SoftControl

TPS 6.1.398

SoftControl Pilot Project Plan

Contents

1. Testing procedure for the pilot project

This document is designed for the Client and contains the information that will help the Client to carry out the pilot project.

1.1 Purpose of the pilot project

Purpose of the pilot project is to test the reported functional and operational characteristics of the information security product SoftControl, to prepare the solution for deployment on the operational infrastructure, and to provide personnel with the skills required for use of the software product.

The following tasks shall be accomplished within the pilot project:

- Compliance tests:
  - ❑ Compliance with the hardware configuration on the devices
  - ❑ Compliance with specific versions of operating systems installed on the devices
  - ❑ Network compliance (check of operation of the client-server configuration with the network equipment and of communication channels performance)
- Operational tests:
  - ❑ Local and remote installation of the client components
  - ❑ Group control policies management

1.2 Specifications of the pilot project test bench

To confirm that the parties (the Client and the Contractor of the project) are ready for pilot testing on the Client's infrastructure, compliance with the specifications for deployment shall be confirmed for the three SoftControl components: the server module SoftControl Server, the management console SoftControl Admin Console, and the client module SoftControl SysWatch.See document *http://kb.safensoft.com/index.php/Файл:Технические_условия_Syswatch.pdf.* (in Russian).

The pilot project test bench includes the following devices:

- Device (or virtual machine) for deployment of the management server. See 1.4, table 1 [5] for system requirements.
- Device (or virtual machine) for initial deployment of the SoftControl SysWatch client, preparing the package installer, and conducting functional and operational tests (hereinafter – device 1). See 1.4, table 3 [5] for system requirements.
- Device that is used in the Client infrastructure and requires implementation of protection measures. The device is required to test deployment of the SoftControl SysWatch client with the package installer and to run functional and operational tests (hereinafter – standard device). See 1.4, table 3 [5] for system requirements.

Requirements for the network infrastructure in the pilot project:

- Device 1 and standard device shall have access to ports 8000, 8088 on SoftControl Server.
- Port 8080 shall be available on SoftControl Server for connection to SoftControl Admin Console.

1.3 Procedure

Testing consists of the following successive stages:

1) Ratification by the Client of a testing plan, which defines responsible personnel within the participating organizations.
2) Software installation.
3) Operational and functional tests.
4) Final review, filling in and signing of checklist for the performed tests.

At all the testing stages, the participating organizations provide each other with mutual counseling and exchange information.

Results of the testing shall be submitted in form of the filled checklist. Each test described in the pilot project plan shall be carried out for each client component within the pilot zone. Outcome of all performed tests shall be included in the checklist.

Results of the testing shall be used to confirm compliance of the product with reported functional and operational characteristics.

Control policies, batch installers, and instructions that were created during the testing process may be used for deploying and operating the software product on the Client's network of devices.

1.4 System requirements

Table 1. Minimal system requirements for SoftControl Server

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

Additional requirements:

- Microsoft® .NET Framework 4.5.

- Microsoft® SQL Server® 2008 / SQL Server® 2012 / SQL Server® 2014 SP1 / SQL Server® 2016 / SQL Server® 2017.
- For SQL Server® 2014 Express SP1 or SQL Server® 2012 installation on Windows Server 2008 R2, Service Pack 1 (SP1) should be installed in the system.
- For server operating systems: only desktop installation options are supported.

Table 2. Minimal system requirements for SoftControl Admin Console

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

Additional software:

- Microsoft® .NET Framework 4.5.
- For server operating systems: only desktop installation options are supported.

Table 3. Minimal system requirements for SoftControl SysWatch

OS	CPU frequency	RAM size	HDD free space
Client operating systems:			150MB +

OS	CPU frequency	RAM size	HDD free space
Microsoft® Windows® XP (SP2) *32-bit*[1,2]	800MHz	512MB	extra 120MB or more for anti-virus database updates
Microsoft® Windows® XP (SP3) *32-bit*[1]	800MHz	512MB	
Microsoft® Windows® XP (SP2) *64-bit*[1]	800MHz	512MB	
Microsoft® Windows® XP Embedded (SP2 and above)[1]	800MHz	256 МБ	
Microsoft® Windows® Embedded for Point of Service 1.0[1]	800MHz	256 МБ	
Microsoft® Windows® 7 (SP1) *32-bit*[3]	1GHz	1GB	
Microsoft® Windows® 7 (SP1) *64-bit*[3]	1GHz	2GB	
Microsoft® Windows® 8 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8 *64-bit*	1GHz	2GB	
Microsoft® Windows® 8.1 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8.1 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 IoT Enterprise *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 IoT Enterprise *64-bit*	1GHz	2GB	
Microsoft® Windows® 11 *64-bit*	1GHz	4GB	
Server operating systems:			
Microsoft® Windows® Server 2003 (SP2) *32-bit*[1,4]	800MHz	512MB	
Microsoft® Windows® Server 2003 (SP2) *64-bit*[1,4]	800MHz	512MB	
Microsoft® Windows® Server 2008 R2 *64-bit*[3,5]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 *64-bit*[5]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 R2 *64-bit*[5]	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit*[5]	1.4GHz	2GB	
Microsoft® Windows® Server 2019 *64-bit*[5]	1.4GHz	2GB	
Microsoft® Windows® Server 2022 *64-bit*[5]	1.4GHz	2GB	

Note: all popular platforms with the above-mentioned operating systems are supported.

Additional requirements:

1. Visual C++ 2008 SP1 Redistributable Package x86 (including for 64-bit OSs).
2. Additional operations may be required for Windows XP SP2 (see Updating SoftControl SysWatch and antivirus bases on Windows XP SP2 [81]).
3. Update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature verification).
4. Update KB968730 or equivalent (support of the SHA-256 algorithm for digital signature verification).
5. Only desktop installation options are supported.

2. Testing checklist

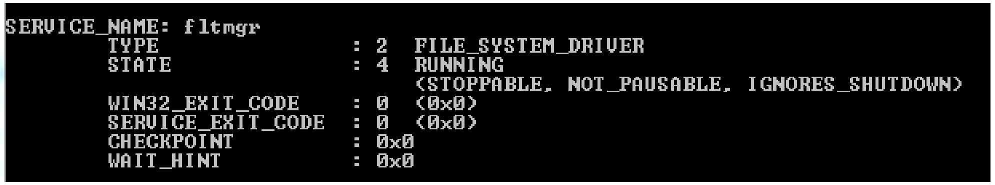
2.1 Check of Client's infrastructure state

2.1.1 How to check compliance with the Specifications for deployment

Table 4. Compliance check

No.	Action	Expected outcome	Comment
4.1	Fill in the data sheet with hardware and software characteristics of the devices in the pilot zone and of the workstation for deployment of the SoftControl Service Center server component.	□ The data sheet contains required information.	Information about installed antivirus programs and other specially configured software is required for giving recommendations regarding fine-tuning for compliance with the SoftControl system. See *SW_4.2_and_higher +KAV+NOD32.docx* (in Russian) for compliance settings.
4.2	Check that hardware and software characteristics of the devices in the data sheet comply with the deployment specifications in the checklist.		
4.2.1	Check that hardware and software characteristics of the workstation for deployment of the SoftControl Service Center server component comply with the deployment specifications.	□ Characteristics comply with the specifications for deployment.	In order to deploy the SoftControl Service Center server component, install Microsoft .Net Framework 4.5 on the workstation. You can download and install Microsoft .Net Framework 4.5 by clicking on this link: https://www.microsoft.com/en-us/download/details.aspx?id=42642.
4.2.2	Make sure that Filter Manager is present in the operating system of the devices.	□ Presence of Filter Manager in the system is confirmed.	There is a special command in the command prompt that can do this.*

