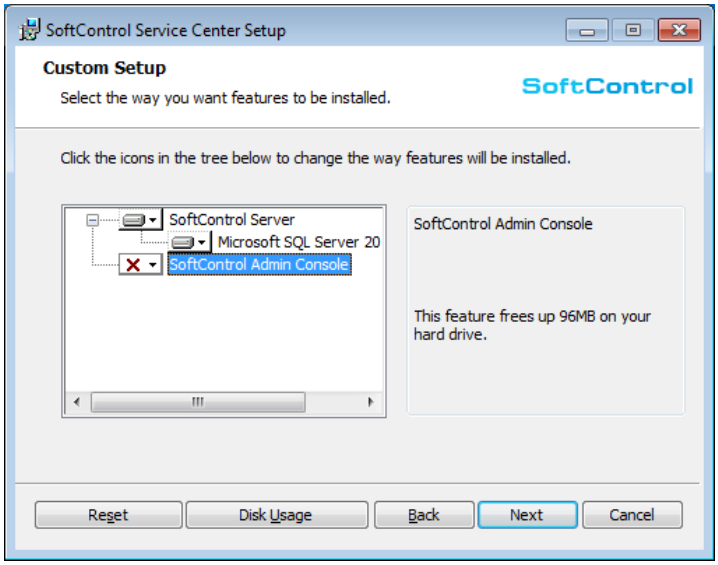

Figure 135. Selecting components to remove

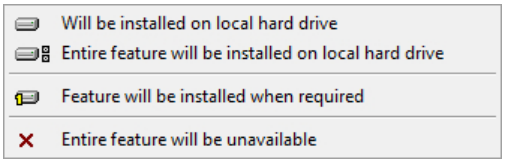

Figure 136. Component installation options

5) Click **Change** (fig. Ready to uninstall 140).

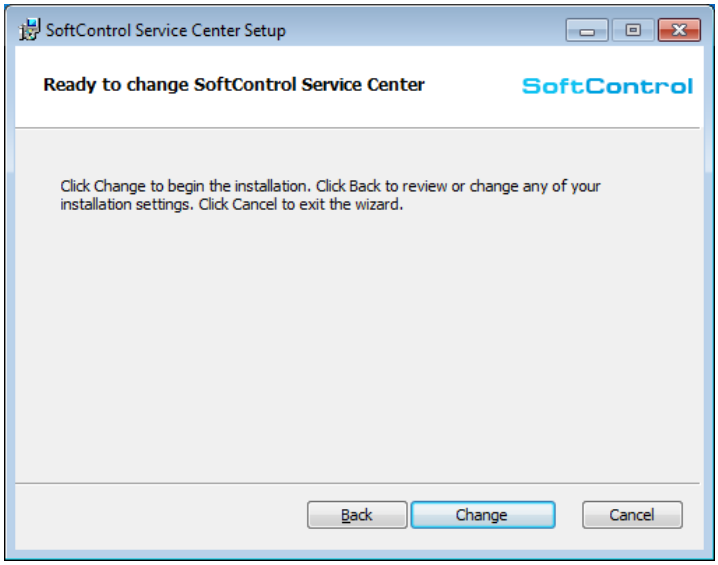

Figure 137. Ready to uninstall

6) Wait until uninstallation completes (fig. Uninstallation progress [141]).

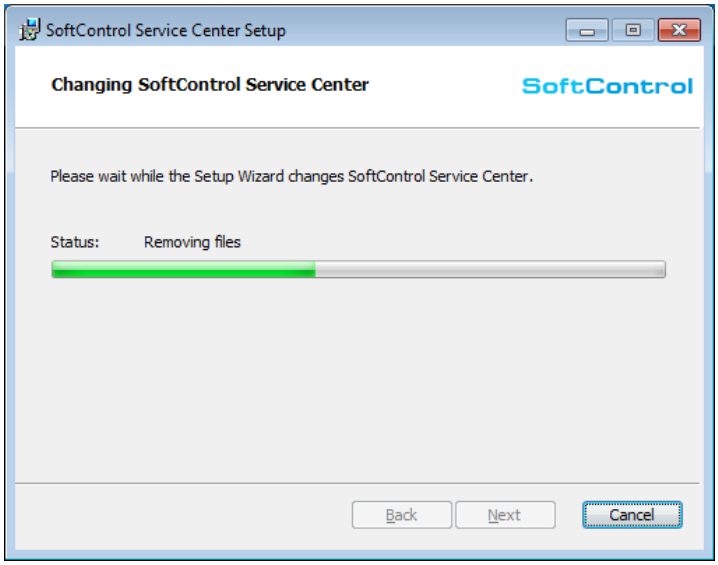

Figure 138. Uninstallation progress

7) After the *Completed the SoftControl Service Center Setup Wizard* message is displayed, click **Finish** (fig. Finishing uninstallation [141]).

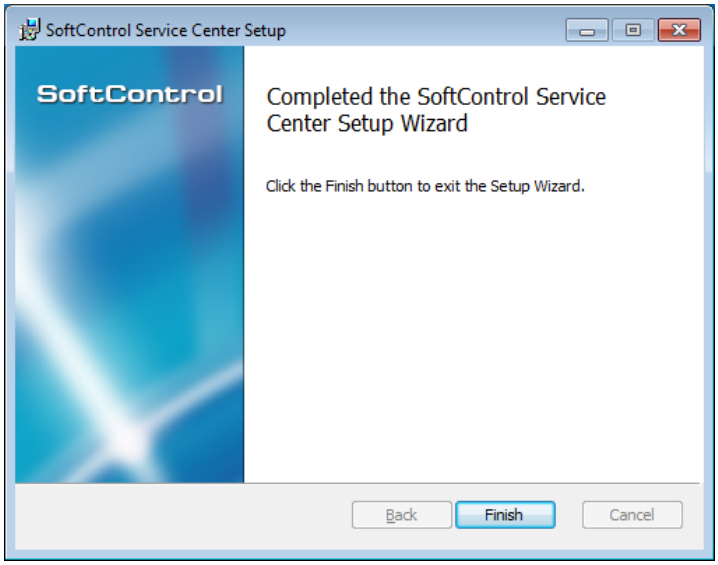

Figure 139. Finishing uninstallation

If SoftControl Server has been installed with the embedded DBMS, 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. Supplemental information

7.1. About server's certificates

This section describes the most important aspects of cryptographic protection of the communication channel between SoftControl Service Center and the SoftControl SysWatch 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:

- **Root** – this certificate is a certificate of a certification authority in the context of a SoftControl Service Center-based ISS, and it is located in the Windows storage. All other kinds of product certificates are signed with the root certificate, which is one of the indications that they are valid.
- **Server** – the certificate of the server part that is used for interaction with the clients and is located in the Windows storage.
- **Common client** – the certificate of the client part; it is used to register the clients on the server. This certificate is common for all the new clients and is only designed to send the first request to the server. The certificate is integrated into the encrypted client configuration file [22] that is applied to the client at an endpoint. It can also be exported to a file by the following path:
  `C:\ProgramData\SoftControl\Client.pem`
- **Specific client** – the certificate of the client part; it is issued by the server component after registration confirmation [41] 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 [42]) or issue another certificate (updating [42]).

