SoftControl

TPS 5.0.18

SoftControl Pilot Project Plan

Dear user!

Safe'N'Sec Corporation thanks you for choosing TPSecure 5.0.18. Specialists of the company do their best to make sure our software both meets the highest requirements in a field of information protection and is easy use. We hope you find TPSecure 5.0.18 helpful.

Postal address:

127106 Russia, Moscow

Botanicheskaya street, house number 10d building 1

Safe'N'Sec Corporation

Tel:

+7 (495) 967-14-51

Fax:

+ 7 (495) 967-14-52

E-mails:

Customer service: support@safensoft.com

Sales team: sales@safensoft.com

Website: http://www.safensoft.com

Contents

1. Testing procedure for 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 Organizational requirements for conduction of the pilot project

In order to conduct pilot testing of the Client's infrastructure, it is necessary to confirm compliance with the Specifications for deployment of the three SoftControl components: the server module **SoftControl Server**, the management console **SoftControl Admin Console**, and the client module **SoftControl SysWatch**.

1.3 Procedure

Testing consists of the following successive stages:

1) Ratification of a testing plan, which defines responsible personnel within the participating organizations
2) Software installation
3) Operational and functional tests
4) Counseling provided by both sides, final review, and signing of the checklist for the performed tests

Results of the testing shall be submitted in form of a checklist. Each test described in the pilot project plan shall be carried out for each client component within the pilot zone. Outcome of all per-

formed tests shall be included in the checklist.

Results of the testing may be used for the following:

- To confirm compliance of the product with the reported functional and operational characteristics.
- In the process of deploying and operating the software product on Client's network of devices. In this case, control policies, batch installers, and instructions that were created during the testing process may be helpful..

1.4 System requirements

SoftControl Server requirements

Table 1. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
▪ 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® Server 2008 (SP2) (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10 ▪ Microsoft® Windows® Server 2016	3GHz	4GB	100MB + extra 4GB (for embedded DBMS installation)

Additional software:

- Microsoft® .NET Framework 4.5.

SoftControl Admin Console requirements

Table 2. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
▪ 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® 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 ▪ Microsoft® Windows® Server 2016	3GHz	4GB	100MB

Additional software:

- Microsoft® .NET Framework 4.5.

SoftControl SysWatch requirements

Table 3. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
Client operating systems:			150MB + extra 120MB or more for antivirus database updates
Microsoft® Windows® XP (SP2 and above) *32-bit*	800MHz	512MB	
Microsoft® Windows® XP (SP2) *64-bit*	800MHz	512MB	
Microsoft® Windows® XP Embedded (SP2 and above)	800MHz	256 MБ	
Microsoft® Windows® Embedded for Point of Service 1.0	800MHz	256 MБ	
Microsoft® Windows® 7 (SP1) *32-bit*	1GHz	1GB	
Microsoft® Windows® 7 (SP1) *64-bit*	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	
Server operating systems:			
Microsoft® Windows® Server 2003 (SP2) *32-bit*	800MHz	512MB	
Microsoft® Windows® Server 2003 (SP2) *64-bit*	800MHz	512MB	
Microsoft® Windows® Server 2008 R2 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2012 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2012 R2 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit* (for Server with Desktop Experience installation option)	1.4GHz	2GB	

Additional requirements:

- Visual C++ 2008 SP1 Redistributable Package when installing SoftControl SysWatch on Windows XP.
- For Windows 7 and Windows Server 2008 R2: update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature verification).

SoftControl DLP Client requirements

Table 4. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
Client operating systems:			20MB
Microsoft® Windows® XP (SP3) *32-bit*	800MHz	512MB	
Microsoft® Windows® XP (SP2) *64-bit*	800MHz	512MB	
Microsoft® Windows® XP Embedded (SP2 и выше)	800MHz	512MB	
Microsoft® Windows® Embedded for Point of Service 1.0	800MHz	512MB	
Microsoft® Windows® 7 (SP1) *32-bit*	1GHz	1GB	
Microsoft® Windows® 7 (SP1) *64-bit*	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	
Server operating systems:			
Microsoft® Windows® Server 2003 (SP2) *32-bit*	800MHz	512MB	
Microsoft® Windows® Server 2003 (SP2) *64-bit*	800MHz	512MB	
Microsoft® Windows® Server 2008 R2 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2012 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2012 R2 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit*	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit* (for Server with Desktop Experience installation option)	1.4GHz	2GB	

Additional requirements:

- For Windows 7 and Windows Server 2008 R2: update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature verification).

2. Testing checklist

2.1 Check of Client's infrastructure state

2.1.1 How to check compliance with the Specifications for deployment

Table 5. Compliance check

No.	Action	Expected outcome	Comment
5.1	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.
5.2	Check that hardware and software characteristics of the devices in the data sheet comply with the deployment specifications.	❑ Compliance with the Specifications for deployment is confirmed.	
5.3	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.
5.4	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

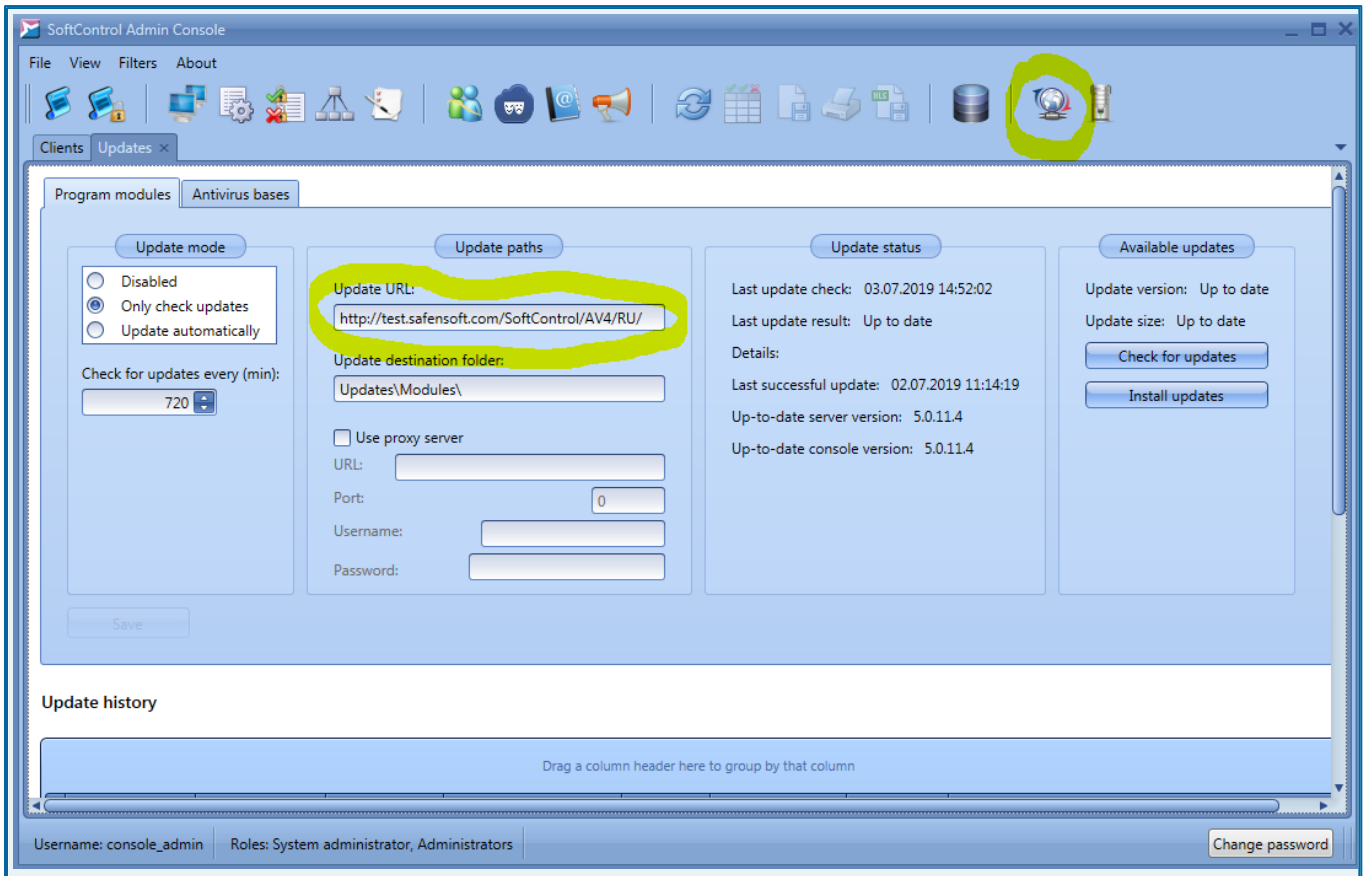
Table 6. SoftControl Service Center deployment