* Type *sc query fltmgr* in the prompt window. You will see a message about the state of Filter Manager if it is installed. Otherwise, the prompt will show an error message.



```
SERVICE_NAME: fltmgr
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

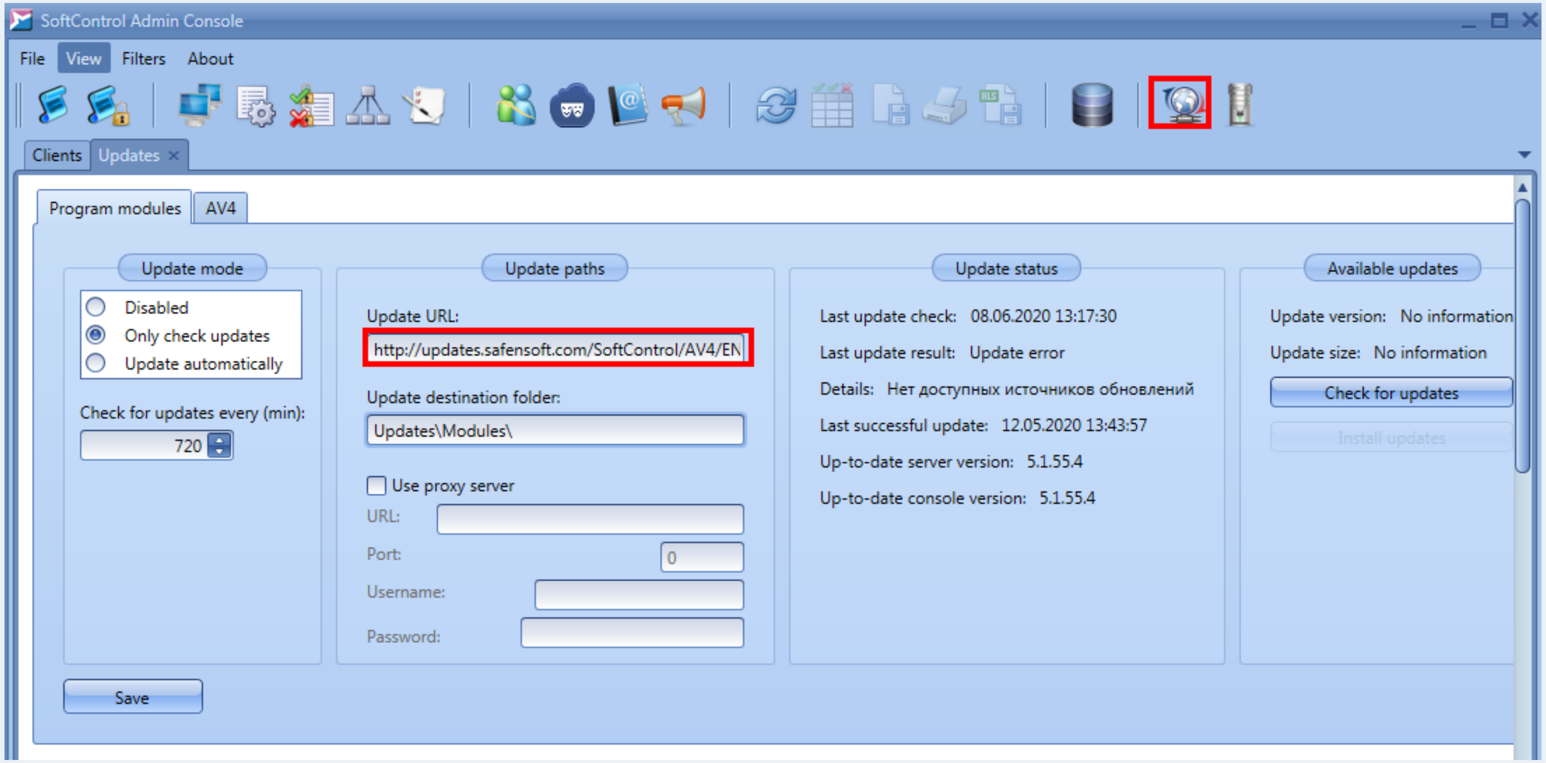
2.2 SoftControl test bench deployment

2.2.1 How to deploy the server component SoftControl Service Center

Table 5. SoftControl Service Center deployment

No.	Action	Expected outcome	Comment
5.1	Install the following components: SoftControl Server, SoftControl Admin Console, MS SQL 2014 Express.	□ The server component has been successfully installed and initially configured.	Installation is performed by Client's personnel. Administrator rights are required. All components can be installed from the single installer; select the **Complete** mode. It will install the following components: • SoftControl Server; • SoftControl Admin Console; • Microsoft SQL 2014 Express.
* You can also install SoftControl Service Center on the enterprise MS SQL Server DBMS that you use. In this case, select **Typical** installation. The embedded Microsoft SQL 2014 Express will not be installed then.			
5.2	Configure SoftControl Service Center.		Configuring is performed by Client's personnel.
5.2.1	Create an Administrator user account in SoftControl Service Center, set Administrator's password.	□ SoftControl Service Center Administrator's password has been set.	The password is set by Client's personnel. Password requirements: at least 7 characters; digits, Latin letters (uppercase and lowercase), special characters. See section 3.2 "Setting up the server" of "SoftControl Service Center Administrator guide".
5.2.2	Set the main and backup IP-addresses for SoftControl Service Center.	□ "Clients host" window in SoftControl Admin Console shows the configured IP-addresses.	You will need the workstation IP address that is available for the devices. You will need available backup IP addresses (optional).
5.2.3	Log in to SoftControl Admin Console as Administrator.	□ Administrator has logged in successfully.	
5.2.4	Set up the update paths for antivirus databases and software modules.*	□ Update paths for antivirus databases and software modules have been set up.	SoftControl Service Center shall be connected to the Internet in order to download updates for antivirus databases and software modules. If there is no connection, you can download them manually.
* You have to perform the following steps in order to set up updates for antivirus databases and software modules on SoftControl Service Center: 1) Click 🌐 (**Updates**) in SoftControl Admin Console. 2) A window with two tabs will open. **Program modules** tab will be open by default. In **Update paths** area, edit text in **Update URL** field. Insert your test (release) license key in the update path `http://updates.safensoft.com/SoftControl/AV4/EN/` as follows: `http://updates.safensoft.com/<license key>/SoftControl/AV4/EN/`.			

For this tab, it's best to leave **Only check updates** selected in **Update mode** area.



○ Disabled
● Only check updates
○ Update automatically

Check for updates every (min): 720

Update URL: http://updates.safensoft.com/SoftControl/AV4/EN

Update destination folder: Updates\Modules\

□ Use proxy server

URL:

Port: 0

Username:

Password:

Last update check: 08.06.2020 13:17:30

Last update result: Update error

Details: Нет доступных источников обновлений

Last successful update: 12.05.2020 13:43:57

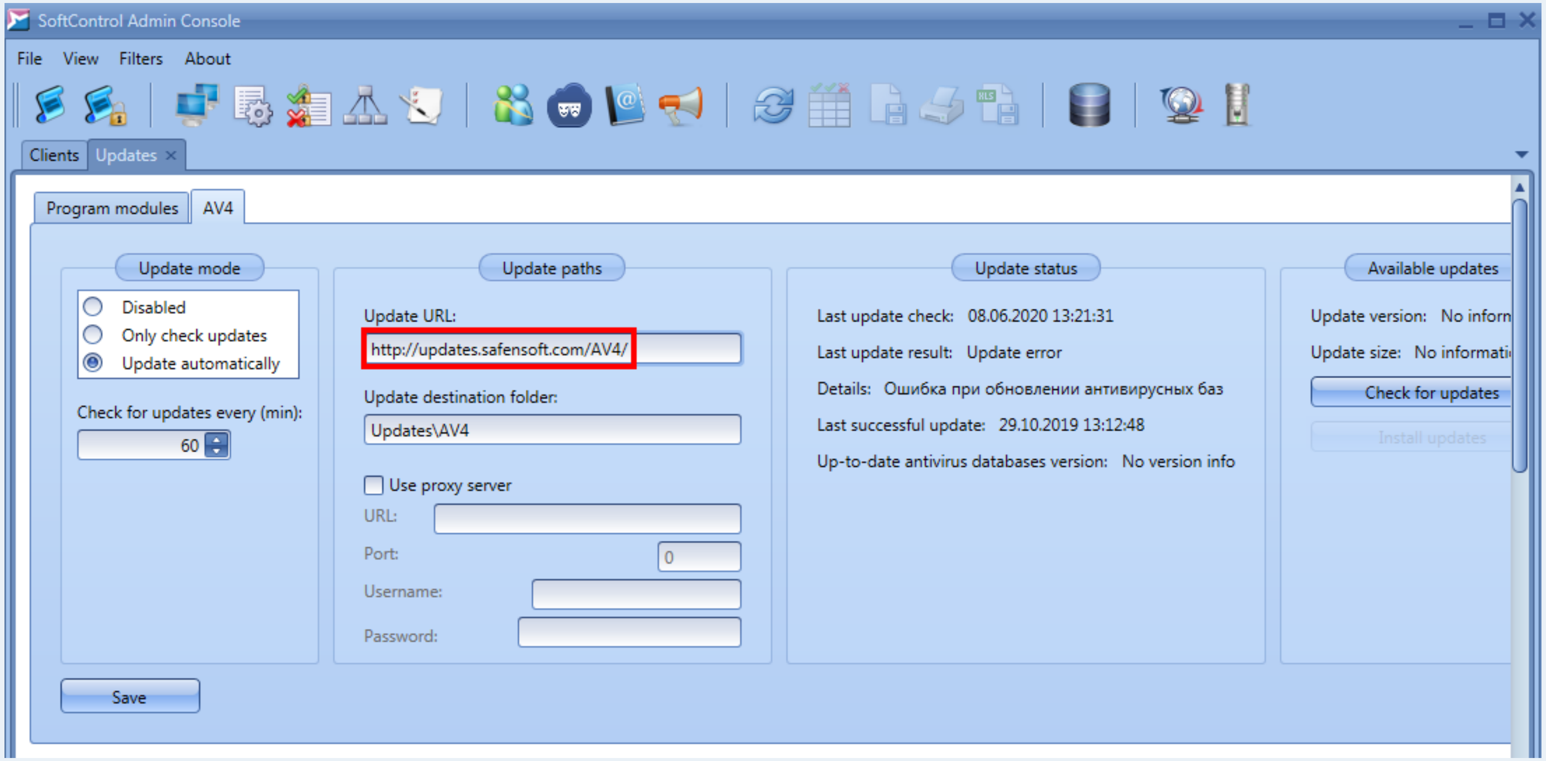
Up-to-date server version: 5.1.55.4

Up-to-date console version: 5.1.55.4

Update version: No information

Update size: No information

3) To set up antivirus database updates, switch to **Antivirus bases** tab. In **Update paths** area, edit text in **Update URL** field. Insert your test (release) license key in the update path `http://updates.safensoft.com/SoftControl/AV4/EN/` as follows: `http://updates.safensoft.com/<license key>/SoftControl/AV4/EN/`. For **Antivirus bases** tab, it is recommended to leave **Update automatically** selected in **Update mode** area.



Update mode:
- ○ Disabled
- ○ Only check updates
- ● Update automatically

Check for updates every (min): 60

Update URL: http://updates.safensoft.com/AV4/

Update destination folder: Updates\AV4

□ Use proxy server

URL:

Port: 0

Username:

Password:

Last update check: 08.06.2020 13:21:31

Last update result: Update error

Details: Ошибка при обновлении антивирусных баз

Last successful update: 29.10.2019 13:12:48

Up-to-date antivirus databases version: No version info

Update version: No inforn

Update size: No informati

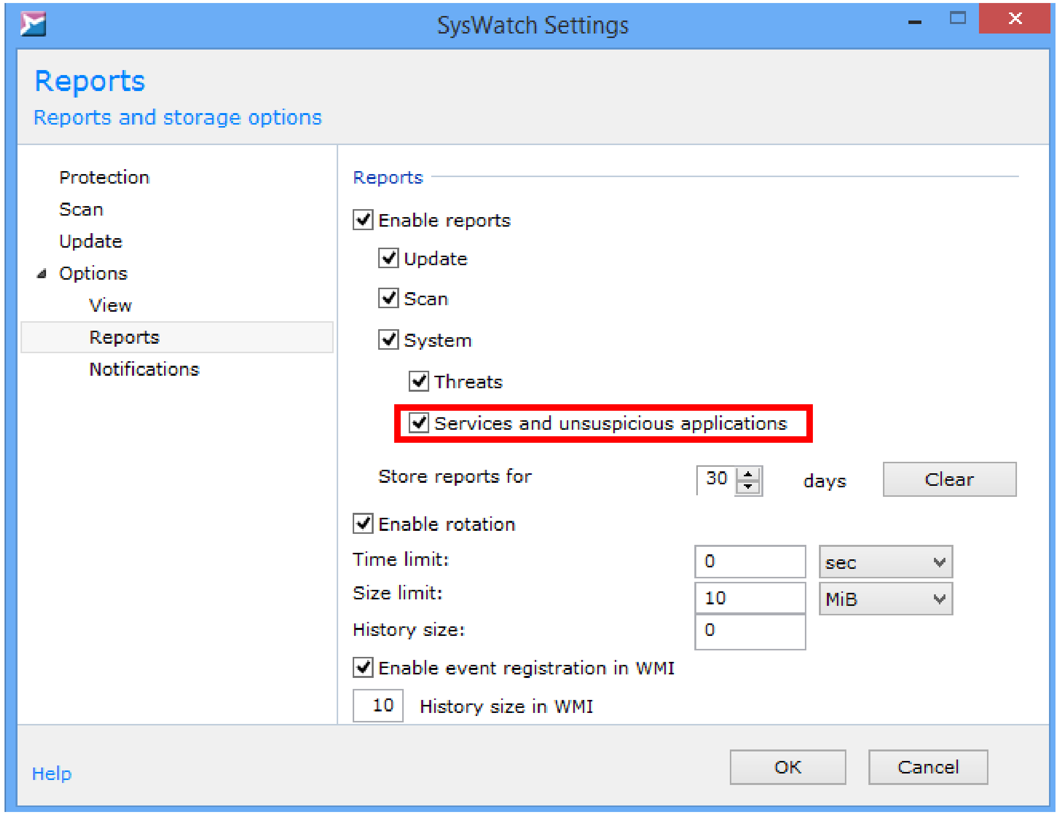
5.3	Copy and save the configuration file for initial connection between SoftControl SysWatch client modules and SoftControl Service Center – *ClientSettings.xmlc*.	□ *ClientSettings.xmlc* configuration file has been saved.	*ClientSettings.xmlc* is located at *C:\ProgramData\SafenSoft* on the server.

2.2.2 How to deploy the client module SoftControl SysWatch on device 1

Table 6. SoftControl SysWatch deployment

No.	Action	Expected outcome	Comment
6.1	Run self-test on the device to check its performance and functioning.	☐ Device functional self-test has been successful.	Functional self-test of the device is performed by Client's personnel.
6.2	Install and perform initial configuring of the client component SoftControl SysWatch.		
6.2.1	Install the client component SoftControl SysWatch in the logging mode.* Select one of the two client module installation packages depending on whether you have an antivirus installed: • *SysWatch.msi* with the embedded antivirus; • *SysWatch_Patch.msi* without the antivirus.	☐ Successful installation, the installation log does not contain any errors.	System administrator rights are required. If you are installing *SysWatch_Patch.msi* without the antivirus, you have to adjust compatibility settings for the antivirus you have installed on the device. See *SW_<version_number_and_higher>+KAV+NOD32.docx* (in Russian).
* Use the command prompt to perform installation in the logging mode: • `msiexec /i "C:\Installers\SysWatch.msi" /log C:\Installers\installlog.txt` • `msiexec /i "C:\Installers\SysWatch_Patch.msi" /log C:\Installers\installlog.txt` For the pilot project stage, uncheck **Collect system profile after installation** when you install the client module SoftControl SysWatch. Profile collection is a lengthy operation. Its duration can be compared to antivirus scanning. Due to this, you can install SoftControl SysWatch without profile collection on devices that are not very efficient (self-service devices, ATMs, process control application consoles). In this case, you can collect the profile remotely by sending a task from SoftControl Service Center. See How to deploy the client component SoftControl SysWatch on a standard device from a package installer remotely 33 for installation of SoftControl SysWatch by means of the batch installer without profile collection upon installation (with following update of antivirus databases and profile collection from the server).			
6.2.2	Create preset control policy parameters in SoftControl SysWatch.		Specific parameters can be recommended for specific devices. See *TPS_<version_number>-Deployment_Guide-RU.pdf (in Russian)*.
6.2.2.1	Turn on logging of services and unsuspicious applications. *	☐ The *system_.txt* log contains system application activity events.	This allows you to get a detailed log of events that relate to application activity in the system of the device. It's helpful for determining collisions and creating exceptions in control rules.

* In order to turn on logging of **Services and unsuspicious applications**, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. SoftControl SysWatch window will open. Select **Options** –> **Reports** on the left and make sure that **Services and unsuspicious applications** is checked. If it is not checked, check it and click **OK** to apply the settings.



Reports

Reports and storage options

Reports

☑ Enable reports

☑ Update

☑ Scan

☑ System

☑ Threats

☑ Services and unsuspicious applications

Store reports for 30 days

☑ Enable rotation

Time limit: 0 sec

Size limit: 10 MiB

History size: 0

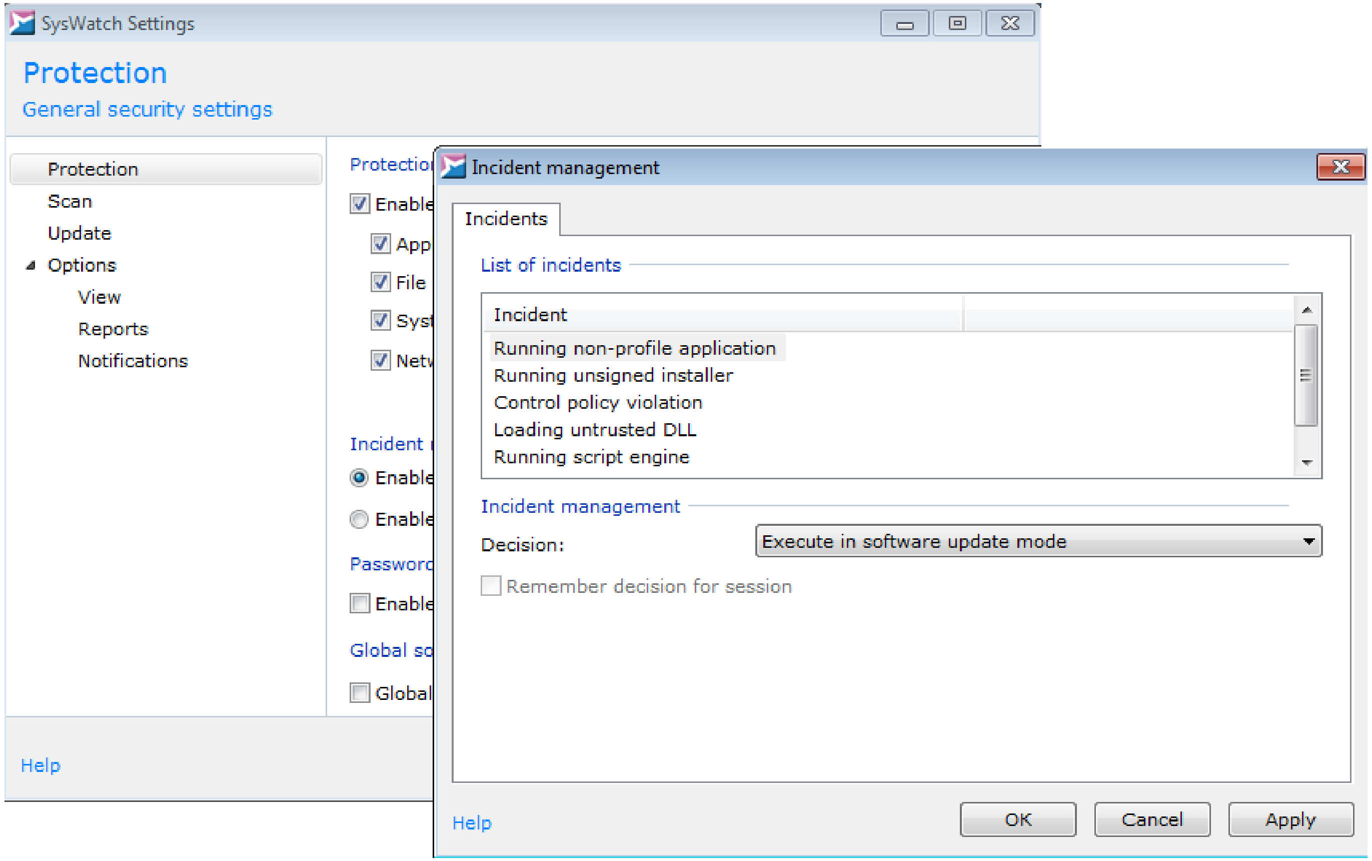
☑ Enable event registration in WMI

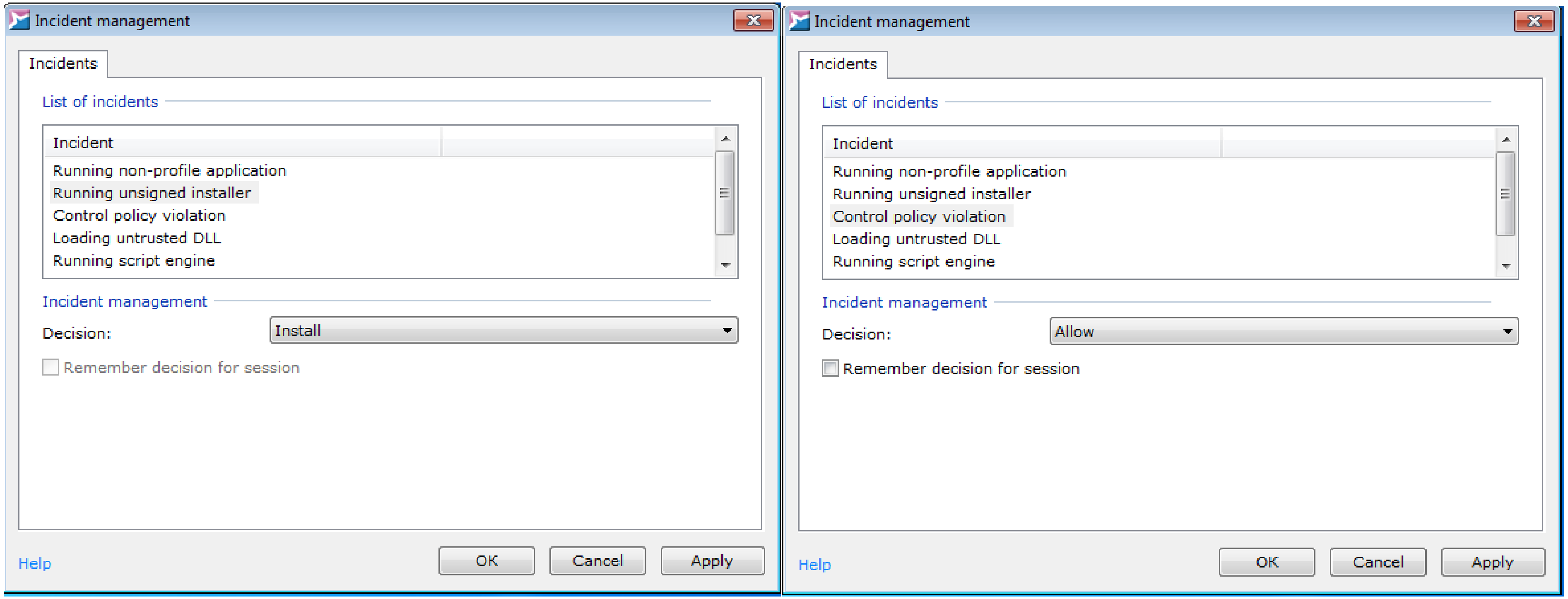
10 History size in WMI