7.2. 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\SoftControl\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 NetBIOS name>" Port="<connection port>" />
   ```
4) Save changes in the configuration file.
5) Change NetBIOS 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.

7.3. SoftControl Service Center backup

In some cases, you might need to create a backup copy[145] of the SoftControl Service Center components, so as to restore[146] 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.

7.3.1. Creating the backup copy

A backup copy of the SoftControl Service Center files includes the SoftControl Server configuration files and certificates[143] that are necessary for restoring. SoftControl Admin Console user filters[113] 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[145]).

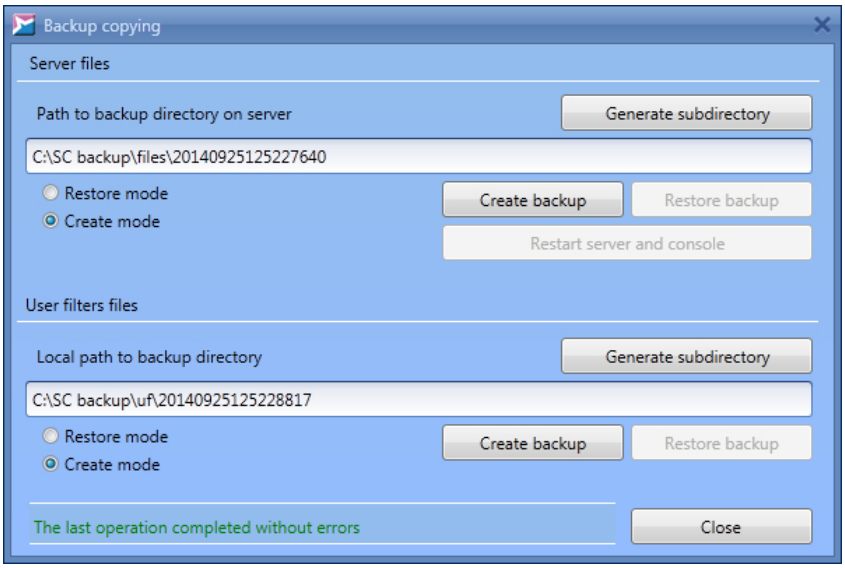

Figure 140. Creating a backup copy

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[145]).

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.

7.3.2. 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 [9] 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 [19] 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 [146]).

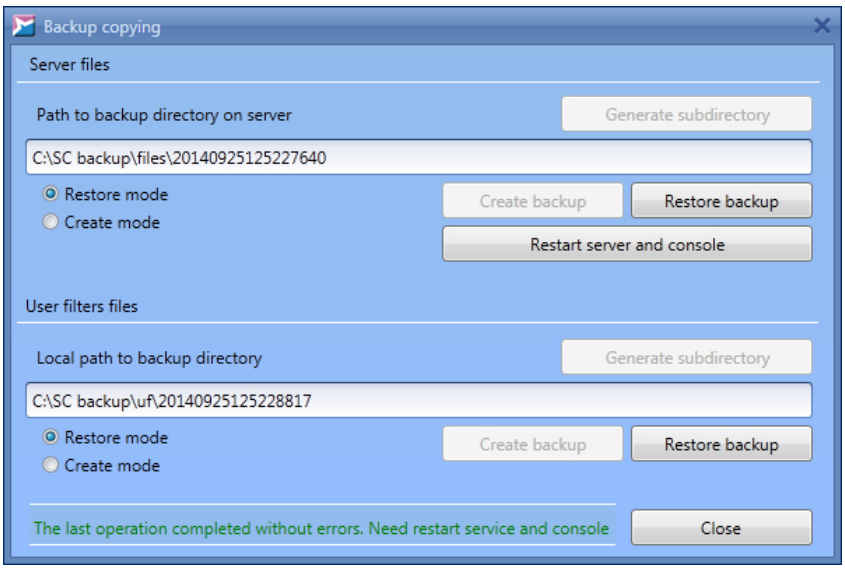

Figure 141. Restoring from a backup copy

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 [146] for the **User filter files** area in the **Backup copying** window (fig. Restoring from a backup copy [146]).