No.	Action	Expected outcome	Comment

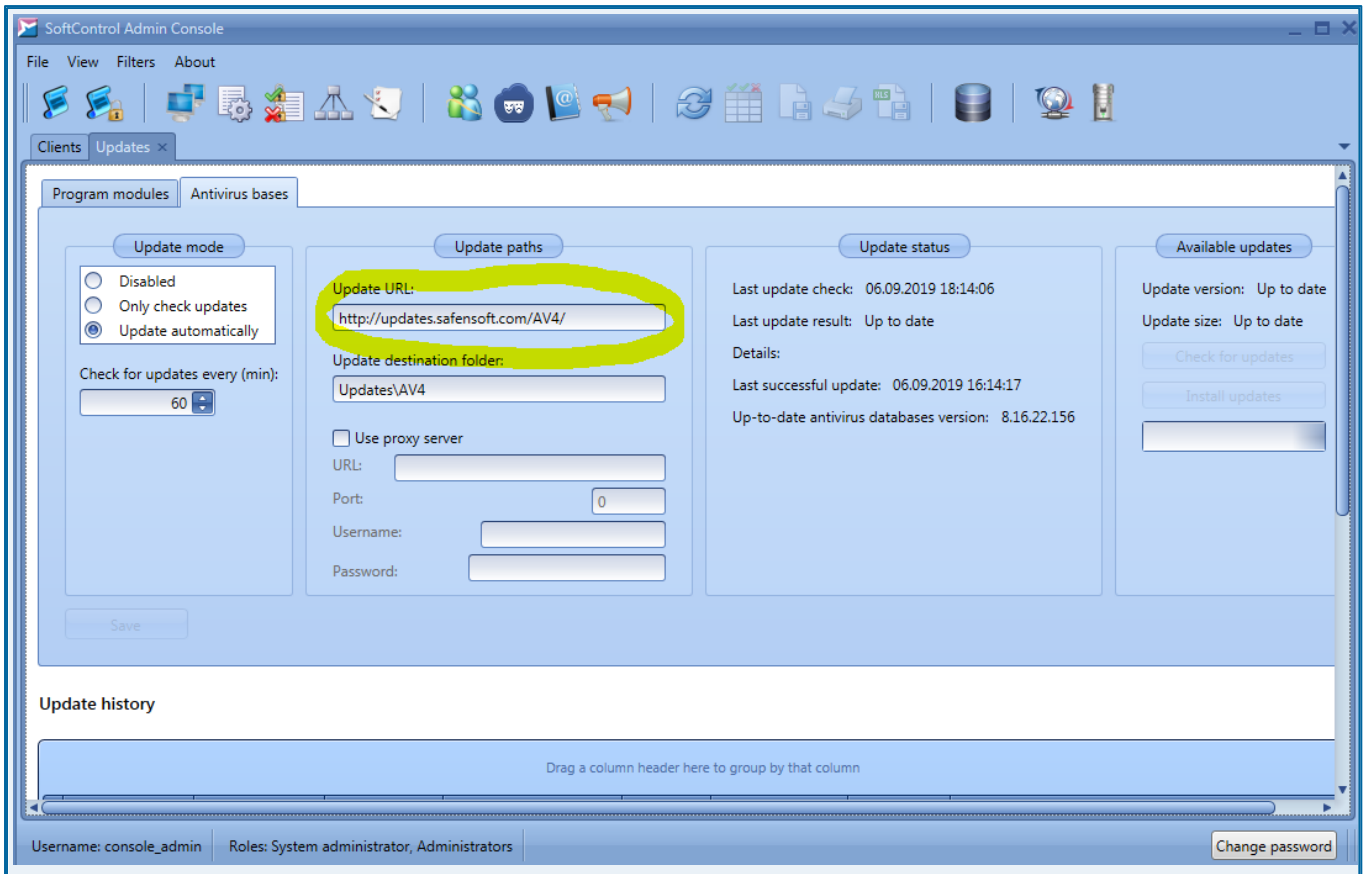
6.1	Install the following components: SoftControl Server, SoftControl Admin Console, MS SQL 2014 Express.	❑ The server component has been successfully installed and initially configured.	Installation is performed by Client's personnel. Administrator rights are required. All components can be installed 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.			
6.2	Configure SoftControl Service Center.		Configuring is performed by Client's personnel.
6.3	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".
6.4	Set the main and backup IP-addresses for SoftControl Service Center.	❑ "Server settings" 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).
6.5	Log in to SoftControl Admin Console as Administrator.	❑ Administrator has logged in successfully.	
6.6	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.



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.



6.7	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

Table 7. SoftControl SysWatch deployment

No.	Action	Expected outcome	Comment
7.1	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.
7.2	Install and perform initial configuring of the client component SoftControl SysWatch.		
7.3	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;	❑ 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)*.

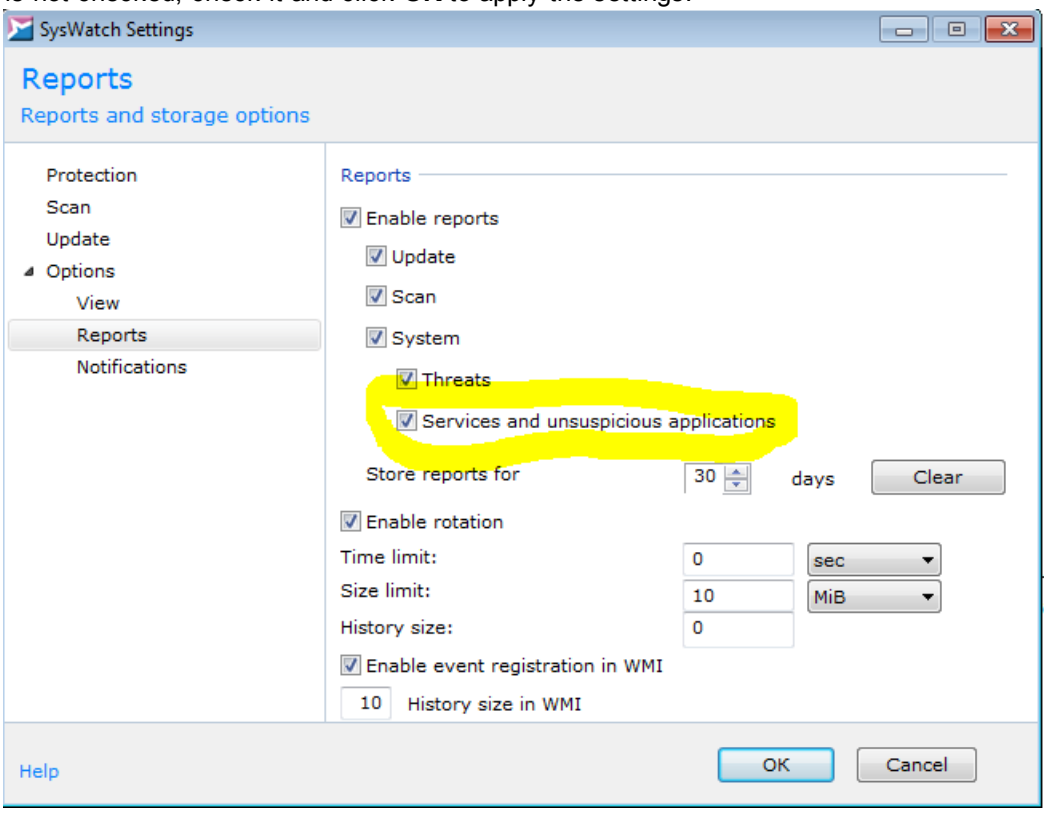
	• *SysWatch_Patch.msi* without the antivirus.		

* 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 (22) 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).

7.4	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)*.
7.5	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.