6.2.2.2	Turn on the auditing mode.*	❑ The auditing mode is on.	When the auditing mode is on, SoftControl SysWatch does not block applications upon **Running non-profile application**, **Running unsigned installer**, **Policy violation**, **Loading untrusted DLL**, **Running script engine**, and **Modification of PE file by non-installer** events. It means that performance of system tasks and applications will not be affected by operations of the defense module.

* In order to turn on the auditing mode, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. SoftControl SysWatch windows will open. Select **Protection** on the left and make sure that **Enable automatic incident processing** is checked (**Incident management** area). Click **Configure**. In **Incident management**, set the following settings:

- Running non-profile application – Execute in software update mode;
- Running unsigned installer – Install;
- Control policy violation – Allow;
- Loading untrusted DLL – Allow;
- Running script engine – Allow;
- Modification of PE file by non-installer – Allow.


SysWatch Settings
Protection
General security settings
Protection
Scan
Update
Options
View
Reports
Notifications
Protectio
☑ Enable
☑ App
☑ File
☑ Syst
☑ Netv
Incident
● Enable
○ Enable
Passwor
☐ Enable
Global sc
☐ Global
Help
Incident management
Incidents
List of incidents
Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine
Incident management
Decision:
Execute in software update mode
☐ Remember decision for session
Help
OK
Cancel
Apply



Incident management

Incidents

List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Install

□ Remember decision for session

Incident management

Incidents

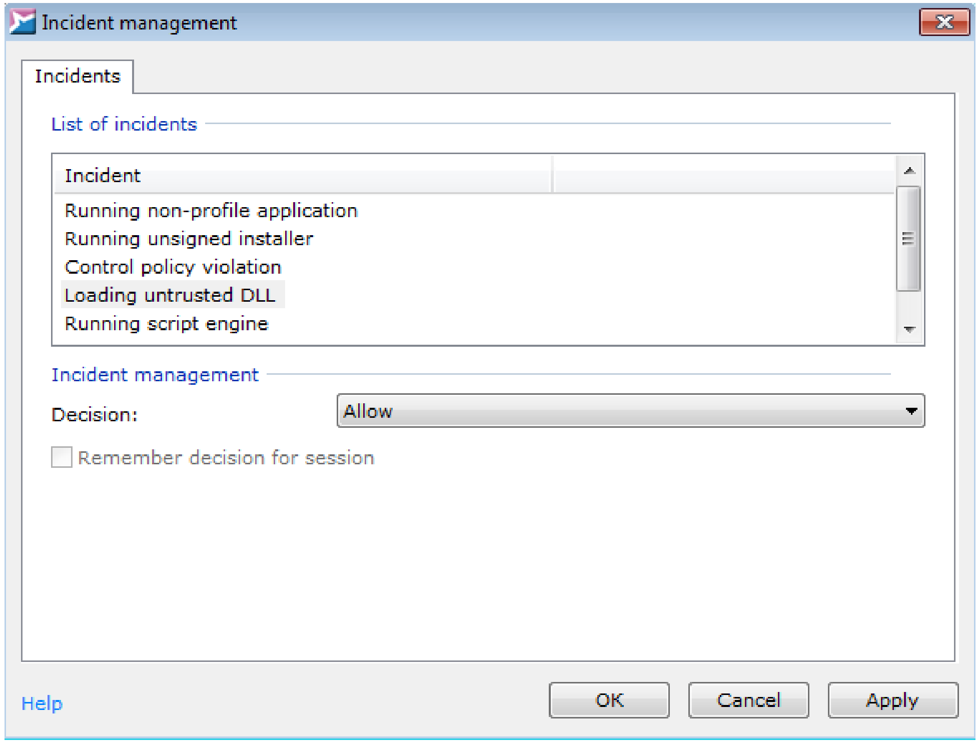
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



Incident management

Incidents

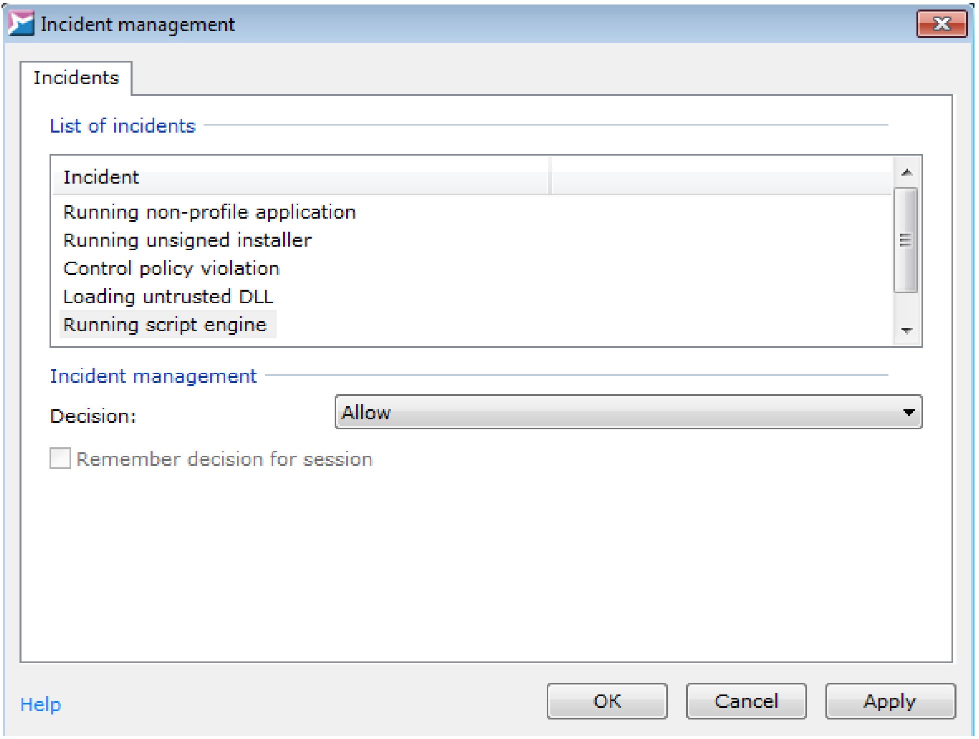
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



Incident management

Incidents

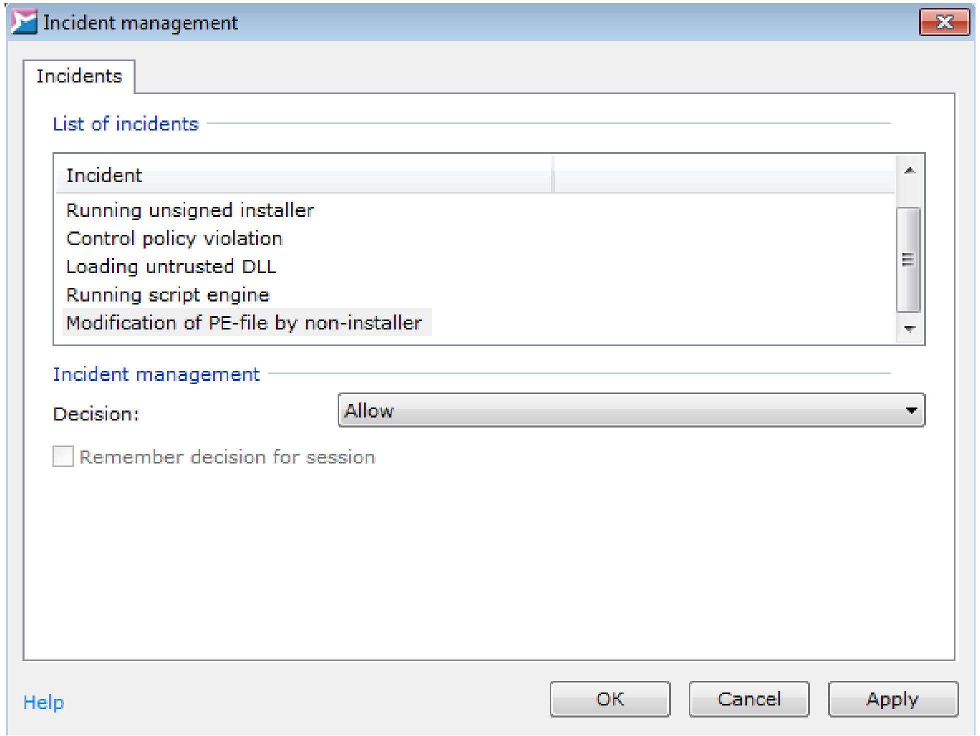
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



Incident management

Incidents

List of incidents

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

Incident management

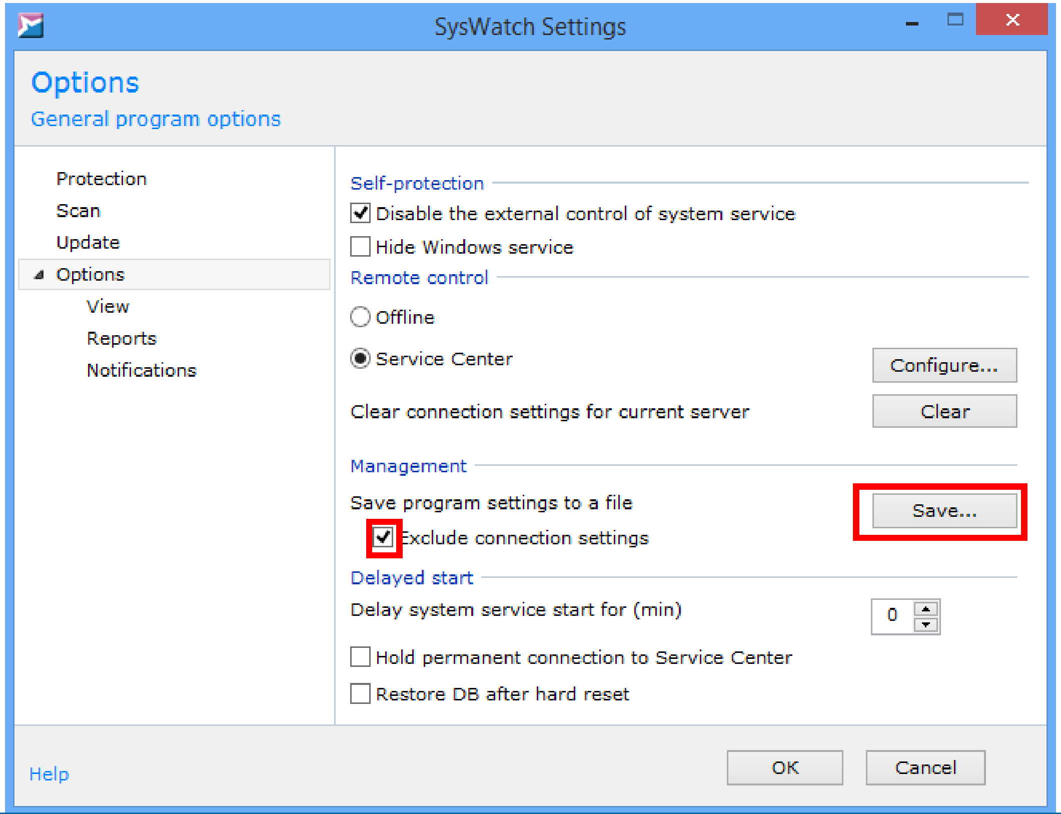
Decision: Allow

□ Remember decision for session

Click **Apply**.

6.2.3	Save *Config.xmlc* – the configuration file for the client module SoftControl SysWatch installed on the device. This file contains preset configuration for compliance and exclusion of control policies.*	❑ *Config.xmlc* has been saved.	The configuration file will be used for the package installer.

* In order to save the configuration file *Config.xmlc*, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. SoftControl SysWatch windows will open. Select **Options** on the left. Check **Exclude connection settings** in **Management** area and click **Save**. Select the destination folder (e.g., **My documents**) and save the file as *Config.xmlc*.



SysWatch Settings

Options

General program options

Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

☑ Exclude connection settings

Delayed start

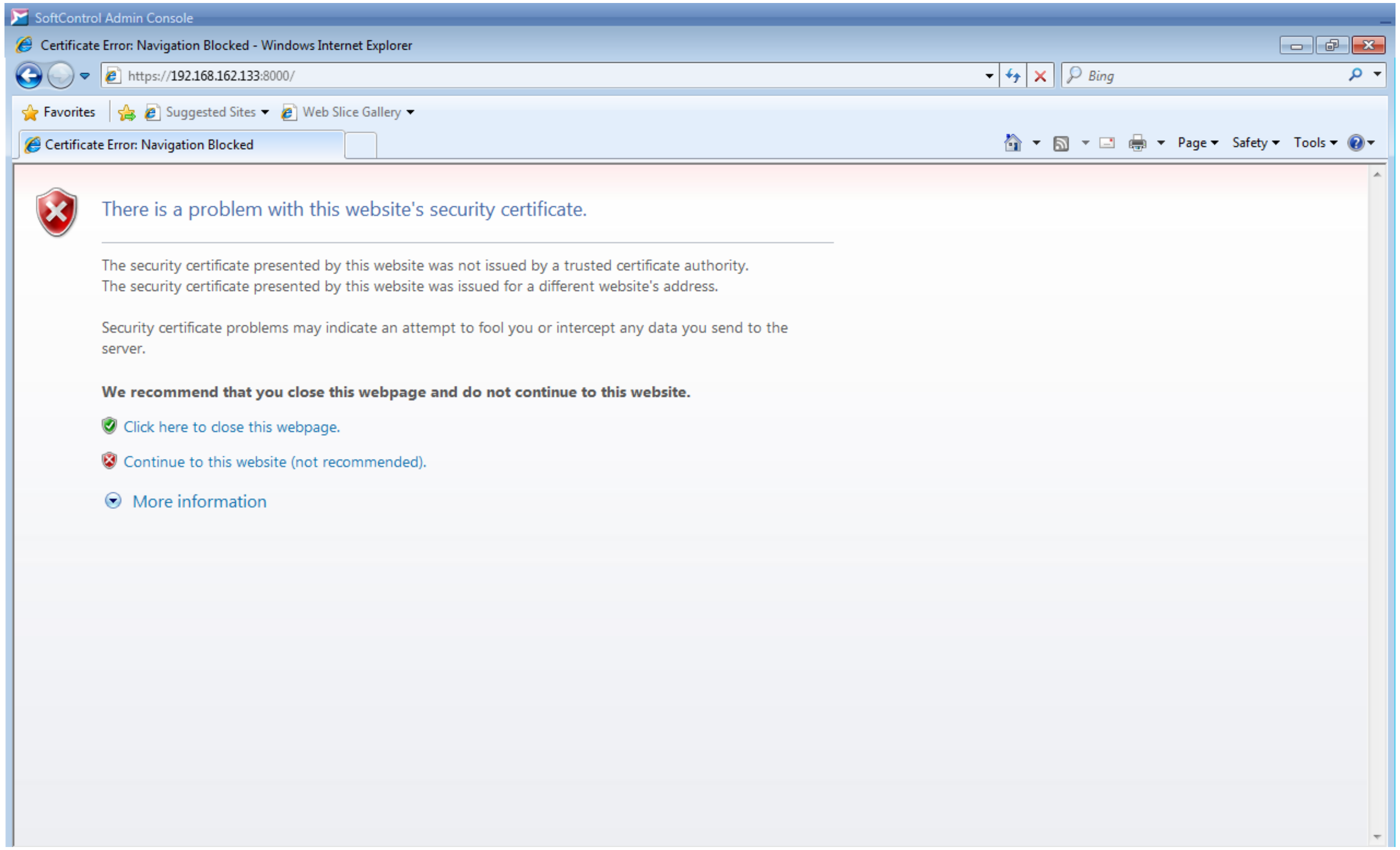
Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

6.3	Check the device network configuration in regards to availability of connection between the devices and the server by ports 8000 and 8088.*	❑ Port connection has been confirmed.	If the workstation for deployment of SoftControl Service Center is inside a domain, add the server certificate to the list of trusted certificates in the domain policy settings.

* Open Internet Explorer on the client device and enter the address of SoftControl Server and the port for client's connection (8000 by default), e.g., https://192.168.1.181:8000. If the server is available, the browser will display the message about an unknown certificate.
If SoftControl Admin Console is installed separately from SoftControl Server (on a different computer), you will need to check the connection with SoftControl Service Center. To do this, enter the server address and the port number for SoftControl Admin Console (8088 by default) in Internet Explorer, e.g., http://192.168.1.181:8088. If the server is available, the browser will display the message about an unknown certificate.


SoftControl Admin Console
Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.162.133:8000/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Certificate Error: Navigation Blocked
Page
Safety
Tools

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

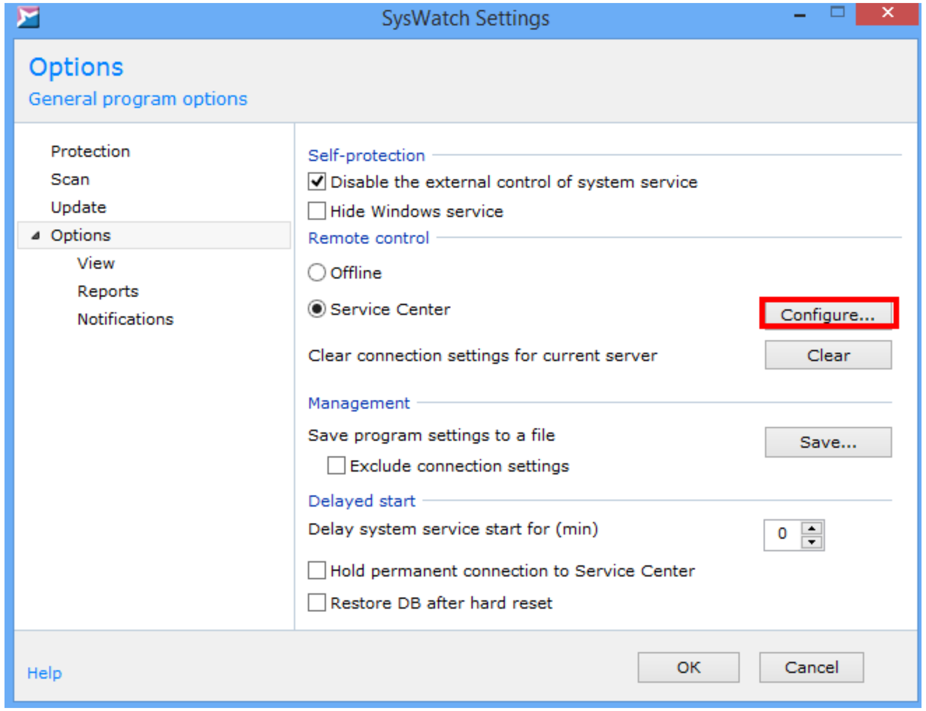
Continue to this website (not recommended).

More information

6.4	Connect the client module SoftControl SysWatch to SoftControl Service Center.*		Request to connect to the server has been sent.

In order to save the configuration file *Config.xmlc*, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. SoftControl SysWatch windows will open. Select **Options** on the left. Check **Exclude connection settings** in **Management** area and click **Save**. Select the destination folder (e.g., **My documents**) and save the file as *Config.xmlc*.

* In order to connect the client module to SoftControl Service Center, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. Then select **Options** on the left. In **Remote control** area, select **Service Center** and click **Configure**.



SysWatch Settings

Options

General program options

Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

□ Exclude connection settings

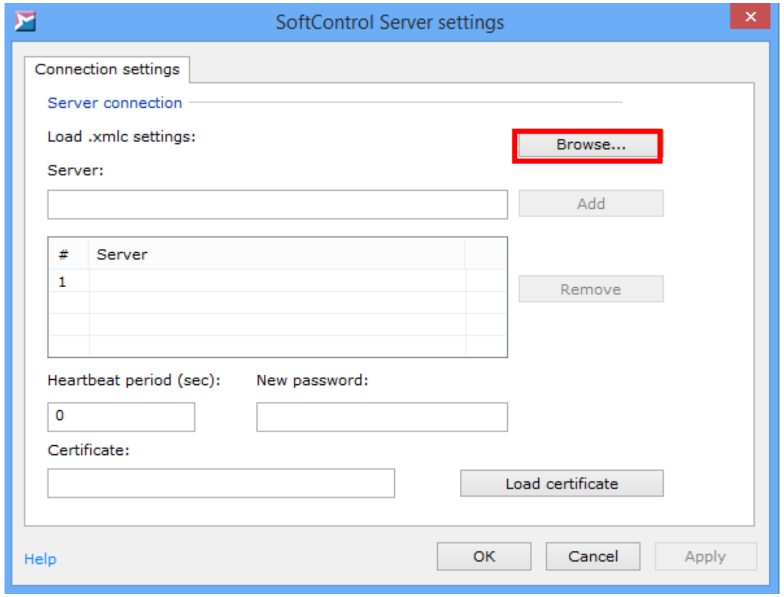
Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

SoftControl server settings window will open. Click **Browse** and open the *ClientSettings.xmlc* from item 5.3[14] that you copied to the client device:



Then click **OK** to send a connection request to SoftControl Service Center.

6.5	Reload the client device.	□ The client device has been reloaded.	
6.6	Run device self-test to check efficiency and performance.	□ Device functional self-test has been successful.	Functional self-test of the device is performed by Client's personnel.
6.7	Build SNSDumpTool logs. *	□ Logs have been built successfully. *C:\SNS\SnsDump.zip file has been created.*	Administrator rights are required for building logs.

* To build SNSDumpTool logs, download the utility for your OS version:

- `http://updates.safensoft.com/<license_number>/39/TOOLS/Setup_SnsDumpTool_x64.exe`,
- `http://updates.safensoft.com/<license_number>/39/TOOLS/Setup_SnsDumpTool_x86.exe`.

Then open the file as Administrator.

6.8	Provide ARUDIT SECURITY, LLC with the configuration file from 6.7(14) and SNSDumpTool logs (*C:\SNS\SnsDump.zip*).	□ *ClientSettings.xmlc* and *SnsDump.zip* files have been mailed to support@safensoft.com.	This step is useful for diagnostics in case you run into any trouble during deployment.

2.3 Operational and functional tests for the SoftControl system

2.3.1 How to create a package installer for the client component SoftControl SysWatch

Table 7. Package installer creation

No.	Action	Expected outcome	Comment
7.1	Prepare the package installer for the client component SoftControl SysWatch[1] with the following contents: • installation package for the client component SoftControl SysWatch (*SysWatch.msi* or *SysWatch_Patch.msi*); • configuration file for initial connection to SoftControl Service Center (*ClientSettings.xmlc*);[2] • preset configuration file (*Config.xmlc*) for auditing mode;[3] • certificate: VeriSign Class 3 Public Primary Certification Authority – *G5.cer*;[4] • installation script that places the certificate of the client module SoftControl SysWatch into the Windows storage;[5] • script for launching the package installer in the quiet mode with logging of the installation process.	□ A CMD script or an SFX archive with *.exe* extension has been created. It contains the contents listed in **Action** column.	The package installer is prepared by Client's personnel. Installation requires administrator rights.
[1] In order to prepare the package installer, place the SoftControl SysWatch installation package, configuration files, the certificate that was used to sign the SoftControl SysWatch installation package (if it is necessary), and the launching script of the package installer into a folder. Here is an example of the package installation script *install-sns.cmd*:			

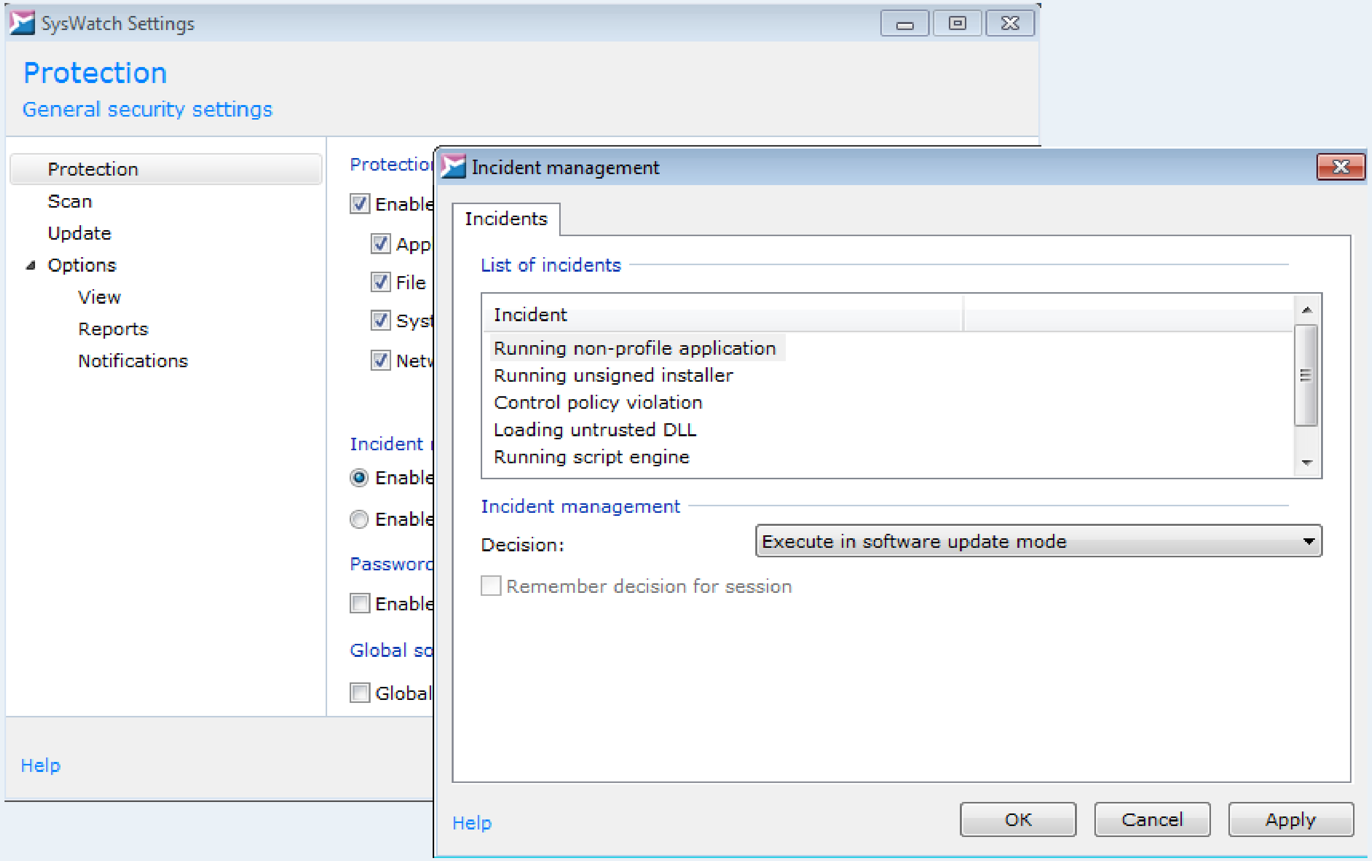
```
@echo off
Set folder=C:\SnS-install
set workdir=%~dp0
set config=%folder%config.xmlc
echo making directory
md %folder%
echo copy files