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 [146].
10) Log in [23] to SoftControl Admin Console. Make sure all the components work.

7.4. Process privileges

Table 35 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 35. 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	Required to shut down a system using a network request.

Privilege	Description
remote computer	
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. 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.

7.5. Sources

Sources of supplemental information are presented in table 36.

Table 36. 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.

8. 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 [151] and attach the text logs of the components to the message. Table 37 lists the required files.

Table 37. SoftControl Service Center components text logs

Component log type	Path
SoftControl Admin Console work log	`<SoftControl Admin Console installation directory>\logs\ConsoleDetailedLog.txt`
SoftControl Server work log	`<SoftControl Server installation directory>\logs\ServerDetailedLog.txt`

SoftControl SysWatch system log	Microsoft® Windows® XP, Microsoft® Windows® Server 2003:
	`C:\Documents and Settings\All Users\Application Data\S.N.Safe&Software\Safe'n'Sec\Reports\system_<dd.mm.yy>_<hh.mm.ss.mmm>.txt`
	Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:
	`C:\ProgramData\S.N.Safe&Software\Safe'n'Sec\Reports\system_<dd.mm.yy>_<hh.mm.ss.mmm>.txt`

9. 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.

10. Appendix

10.1. Installing and setting up Microsoft® SQL Server® 2008

This section describes how to install and set up the Microsoft® SQL Server® 2008 DBMS to employ it along with SoftControl Service Center.

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 152).

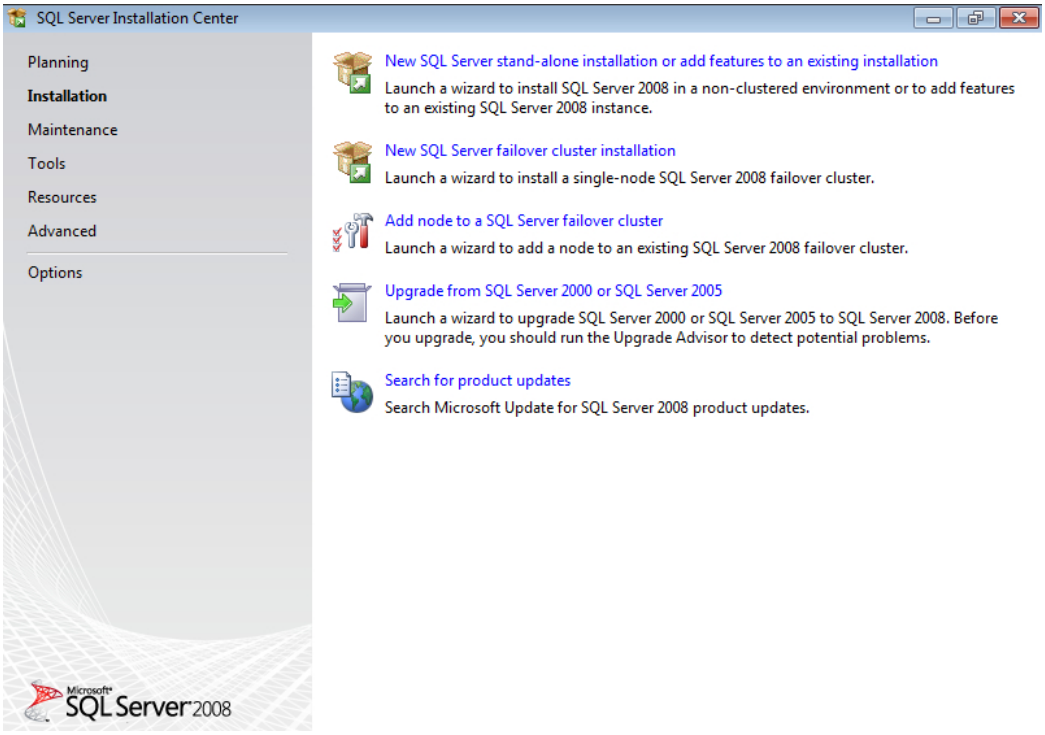

Figure 142. The 'Installation' section

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[153]). You should fix errors before continuing. If there are no problems, click **OK**.

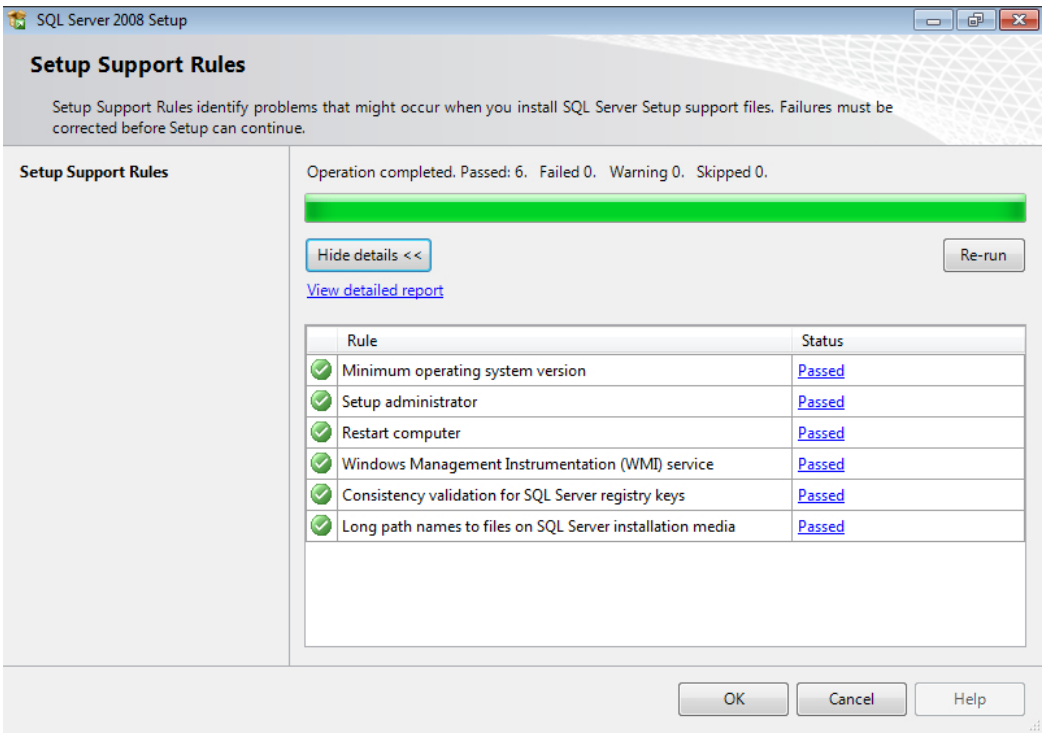

Figure 143. Setup support rules check

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[153]).

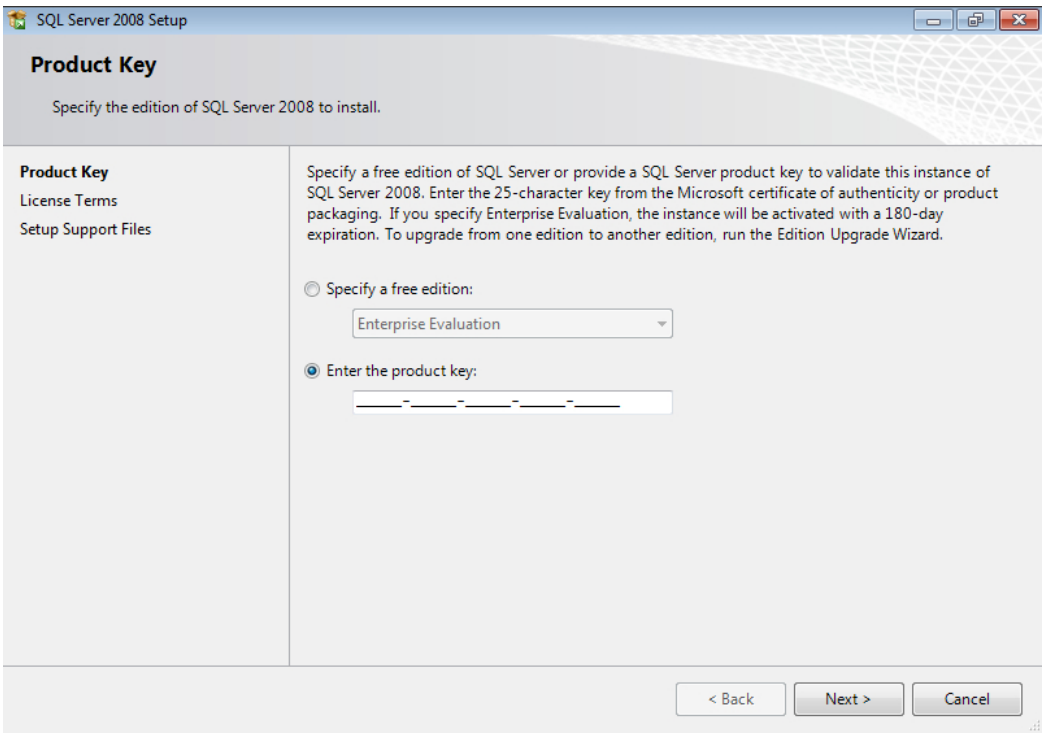

Figure 144. The 'Product Key' section

5) Read the **License Terms**. If you accept the terms, select **I Accept the license terms** and click **Next** (fig. The 'License Terms' 154).

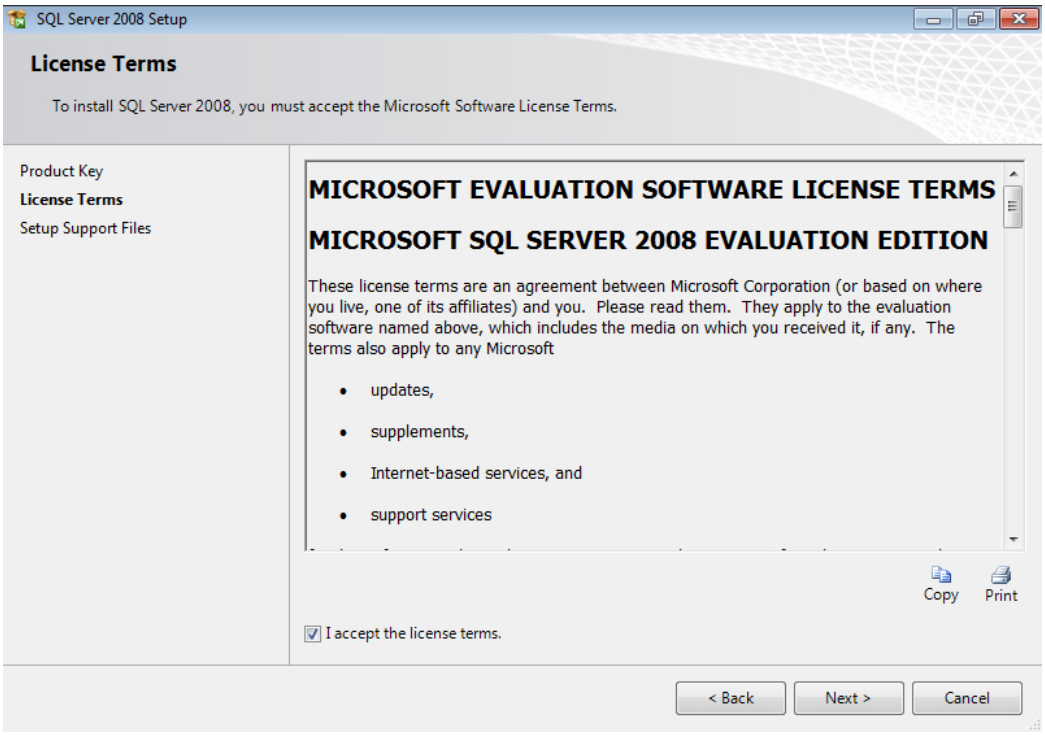

Figure 145. The 'License Terms'

6) Click **Install** in section **Setup Support Files** (fig. The 'Setup Support Files' section[155]).

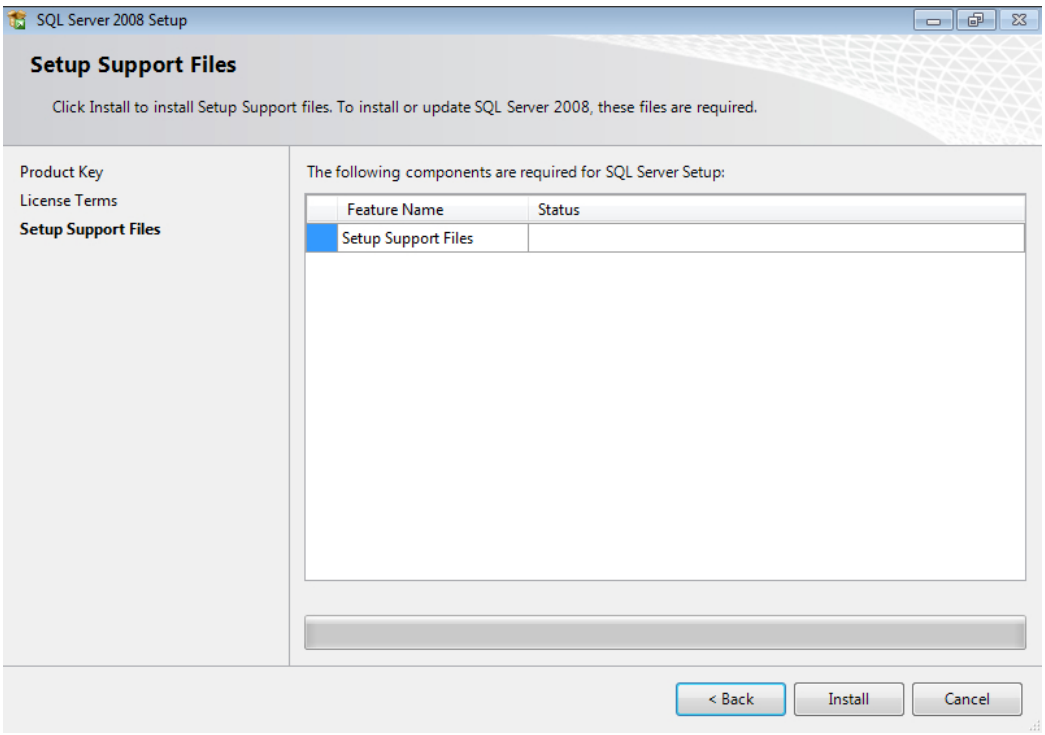

Figure 146. The 'Setup Support Files' section