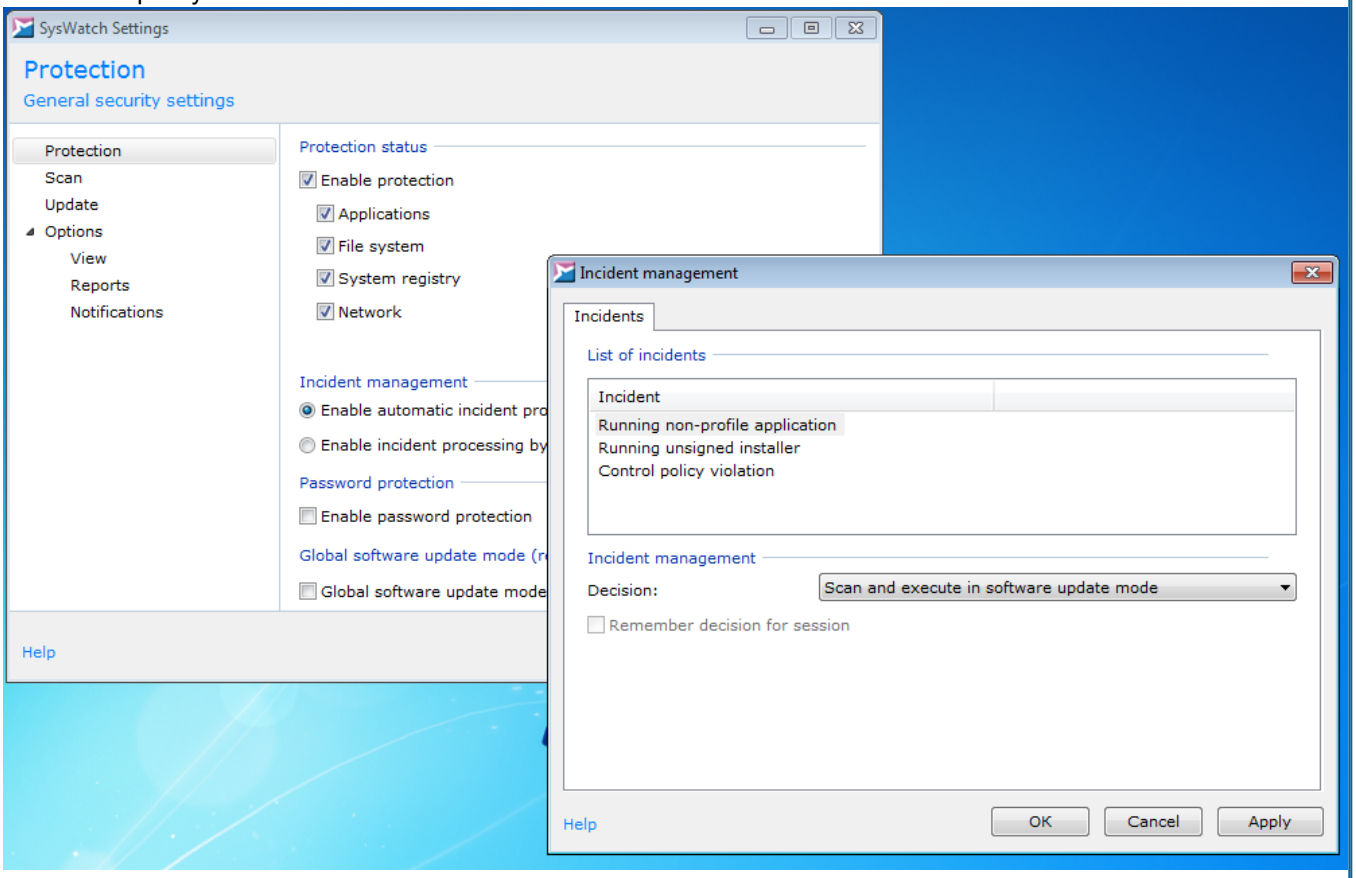
* In order to turn on logging of **Services and unsuspicious applications**, find the SoftControl SysWatch icon in the system tray, click on it with the right button of your mouse, and select **Settings**. SoftControl SysWatch window will open. Select **Options** –> **Reports** on the left and make sure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

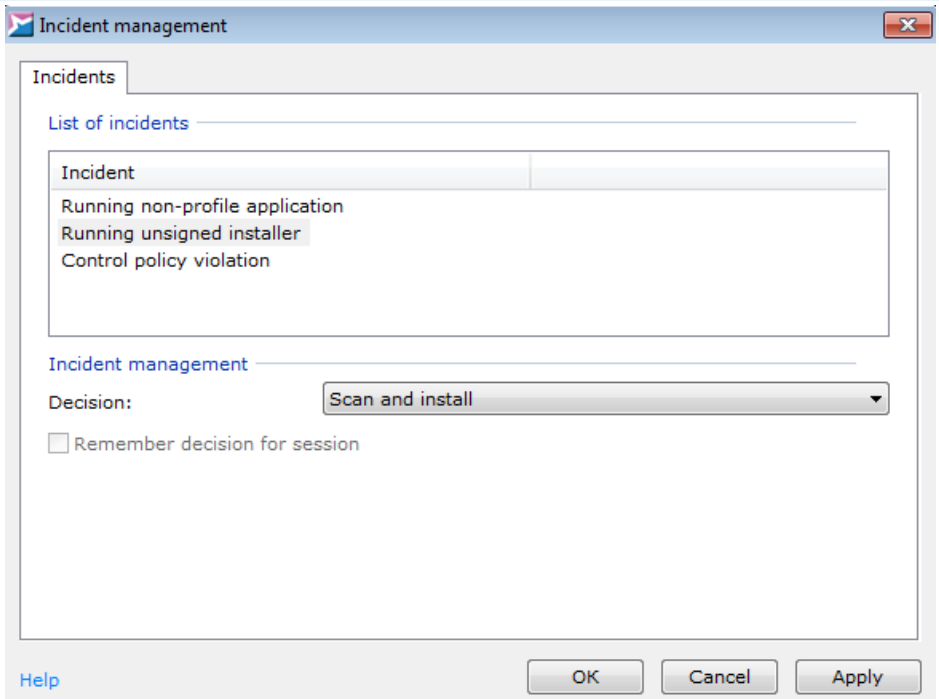


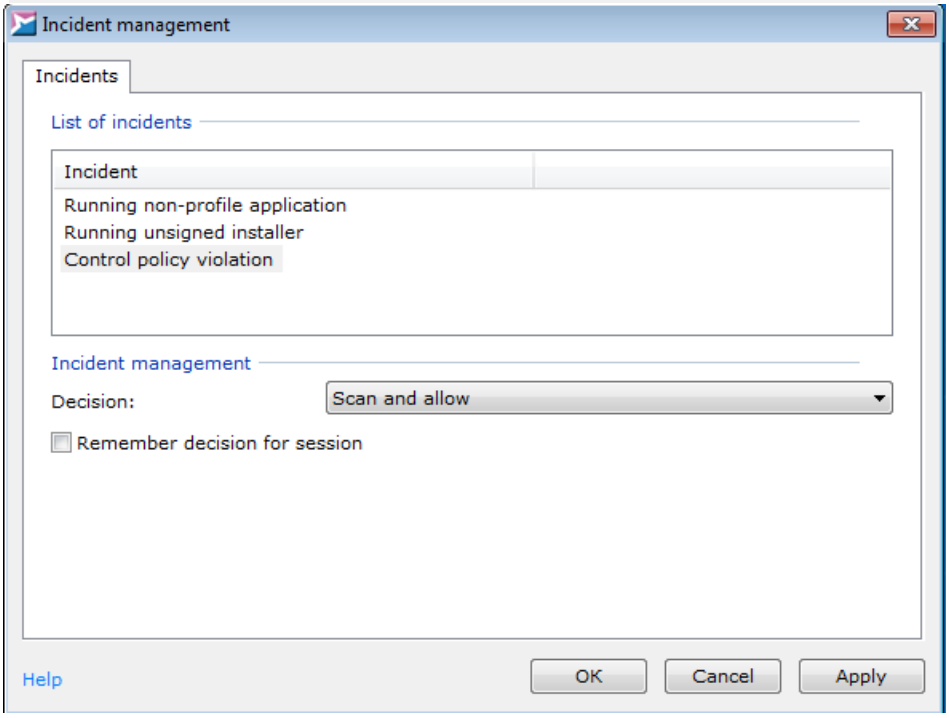
7.6	Turn on the auditing mode.*		When the auditing mode is on, SoftControl SysWatch does not block applications upon **Running non-profile application**, **Running unsigned installer**, and **Policy violation** events. It means that performance of system tasks and applications will not be affected by 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 – Scan and execute in software update mode;
- Running unsigned installer – Scan and install;
- Control policy violation – Scan and allow.



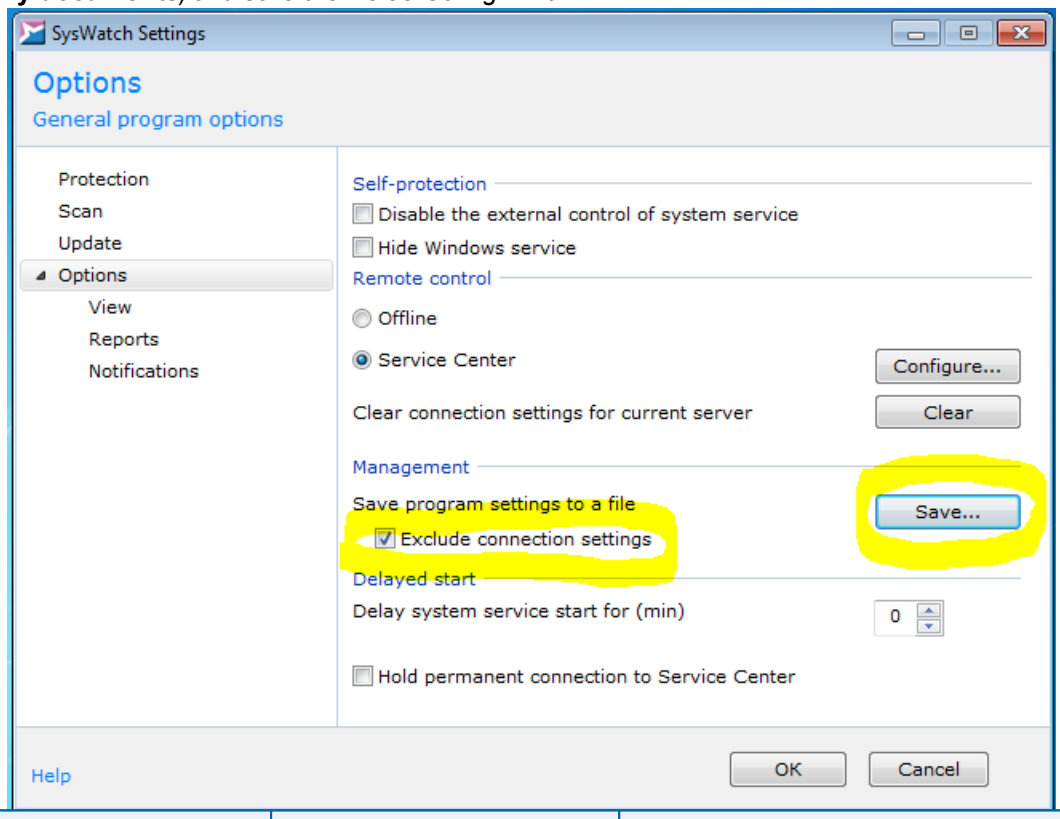




Click **Apply**.