xcopy "%workdir%ClientSettings.xmlc" %folder% /Y
xcopy "%workdir%config.xmlc" %folder% /Y
xcopy "%workdir%SysWatch.msi" %folder% /Y
xcopy "%workdir%VeriSign Class 3 Public Primary Certification Authority - G5.cer" %folder% /Y
echo install cert
certutil -addstore Root "C:\SnS-install\VeriSign Class 3 Public Primary Certification Authority - G5.cer"
echo install syswatch
call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-install\config.xmlc" tsconfig="C:\SnS-install\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-install\install-log.txt"
echo exit
exit
```

This script can be transformed into an SFX archive and signed with Client's certificate.

[2] The configuration file for initial connection to SoftControl Service Center (*ClientSettings.xmlc*) is on the server in *C:\ProgramData\SafenSoft* folder.

[3] In order to turn on the auditing mode, find the SoftControl SysWatch icon in the system tray and click on it with the right button of your mouse. Select **Settings**. SoftControl SysWatch windows will open. Select **Protection** on the left and make sure that **Enable automatic incident processing** is checked (**Incident management** area). Click **Configure**. In **Incident management**, select the following settings:

- Running non-profile application – Execute in software update mode;
- Running unsigned installer – Install;
- Control policy violation – Allow;
- Loading untrusted DLL – Allow;
- Running script engine – Allow;
- Modification of PE file by non-installer – Allow.



Incident management

Incidents

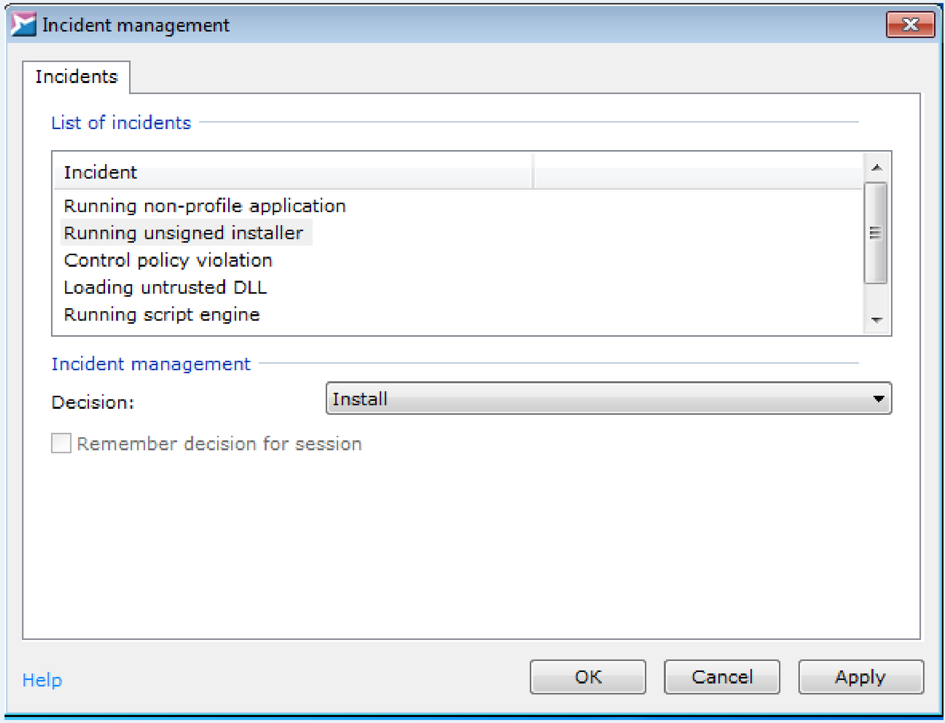
List of incidents

Incident	
Running non-profile application	
Running unsigned installer	
Control policy violation	
Loading untrusted DLL	
Running script engine	

Incident management

Decision: Execute in software update mode

□ Remember decision for session



Incident management

Incidents

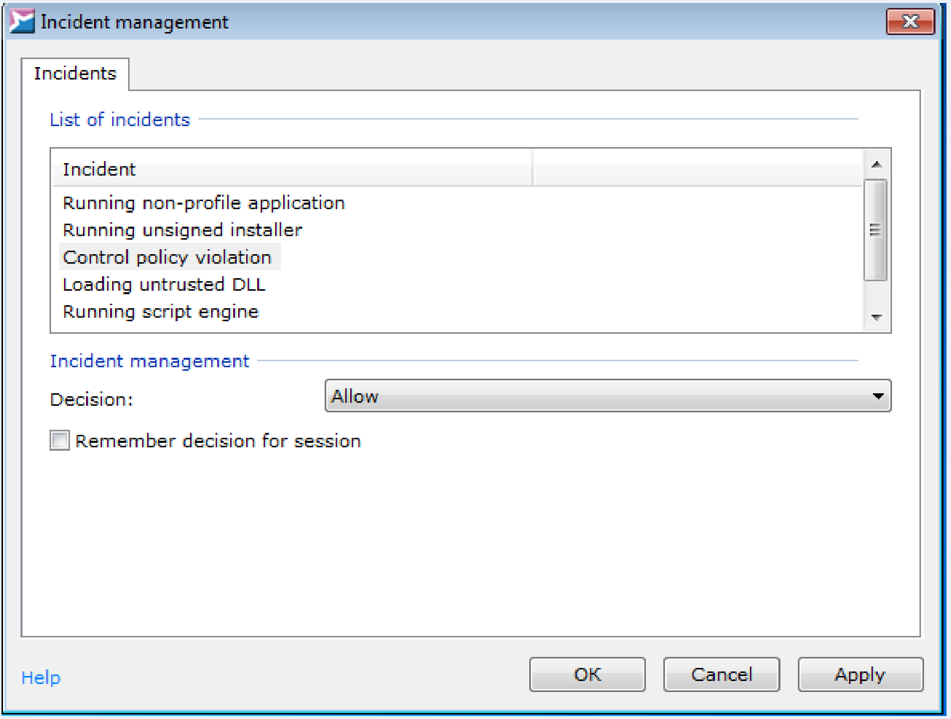
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Install

□ Remember decision for session



Incident management

Incidents

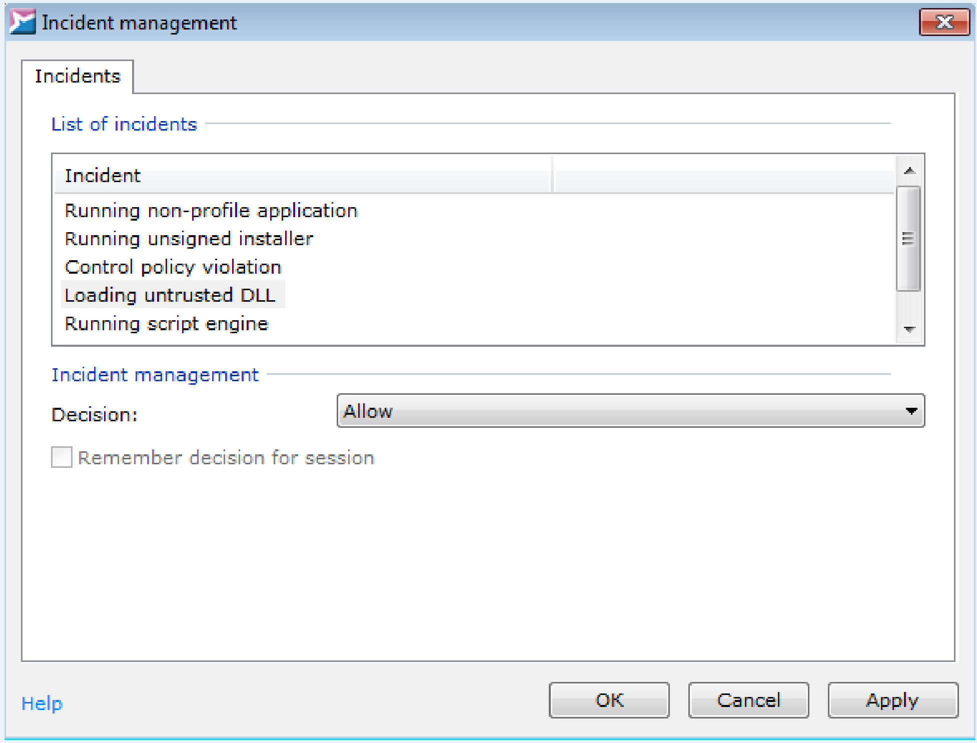
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



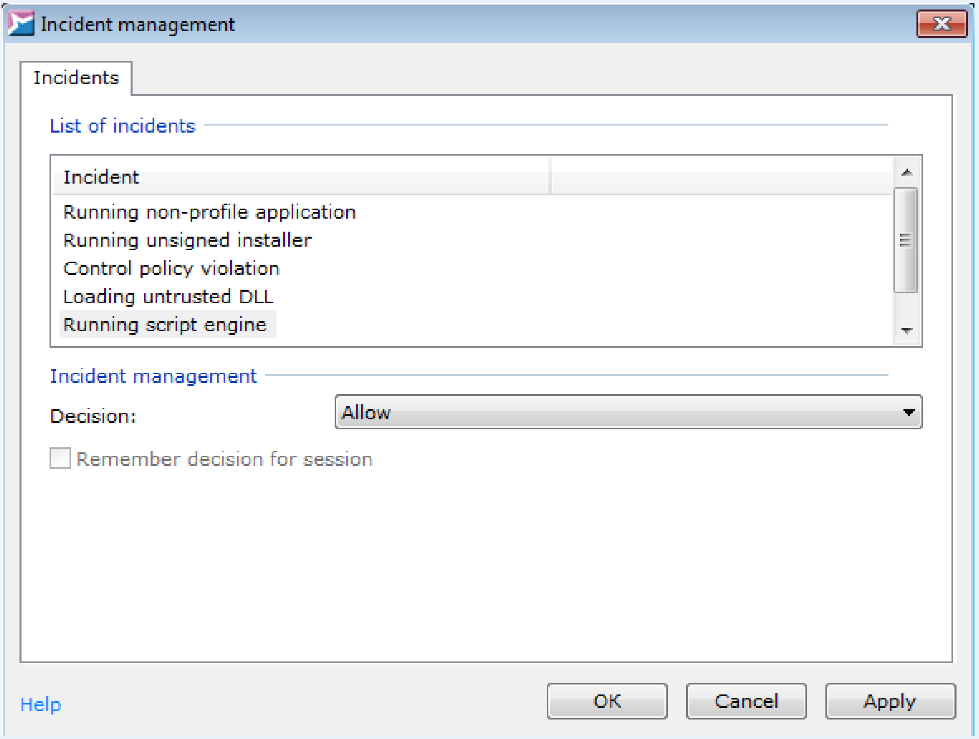
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



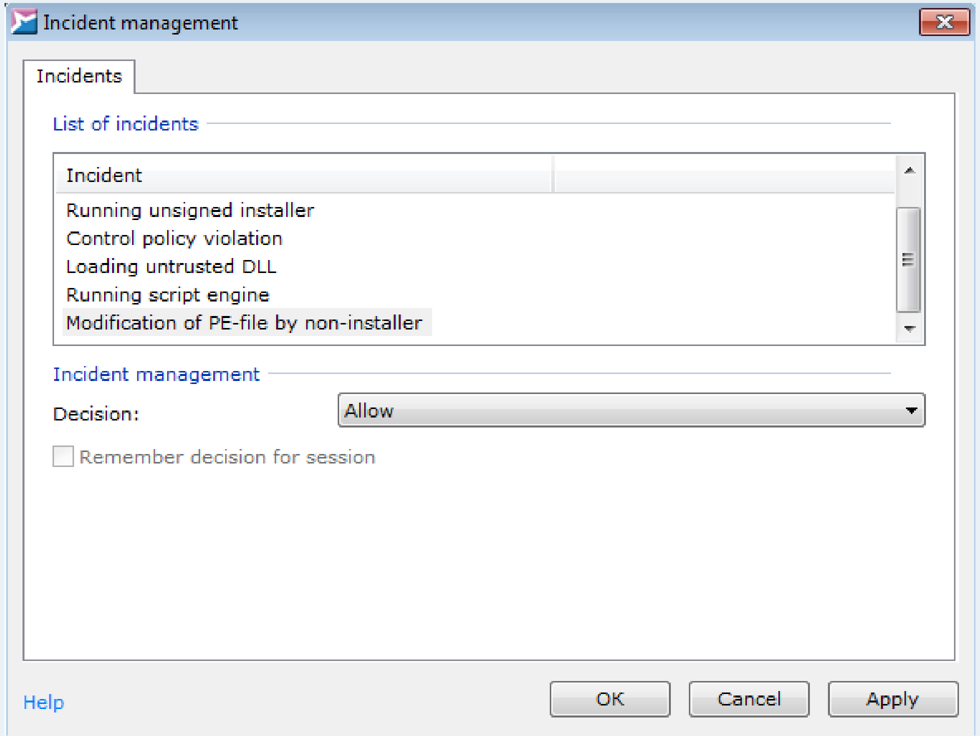
List of incidents

Incident
Running non-profile application
Running unsigned installer
Control policy violation
Loading untrusted DLL
Running script engine

Incident management

Decision: Allow

□ Remember decision for session



Incident management

Incidents

List of incidents

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

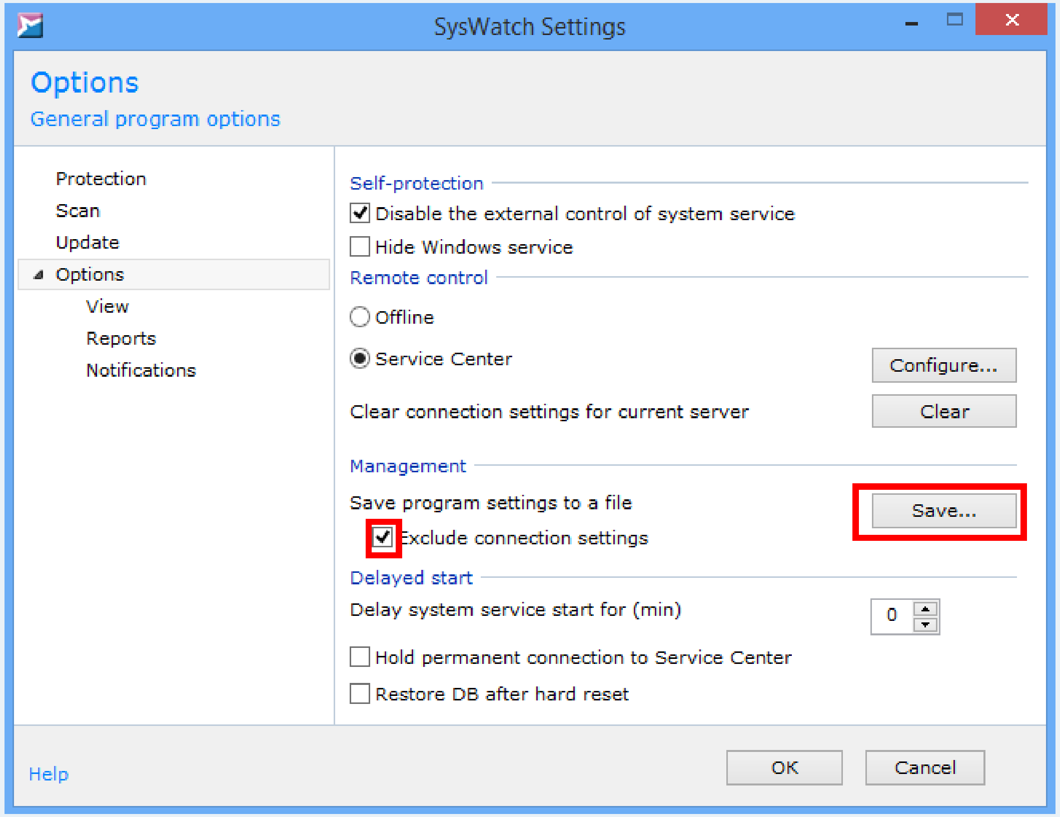
Incident management

Decision: Allow

□ Remember decision for session

Then click **OK**.

To save the configuration file *Config.xmlc*, find the SoftControl SysWatch icon in the system tray and click on it with the right button of your mouse. Select **Settings**. SoftControl SysWatch windows will open. Select **Options** on the left. Check **Exclude connection settings** in **Management** area and click **Save**. Select the destination folder (e.g., **My documents**) and save the file as *Config.xmlc*.



SysWatch Settings

Options

General program options

Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

☑ Exclude connection settings

Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

[4] You can get the VeriSign Class 3 Public Primary Certification Authority certificate (*G5.cer*) from the client host that SoftControl SysWatch is installed on (trusted root certification authorities list).

[5] To add the certificate of the client module SoftControl SysWatch to the Windows storage, you will need the *certutil.exe* utility with its library *certadm.dll*. They are both included in the Windows Server 2003 Administration Tools Pack: https://www.microsoft.com/en-US/Download/details.aspx?id=16770.

2.3.2 How to deploy the client component SoftControl SysWatch on a standard device from a package installer remotely

Table 8. Remote deployment of SoftControl SysWatch

No.	Action	Expected outcome	Comment
8.1	Deploy the client component SoftControl SysWatch from the package installer on a standard device in the pilot zone.		SoftControl SysWatch client shall be deployed from the package installer on a device that has the same parameters as the device that was used for creating the settings in items 6.3[14] and 6.2.3[21].
8.1.1	Deliver the package installer of the client component SoftControl SysWatch to a standard device by means of a remote file exchange environment.	❑ The package installer has been added to the file system on the device.	The package installer is delivered to the file system of the device by means of the Client's remote file exchange environment. Note how long this operation takes in order to set the standard time for the deployment operation.
8.1.2	Run the package installer launching script* with remote administration tools.	❑ The SoftControl SysWatch installation log has been created without errors. ❑ There is a new SoftControl SysWatch client in SoftControl Admin Console. The new client's status is **Pending.**	The package installer is launched by the Client's personnel with remote administration tools deployed on standard the Client's standard device.
* Here is an example of a launching script. In this case, the installation package for the client module SoftControl SysWatch, the configuration file for the master image of SoftControl SysWatch *config.xmlc*, and the configuration file for connection to the server *ClientSettings.xmlc* are located at *C:\SnS-install*. `call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-install\config.xmlc" tsconfig="C:\SnS-install\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-install\install-log.txt"`			
8.1.3	Administrator can see a new client in SoftControl Admin Console.	❑ There is a new SoftControl SysWatch client in SoftControl Admin Console. The new client's status is **Pending**.	

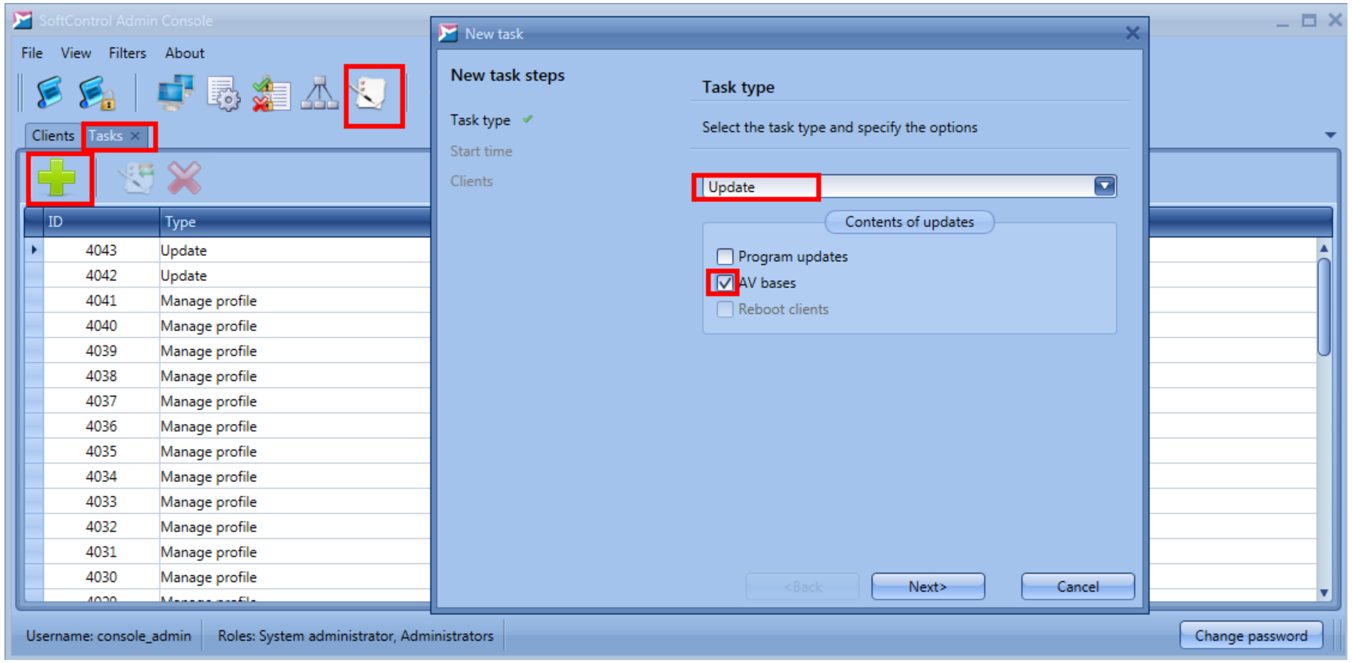
2.3.3 How to create and apply group control policy configurations from the server SoftControl Service Center

Table 9. Creation and application of configurations from SoftControl Server

No.	Action	Expected outcome	Comment
9.1	Create and apply group control policy configurations from SoftControl Server.		There shall be several control policy configurations for different use cases: • "Production" – the strictest control policy configuration. It protects software from all change attempts. This configuration shall be applied to a device in its normal operation state (servicing Bank customers). It is not for maintenance works. • "For Services" – a control policy configuration that allows performance of permitted maintenance actions with the software on the device while the protection mode on.
9.1.1	Create group control policy configurations.		
9.1.1.1	Create control policy configurations: "Production" and "Production-Audit" (based on "Production").	❑ "Production" and "Production-Audit" configurations have been created.	Control policy configurations are created by the Client's personnel and are subject to adjustment in accordance with the Client's information security policy. Standard control policy configurations are described in *Политики_контроля_SoftControl_ATM.xlsx* (in Russian). You will need a USB drive to perform tests when you create control policies for the USB whitelist.
9.1.2	Create organizational units.		An organizational unit is a group of devices with common group control policies.
9.1.2.1	Create "Production" organizational unit and assign "Production-Audit" configuration to it.	❑ "Production" organizational unit has been created and assigned "Production-Audit" configuration.	
9.1.3	Move clients to organizational units with group policy configurations.		
9.1.3.1	Move SoftControl SysWatch clients to "Production" organizational unit.	❑ SoftControl Admin Console displays SoftControl SysWatch client's settings state as **Applied**	

		successfully and the "Production" organizational unit. ❑ The event log for SoftControl SysWatch in SoftControl Admin Console has a *Settings changed from server* record. You can view additional information.	
9.2	Start the task to update antivirus databases on device 1.* (This operation can be optional if you need to save traffic on the endpoint device.)	❑ SoftControl Admin Console displays SoftControl SysWatch client's state as **Update – Installed** (**Info** column).	Updating of AV4 antivirus databases **requires** installation of "Microsoft Visual C++ 2008 Redistributable Package" (*vcredist_x86_2008.exe*).