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[155]). You should fix errors before continuing. If there are no problems, click **Next**.

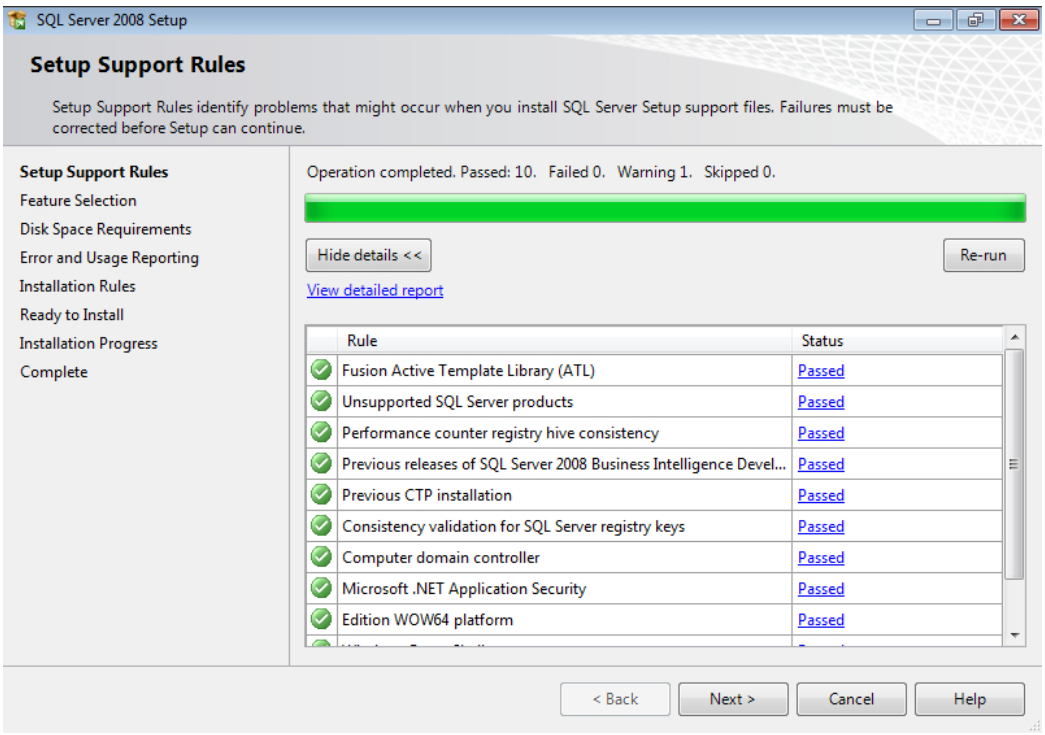

Figure 147. The 'Setup Support Rules' section. Details

8) In the **Feature Selection** section, click **Select All**, specify the installation path in the **Shared feature directory** field and click **Next** (fig. The 'Feature Selection' section 156).

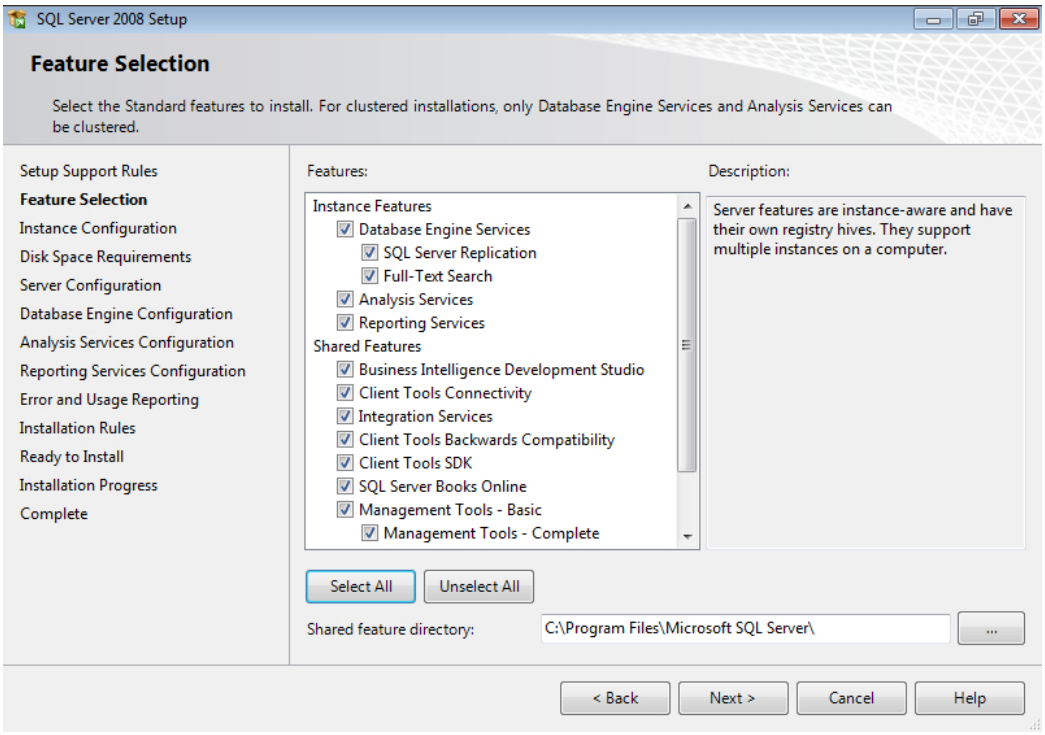

Figure 148. The 'Feature Selection' section

9) Select **Default Instance** and click **Next** in the **Instant Configuration** section (fig. The 'Instance Configuration' section 157).

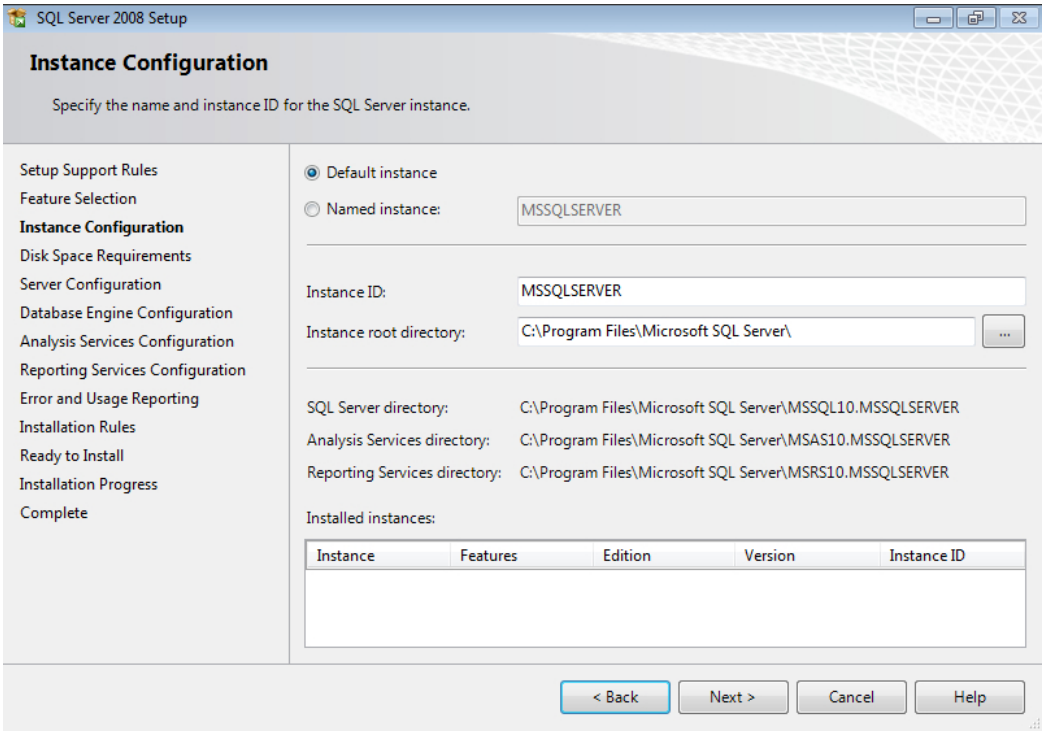

Figure 149. The 'Instance Configuration' section

10) Click **Next** in the **Disc Space Requirements** section (fig. The 'Disc Space Requirements' section 157).

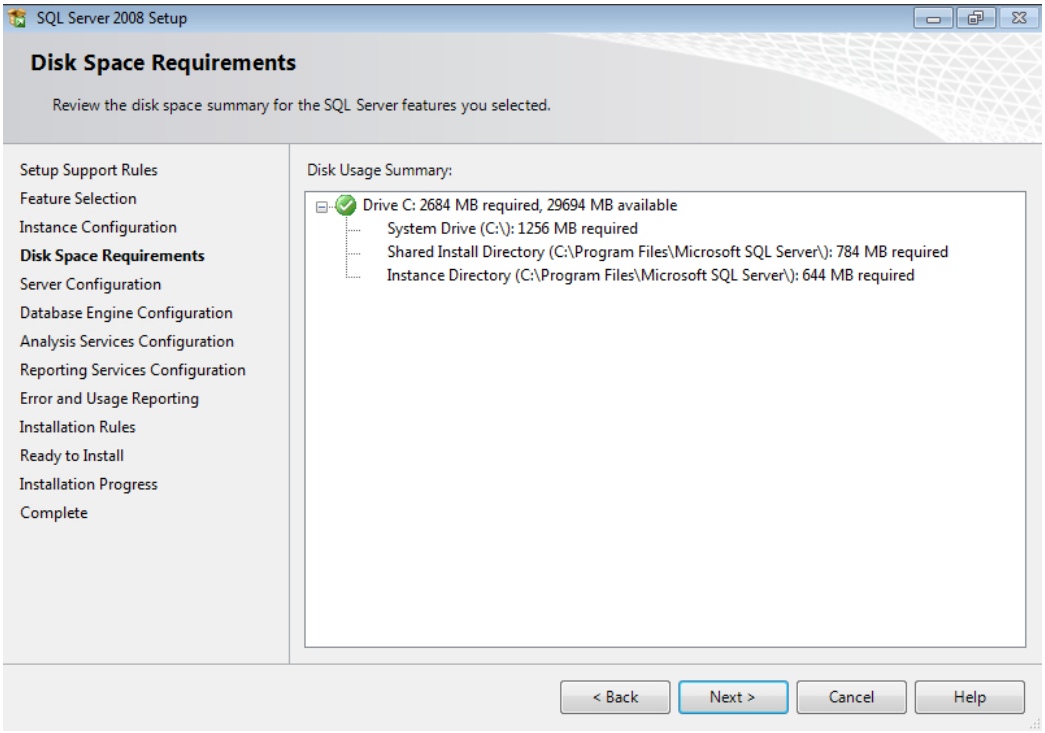

Figure 150. The 'Disc Space Requirements' section

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 158).

Select the **NETWORK SERVICE** account in the displayed window and click **OK** (fig. Account 159).

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 159).

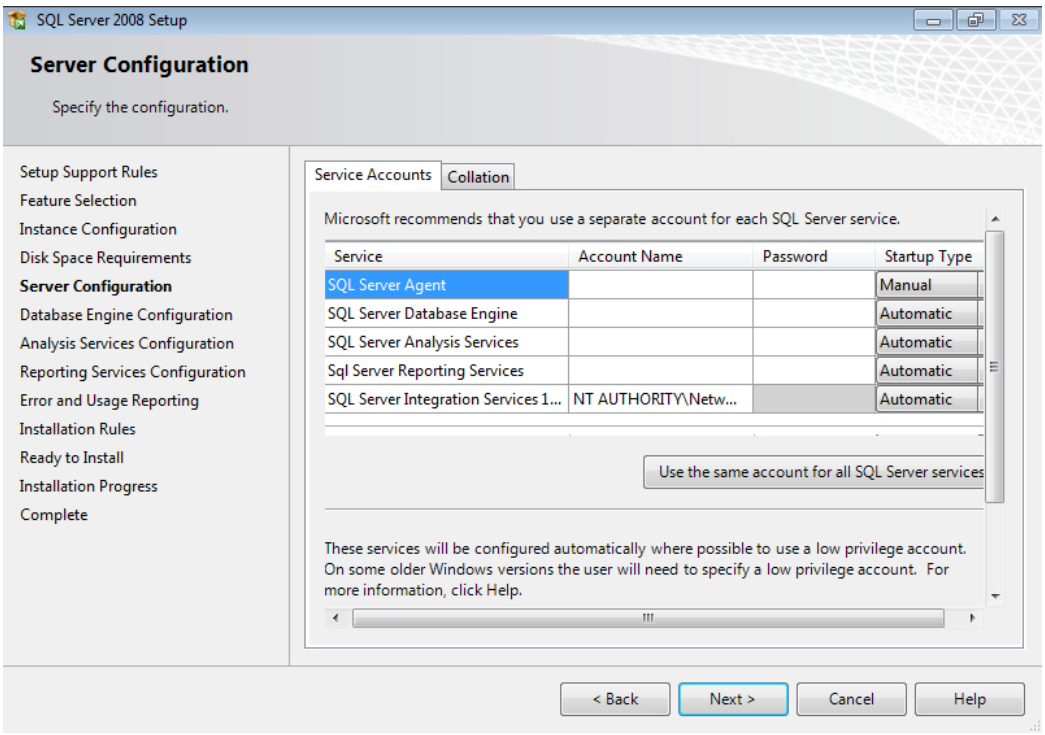

Figure 151. The 'Service Accounts' tab of the 'Server Configuration' section

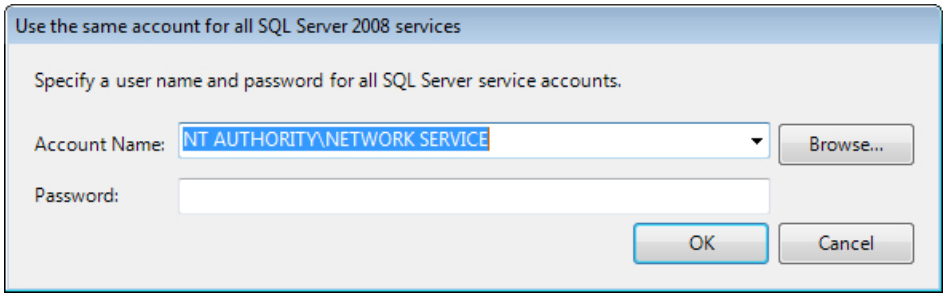

Figure 152. Account

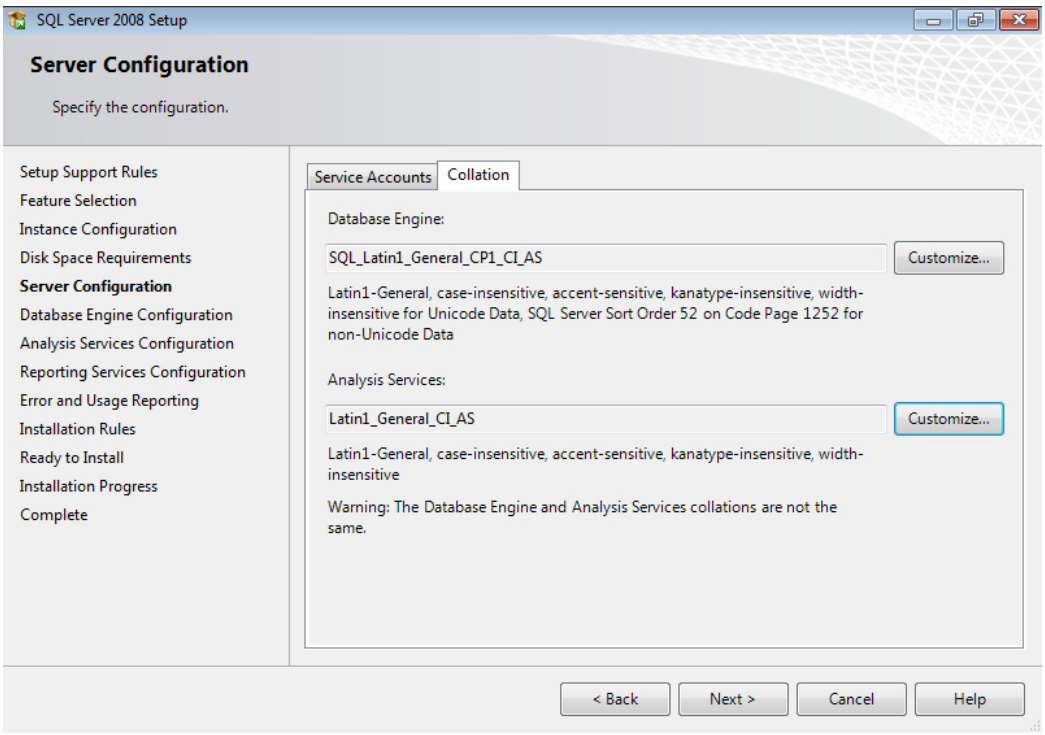