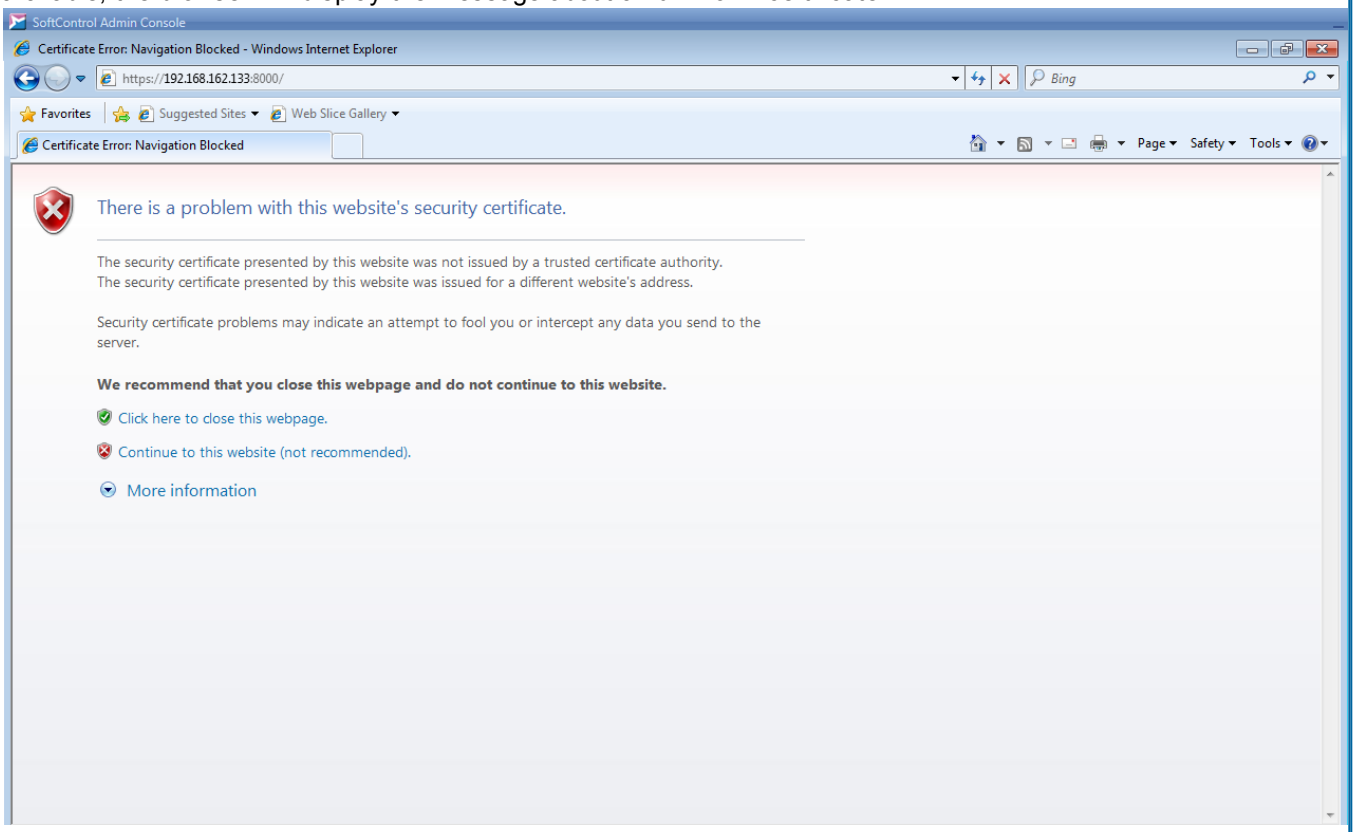
7.7	Save *Config.xmlc* – the configuration file for the client module SoftControl SysWatch installed on the device. This file contains preset configuration for compliance and exclusion of control policies.*	❑ *Config.xmlc* has been saved.	The configuration file will be used for the package installer.

* 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*.



7.8	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.

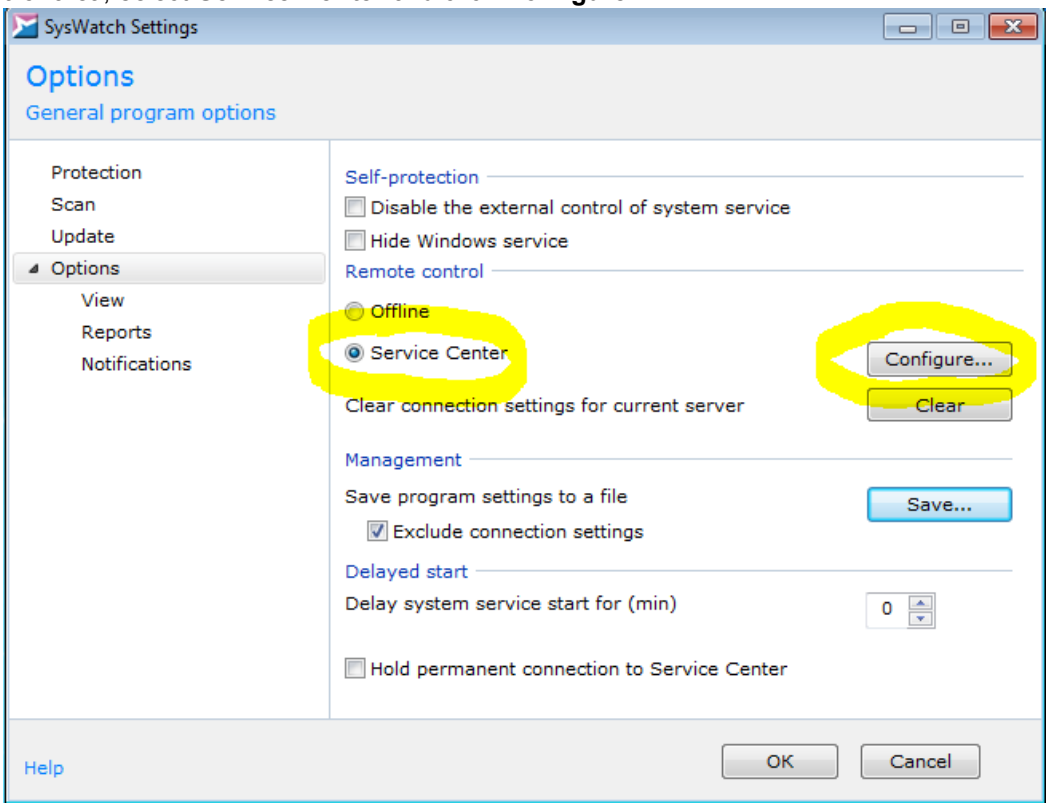
* Open Internet Explorer on the client device and enter the address of SoftControl Server and the port for client's connection (8000 by default), e.g., https://192.168.1.181:8000. If the server is available, the browser will display the message about an unknown certificate.
If SoftControl Admin Console 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.