* In order to start the task to update antivirus databases, click on icon (**Tasks**) in SoftControl Admin Console to open the **Tasks** tab. Click on ✚ (**New**). **New task** window will open. Select **Task type – Update**, check **AV bases**, and click **Next:**



Task type: Update

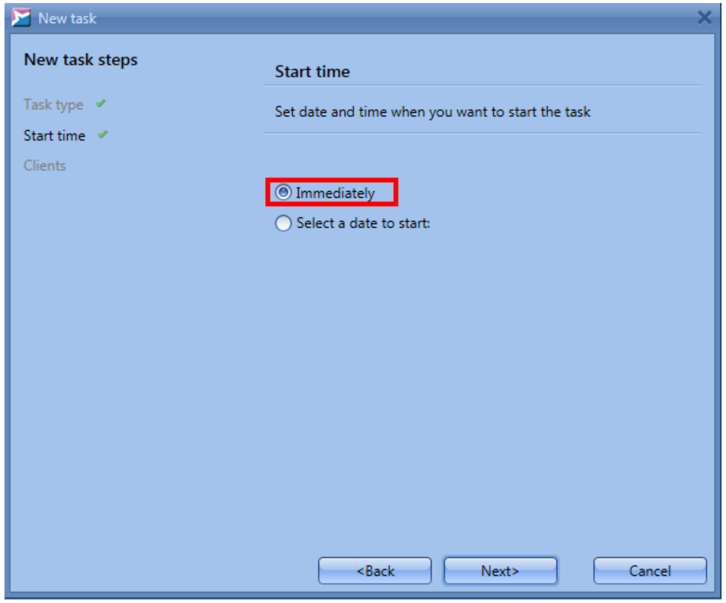
□ Program updates
☑ AV bases
□ Reboot clients

ID	Type
4043	Update
4042	Update
4041	Manage profile
4040	Manage profile
4039	Manage profile
4038	Manage profile
4037	Manage profile
4036	Manage profile
4035	Manage profile
4034	Manage profile
4033	Manage profile
4032	Manage profile
4031	Manage profile
4030	Manage profile

Username: console_admin

Roles: System administrator, Administrators

In the next window, specify time for the task (**Immediately** in our case) and click **Next**.



New task

New task steps

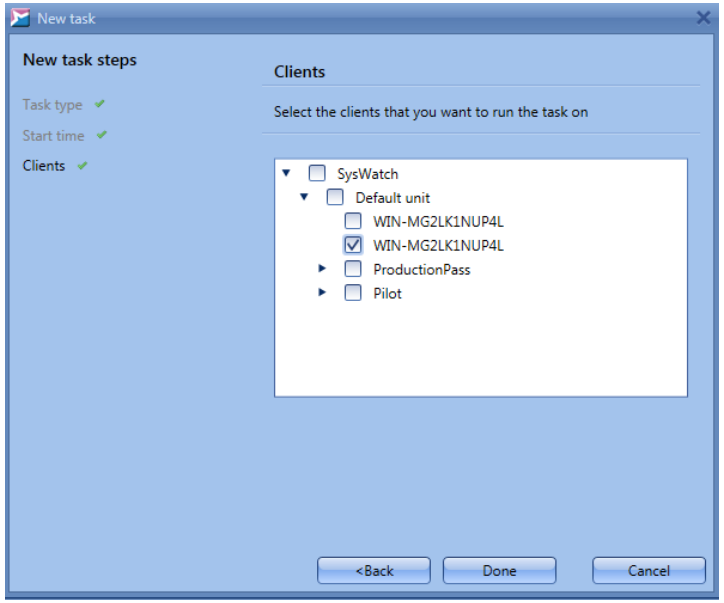
Task type ✓
Start time ✓
Clients

Start time

Set date and time when you want to start the task

● Immediately
○ Select a date to start:

In the **Clients** window, select the clients that you want antivirus databases to be updated on. Click **Done**.



New task

New task steps

Task type ✓

Start time ✓

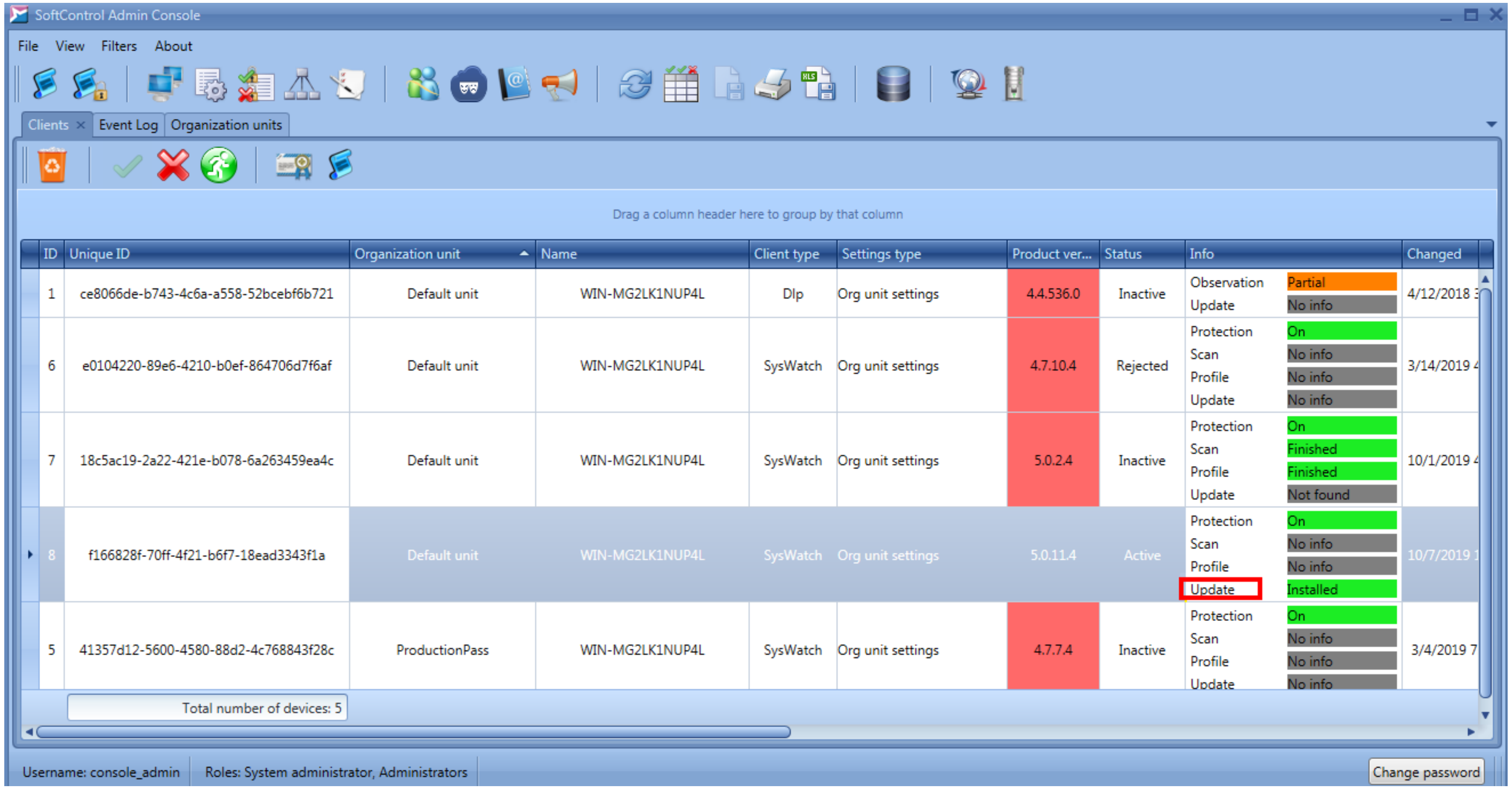
Clients ✓

Clients

Select the clients that you want to run the task on

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

When the update is completed, you will see **Installed** status in the **Info – Update** field for SoftControl SysWatch client (**Clients** tab).


SoftControl Admin Console
File
View
Filters
About
Clients
Event Log
Organization units
Drag a column header here to group by that column

ID	Unique ID	Organization unit	Name	Client type	Settings type	Product ver...	Status	Info		Changed
1	ce8066de-b743-4c6a-a558-52bcebf6b721	Default unit	WIN-MG2LK1NUP4L	Dlp	Org unit settings	4.4.536.0	Inactive	Observation Update	Partial No info	4/12/2018 :
6	e0104220-89e6-4210-b0ef-864706d7f6af	Default unit	WIN-MG2LK1NUP4L	SysWatch	Org unit settings	4.7.10.4	Rejected	Protection Scan Profile Update	On No info No info No info	3/14/2019 4
7	18c5ac19-2a22-421e-b078-6a263459ea4c	Default unit	WIN-MG2LK1NUP4L	SysWatch	Org unit settings	5.0.2.4	Inactive	Protection Scan Profile Update	On Finished Finished Not found	10/1/2019 4
8	f166828f-70ff-4f21-b6f7-18ead3343f1a	Default unit	WIN-MG2LK1NUP4L	SysWatch	Org unit settings	5.0.11.4	Active	Protection Scan Profile Update	On No info No info Installed	10/7/2019 1
5	41357d12-5600-4580-88d2-4c768843f28c	ProductionPass	WIN-MG2LK1NUP4L	SysWatch	Org unit settings	4.7.7.4	Inactive	Protection Scan Profile Update	On No info No info No info	3/4/2019 7

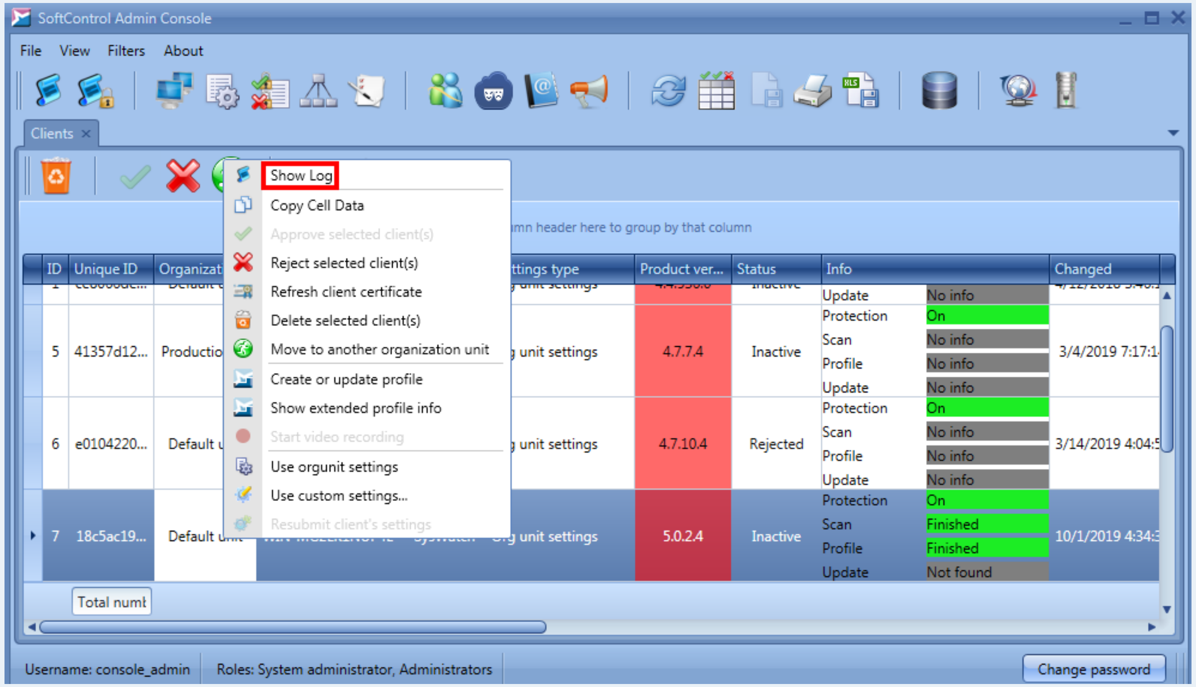
Total number of devices: 5

Username: console_admin Roles: System administrator, Administrators

9.3	Create and run the task for antivirus scanning on device 1. (This operation can be optional if it is important to save traffic on the endpoint device.)	❑ SoftControl Admin Console displays SoftControl SysWatch client's state in the **Info** column as **Scan – Finished**.	Antivirus scanning task is created and executed in line with antivirus database updating.
9.4	Create and run the task for profile collection on device 1.	❑ SoftControl Admin Console displays SoftControl SysWatch client's state in the **Info** column as **Profile – Finished**.	Profile collection task is created and executed in line with antivirus database updating.

9.5	Get logs with details of device 1 operation on the server.	❑ Logs have been gathered.	It is strongly advised to reload device 1 during the logging period. The logging period shall amount to one workday.
9.6	Export the device 1 operation log as *.xls*. Send the log to the customer support service: support@safesoft.com.	❑ The device 1 operation log has been sent to customer support.	In response, you will receive advice on additional compatibility settings, if any are required.

*In order to export logs as *.xls*, click on device 1 with the right button of your mouse on the **Clients** tab and select **Show log**.

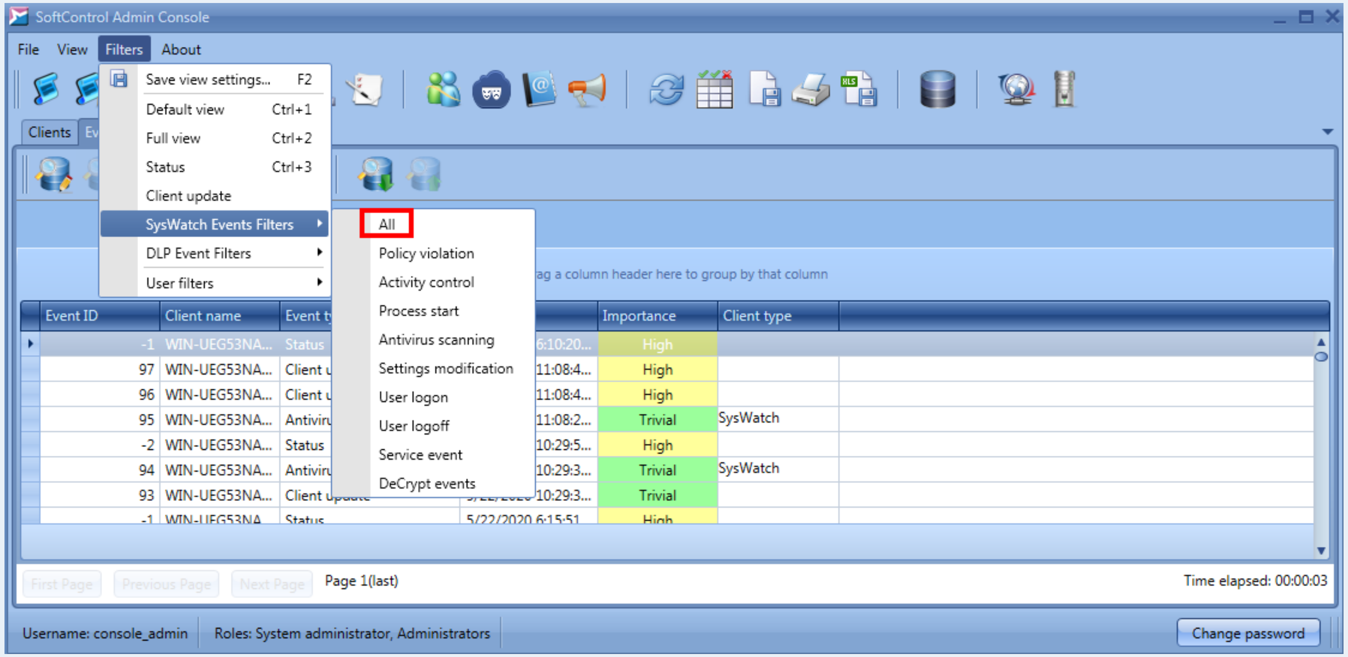

SoftControl Admin Console
File
View
Filters
About
Clients
Show Log
Copy Cell Data
Approve selected client(s)
Reject selected client(s)
Refresh client certificate
Delete selected client(s)
Move to another organization unit
Create or update profile
Show extended profile info
Start video recording
Use orgunit settings
Use custom settings...
Resubmit client's settings
...mn header here to group by that column
Total numb
Change password

ID	Unique ID	Organizat...	...ttings type	Product ver...	Status	Info		Changed
5	41357d12...	Productio...	...unit settings	4.7.7.4	Inactive	Protection Scan Profile Update	On No info No info No info	3/4/2019 7:17:1...
6	e0104220...	Default ...	...unit settings	4.7.10.4	Rejected	Protection Scan Profile Update	On No info No info No info	3/14/2019 4:04:5...
7	18c5ac19...	Default unit	...Org unit settings	5.0.2.4	Inactive	Protection Scan Profile Update	On Finished Finished Not found	10/1/2019 4:34:3...

Username: console_admin

Roles: System administrator, Administrators

The **Log** tab will open. In **Filters** menu, select **SysWatch Event Filters – All**.



Event ID	Client name	Event t		Importance	Client type
-1	WIN-UEG53NA...	Status	6:10:20...	High	
97	WIN-UEG53NA...	Client u	11:08:4...	High	
96	WIN-UEG53NA...	Client u	11:08:4...	High	
95	WIN-UEG53NA...	Antiviru	11:08:2...	Trivial	SysWatch
-2	WIN-UEG53NA...	Status	10:29:5...	High	
94	WIN-UEG53NA...	Antiviru	10:29:3...	Trivial	SysWatch
93	WIN-UEG53NA...	Client update	5/22/2020 10:29:3...	Trivial	
-1	WIN-UEG53NA...	Status	5/22/2020 6:15:51	High	

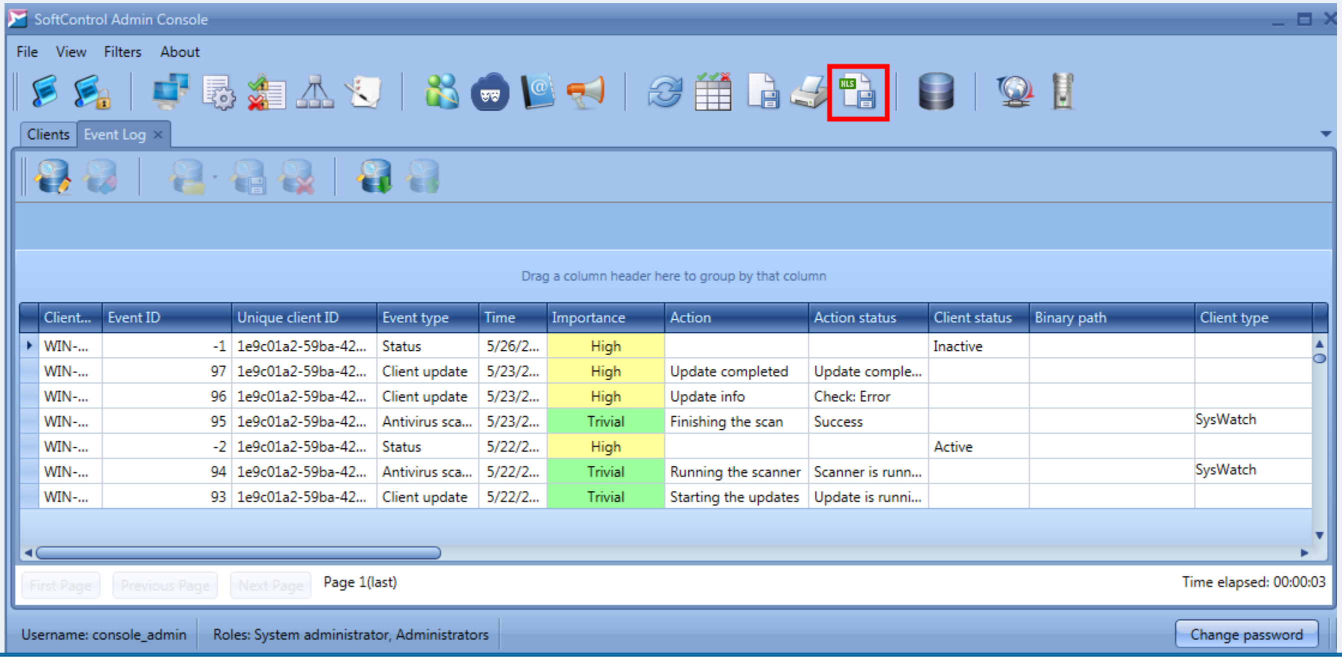
Page 1(last)

Time elapsed: 00:00:03

Username: console_admin

Roles: System administrator, Administrators

Then click on icon (**Export to Excel**) and save the file.



Drag a column header here to group by that column

Client...	Event ID	Unique client ID	Event type	Time	Importance	Action	Action status	Client status	Binary path	Client type
WIN-...	-1	1e9c01a2-59ba-42...	Status	5/26/2...	High			Inactive		
WIN-...	97	1e9c01a2-59ba-42...	Client update	5/23/2...	High	Update completed	Update comple...			
WIN-...	96	1e9c01a2-59ba-42...	Client update	5/23/2...	High	Update info	Check: Error			
WIN-...	95	1e9c01a2-59ba-42...	Antivirus sca...	5/23/2...	Trivial	Finishing the scan	Success			SysWatch
WIN-...	-2	1e9c01a2-59ba-42...	Status	5/22/2...	High			Active		
WIN-...	94	1e9c01a2-59ba-42...	Antivirus sca...	5/22/2...	Trivial	Running the scanner	Scanner is runn...			SysWatch
WIN-...	93	1e9c01a2-59ba-42...	Client update	5/22/2...	Trivial	Starting the updates	Update is runni...			

Page 1(last)

Time elapsed: 00:00:03

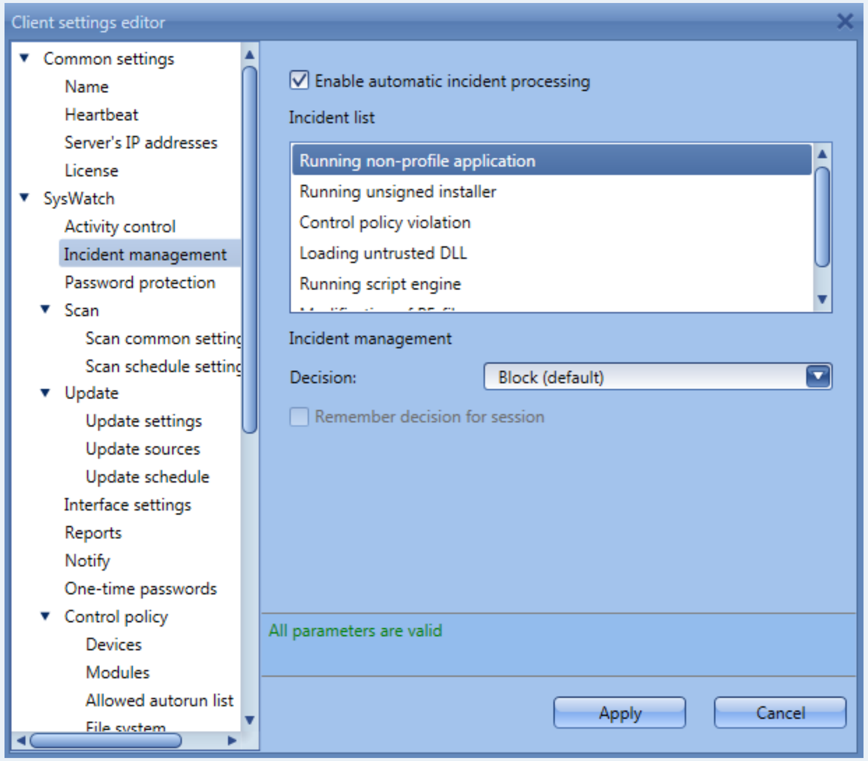
Username: console_admin

Roles: System administrator, Administrators

2.3.4 How to create group control policies. Examples

Table 10. Examples of creating group control policies

No.	Action	Expected outcome	Comment
10.1	Switch the client device from auditing to the operation mode.*	❑ The device is in the operation mode.	If you wish to switch the device from the auditing mode to the operation mode, change client settings on SoftControl Server and apply them to the relevant organizational unit.
* Switching modes is done through client settings on SoftControl Server:			



☑ Enable automatic incident processing

Incident list

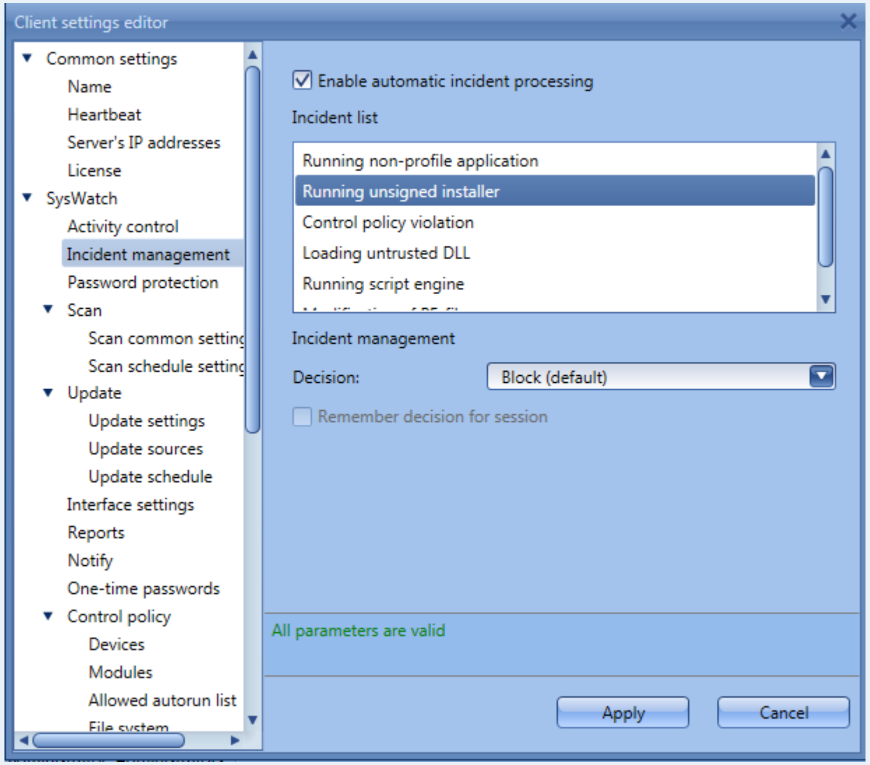
- Running non-profile application
- Running unsigned installer
- Control policy violation
- Loading untrusted DLL
- Running script engine

Incident management

Decision: Block (default)

□ Remember decision for session

All parameters are valid



☑ Enable automatic incident processing

Incident list

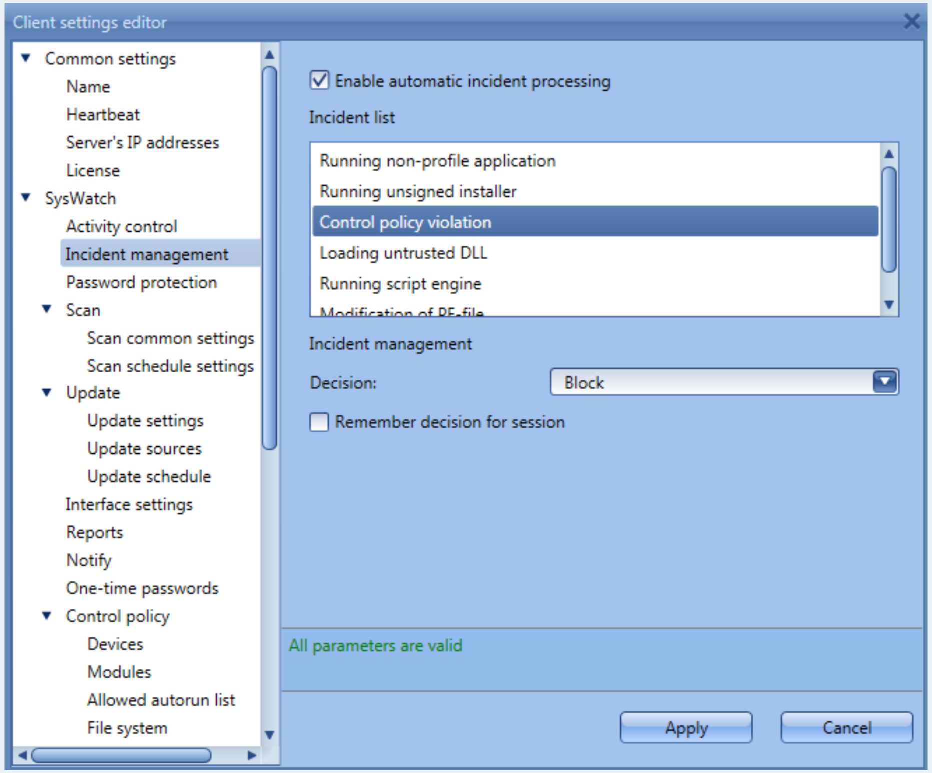
- Running non-profile application
- Running unsigned installer
- Control policy violation
- Loading untrusted DLL
- Running script engine

Incident management

Decision: Block (default)

□ Remember decision for session

All parameters are valid



☑ Enable automatic incident processing

Incident list

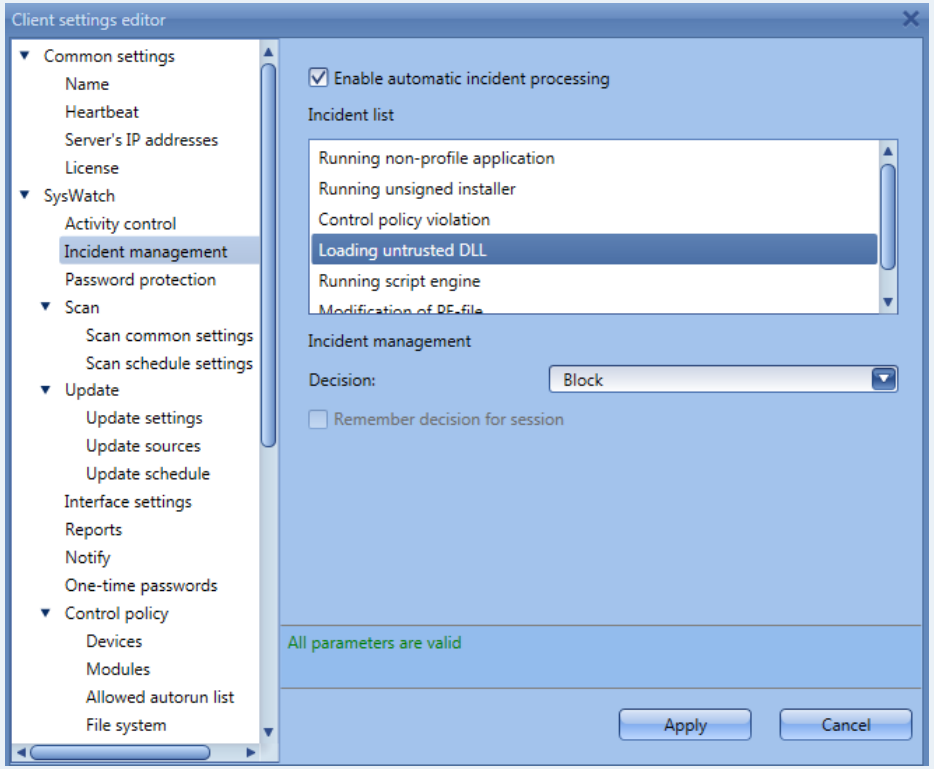
- Running non-profile application
- Running unsigned installer
- Control policy violation
- Loading untrusted DLL
- Running script engine
- Modification of PE-file

Incident management

Decision: Block

☐ Remember decision for session

All parameters are valid