Figure 153. The 'Collation' tab of the 'Server Configuration' section

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 160).

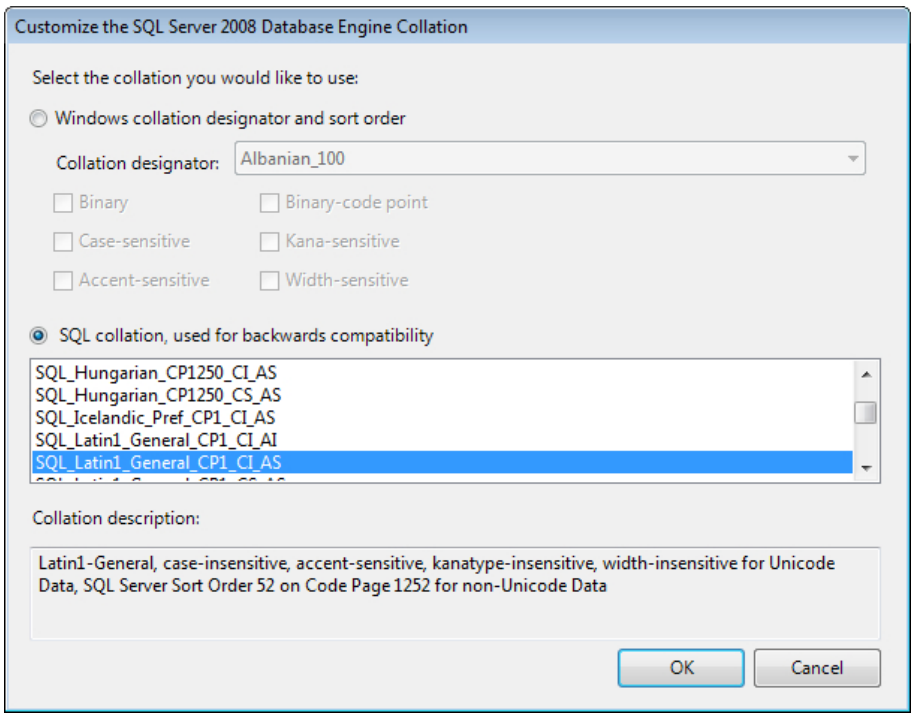

Figure 154. Specifying the collation parameters for the Database Engine component

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 161).

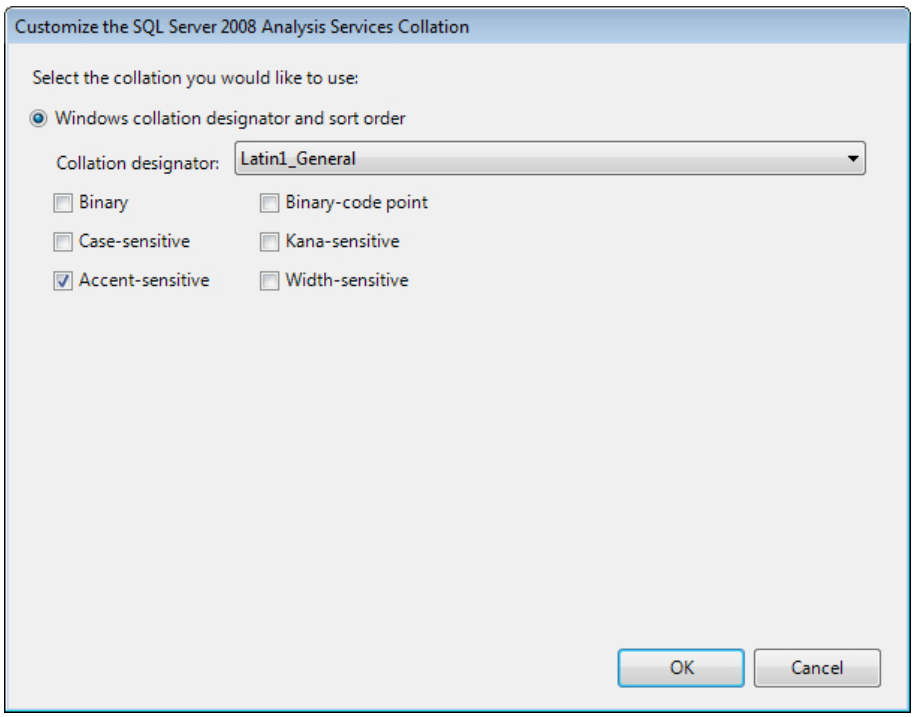

Figure 155. Specifying the collation parameters for the Analysis Services component

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 162). Click **Add Current User** and make sure that the current system account is displayed in the **Specify SQL Server administrators** list; then click **Next**.

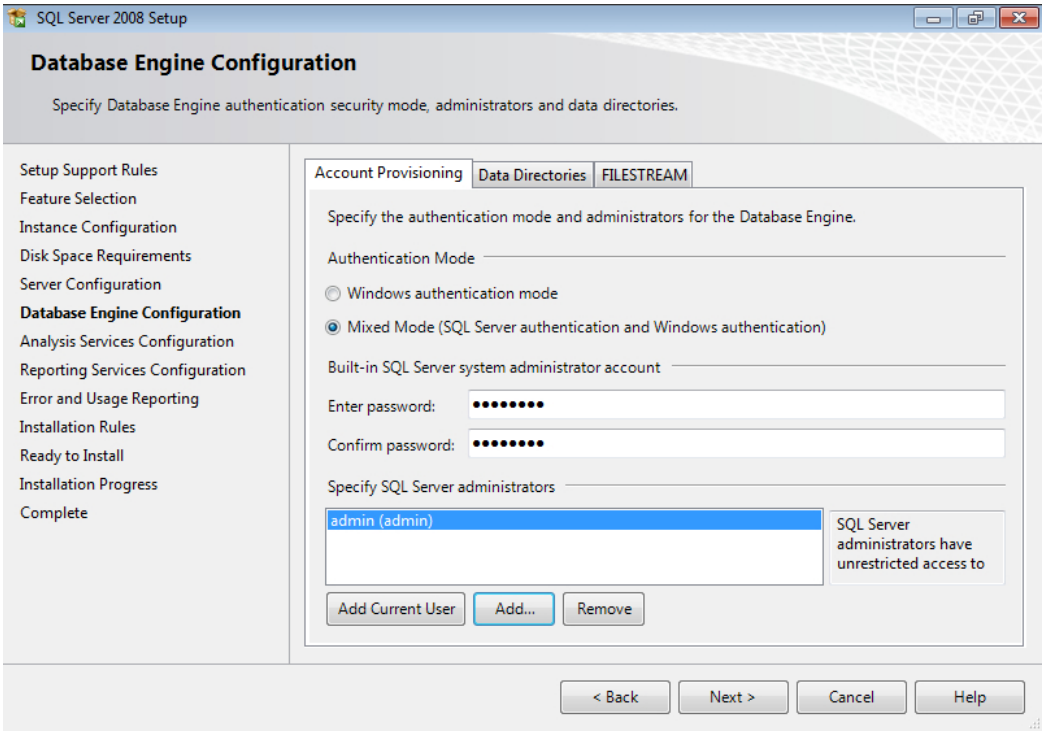

Figure 156. The 'Database Engine Configuration' section

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 163).

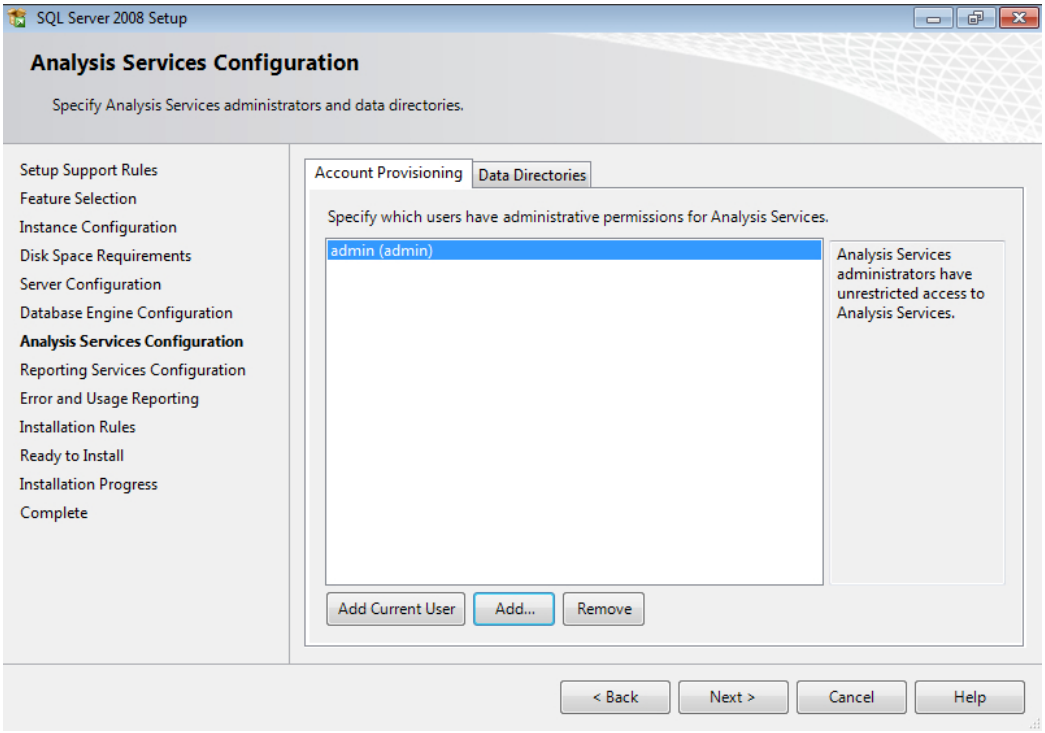

Figure 157. The 'Analysis Services Configuration' section

14) Select **Install the native mode default configuration** and click **Next** in the **Reporting Services Configuration** section (fig. The 'Reporting Services Configuration' section 164).

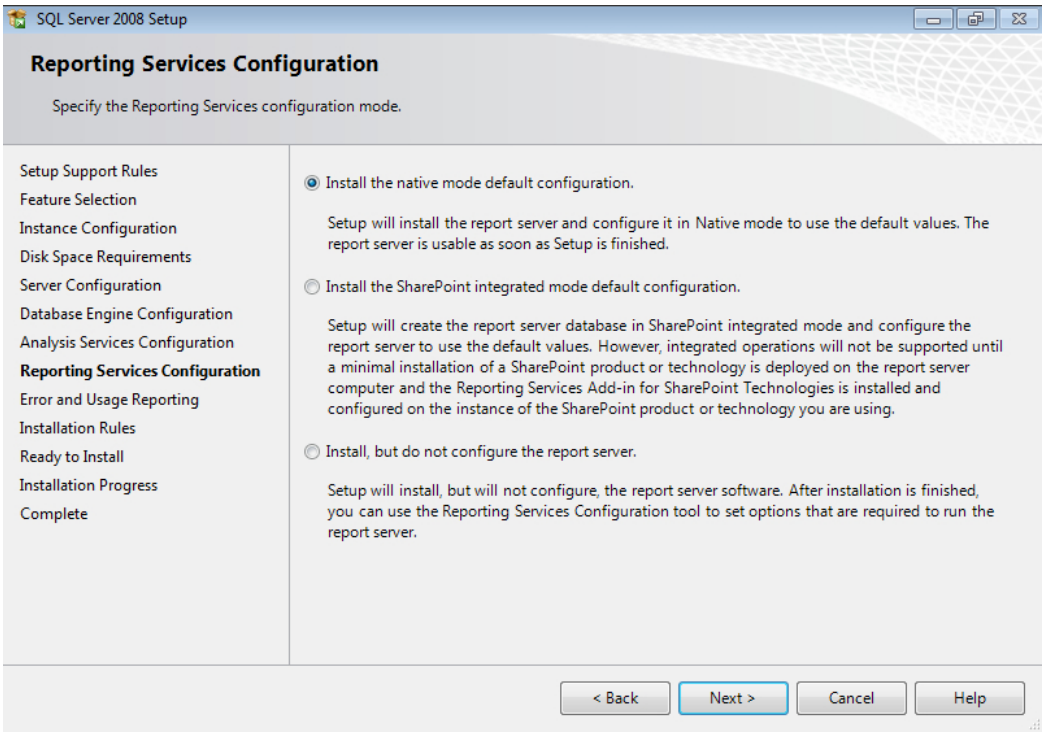

Figure 158. The 'Reporting Services Configuration' section

15) Click **Next** in the **Error and Usage Reporting** secton (fig. The 'Error and Usage Reporting' section (165)).

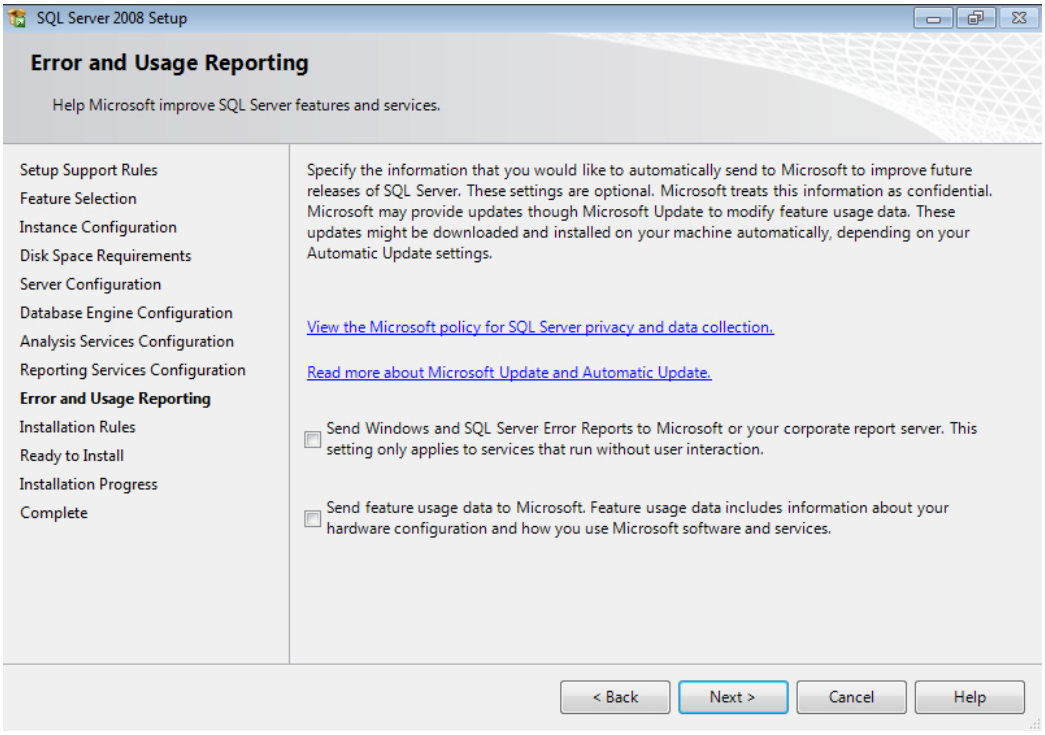

Figure 159. The 'Error and Usage Reporting' section