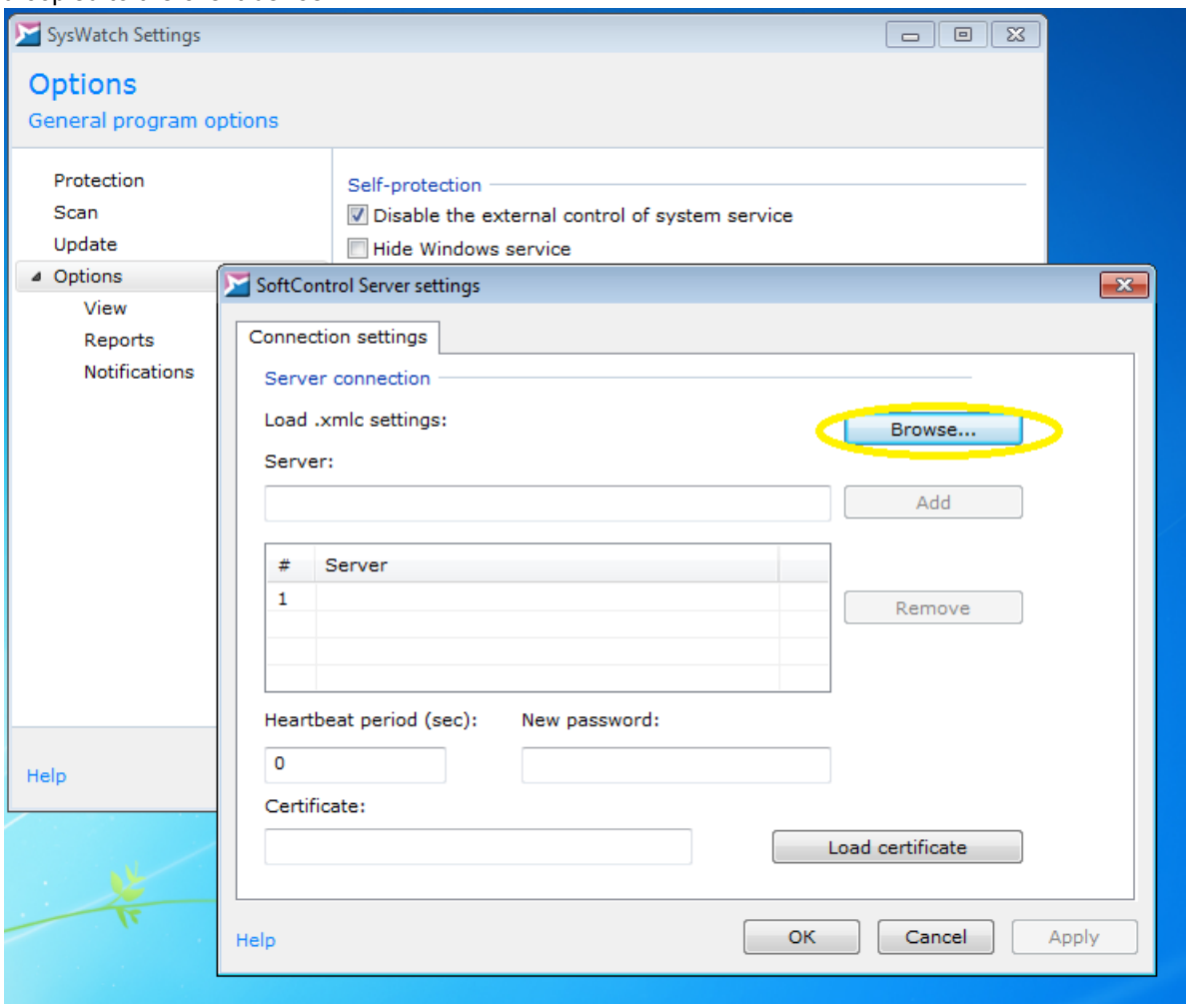
7.9	Connect the client module SoftControl SysWatch to SoftControl Service Center.*		Request to connect to the server has been sent.

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**.



SoftControl server settings window will open. Click **Browse** and open the *ClientSettings.xmlc* from item 6.7 [11] that you copied to the client device:



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

7.10	Reload the client device.		
7.11	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.
7.12	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/39/TOOLS/Setup_SnsDumpTool_x64.exe,
- http://updates.safensoft.com/39/TOOLS/Setup_SnsDumpTool_x86.exe,

Then open the file as Administrator.

7.13	Provide Safe'N'Sec Corporation with the configuration file from 6.7 [11] 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 8. Package installer creation