☑ Enable automatic incident processing

Incident list

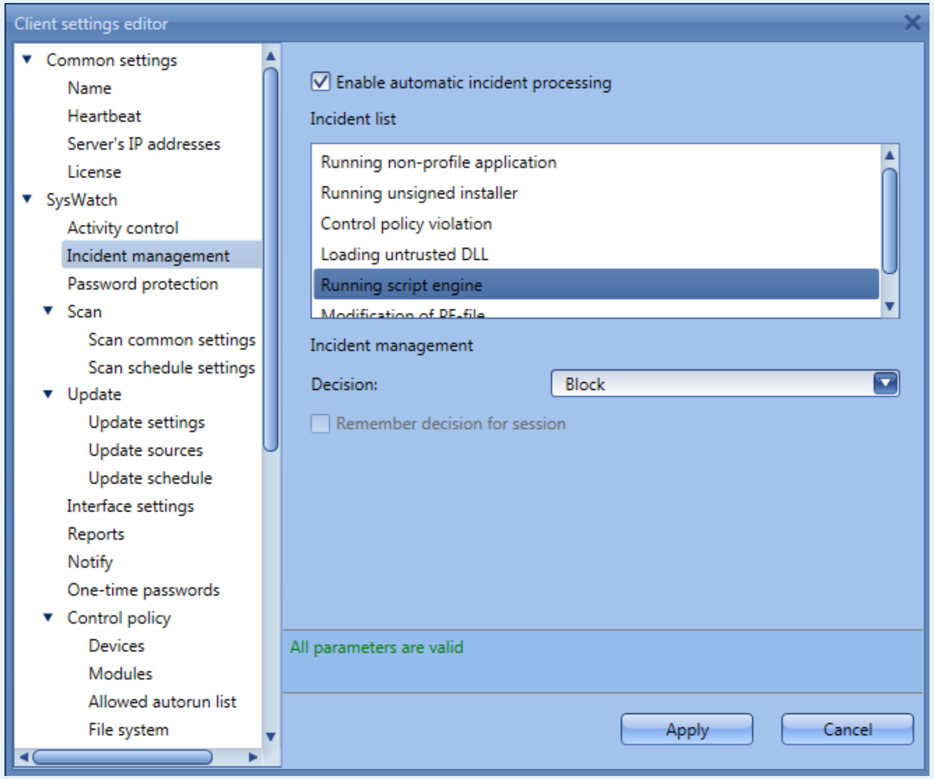
- Running non-profile application
- Running unsigned installer
- Control policy violation
- Loading untrusted DLL
- Running script engine
- Modification of PE-file

Incident management

Decision: Block

☐ Remember decision for session

All parameters are valid



☑ Enable automatic incident processing

Incident list

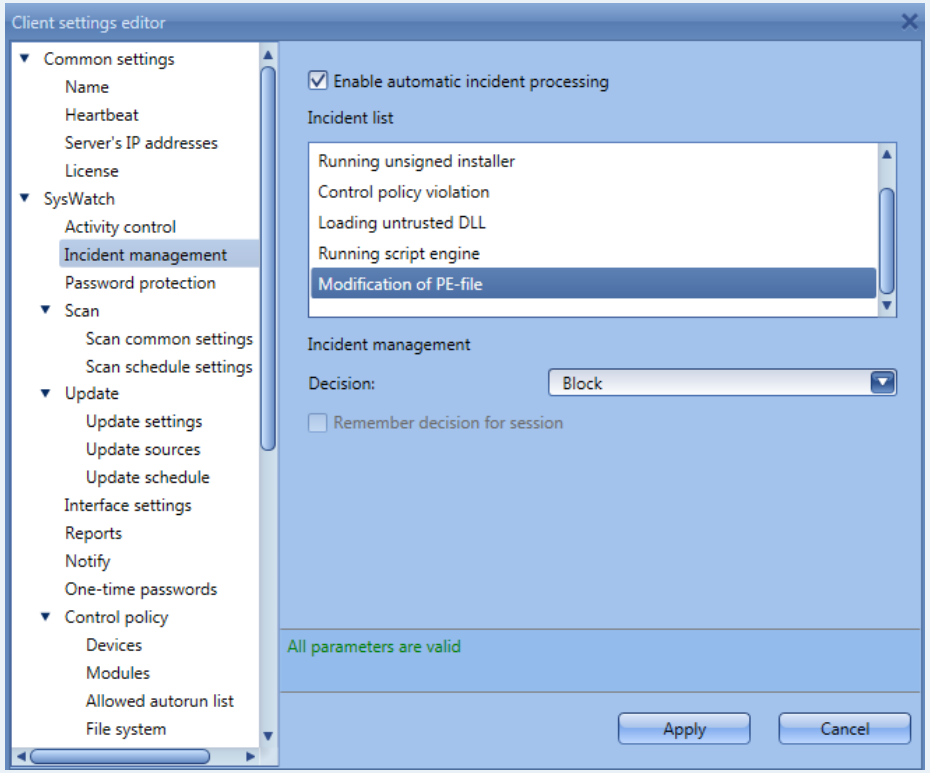
- Running non-profile application
- Running unsigned installer
- Control policy violation
- Loading untrusted DLL
- Running script engine
- Modification of PE-file

Incident management

Decision: Block

☐ Remember decision for session

All parameters are valid



☑ Enable automatic incident processing

Incident list

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

Incident management

Decision: Block

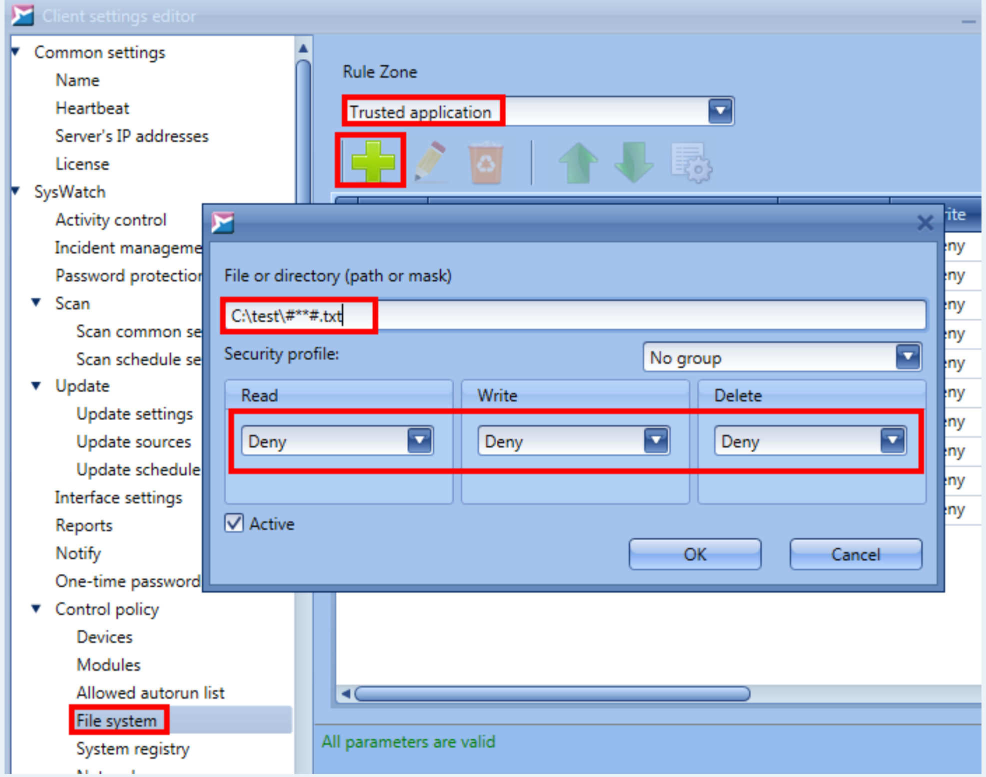
☐ Remember decision for session

All parameters are valid

Once you finish editing the client settings, save them under a new name and apply to the organizational unit which the device belongs to.

10.2	Create rules in control policies and test their performance. Each control zone shall be covered.		
10.2.1	Test rules in control policies for the file system.		
10.2.1.1	Create a rule that forbids reading, writing, and removing of text files in *C:\test\* for all trusted processes.*	❑ A rule has been created that forbids reading, removing, and writing for *C:\test\*.txt* file resource. The rule is applied to all trusted applications.	

* In order to create the rule, edit the client settings:



Rule Zone: Trusted application

File or directory (path or mask): C:\test\#**#.txt

Security profile: No group

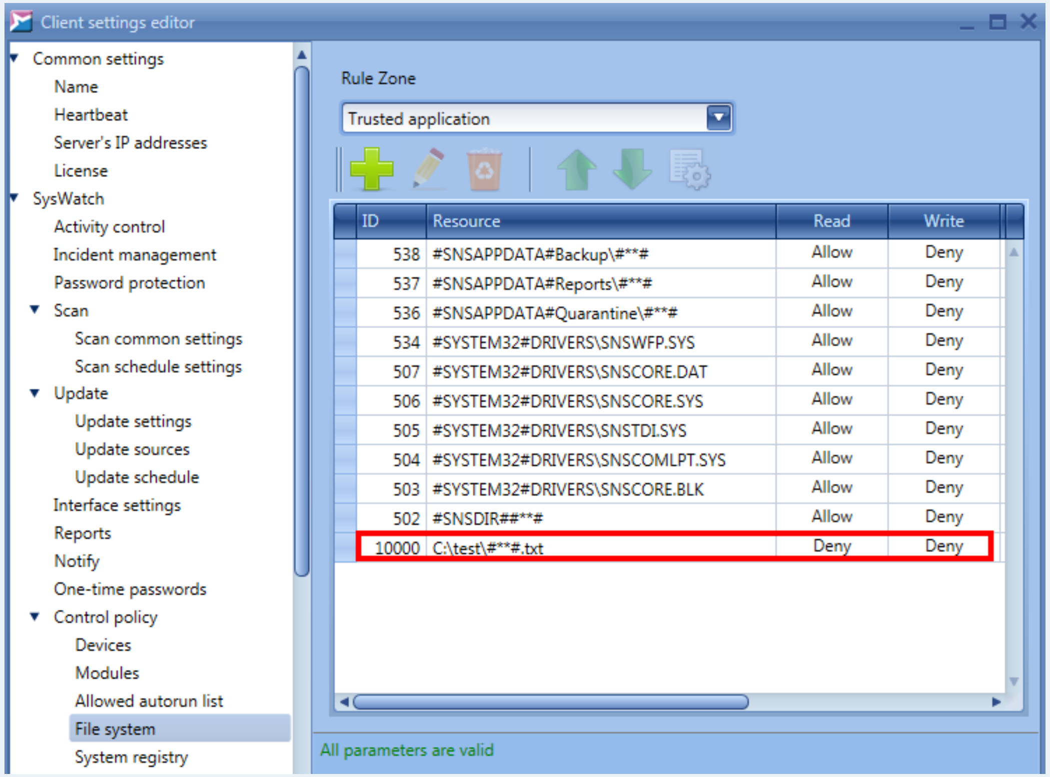
Read: Deny

Write: Deny

Delete: Deny

☑ Active

All parameters are valid



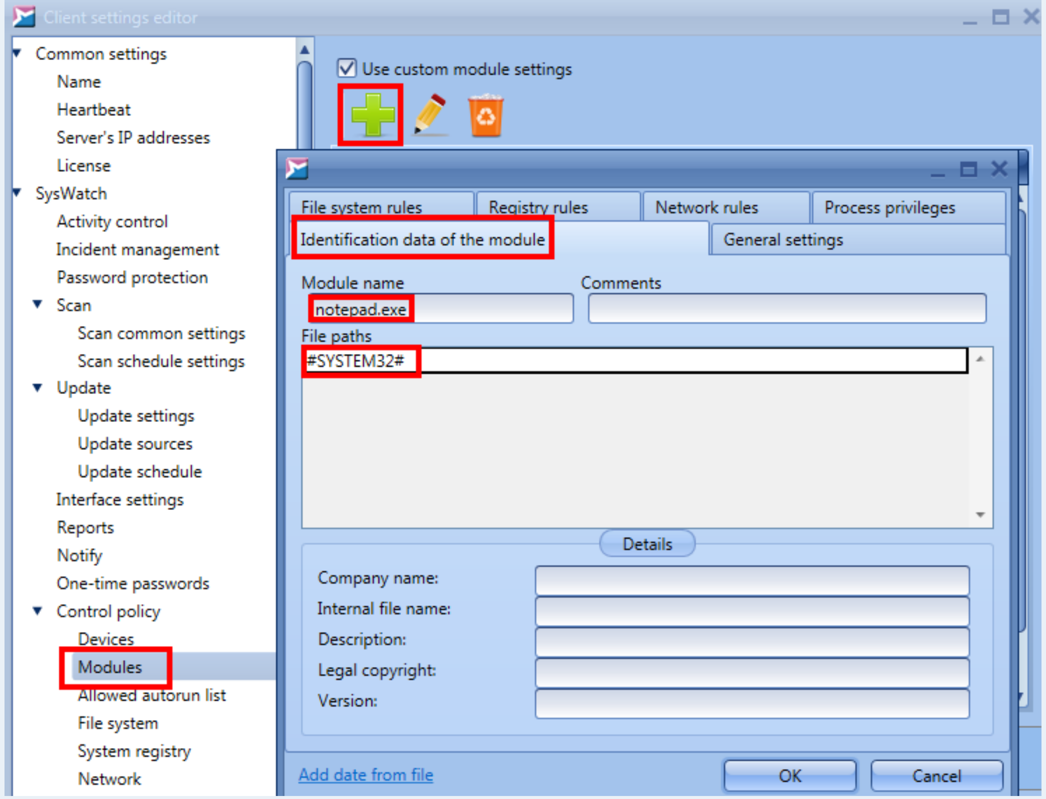
Rule Zone: Trusted application

ID	Resource	Read	Write
538	#SNSAPPDATA#Backup\#**#	Allow	Deny
537	#SNSAPPDATA#Reports\#**#	Allow	Deny
536	#SNSAPPDATA#Quarantine\#**#	Allow	Deny
534	#SYSTEM32#DRIVERS\SNSWFP.SYS	Allow	Deny
507	#SYSTEM32#DRIVERS\SNSCORE.DAT	Allow	Deny
506	#SYSTEM32#DRIVERS\SNSCORE.SYS	Allow	Deny
505	#SYSTEM32#DRIVERS\SNSTDI.SYS	Allow	Deny
504	#SYSTEM32#DRIVERS\SNSCOMLPT.SYS	Allow	Deny
503	#SYSTEM32#DRIVERS\SNSCORE.BLK	Allow	Deny
502	#SNSDIR##**#	Allow	Deny
10000	C:\test\#**#.txt	Deny	Deny

All parameters are valid

10.2.1.2	Create a rule in **Modules** section for *Notepad.exe* that allows reading, writing, and removing of text files in *C:\test\.**	❑ A rule has been created for reading, deleting, and writing of *C:\test\[any_path\name].txt* file resource for *Notepad.exe*	

* In order to create the rule, edit the client settings:



☑ Use custom module settings

Module name: notepad.exe

Comments:

File paths: #SYSTEM32#

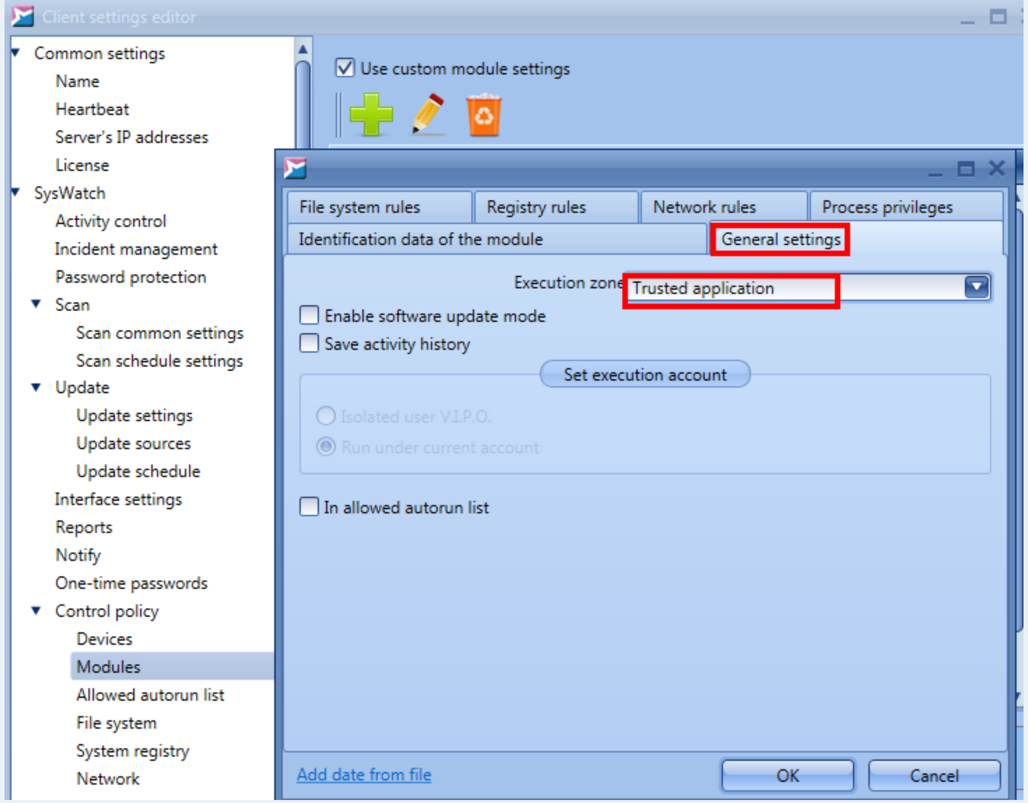
Company name:

Internal file name:

Description:

Legal copyright:

Version:



Client settings editor

- Common settings
  - Name
  - Heartbeat
  - Server's IP addresses
  - License
- SysWatch
  - Activity control
  - Incident management
  - Password protection
  - Scan
    - Scan common settings
    - Scan schedule settings
  - Update
    - Update settings
    - Update sources
    - Update schedule
  - Interface settings
  - Reports
  - Notify
  - One-time passwords
  - Control policy
    - Devices
    - Modules
    - Allowed autorun list
    - File system
    - System registry
    - Network

☑ Use custom module settings

File system rules | Registry rules | Network rules | Process privileges | Identification data of the module | General settings

Execution zone: Trusted application

☐ Enable software update mode

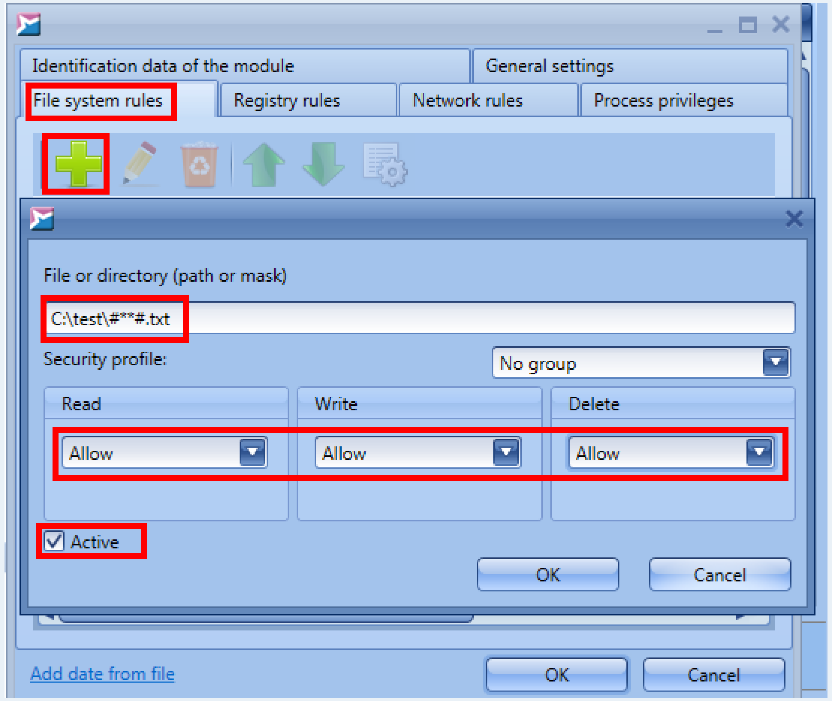
☐ Save activity history

Set execution account

○ Isolated user V.I.P.O.

● Run under current account

☐ In allowed autorun list



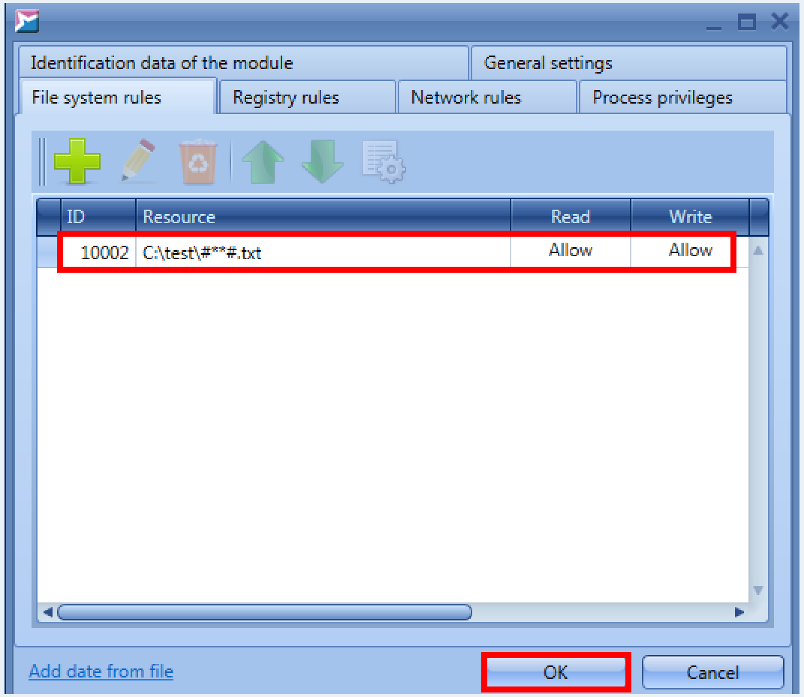
File or directory (path or mask)

C:\test\#**#.txt

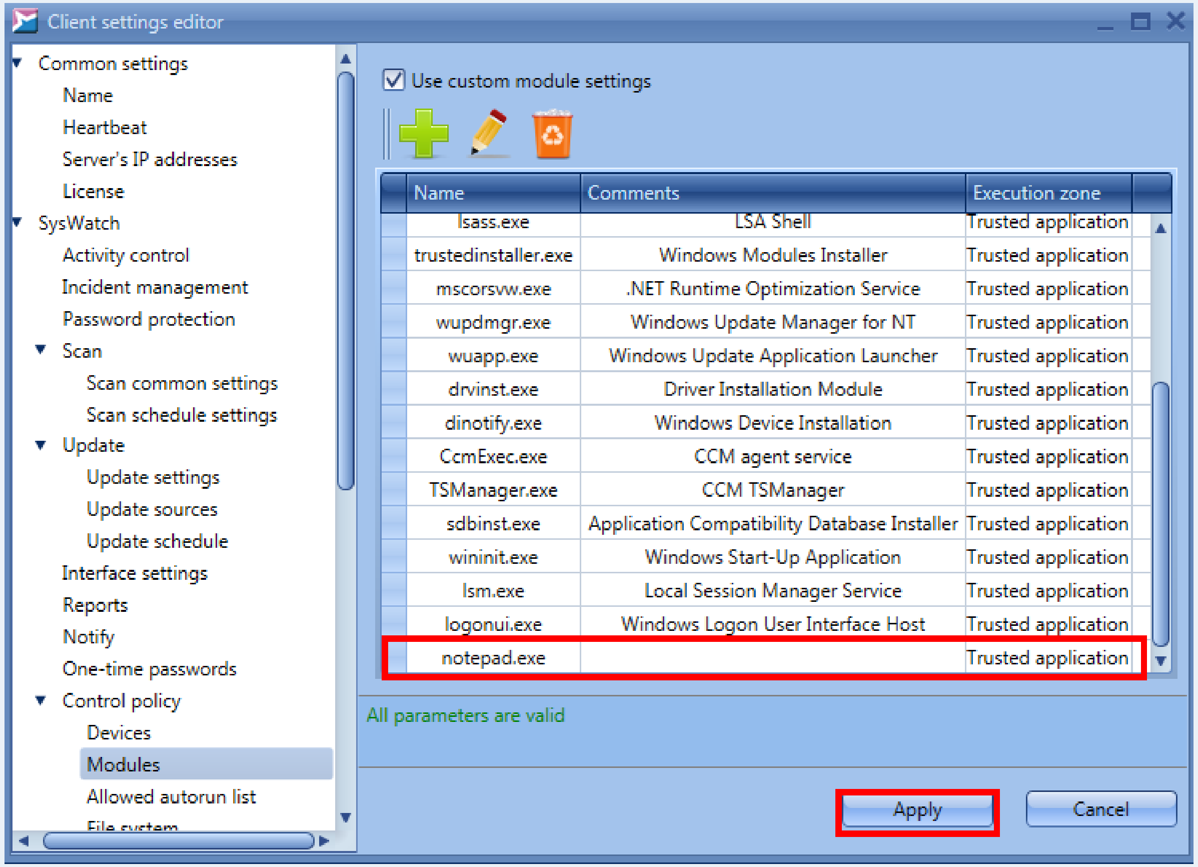
Security profile: No group

Read	Write	Delete
Allow	Allow	Allow

☑ Active



ID	Resource	Read	Write
10002	C:\test\#**#.txt	Allow	Allow



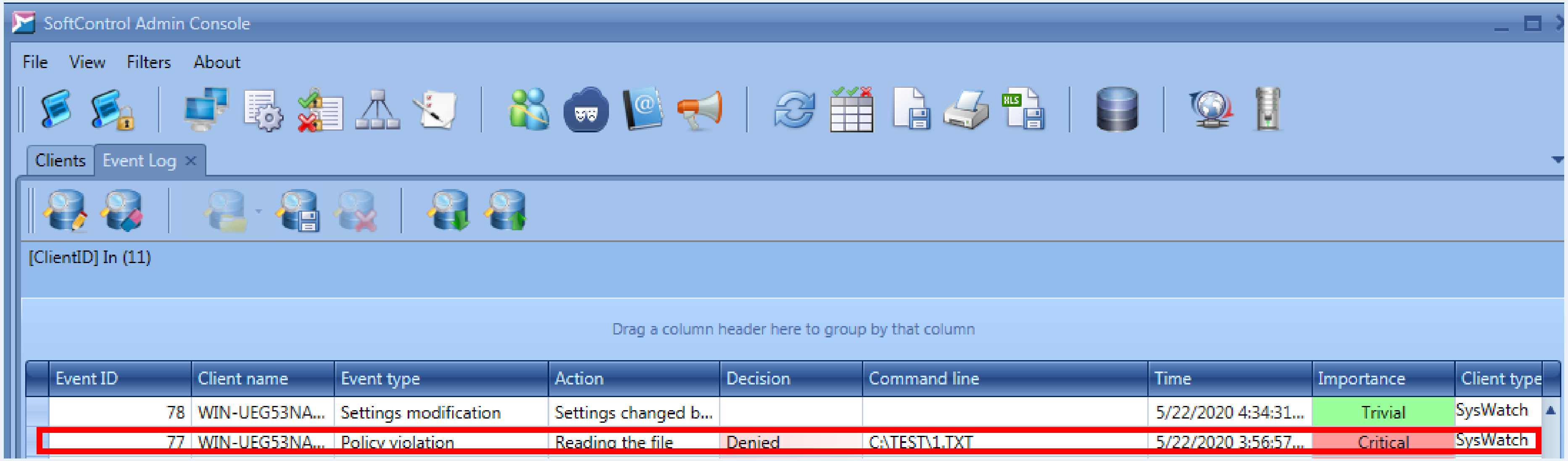
☑ Use custom module settings

Name	Comments	Execution zone
lsass.exe	LSA Shell	Trusted application
trustedinstaller.exe	Windows Modules Installer	Trusted application
mscorsvw.exe	.NET Runtime Optimization Service	Trusted application
wupdmgr.exe	Windows Update Manager for NT	Trusted application
wuapp.exe	Windows Update Application Launcher	Trusted application
drvinst.exe	Driver Installation Module	Trusted application
dinotify.exe	Windows Device Installation	Trusted application
CcmExec.exe	CCM agent service	Trusted application
TSManager.exe	CCM TSManager	Trusted application
sdbinst.exe	Application Compatibility Database Installer	Trusted application
wininit.exe	Windows Start-Up Application	Trusted application
lsm.exe	Local Session Manager Service	Trusted application
logonui.exe	Windows Logon User Interface Host	Trusted application
notepad.exe		Trusted application

All parameters are valid

10.2.1.3	Make an attempt to change *C:\test\1.txt* with *Notepad.exe* and with *Wordpad.exe*.*	❑ When you use *Notepad.exe*, you can change the file without any problems; when you try to do the same with *Wordpad.exe*, you get the *Access denied* error.	

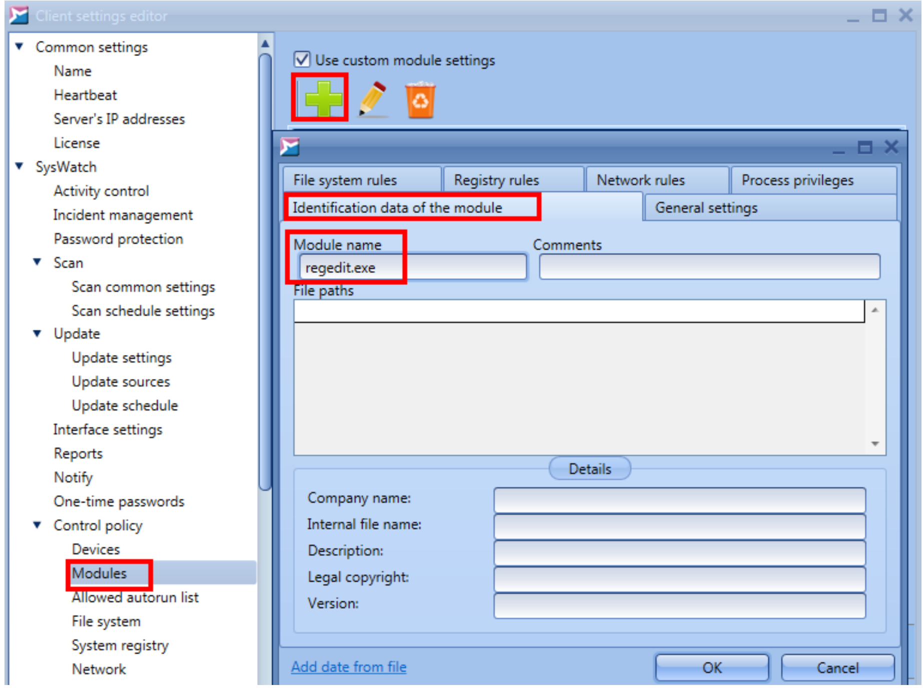
* **Policy violation – Reading the file** event appears in SoftControl Admin Console:


SoftControl Admin Console
File
View
Filters
About
Clients
Event Log
[ClientID] In (11)
Drag a column header here to group by that column

Event ID	Client name	Event type	Action	Decision	Command line	Time	Importance	Client type
78	WIN-UEG53NA...	Settings modification	Settings changed b...			5/22/2020 4:34:31...	Trivial	SysWatch
77	WIN-UEG53NA...	Policy violation	Reading the file	Denied	C:\TEST\1.TXT	5/22/2020 3:56:57...	Critical	SysWatch

10.2.2	Check the rules in control policies for modules.		
10.2.2.1	In **Modules** section, create a rule that blocks the Windows registry editor.*	❑ A setting for blocking *regedit.exe* has been created through **Control policy – Modules**	To create a rule for blocking the Windows registry editor, add *regedit.exe* to the list of private settings for modules and place it into the **Execution zone – Blocked applications**.

* In order to create the rule, edit the client settings:

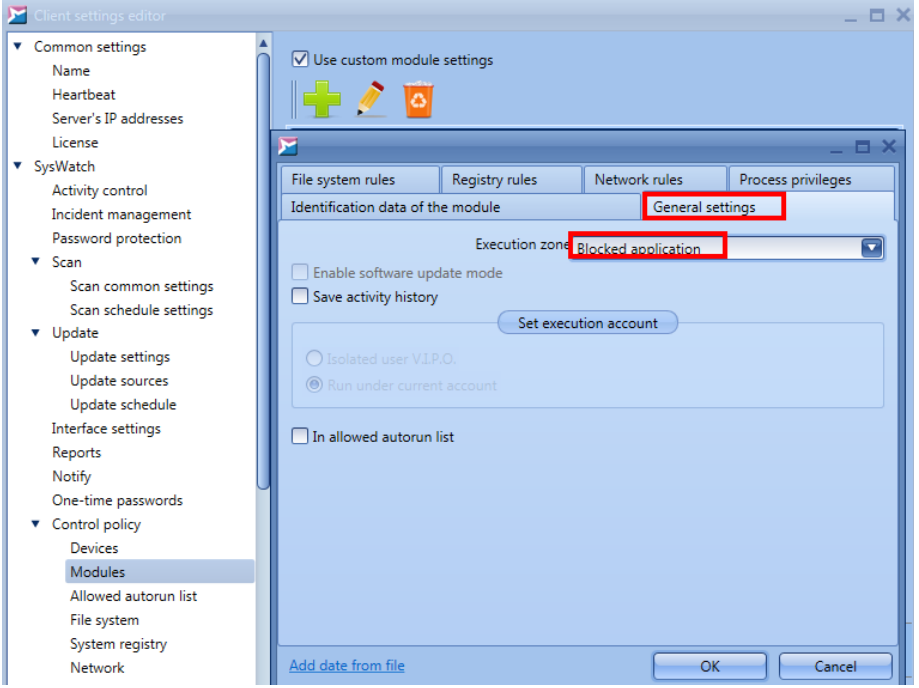


☑ Use custom module settings

Module name: regedit.exe

Comments:

File paths



☑ Use custom module settings

Execution zone: Blocked application

□ Enable software update mode

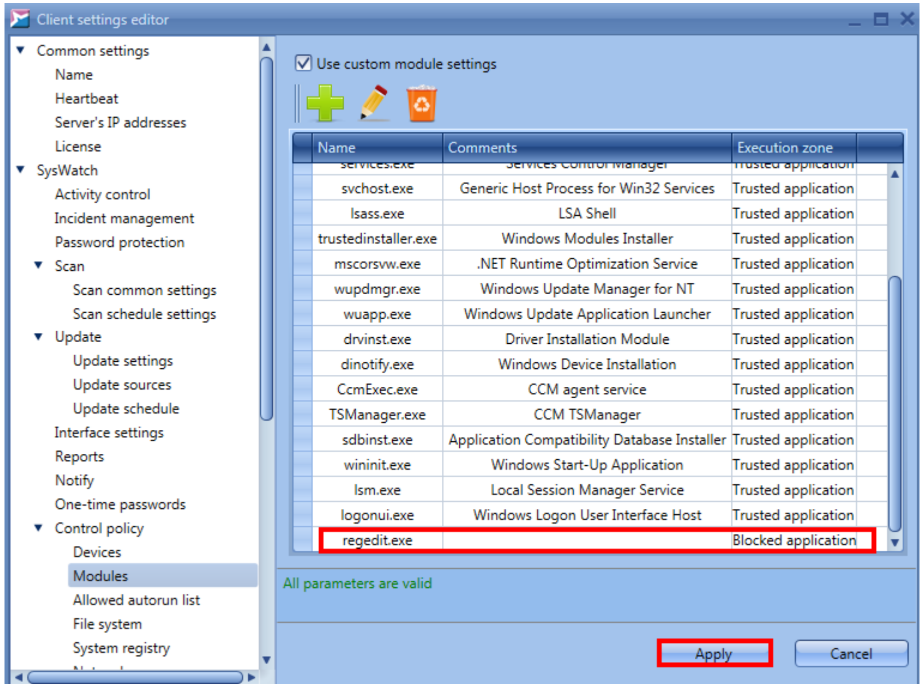
□ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

□ In allowed autorun list

Once you save the settings, a new line will appear in **Control policy – Modules** section:



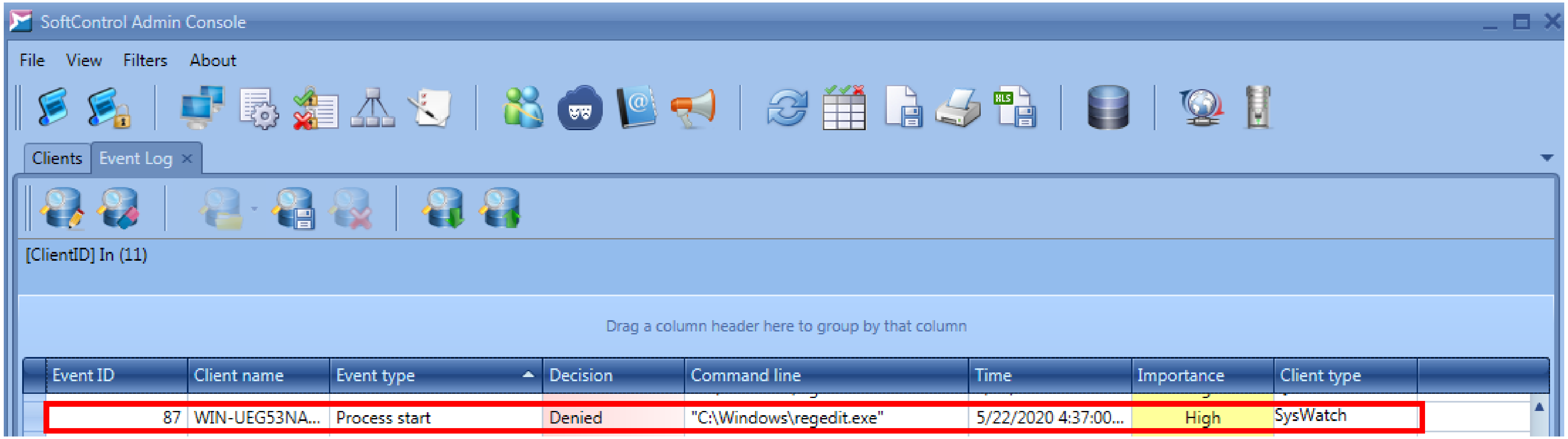
☑ Use custom module settings

Name	Comments	Execution zone
services.exe	Services Control Manager	Trusted application
svchost.exe	Generic Host Process for Win32 Services	Trusted application
lsass.exe	LSA Shell	Trusted application
trustedinstaller.exe	Windows Modules Installer	Trusted application
mscorsvw.exe	.NET Runtime Optimization Service	Trusted application
wupdmgr.exe	Windows Update Manager for NT	Trusted application
wuapp.exe	Windows Update Application Launcher	Trusted application
drvinst.exe	Driver Installation Module	Trusted application
dinotify.exe	Windows Device Installation	Trusted application
CcmExec.exe	CCM agent service	Trusted application
TSManager.exe	CCM TSManager	Trusted application
sdbinst.exe	Application Compatibility Database Installer	Trusted application
wininit.exe	Windows Start-Up Application	Trusted application
lsm.exe	Local Session Manager Service	Trusted application
logonui.exe	Windows Logon User Interface Host	Trusted application
regedit.exe		Blocked application

All parameters are valid

10.2.2.2	Make an attempt to launch *regedit.exe*.	❑ The registry editor does not start. The device console displays *Access denied* message.	You can find **Process start:** *C:\WINDOWS \REGEDIT.EXE* event from (**Blocked** zone) with **Denied** decision in the device logs on SoftControl Server.

* **Process start** event (**Blocked** zone) appears in SoftControl Admin Console:



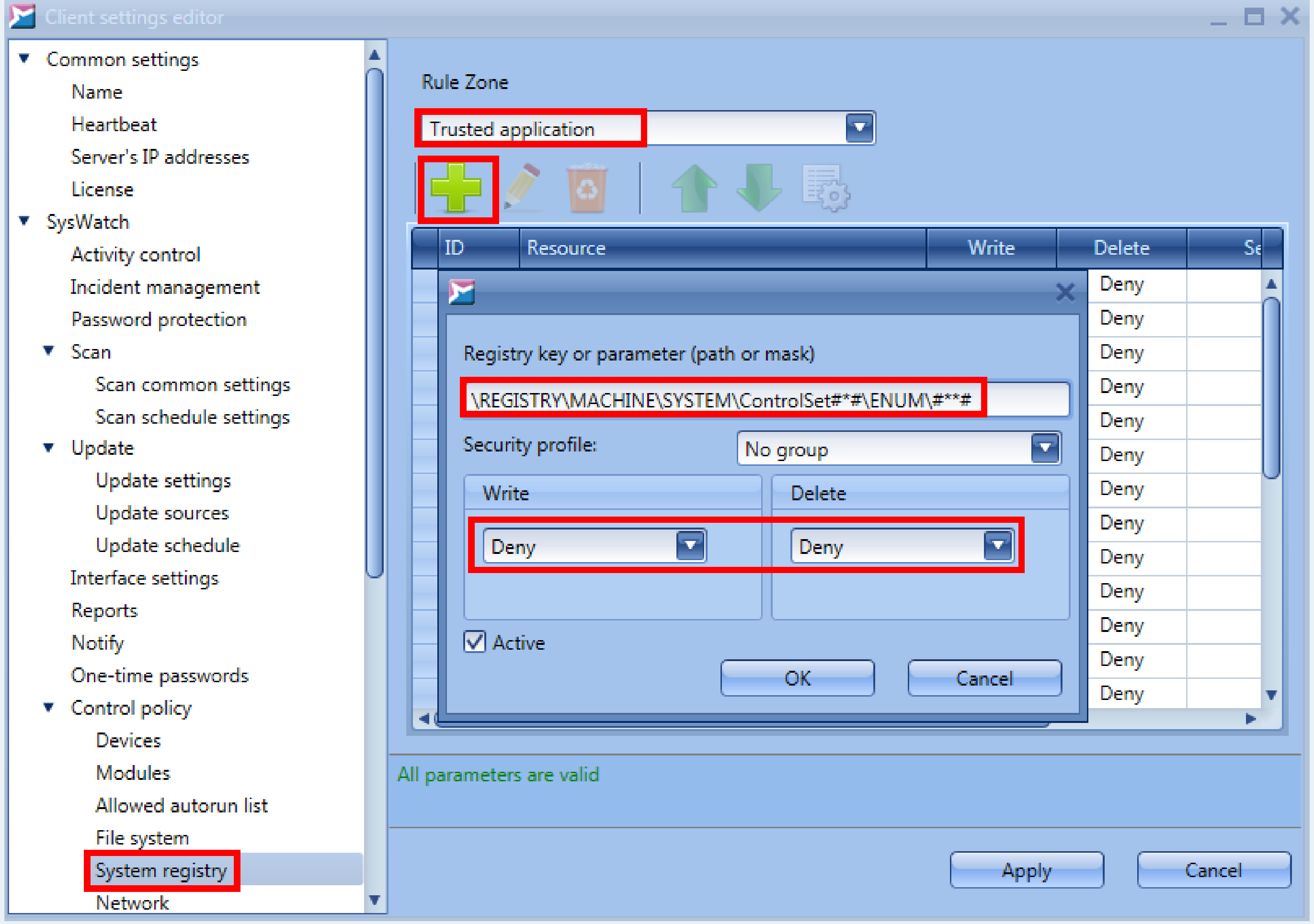
[ClientID] In (11)

Drag a column header here to group by that column

Event ID	Client name	Event type	Decision	Command line	Time	Importance	Client type