16) The **Installation Rules** section checks for problems that might occur when installing Microsoft® SQL Server® 2008 (fig. The 'Installation Rules' section (165)). If there are no problems, click **Next**.

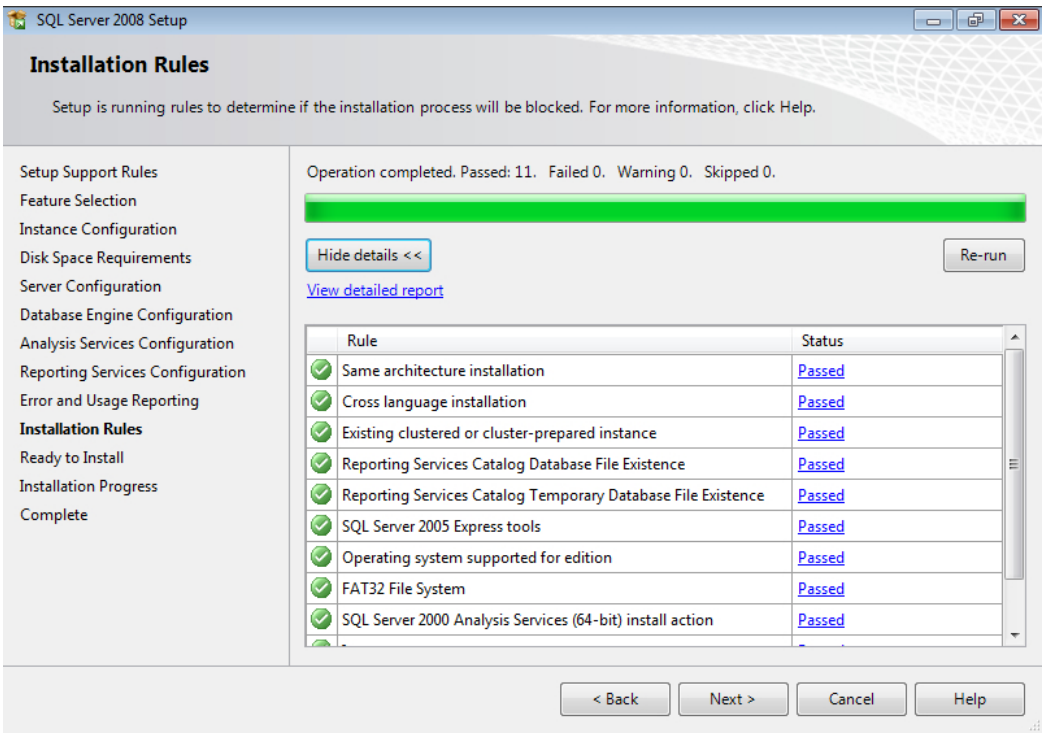

Figure 160. The 'Installation Rules' section

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 166).

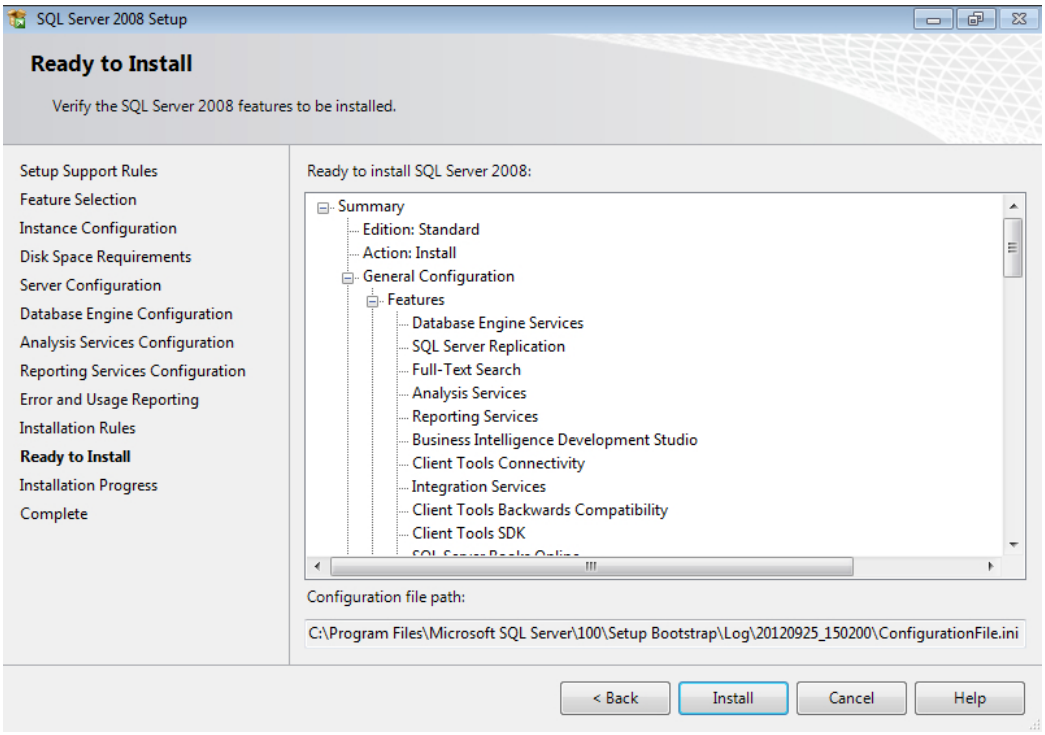

Figure 161. The 'Ready to Install' section

18) The **Installation Progress** section displays the progress of installing the Microsoft SQL Server 2008 components (fig. The 'Installation Progress' section 167).

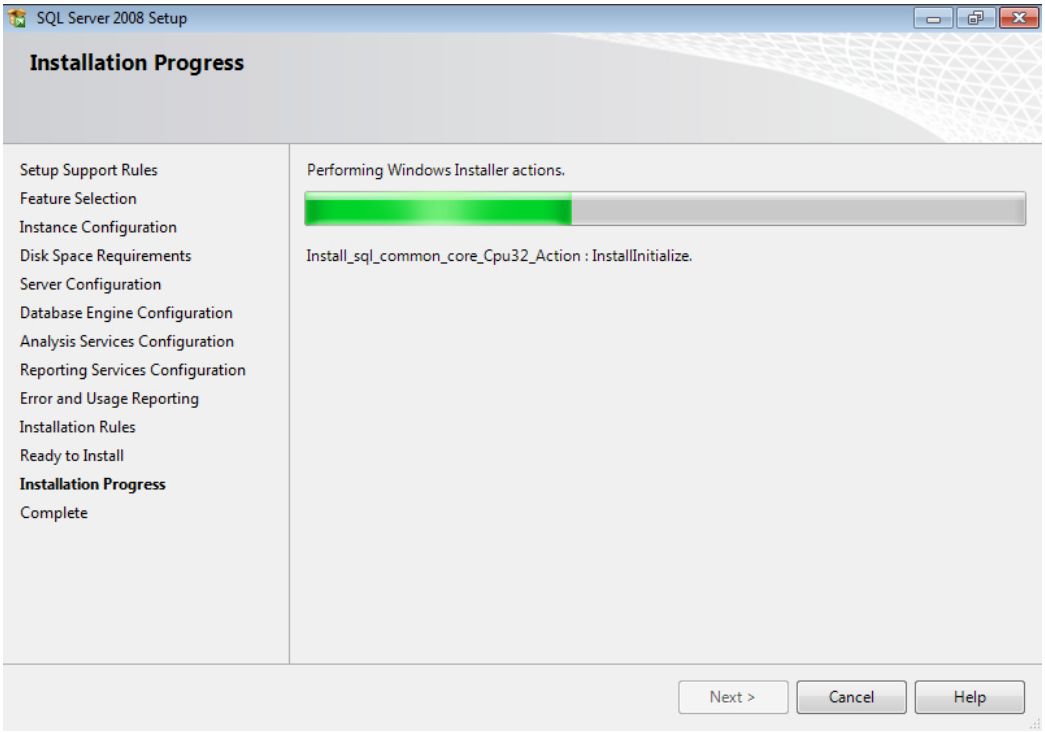

Figure 162. The 'Installation Progress' section

Click **Next** when the installation completes.

Click **Close** in the **Complete** section to complete the installation (fig. The 'Complete' section 167).

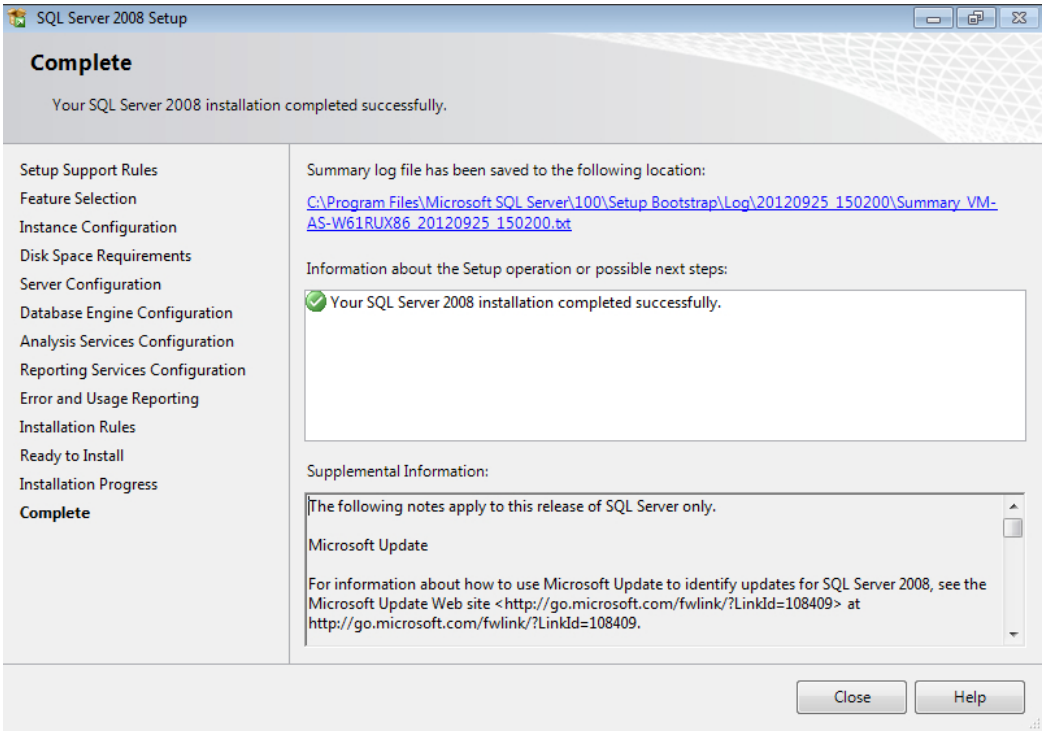

Figure 163. The 'Complete' section

10.2. 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 168).

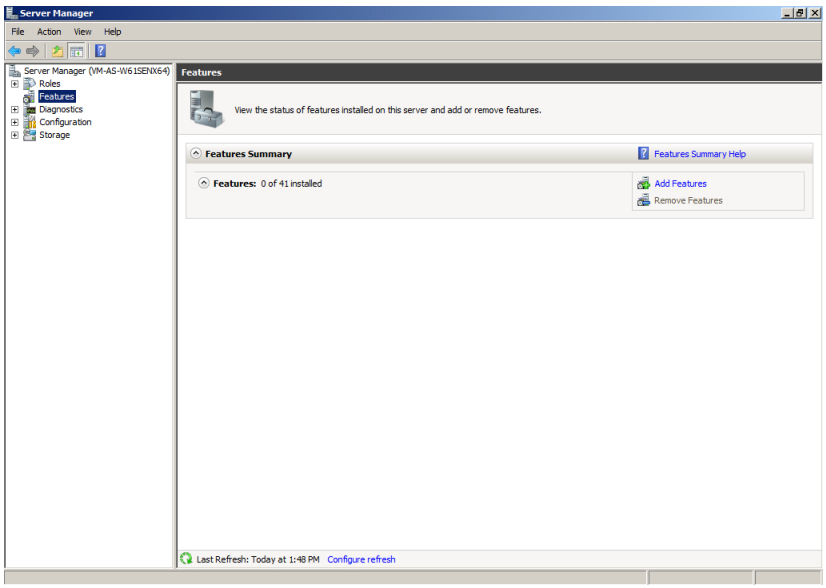

Figure 164. The Server Manager snap-in

2) Tick off **Desktop Experience** in the displayed **Add Features Wizard** window (fig. Selecting components to add 169) (for Microsoft® Windows® Server 2012 / 2012 R2: **User Interfaces and Infrastructure** → **Desktop Experience**).

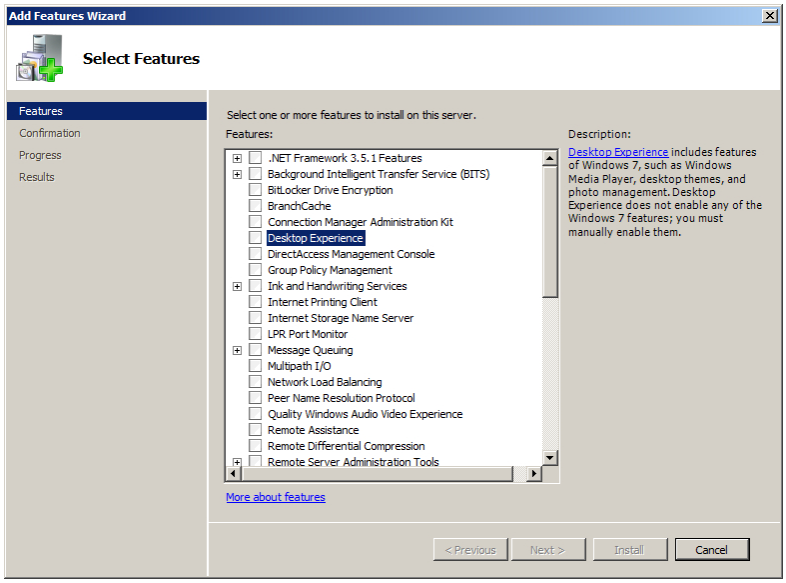