No.	Action	Expected outcome	Comment
8.1	Prepare the package installer for the client component SoftControl SysWatch[1] (19) 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] (20) • preset configuration file (*Config.xmlc*) for auditing mode;[3] (20) • certificate: VeriSign Class 3 Public Primary Certification Authority – *G5.cer*;[4] (22) • installation script that places the certificate of the client module SoftControl SysWatch into the Windows storage;[5] (22) • 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
```

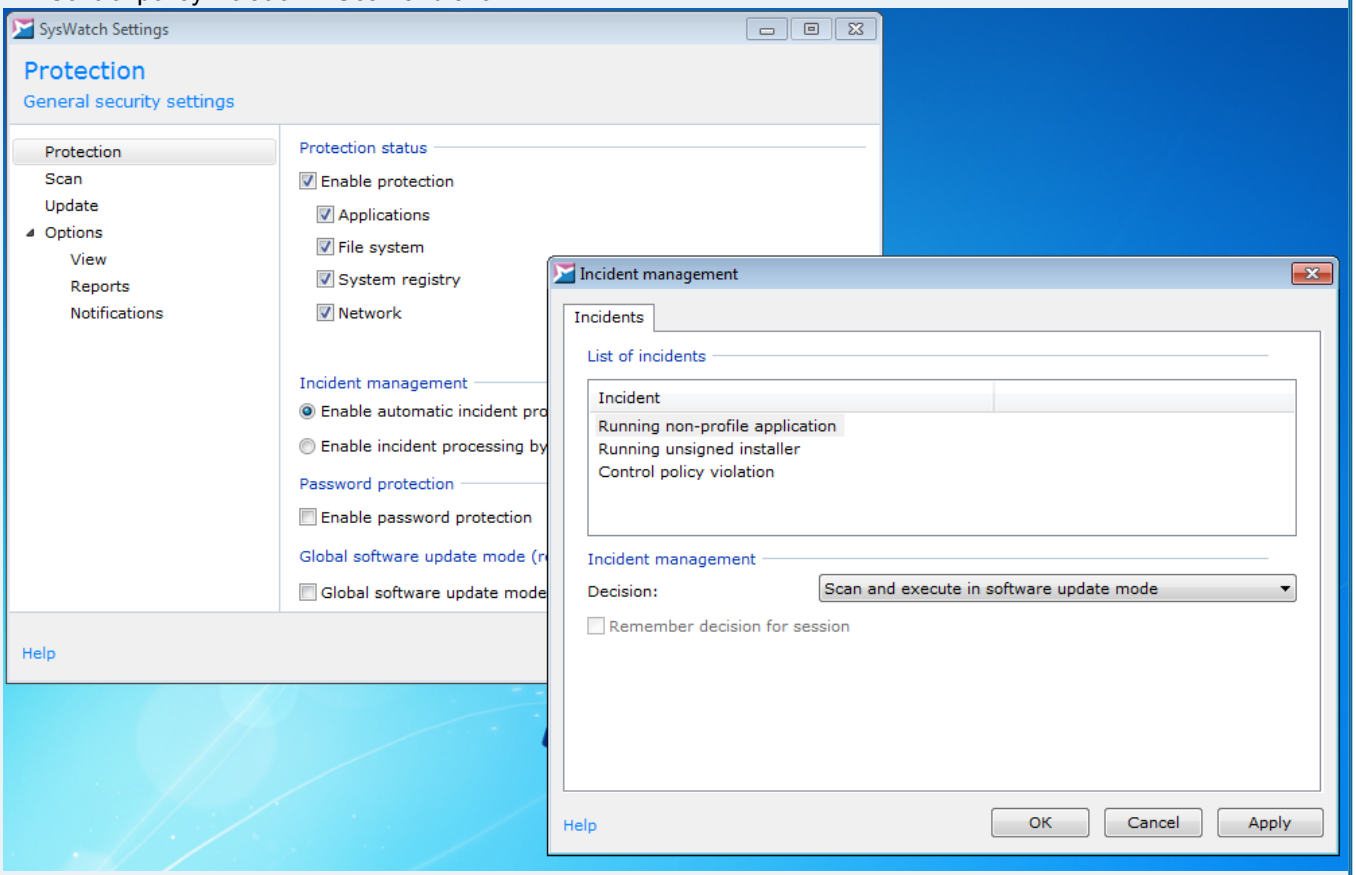
```
echo install cert
certutil -addstore Root "C:\SnS-install\VeriSign Class 3 Public Primary Certification Authority
- G5.cer"
echo install syswatch
call %WINDIR%\system32\msiexec.exe /i "C:\SnS-install\SysWatch.msi" configfilename="C:\SnS-in-
stall\config.xmlc" tsconfig="C:\SnS-install\ClientSettings.xmlc" /quiet /norestart /log "C:\SnS-
install\install-log.txt"
echo exit
exit
```

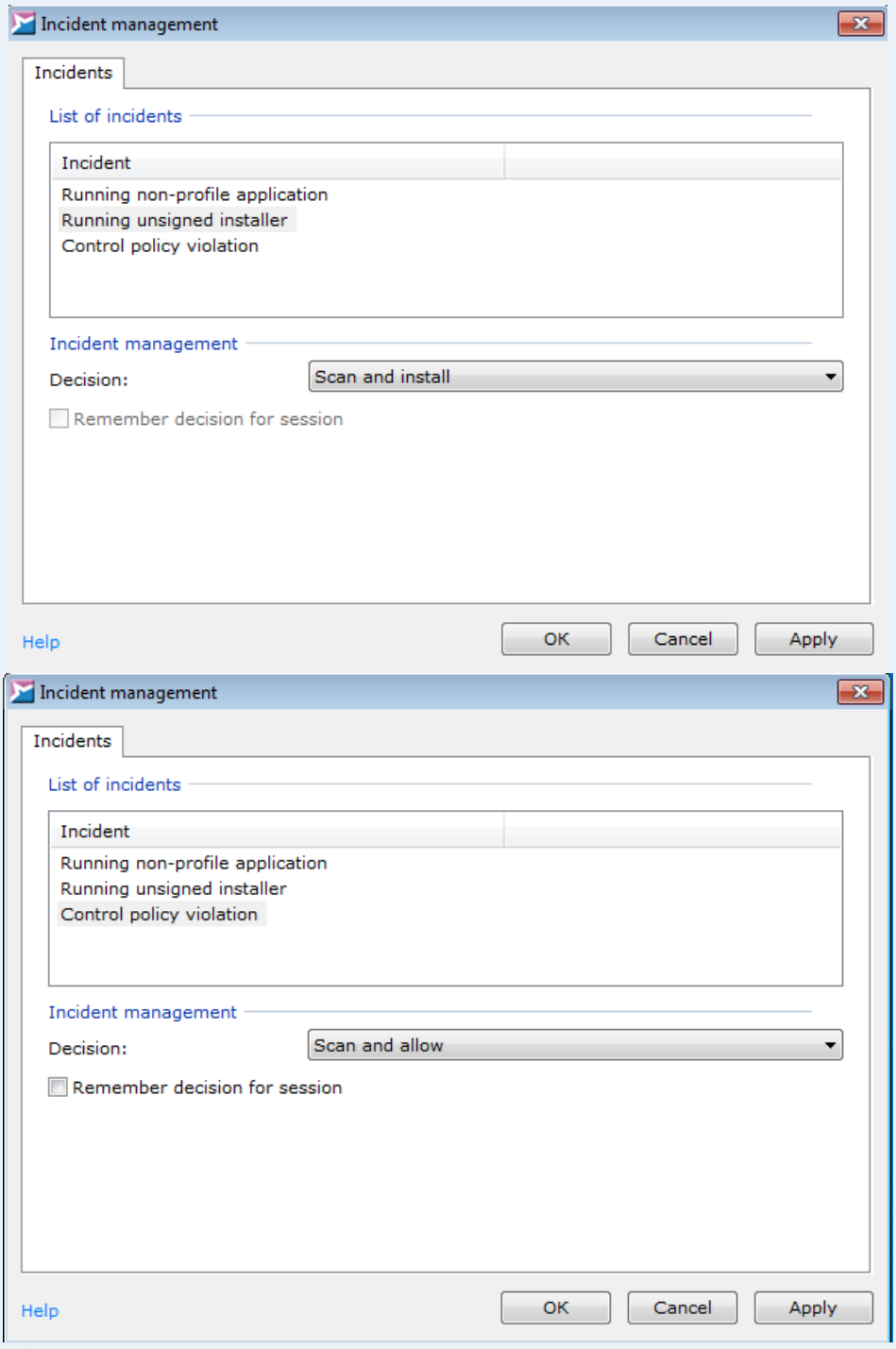
This script can be transformed into an SFX archive and signed with Client's certificate.

[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**, set the following settings:

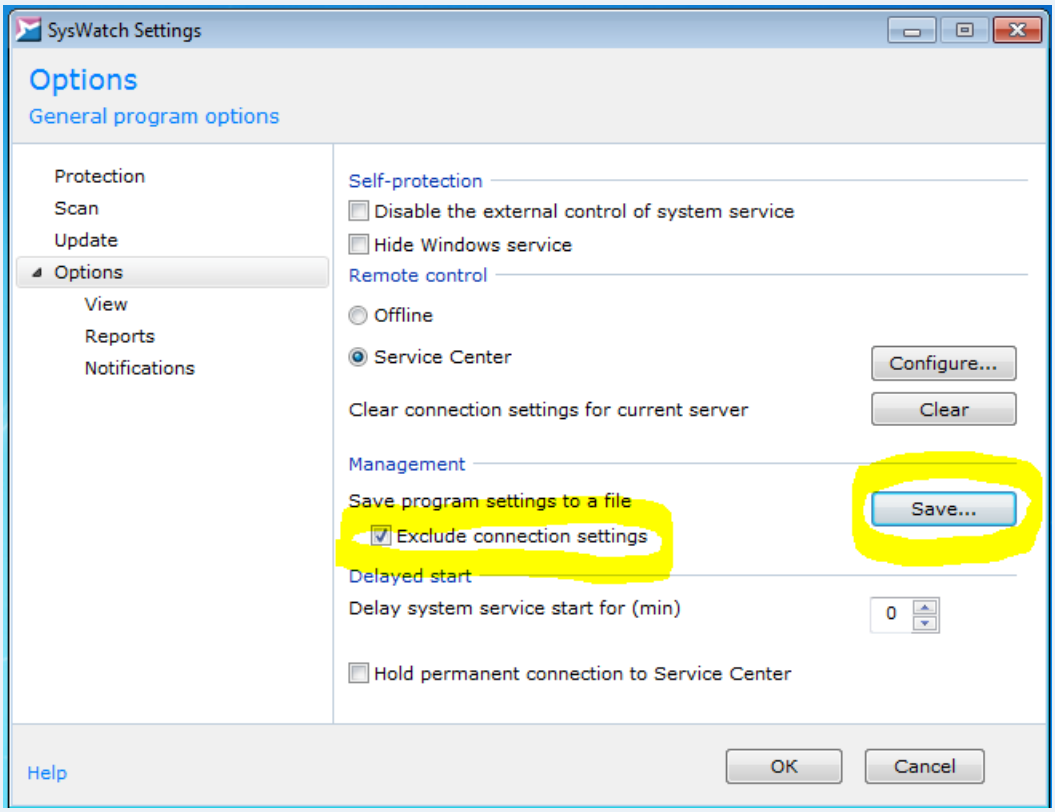
- Running non-profile application – Scan and execute in software update mode;
- Running unsigned installer – Scan and install;
- Control policy violation – Scan and allow.





Click **OK** after you finish.

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*.



[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 9. Remote deployment of SoftControl SysWatch

No.	Action	Expected outcome	Comment