87	WIN-UEG53NA...	Process start	Denied	"C:\Windows\regedit.exe"	5/22/2020 4:37:00...	High	SysWatch

10.2.3	Test rules on control policies for the system registry.		
10.2.3.1	Create a rule that blocks writing in a Windows registry branch of PnP manager scripts that access functional drivers of the devices. As an example, we consider a USB drive that has not previously been connected to the client device.*	❑ A rule has been created for the **Trusted applications** that block writing and deleting.	Registry branch for blocking: *\REGISTRY \MACHINE\SYSTEM\ ControlSet #*#\ENUM\#**#.* Create the next rule for the branch *\REGISTRY \MACHINE\SYSTEM\ CurrentControlSet\ENUM \#**#* in the same way. These rules block operation of new devices which have not been previously connected to the client device.

* In order to create a rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to.



Rule Zone: Trusted application

Registry key or parameter (path or mask): \REGISTRY\MACHINE\SYSTEM\ControlSet#*#\ENUM\#**#

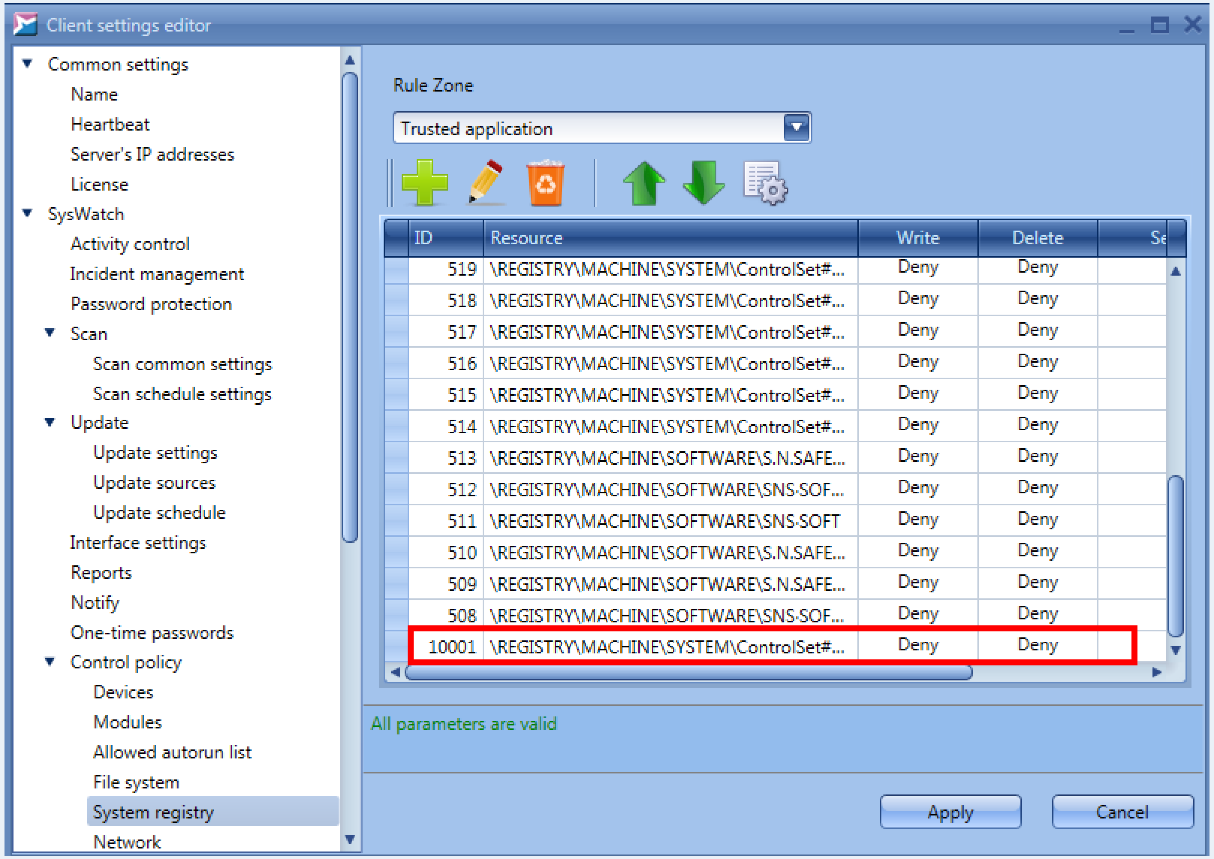
Security profile: No group

Write: Deny

Delete: Deny

☑ Active

All parameters are valid



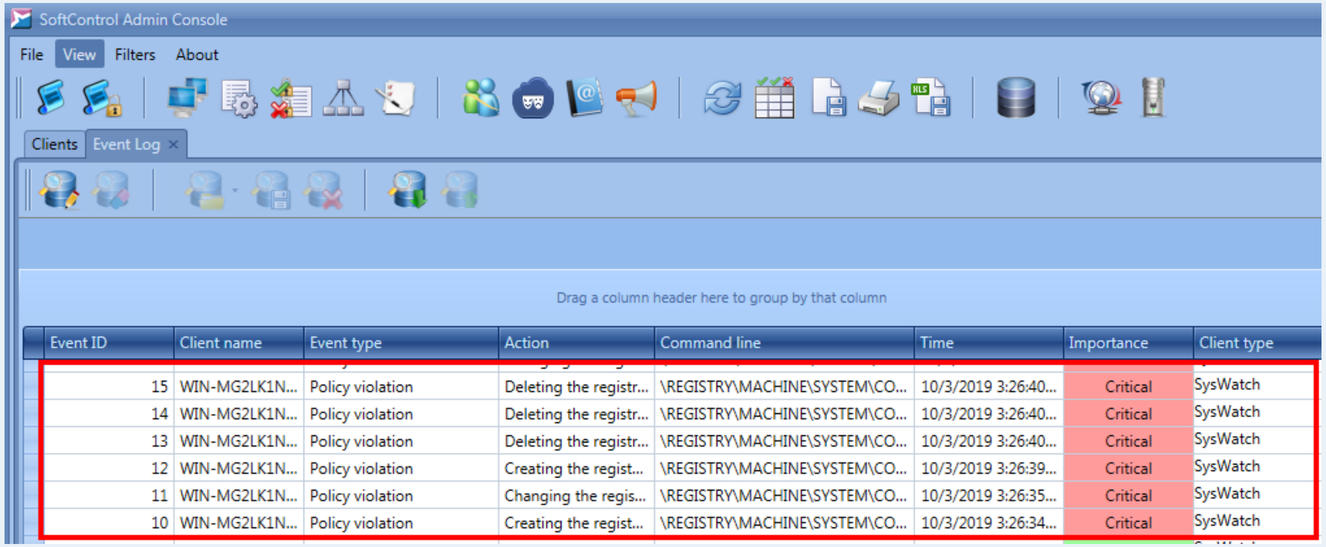
Rule Zone: Trusted application

ID	Resource	Write	Delete	Se
519	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
518	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
517	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
516	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
515	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
514	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	
513	\REGISTRY\MACHINE\SOFTWARE\S.N.SAFE...	Deny	Deny	
512	\REGISTRY\MACHINE\SOFTWARE\SNS-SOF...	Deny	Deny	
511	\REGISTRY\MACHINE\SOFTWARE\SNS-SOFT	Deny	Deny	
510	\REGISTRY\MACHINE\SOFTWARE\S.N.SAFE...	Deny	Deny	
509	\REGISTRY\MACHINE\SOFTWARE\S.N.SAFE...	Deny	Deny	
508	\REGISTRY\MACHINE\SOFTWARE\SNS-SOF...	Deny	Deny	
10001	\REGISTRY\MACHINE\SYSTEM\ControlSet#...	Deny	Deny	

All parameters are valid

10.2.3.2	Make an attempt to connect a new USB drive (which has not been previously connected to the host) to the device you are testing.	❑ The USB drive does not connect to the device. You get a message that drivers for the USB drive have not been installed.	In the device logs on SoftControl Server, you can see **Policy violation** event; action – **Creating the registry key**, details – **(ACE_[rule_number] =)**, decision – **Denied**.*

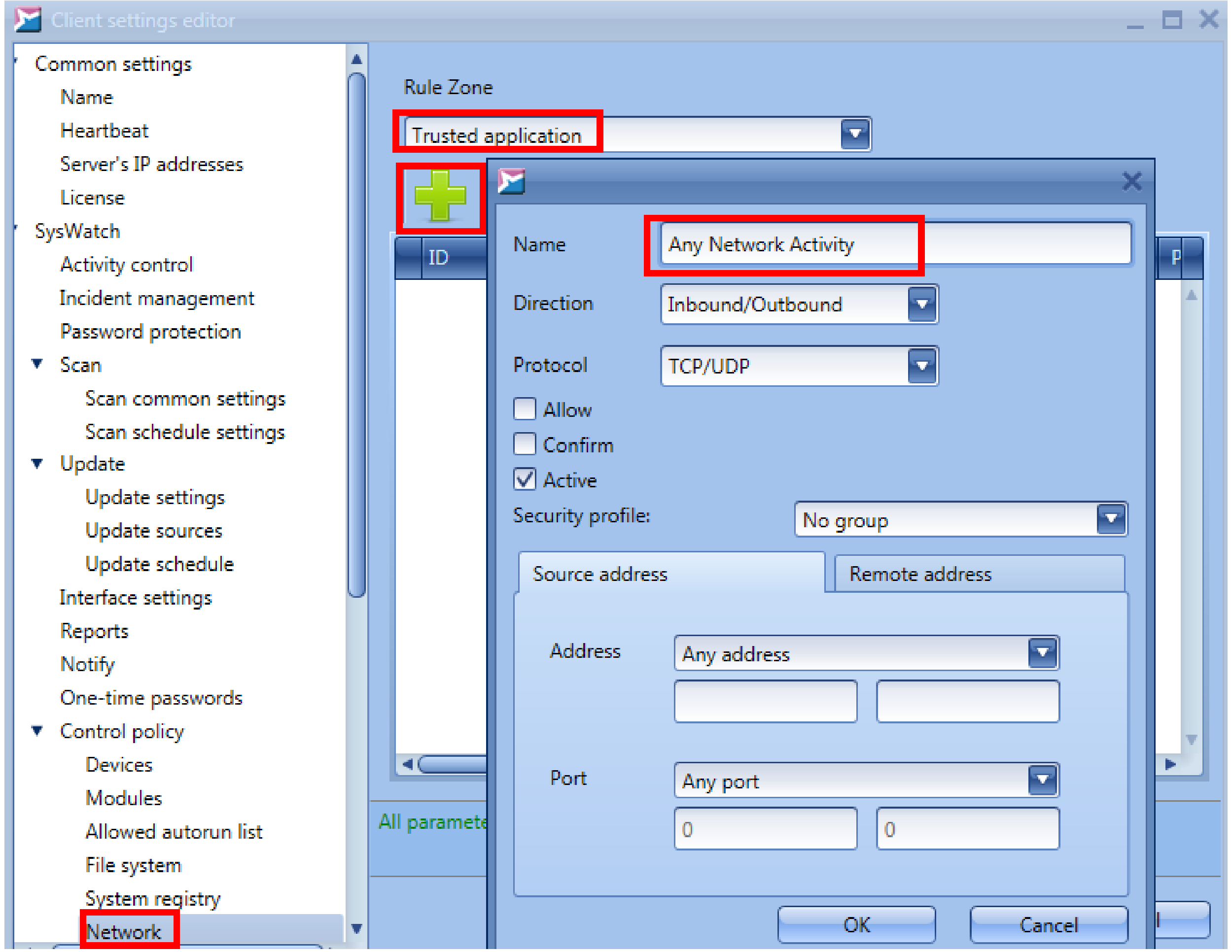
*You can see **Policy violation** event, **Creating the registry key** action in SoftControl Admin Console:


SoftControl Admin Console
File
View
Filters
About
Clients
Event Log
Drag a column header here to group by that column

Event ID	Client name	Event type	Action	Command line	Time	Importance	Client type
15	WIN-MG2LK1N...	Policy violation	Deleting the registr...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:40...	Critical	SysWatch
14	WIN-MG2LK1N...	Policy violation	Deleting the registr...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:40...	Critical	SysWatch
13	WIN-MG2LK1N...	Policy violation	Deleting the registr...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:40...	Critical	SysWatch
12	WIN-MG2LK1N...	Policy violation	Creating the regist...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:39...	Critical	SysWatch
11	WIN-MG2LK1N...	Policy violation	Changing the regis...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:35...	Critical	SysWatch
10	WIN-MG2LK1N...	Policy violation	Creating the regist...	\REGISTRY\MACHINE\SYSTEM\CO...	10/3/2019 3:26:34...	Critical	SysWatch

10.2.4	Test rules in control policies of **Network** section.		
10.2.4.1	Create a rule that blocks any network activity for trusted applications.*	❑ A rule has been created that blocks any network activity for trusted applications.	

* In order to create the rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to. Find below the instructions on how to create the **Any Network Activity** rule that blocks the network for all trusted applications:



Rule Zone: Trusted application

Name: Any Network Activity

Direction: Inbound/Outbound

Protocol: TCP/UDP

□ Allow

□ Confirm

☑ Active

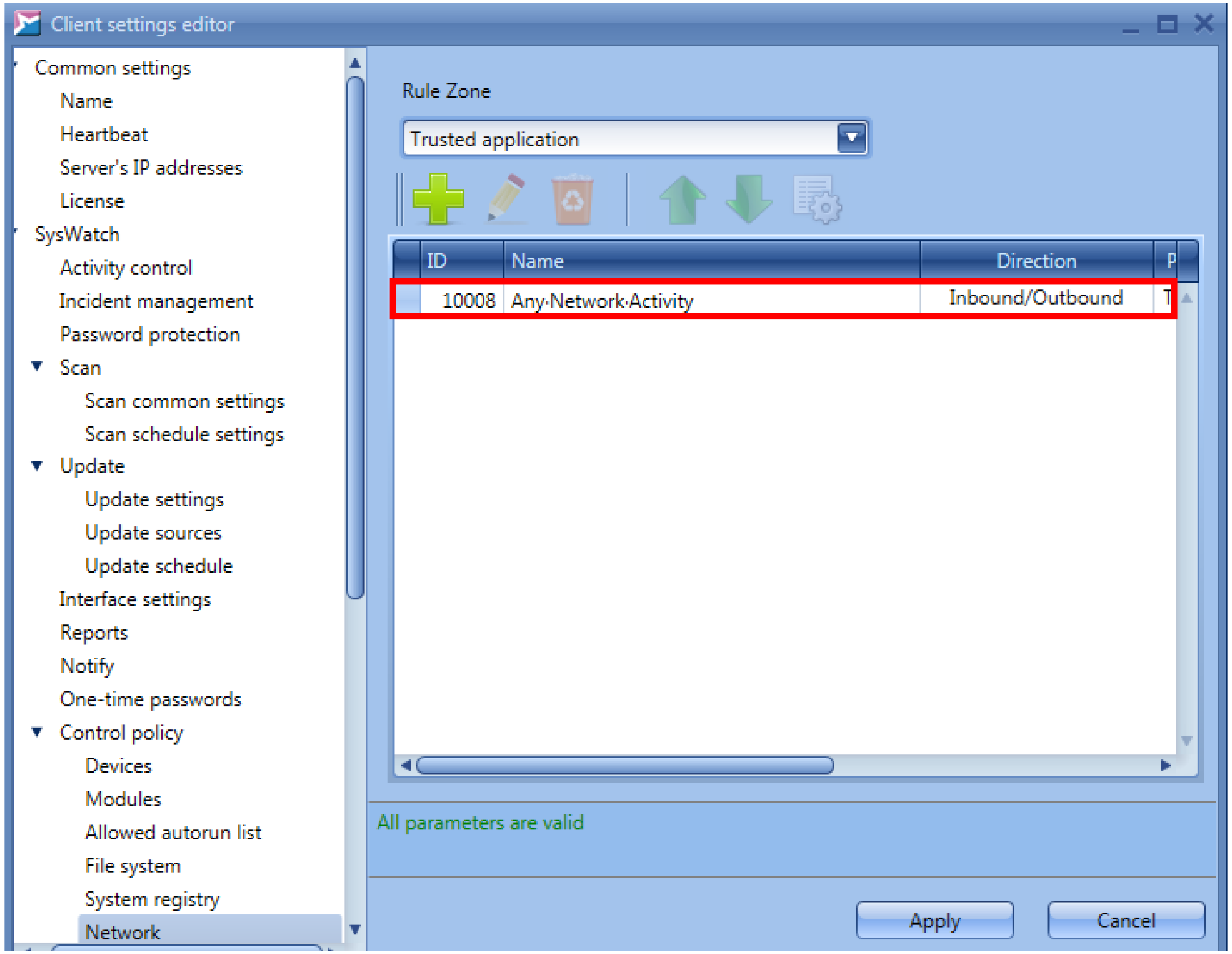
Security profile: No group

Source address | Remote address

Address: Any address

Port: Any port

0 0



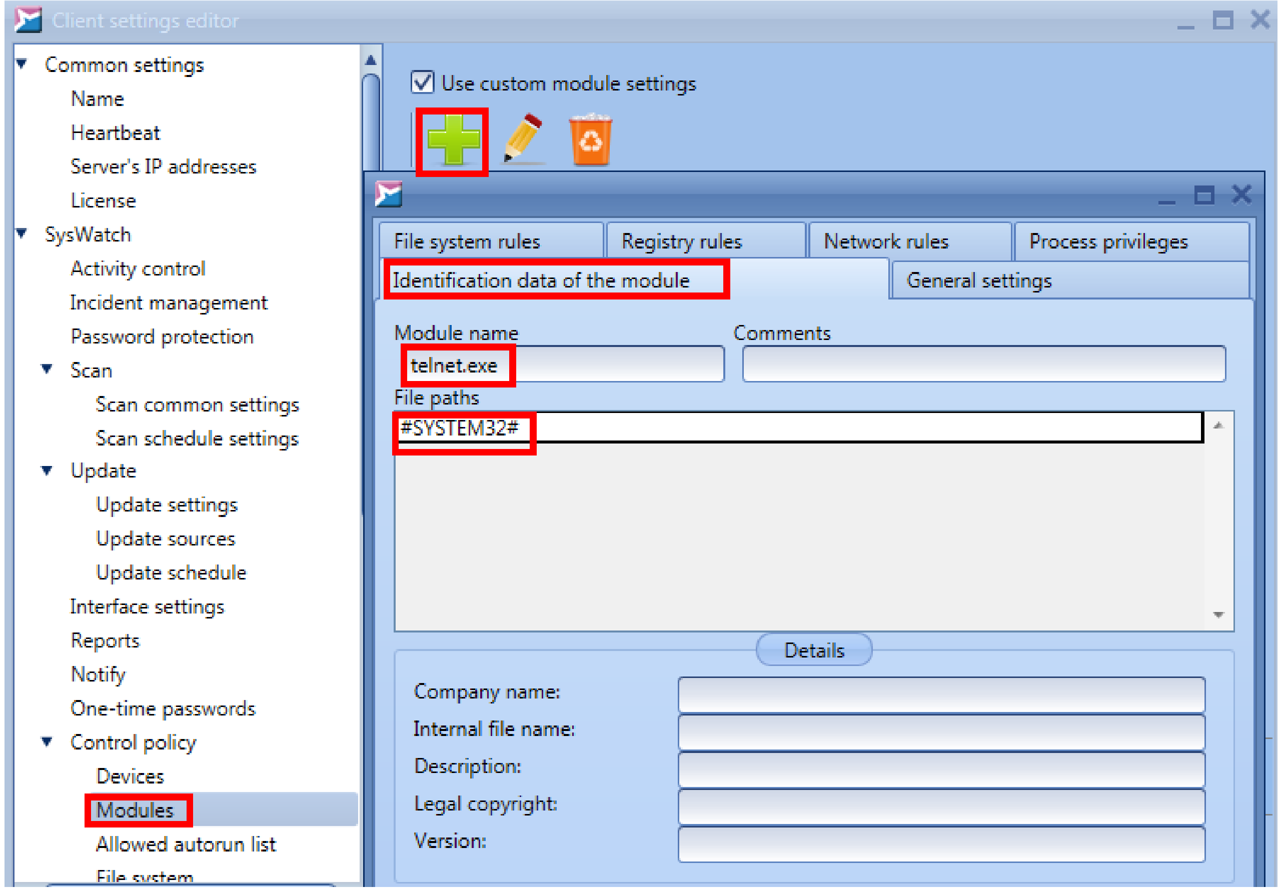
Rule Zone: Trusted application

ID	Name	Direction	P
10008	Any·Network·Activity	Inbound/Outbound	T

All parameters are valid

10.2.4.2	Create a rule that allows the *Telnet* application (*C:\windows\system32\telnet.exe*) to access *ya.ru* (87.250.250.242:80).*	❑ A rule that allows *Telnet* application (*C:\windows\system32\telnet.exe*) to access *ya.ru* (87.250.250.242:80) has been created.	

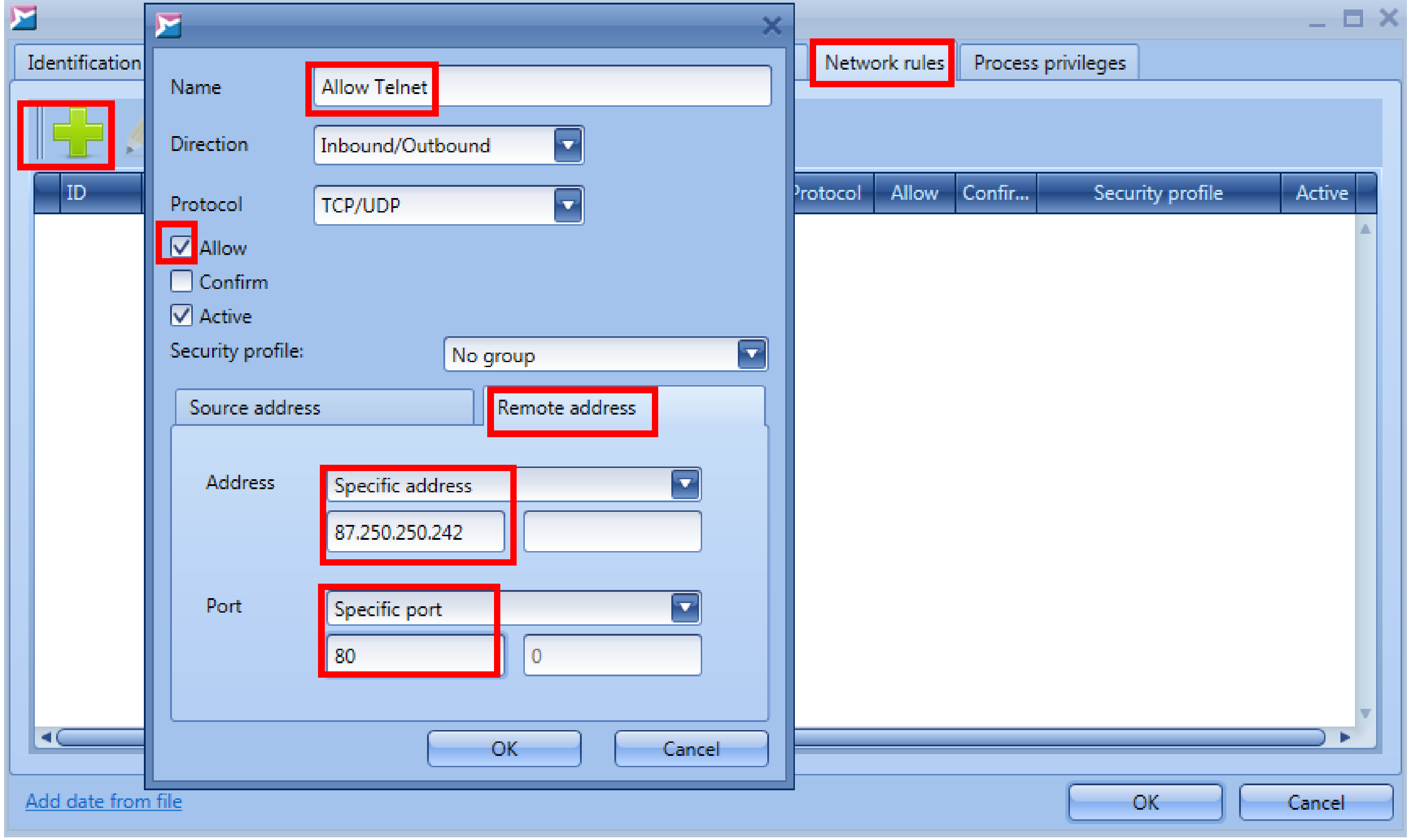
*In order to create the rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to. Find below the instructions on how to create a rule that allows *telnet.exe* from *#SYSTEM32#* folder to access the remote address *ya.ru* (87.250.250.242:80):



☑ Use custom module settings

Module name: telnet.exe

File paths: #SYSTEM32#



Name: Allow Telnet

Direction: Inbound/Outbound

Protocol: TCP/UDP

☑ Allow

□ Confirm

☑ Active

Security profile: No group

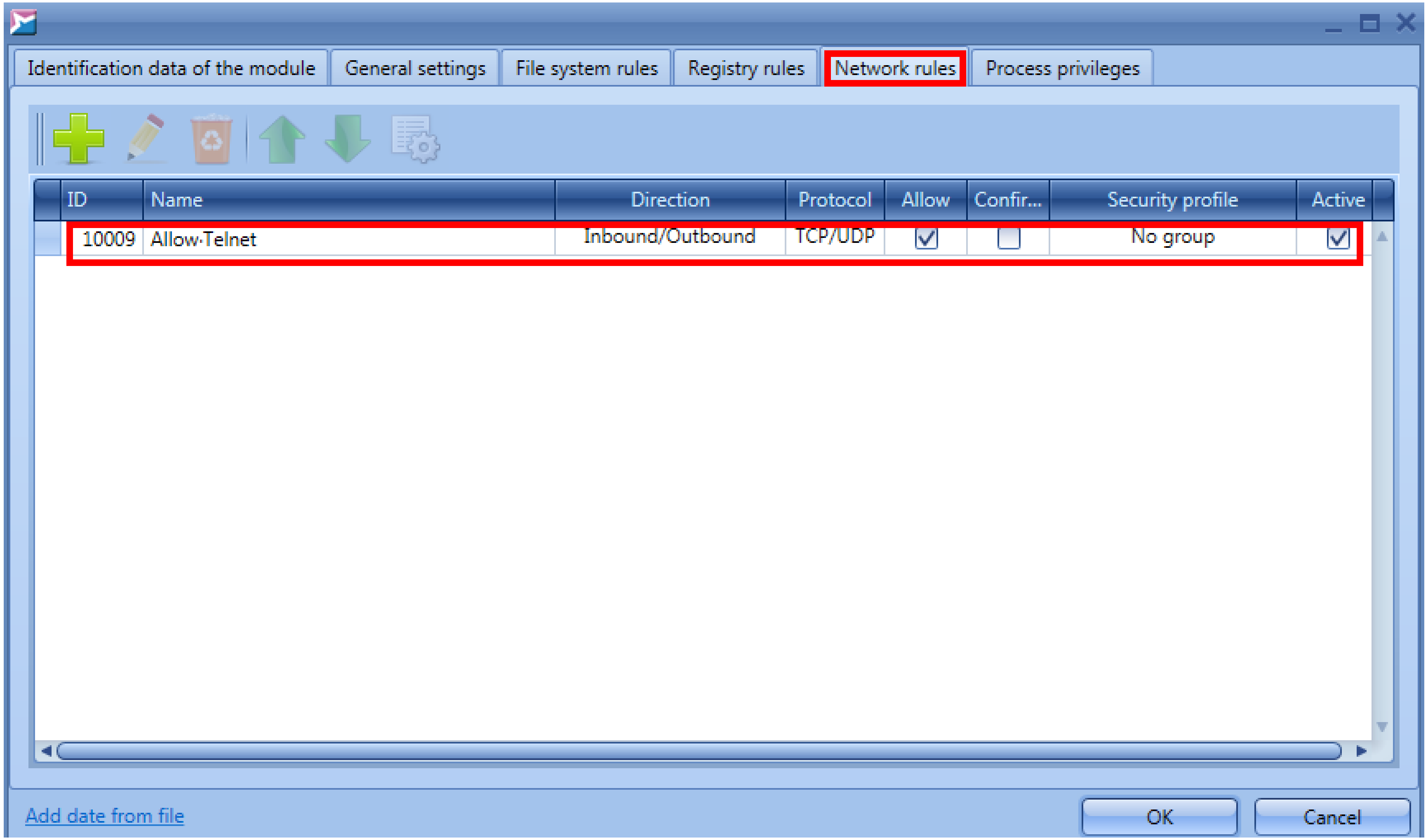
Source address | Remote address

Address: Specific address

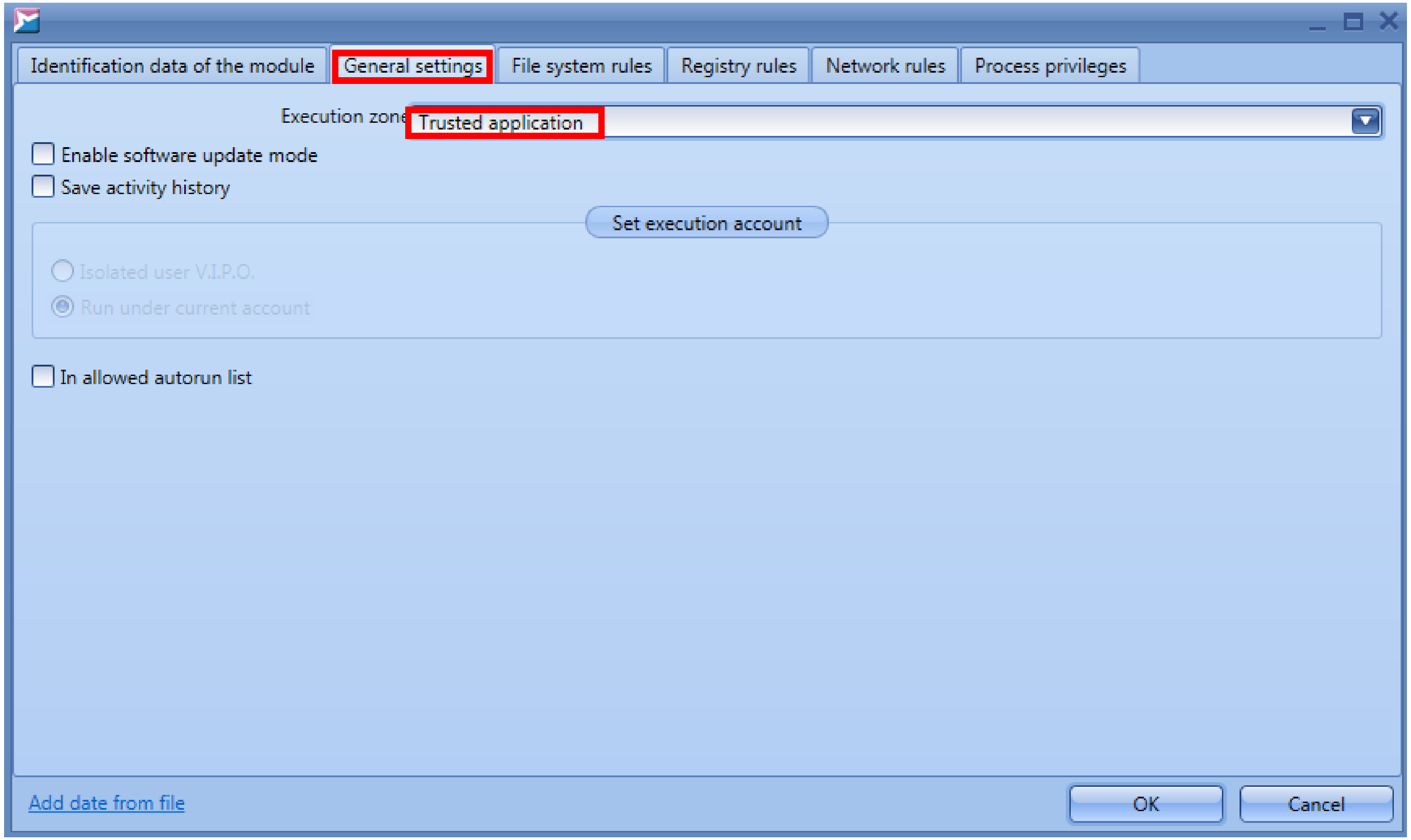
87.250.250.242

Port: Specific port

80 | 0



ID	Name	Direction	Protocol	Allow	Confir...	Security profile	Active
10009	Allow·Telnet	Inbound/Outbound	TCP/UDP	☑	□	No group	☑



Execution zone: Trusted application

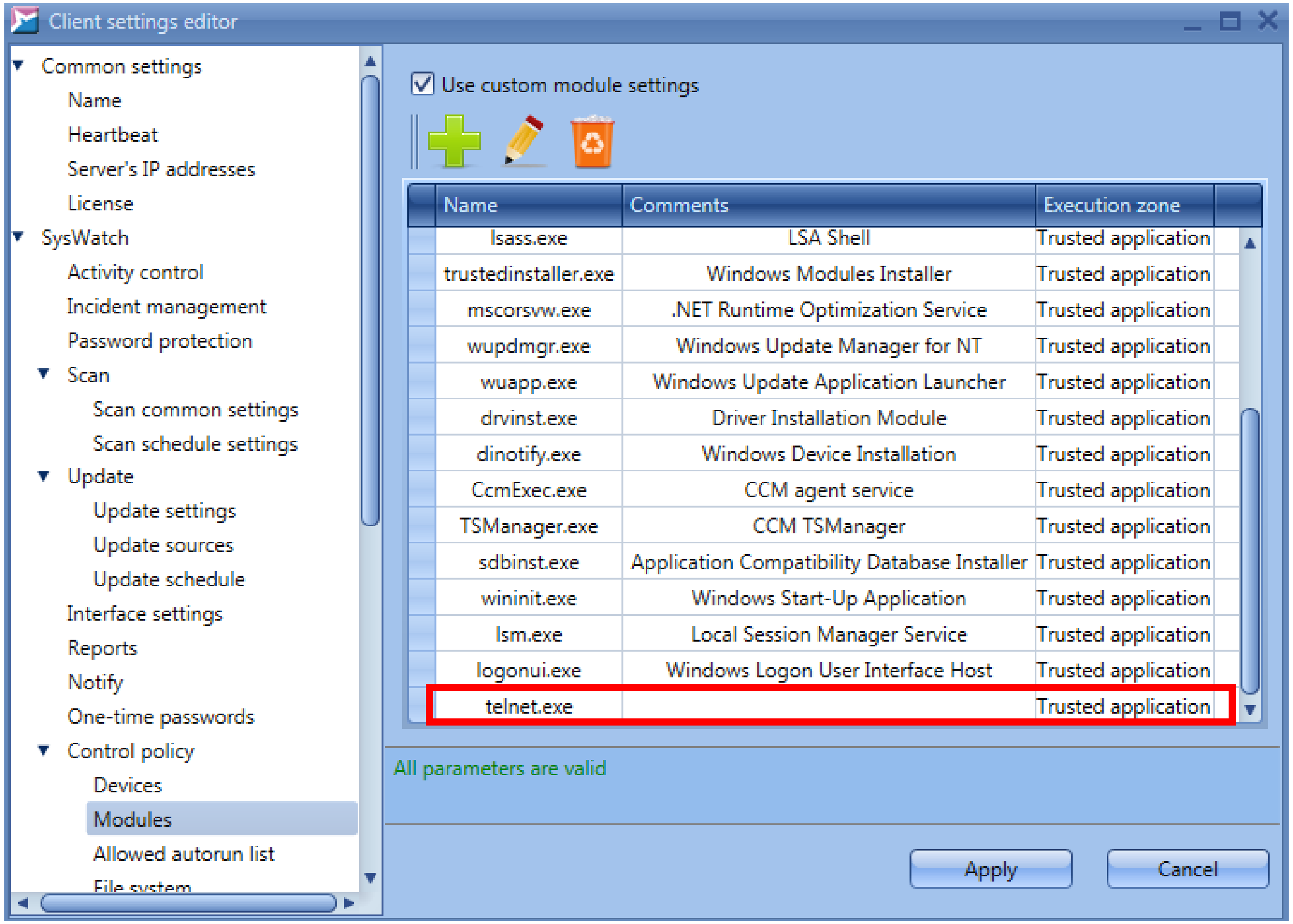
☐ Enable software update mode

☐ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

☐ In allowed autorun list



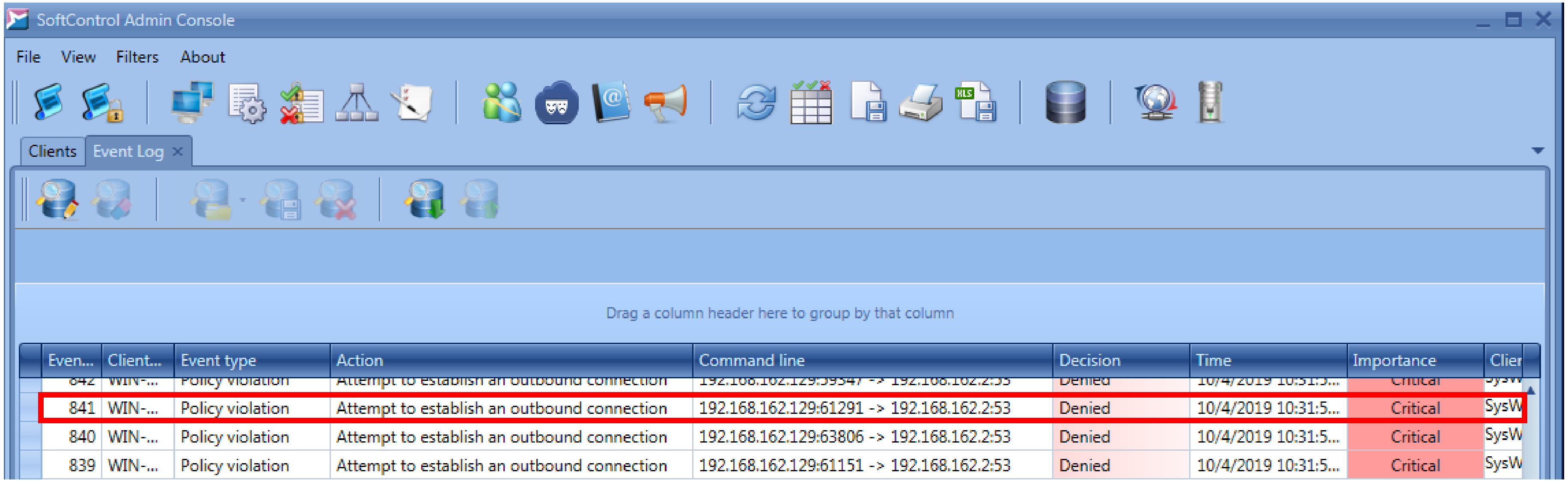
☑ Use custom module settings

Name	Comments	Execution zone
lsass.exe	LSA Shell	Trusted application
trustedinstaller.exe	Windows Modules Installer	Trusted application
mscorsvw.exe	.NET Runtime Optimization Service	Trusted application
wupdmgr.exe	Windows Update Manager for NT	Trusted application
wuapp.exe	Windows Update Application Launcher	Trusted application
drvinst.exe	Driver Installation Module	Trusted application
dinotify.exe	Windows Device Installation	Trusted application
CcmExec.exe	CCM agent service	Trusted application
TSManager.exe	CCM TSManager	Trusted application
sdbinst.exe	Application Compatibility Database Installer	Trusted application
wininit.exe	Windows Start-Up Application	Trusted application
lsm.exe	Local Session Manager Service	Trusted application
logonui.exe	Windows Logon User Interface Host	Trusted application
telnet.exe		Trusted application

All parameters are valid

10.2.4.3	Make an attempt to access *ya.ru* (87.250.250.242:80) and 192.168.1.180:8000 (a random address is given for example) by *telnet.exe*.	❑ Connection to 87.250.250.242:80 has been established successfully. Connection to 192.168.1.180:8000 has not been established.	In the device logs on SoftControl Server, you can see **Policy violation** event; action – **Attempt to establish an outgoing connection**, executed file – *C:\WINDOWS\SYSTEM32\TELNET.EXE*, details – **(ACE[rule_number] =)**, decision – **Denied.***

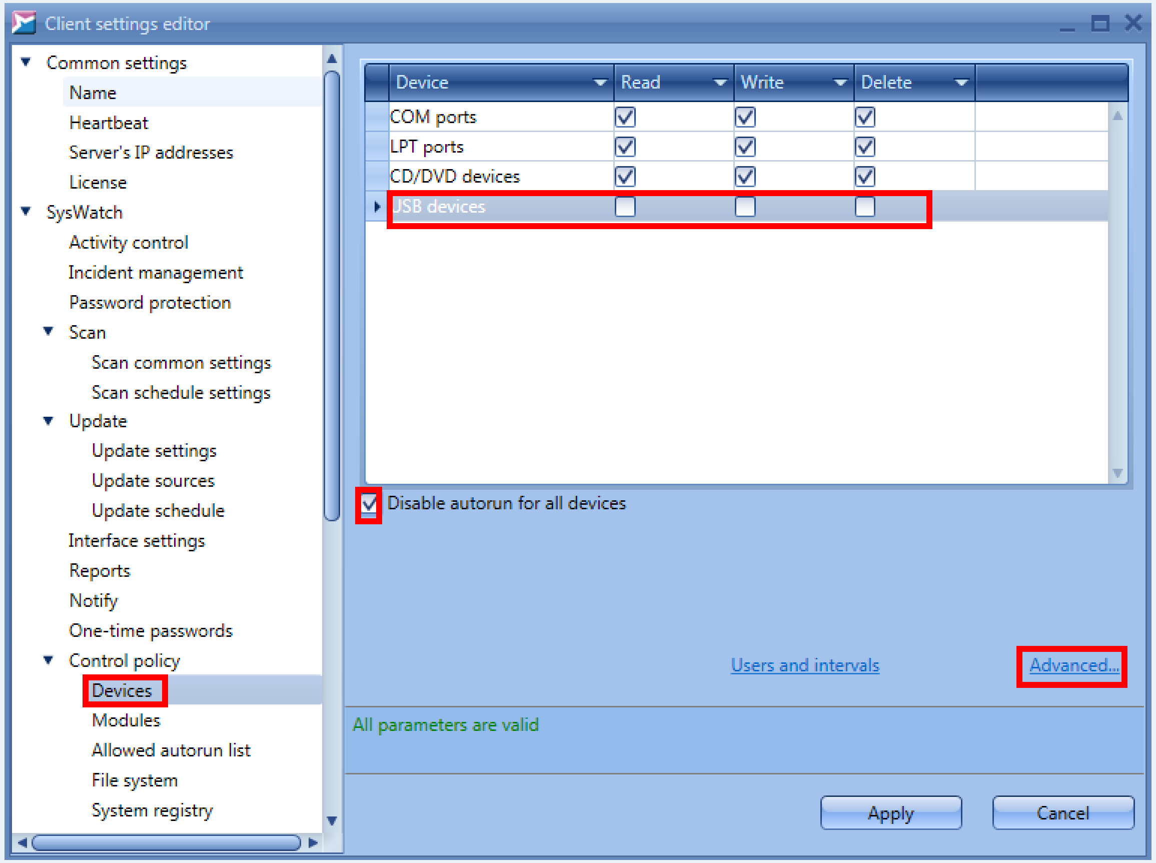
* **Policy violation – Attempt to establish an outbound connection** event appears in SoftControl Admin Console:


SoftControl Admin Console
File
View
Filters
About
Clients
Event Log
Drag a column header here to group by that column

Even...	Client...	Event type	Action	Command line	Decision	Time	Importance	Clier
842	WIN-...	Policy violation	Attempt to establish an outbound connection	192.168.162.129:59347 -> 192.168.162.2:53	Denied	10/4/2019 10:31:5...	Critical	SysW
841	WIN-...	Policy violation	Attempt to establish an outbound connection	192.168.162.129:61291 -> 192.168.162.2:53	Denied	10/4/2019 10:31:5...	Critical	SysW
840	WIN-...	Policy violation	Attempt to establish an outbound connection	192.168.162.129:63806 -> 192.168.162.2:53	Denied	10/4/2019 10:31:5...	Critical	SysW
839	WIN-...	Policy violation	Attempt to establish an outbound connection	192.168.162.129:61151 -> 192.168.162.2:53	Denied	10/4/2019 10:31:5...	Critical	SysW

10.2.5	Test rules in control policies for the devices.		
10.2.5.1	Create a rule that blocks access to the file system for USB drives. Also create a whitelist and include a trusted USB device in it.*	❑ Access to the file system is forbidden to all USB drives except the ones in the whitelist.	