Figure 165. Selecting components to add

3) When the dialog box with information about required components appears, click **Add Required Features** (fig. Requesting to add the required components 169).

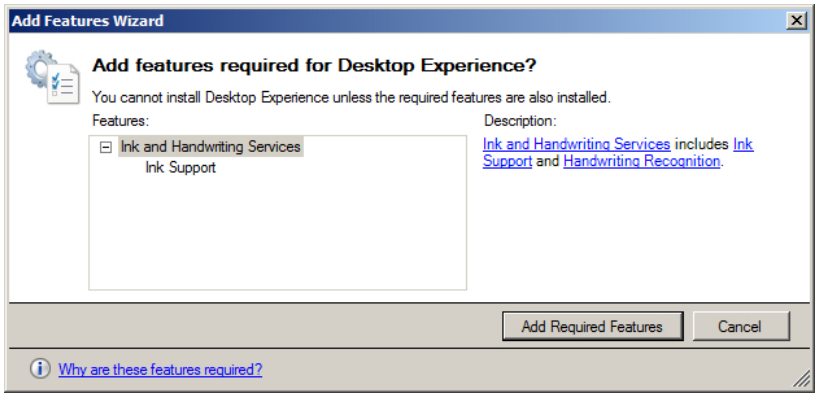

Figure 166. Requesting to add the required components

4) Make sure that the **Desktop Experience** component is selected and click **Next** (fig. Selecting components to add 169).

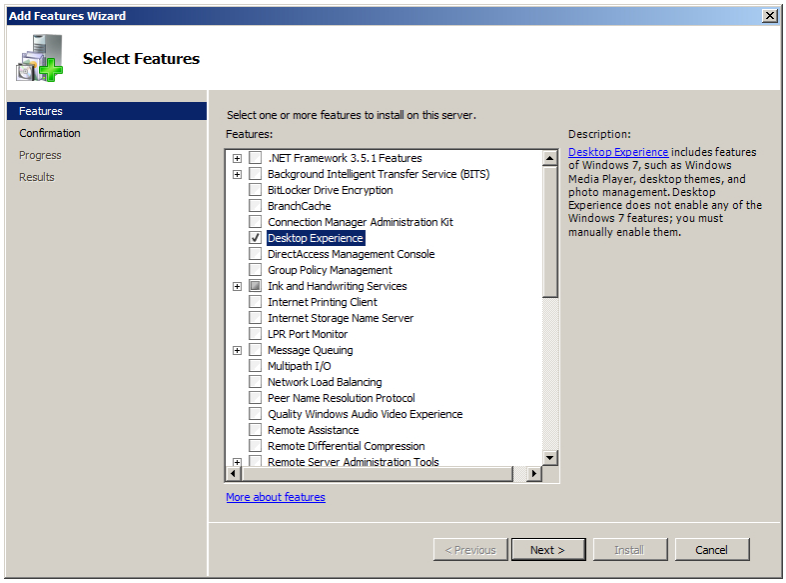

Figure 167. Selecting components to add

5) Click **Next** in the **Confirmation** step (fig. Confirming installation selection 170).

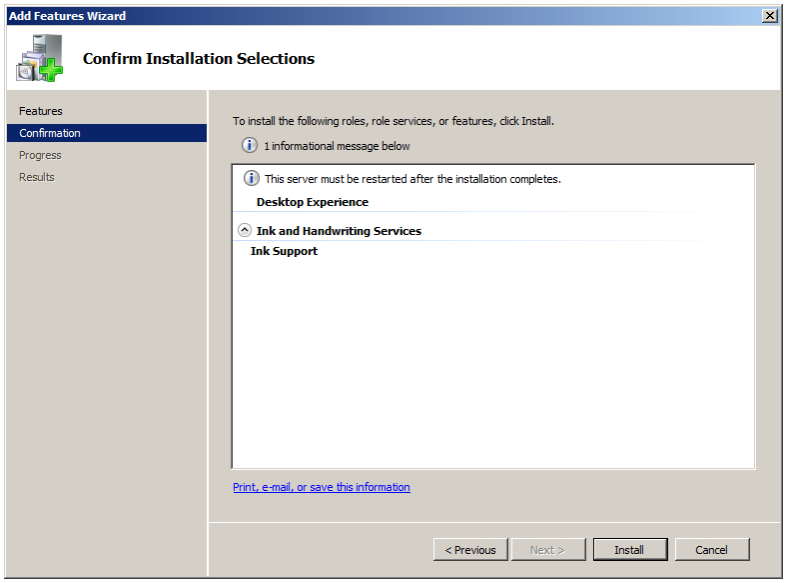

Figure 168. Confirming installation selection

6) Wait until the installation completes (fig. Installation progress 170).

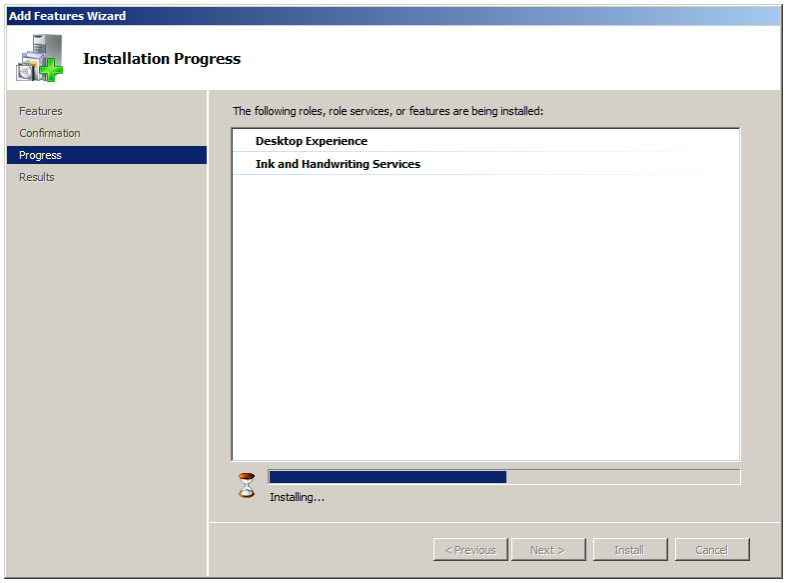

Figure 169. Installation progress

7) Click **Close** in the **Results** step (fig. Finished adding the components 171).
8) Select **Yes** in the dialog box that suggests system restart. The system is then restarted to complete the installation (fig. Requesting system restart 171).
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 172).

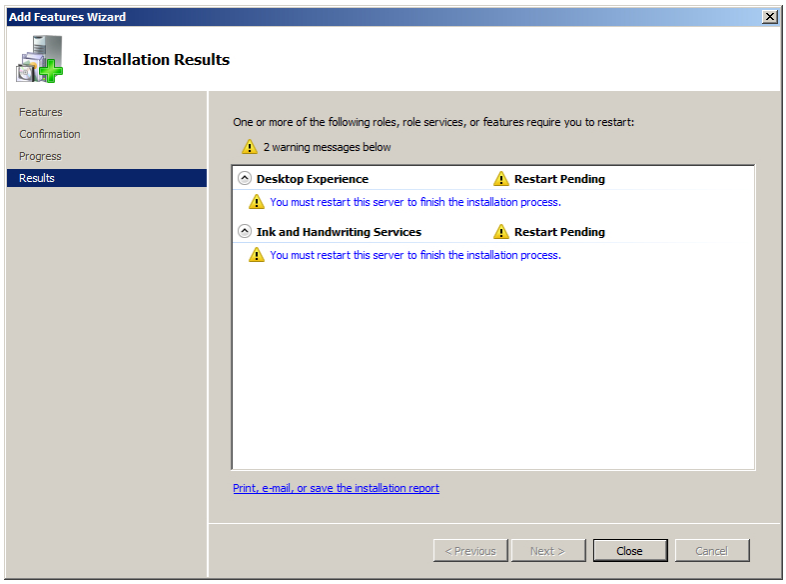

Figure 170. Finished adding the components

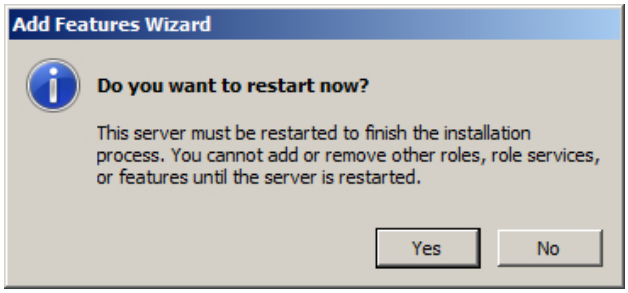

Figure 171. Requesting system restart

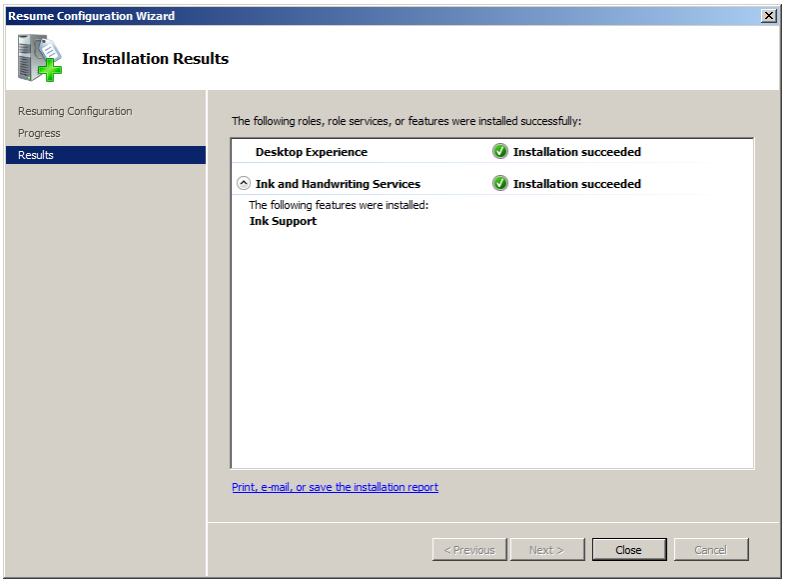

Figure 172. The result of adding the components