9.1	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 6.7 (11) and 7.7 (14)
9.2	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 Client's remote fie exchange environment. Note how long this operation takes in order to set the standard time for the deployment operation

9.3	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 Client's personnel with remote administration tools deployed on standard Client's 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"`			
9.4	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**.	

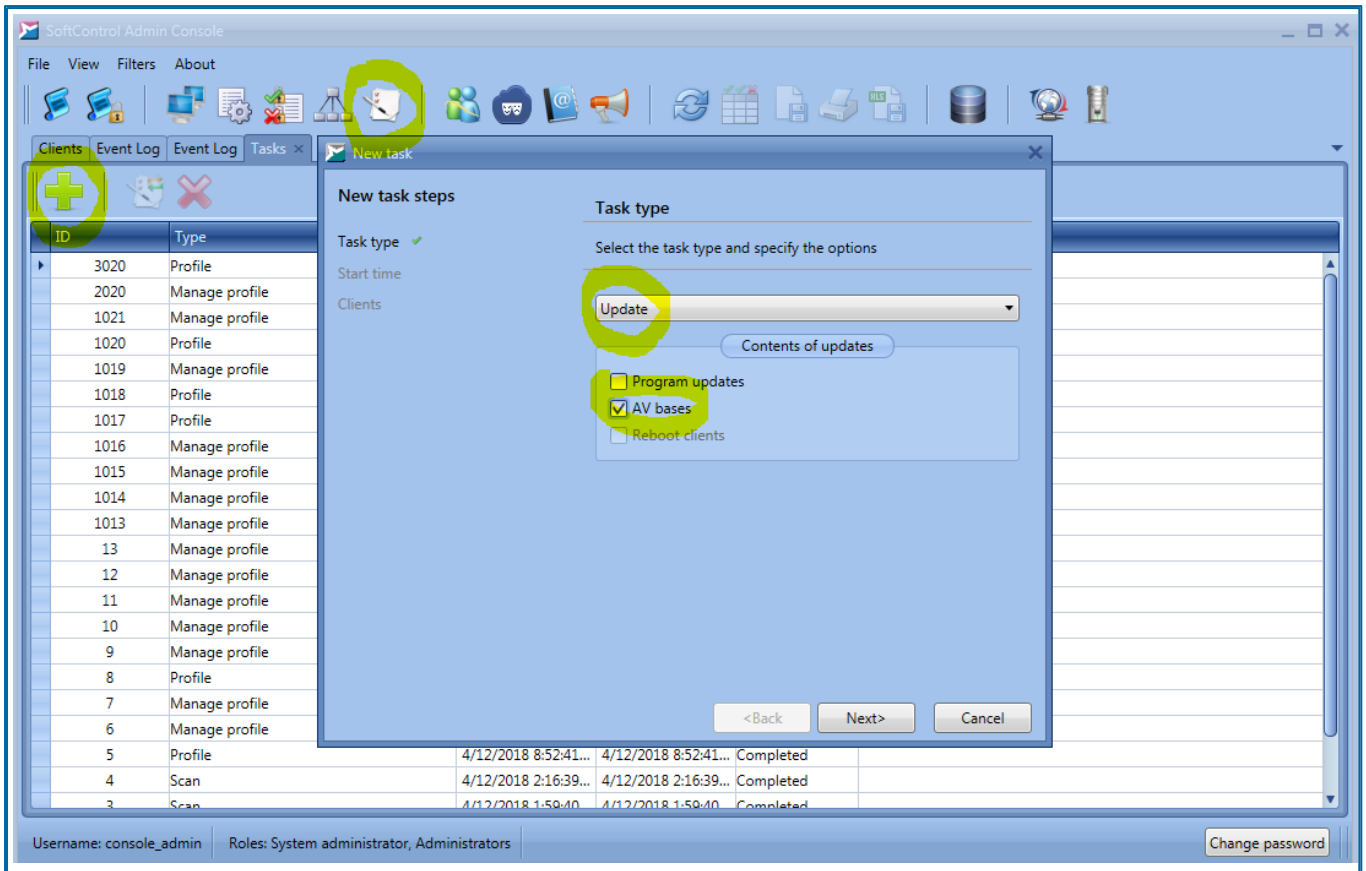
2.3.3 How to create and apply group control policy configurations from the server SoftControl Service Center

Table 10. Creation and application of configurations from SoftControl Server

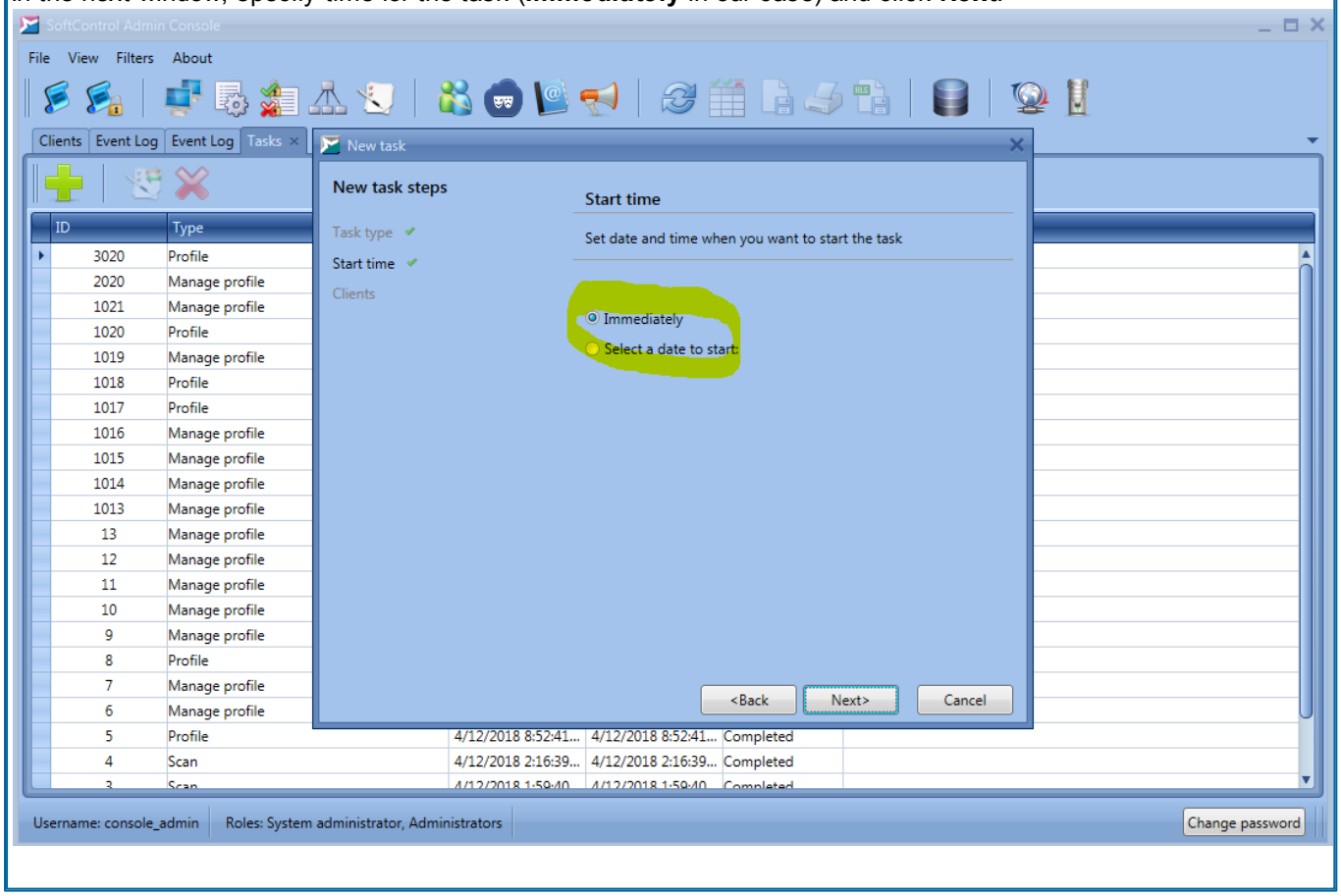
No.	Action	Expected outcome	Comment
10.1	Create and apply group control policy configurations from SoftControl Server.		There shall be several control policy configurations for different use cases: • "Production" – the strictest control policy configuration. It protects software from all change attempts. 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.
10.2	Create group control policy configurations.		

10.3	Create "Production" control policy configuration.	❑ "Production" and "Production-Audit" configurations have been created.	Control policy configurations are created by Client's personnel and are subject to adjustment in accordance with Client's information security policy. Standard control policy configurations are described in *Control Policies Политики_контроля_ProductionAudit.xlsx(in Russian)*. You will need a USB drive to perform tests when you create control policies for the USB whitelist.