* In order to create the rule, edit the client settings:

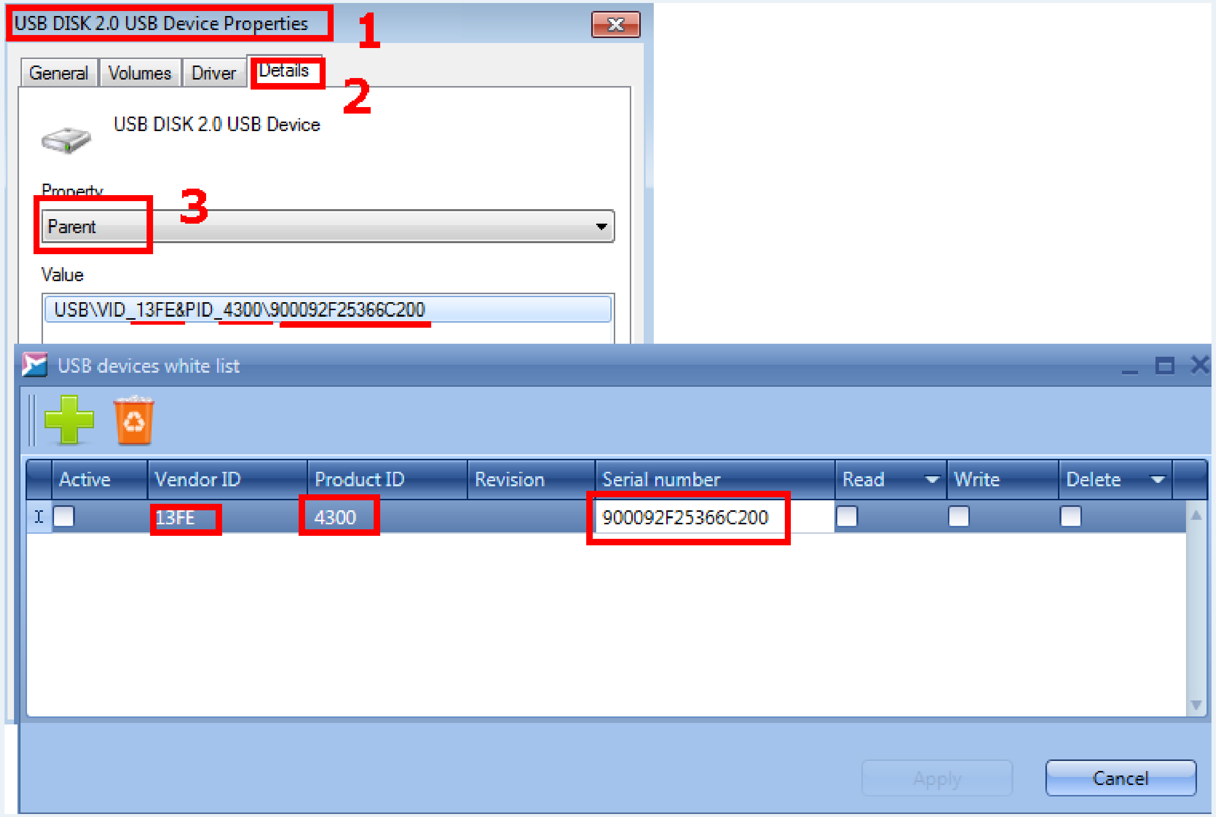


Device	Read	Write	Delete
COM ports	☑	☑	☑
LPT ports	☑	☑	☑
CD/DVD devices	☑	☑	☑
USB devices	□	□	□

☑ Disable autorun for all devices

All parameters are valid

Use the Windows device manager to extract data for the trusted USB drive rule:

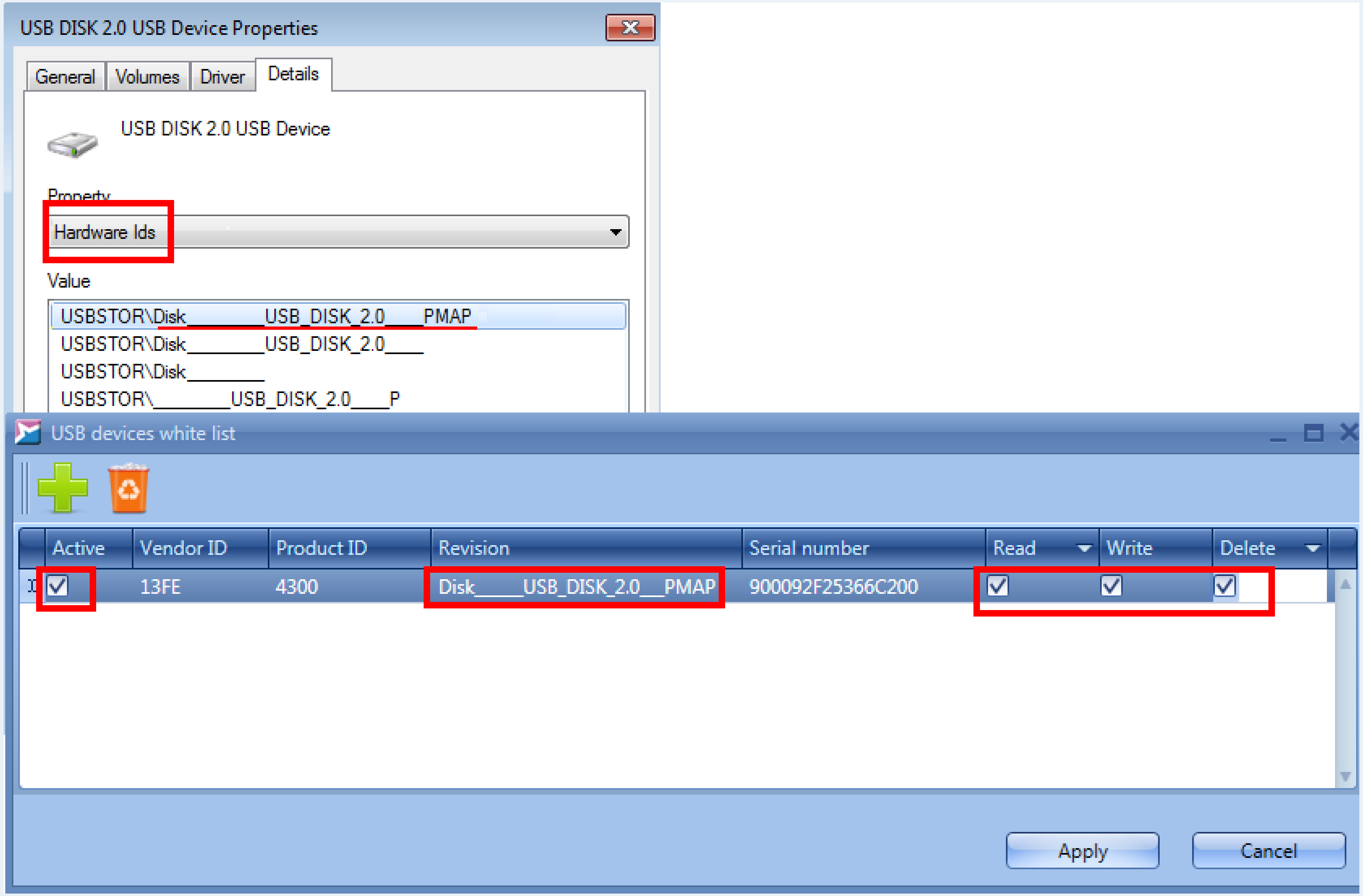


USB DISK 2.0 USB Device

Property: Parent

Value: USB\VID_13FE&PID_4300\900092F25366C200

Active	Vendor ID	Product ID	Revision	Serial number	Read	Write	Delete
□	13FE	4300		900092F25366C200	□	□	□



USB DISK 2.0 USB Device

Property

Hardware Ids

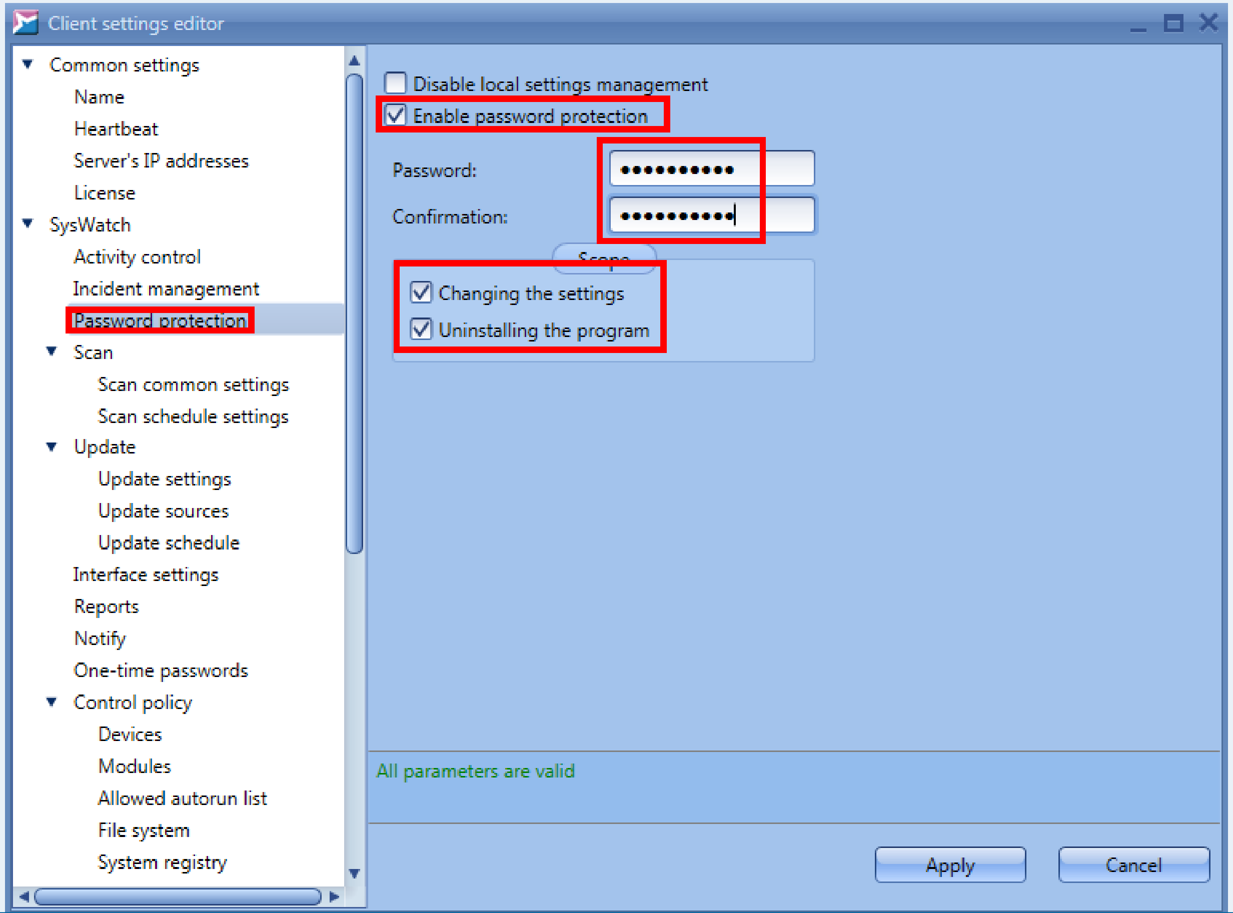
Value

USBSTOR\Disk________USB_DISK_2.0____PMAP
USBSTOR\Disk________USB_DISK_2.0____
USBSTOR\Disk________
USBSTOR________USB_DISK_2.0____P

Active	Vendor ID	Product ID	Revision	Serial number	Read	Write	Delete
☑	13FE	4300	Disk_____USB_DISK_2.0__PMAP	900092F25366C200	☑	☑	☑

Once you create the rules, save them under a new name and apply to the organizational unit to which the device you are testing belongs.			
10.2.5.2	Make an attempt to access the file system by a USB drive from the whitelist and another USB drive that is not in the whitelist.	❑ You are able to access the file system with the whitelisted USB drive; the other one gets an *Access denied* error.	
10.2.6	Test rules in control policies for **Password protection** self-protection functionality.		
10.2.6.1	Set a password for access to GUI, for changing properties, and for deleting the SoftControl SysWatch client module.*	❑ You have to enter the password in order to access GUI, change properties, or delete the SoftControl SysWatch client module.	

* Edit the client settings to set the password:



Client settings editor

☐ Disable local settings management

☑ Enable password protection

Password: ●●●●●●●●●●●

Confirmation: ●●●●●●●●●●●

Scope

☑ Changing the settings

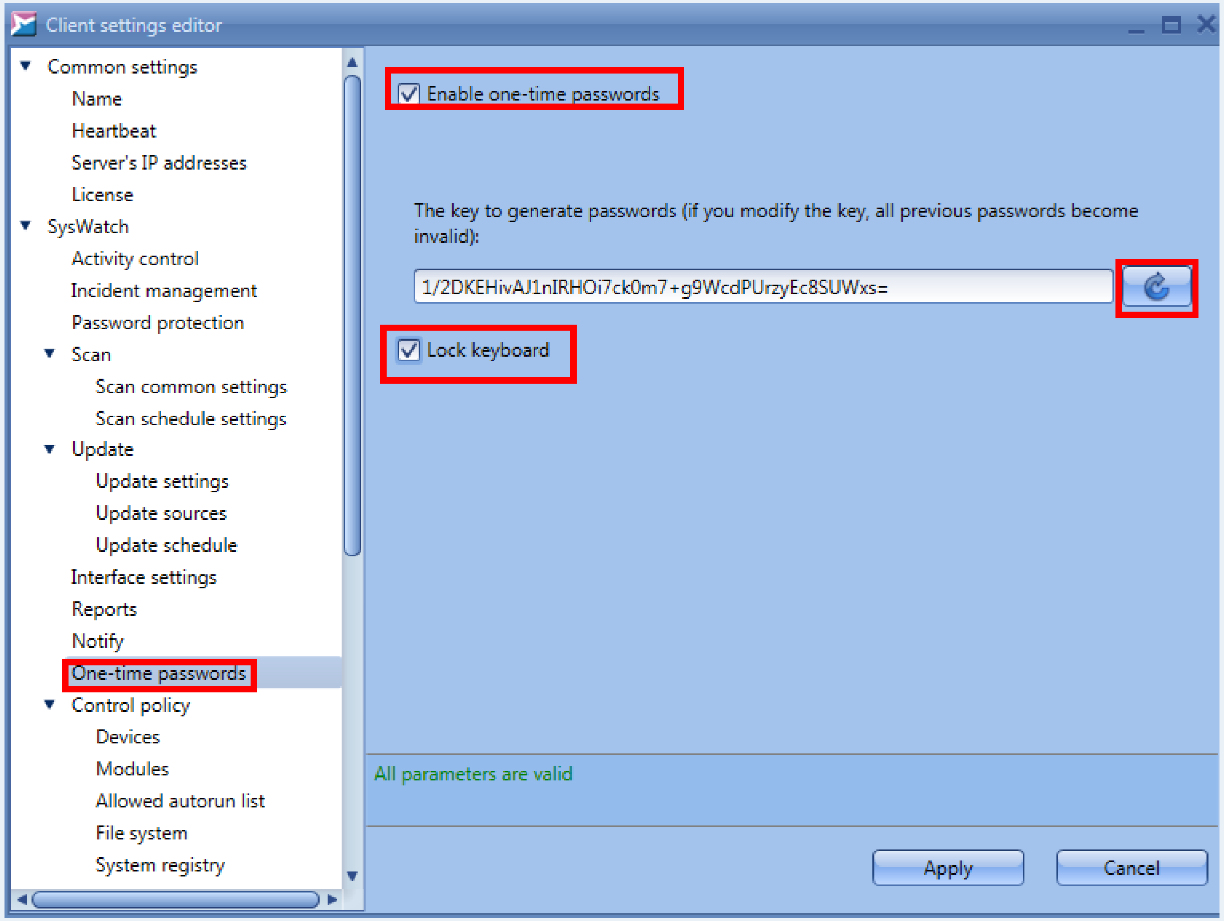
☑ Uninstalling the program

All parameters are valid

10.2.6.2	Check access to GUI, make an attempt to delete the SoftControl SysWatch client module.	❑ You can't access GUI without the password. When you try to delete the SoftControl SysWatch client module, you are requested to enter the password.	

10.2.7	Test rules in control policies for one-time (temporary) passwords.		
10.2.7.1	Activate keyboard blocking and use of one-time (temporary) passwords for access to GUI of the SoftControl SysWatch client module.*	□ One-time passwords and keyboard blocking have been turned on.	A one-time password is a UTC time hash function. So, difference between the UTC time on the client device and SoftControl Admin Console shall not be greater than duration of the password validity. Otherwise, the password access to GUI of the SoftControl SysWatch client module (and to keyboard unblocking) will not function.

* In order to activate use of one-time passwords, edit the client settings, save them under a new name and apply to the organizational unit which the device you are testing belongs to:



☑ Enable one-time passwords

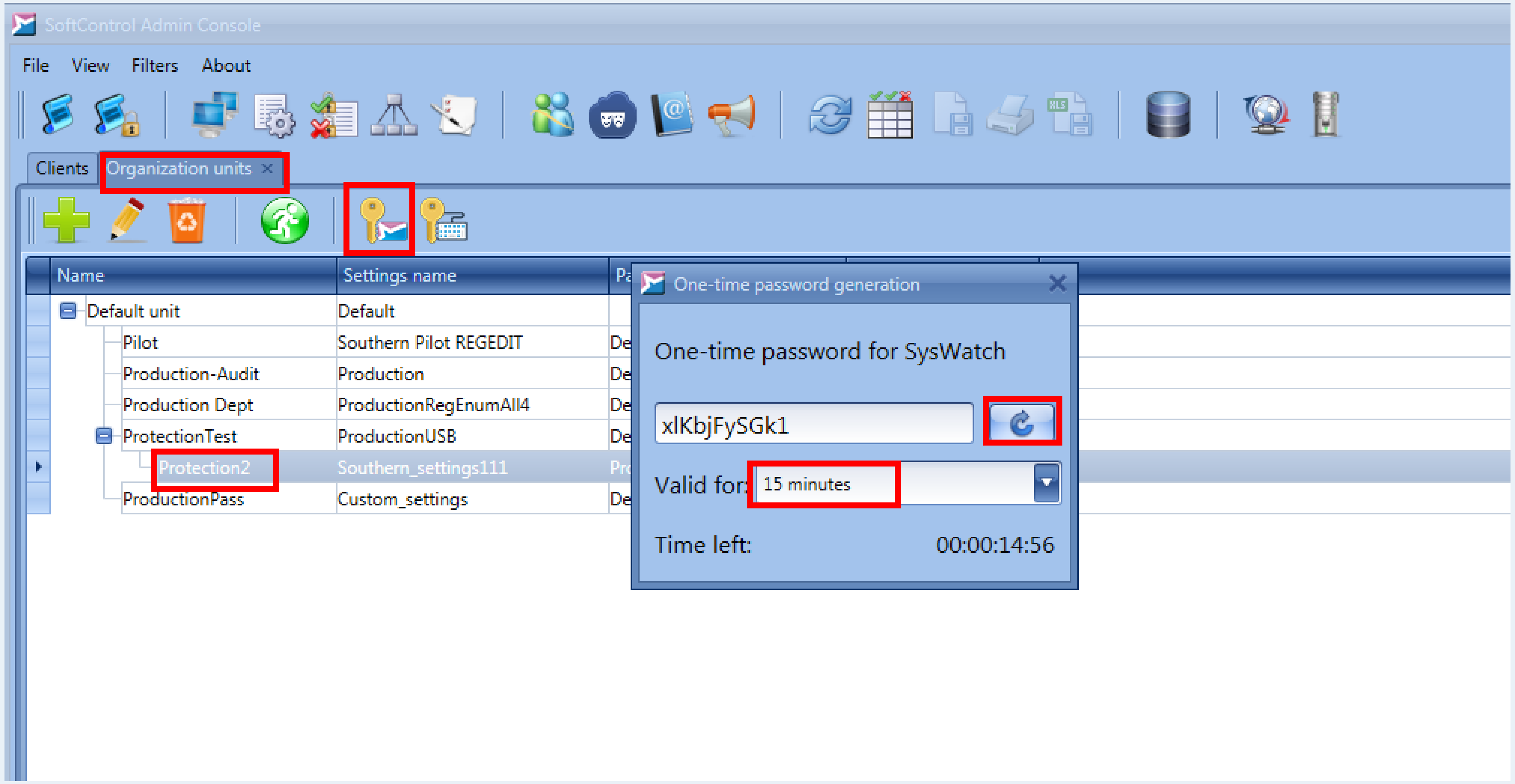
The key to generate passwords (if you modify the key, all previous passwords become invalid):

1/2DKEHivAJ1nIRHOi7ck0m7+g9WcdPUrzyEc8SUWxs=

☑ Lock keyboard

All parameters are valid

Do the following to create a one-time password for access to GUI:



Name	Settings name	Pa
Default unit	Default	
Pilot	Southern Pilot REGEDIT	De
Production-Audit	Production	De
Production Dept	ProductionRegEnumAll4	De
ProtectionTest	ProductionUSB	De
Protection2	Southern_settings111	Pr
ProductionPass	Custom_settings	De

One-time password generation

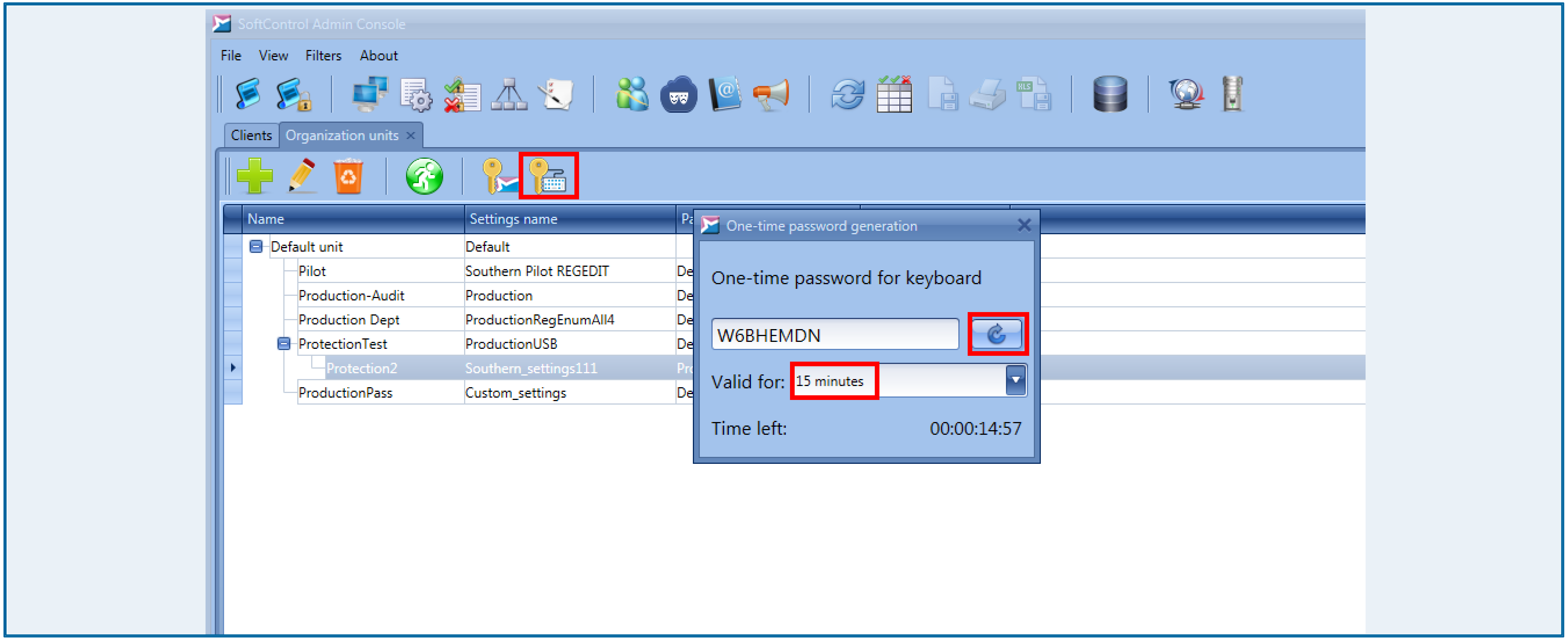
One-time password for SysWatch

xlKbjFySGk1

Valid for: 15 minutes

Time left: 00:00:14:56

Do the following to create a one-time password for keyboard blocking:



Name	Settings name	Pa
Default unit	Default	
Pilot	Southern Pilot REGEDIT	De
Production-Audit	Production	De
Production Dept	ProductionRegEnumAll4	De
ProtectionTest	ProductionUSB	De
Protection2	Southern_settings111	Pr
ProductionPass	Custom_settings	De

One-time password generation

One-time password for keyboard

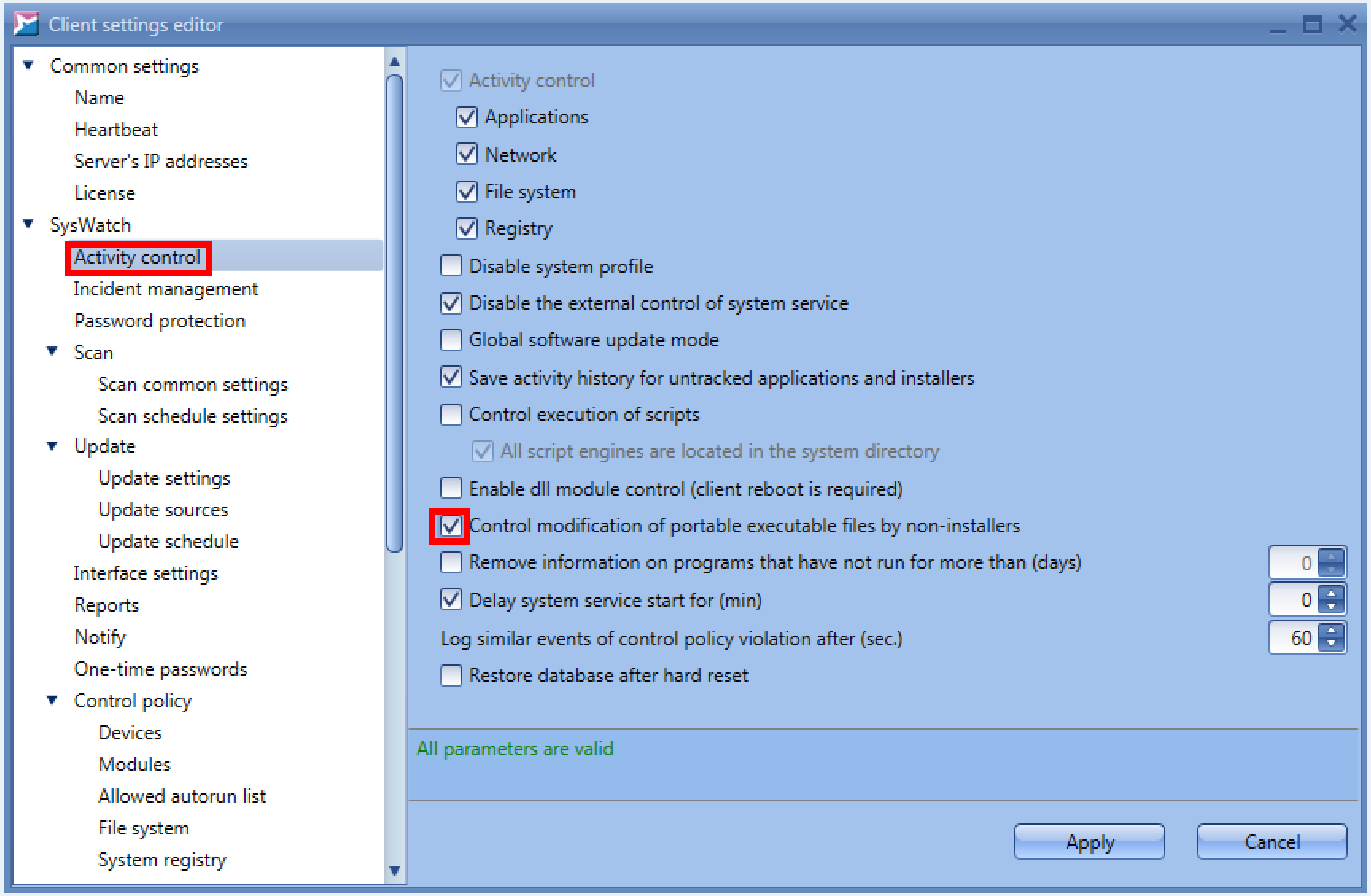
W6BHEMDN

Valid for: 15 minutes

Time left: 00:00:14:57

10.2.7.2	Test operation of one-time passwords.*	❑ The keyboard of the client device does not respond to keys being pressed. You can access GUI of the SoftControl SysWatch client module only after entering the one-time password.	The Information Security Administrator provides the engineer who works locally with the ATM with valid passwords that were generated to unblock the keyboard and access the SoftControl SysWatch client module GUI. The engineer uses these passwords to unblock the keyboard and get access to GUI of the SoftControl SysWatch client module. Note that the generated passwords have only UPPERCASE letters; when you are typing in the password, use lowercase letters.
10.2.8	Test rules in control policies for prohibition of PE files modification.		
10.2.8.1	Forbid modification of PE files to all but trusted installers.*	❑ PE files modification is now forbidden.	

* In order to forbid modification of executable files, edit the client settings:



☑ Activity control

☑ Applications

☑ Network

☑ File system

☑ Registry

□ Disable system profile

☑ Disable the external control of system service

□ Global software update mode

☑ Save activity history for untracked applications and installers

□ Control execution of scripts

☑ All script engines are located in the system directory

□ Enable dll module control (client reboot is required)

☑ Control modification of portable executable files by non-installers

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

☑ Delay system service start for (min) 0

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

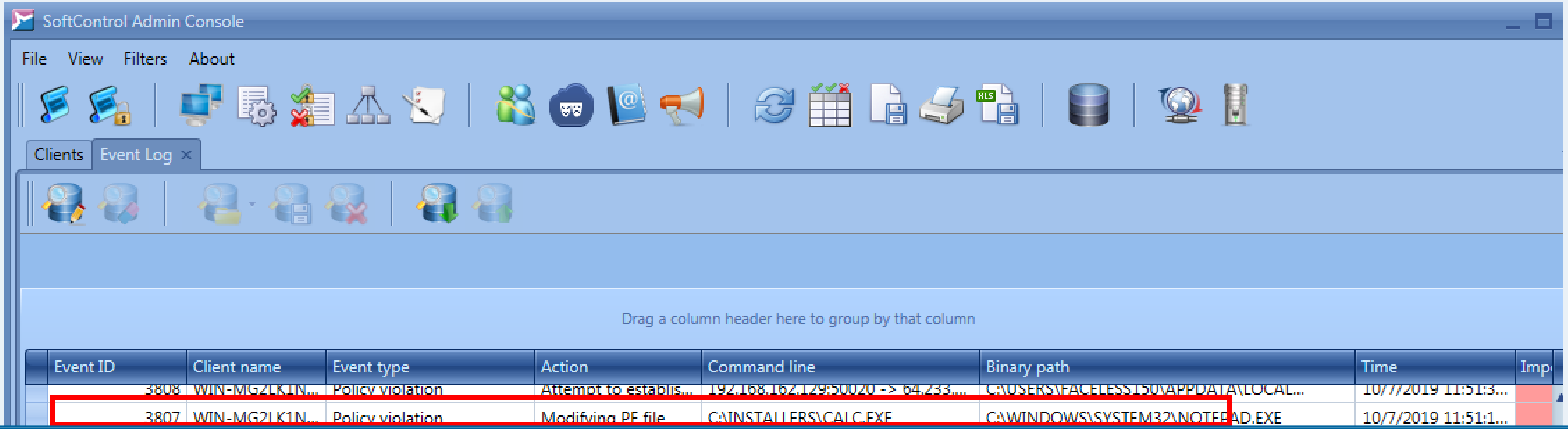
□ Restore database after hard reset

All parameters are valid

Once you create the rules, save the settings under a new name and apply them to the organizational unit which the device you are testing belongs to.

10.2.8.2	Make an attempt to change the calculator executable file (*calc.exe*) with the Windows notepad (*notepad.exe*).*	❑ When you attempt to change the executable file, you will see a message saying it is not possible to make changes to the PE file.	The *calc.exe* file has been copied in advance to *C:\installers*.

* SoftControl Admin Console displays **Policy violation – Modifying PE file** event:



Drag a column header here to group by that column

Event ID	Client name	Event type	Action	Command line	Binary path	Time	Imp
3808	WIN-MG2LK1N...	Policy violation	Attempt to establis...	192.168.162.129:50020 -> 64.233....	C:\USERS\FACELESS150\APPDATA\LOCAL...	10/7/2019 11:51:3...	
3807	WIN-MG2LK1N...	Policy violation	Modifying PE file	C:\INSTALLERS\CALC.EXE	C:\WINDOWS\SYSTEM32\NOTEPAD.EXE	10/7/2019 11:51:1...	

3. Customer support

If you have any questions concerning the installation, setting up and operation of TPSecure 6.1.398, please contact our customer support by e-mail support@safensoft.com.

4. Supplemental information

4.1 Updating SoftControl SysWatch and antivirus bases on Windows XP

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

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

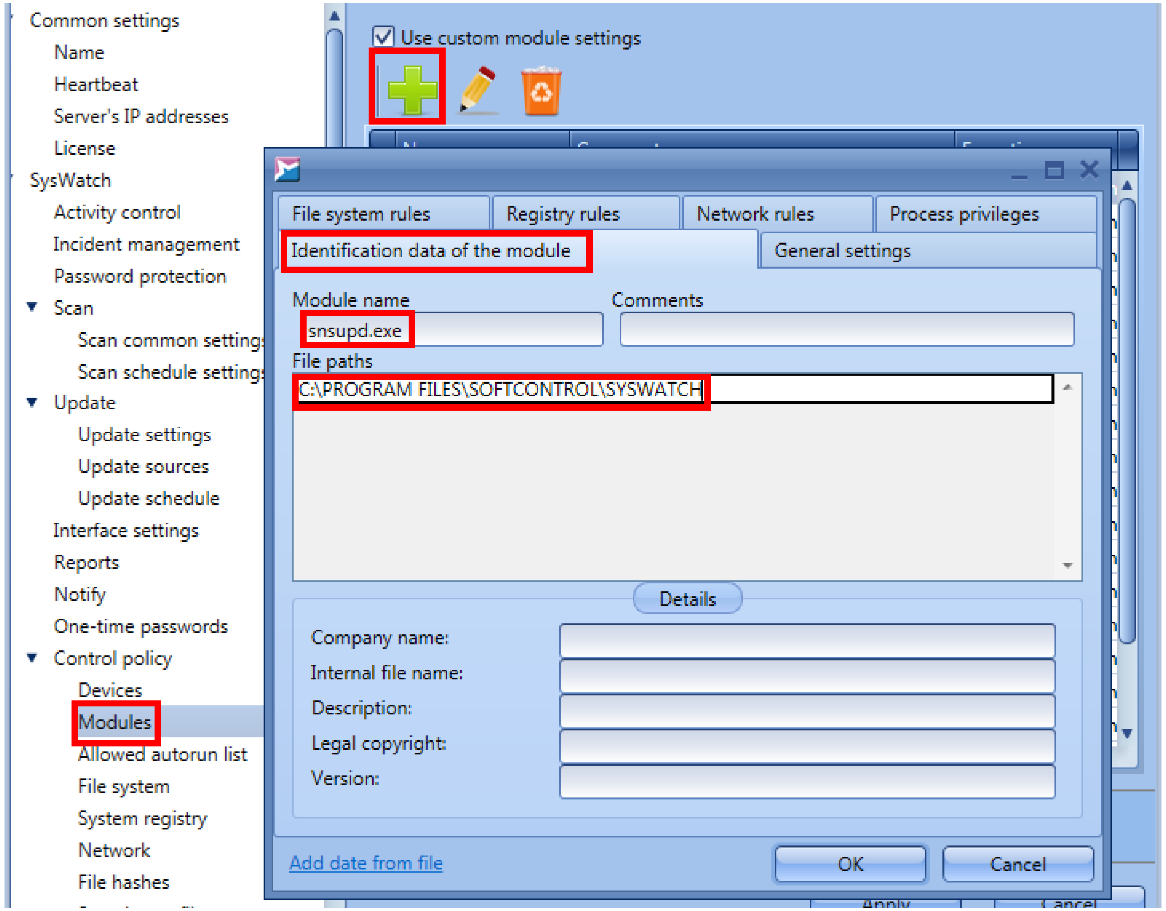
Follow steps in this section to ensure proper update of the SoftControl SysWatch application and antivius bases on 32-bit Windows XP.

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

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

Table 11. Update modules

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



☑ Use custom module settings

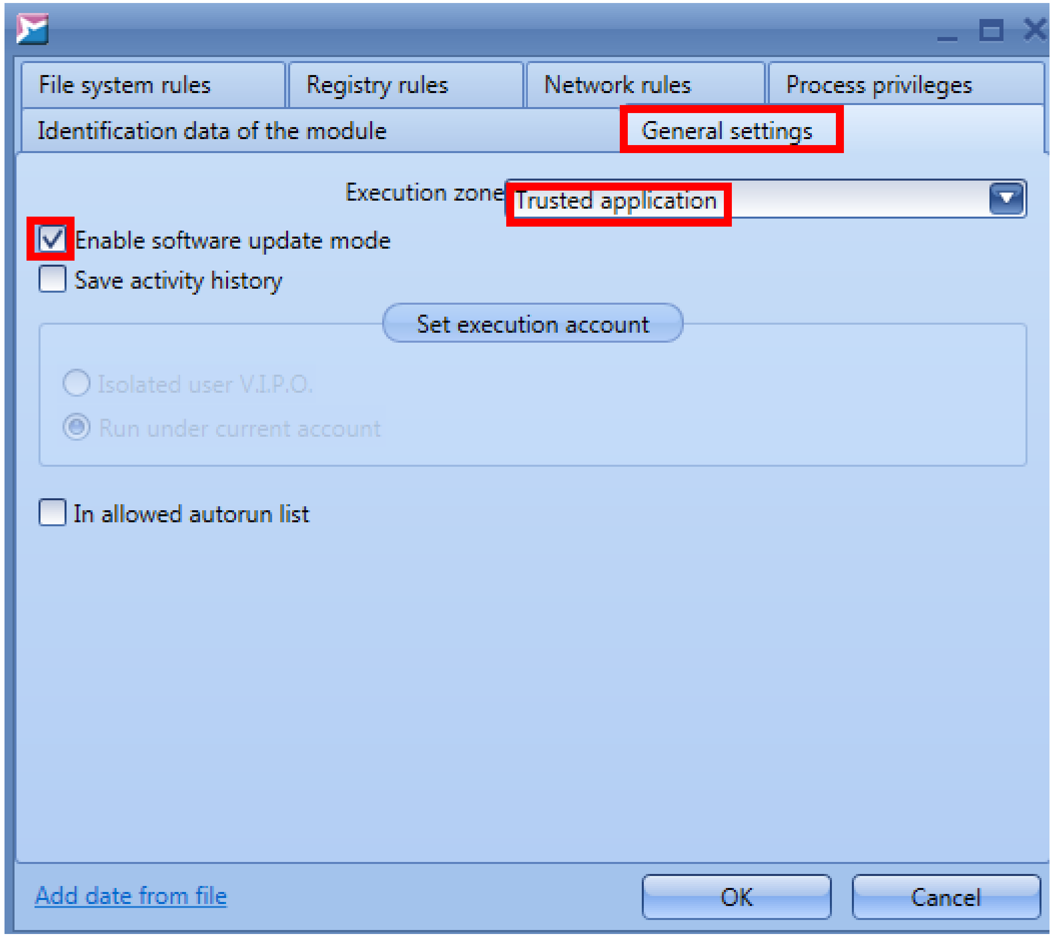
Module name: snsupd.exe

Comments:

File paths: C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH

Figure 1. Setting up an update module (for SoftControl SysWatch)

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



Execution zone: Trusted application

☑ Enable software update mode

□ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

□ In allowed autorun list

Figure 2. Adding the module to trusted applications

6. Click **OK**.

7. Save the client settings under a new name and apply them to the organizational unit of the clients that require updating.

If you are setting up updating for SoftControl SysWatch, now you can create a task to update the antivirus bases or wait for a scheduled update.