10.4	Create organizational units.		An organizational unit is a group of devices with common group control policies.
10.5	Create "Production" organizational unit and assign "Production-Audit" configuration to it.	❑ "Production" organizational unit has been created and assigned "Production-Audit" configuration.	
10.6	Move clients to organizational units with group policy configurations.		
10.7	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 also view additional information.	
10.8	Start the task to update antivirus databases 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 as **Update – Installed** (**Info** column).	Updating of Avira antivirus databases requires installation of "Microsoft Visual C++ 2008 Redistributable Package" (*vcredist_x86_2008.exe*).

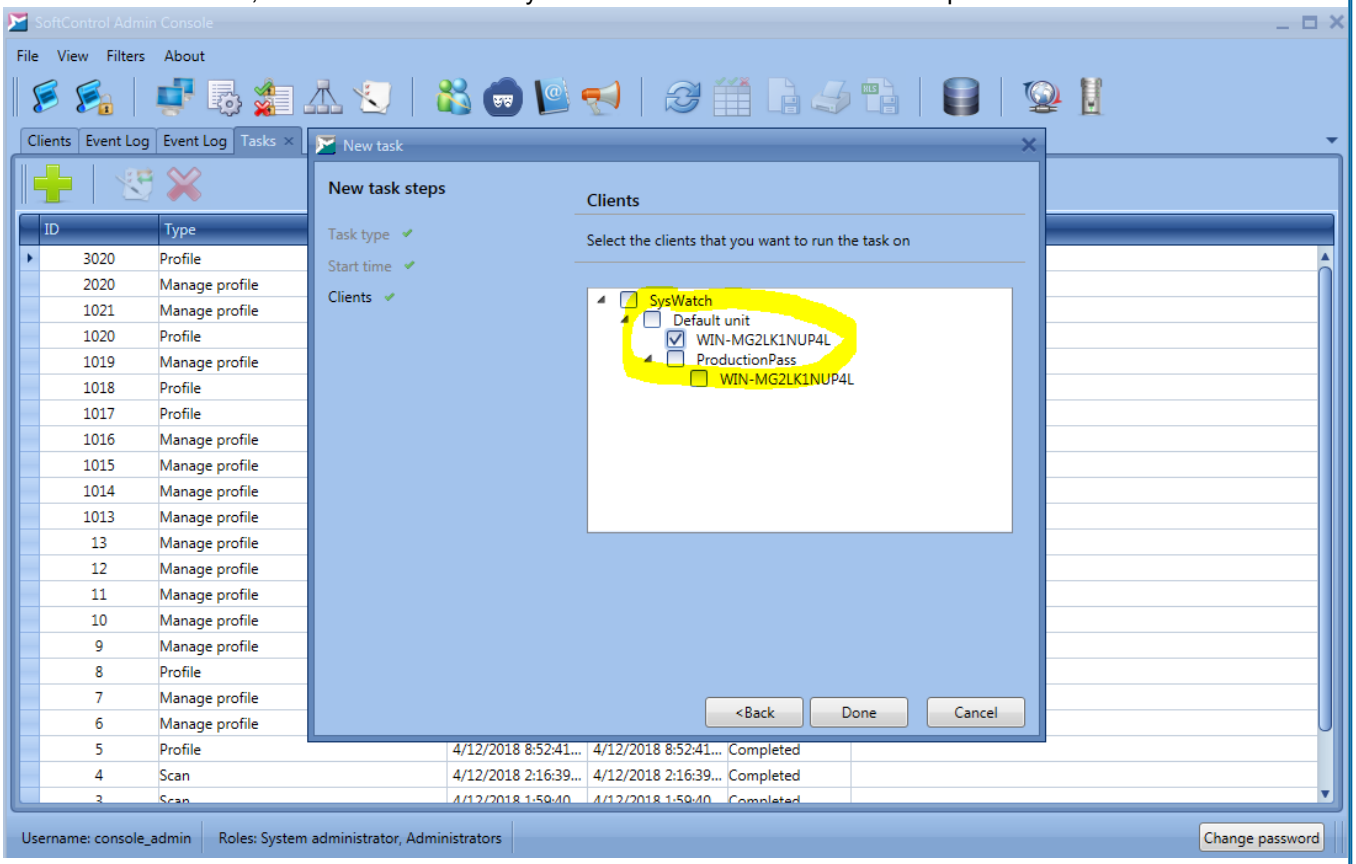
* In order to start the task to update antivirus databases, click on  icon (**Tasks**) in SoftControl Admin Console to open the **Tasks** tab. Click on  (**New**).
New task window will open. Select **Task type – Update**, check **AV bases**, and click **Next:**



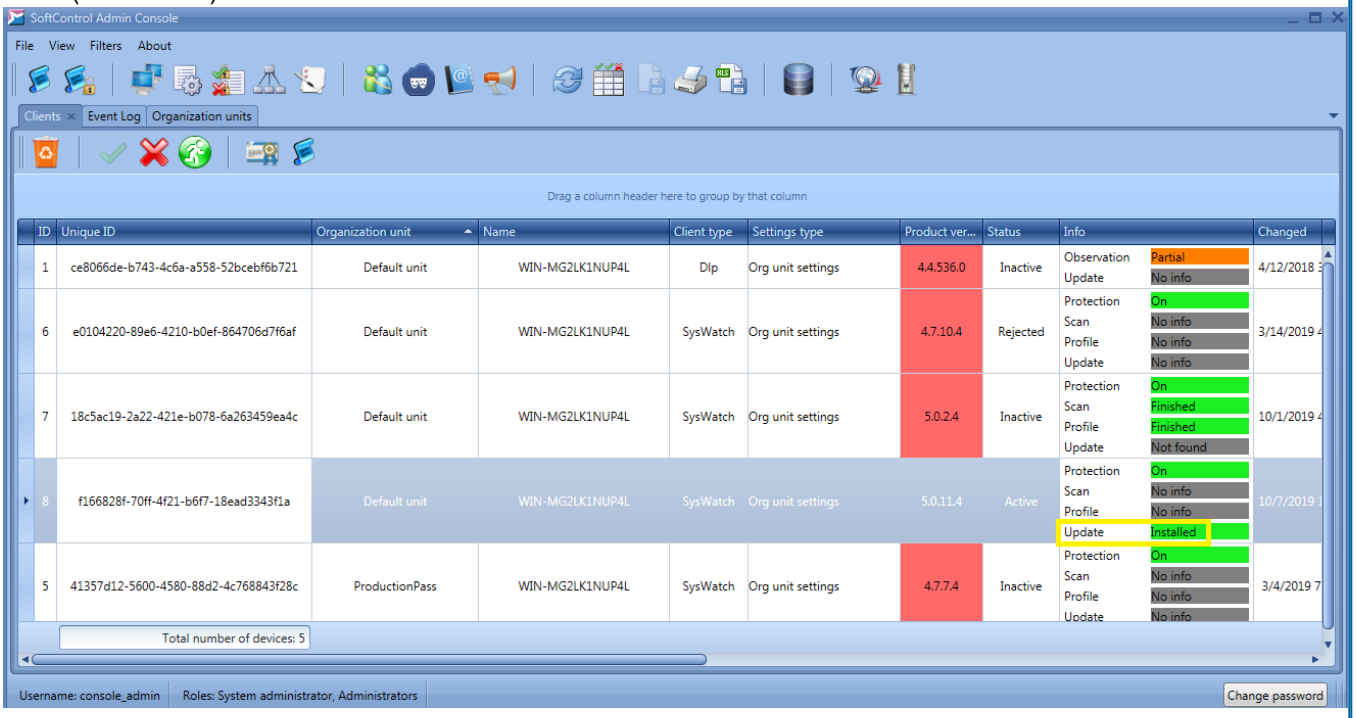
In the next window, specify time for the task (**Immediately** in our case) and click **Next**.



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

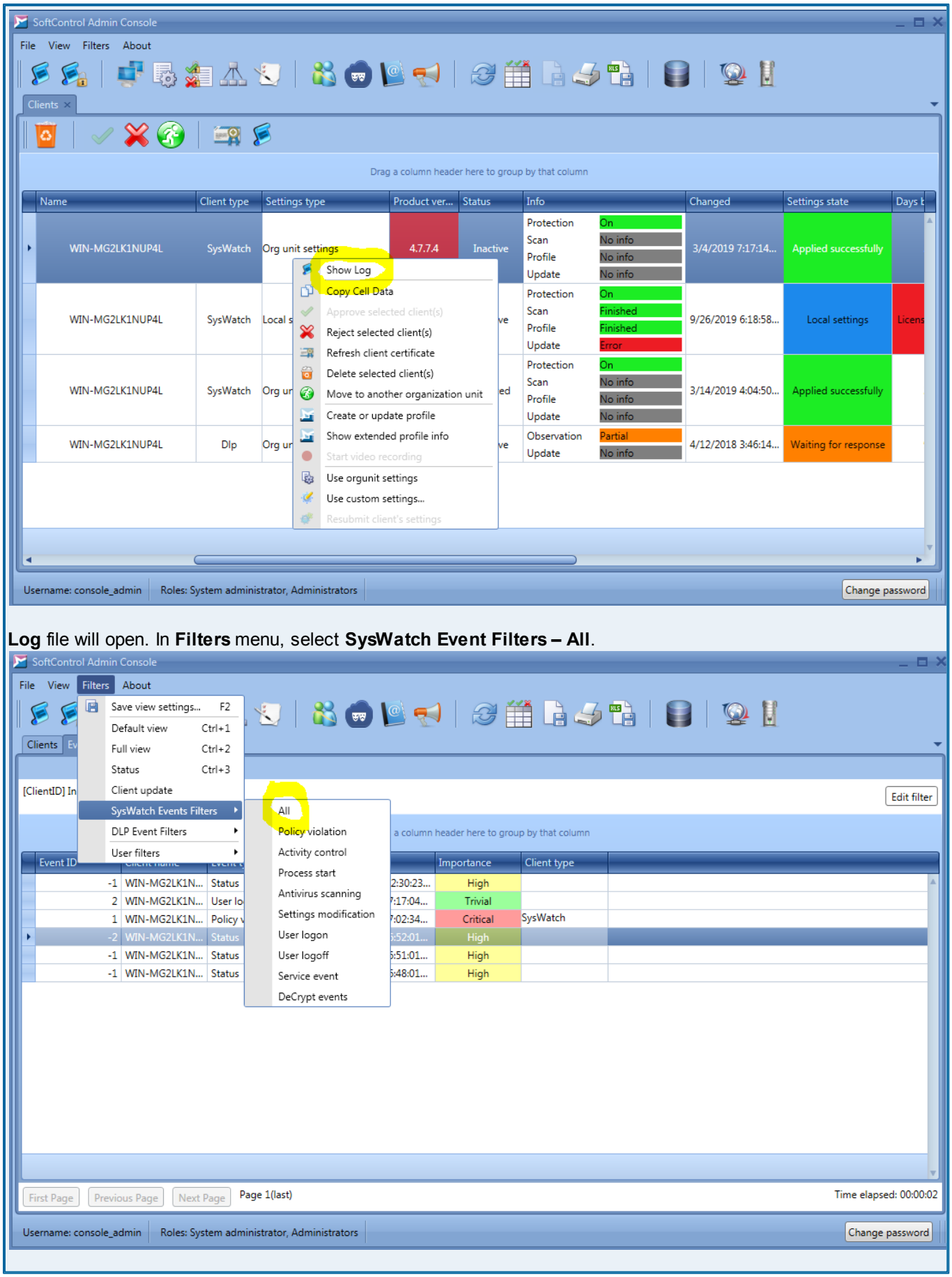


When the update is completed, you will see **Installed** status in the **Info – Update** field for SoftControl SysWatch client (**Clients** tab).



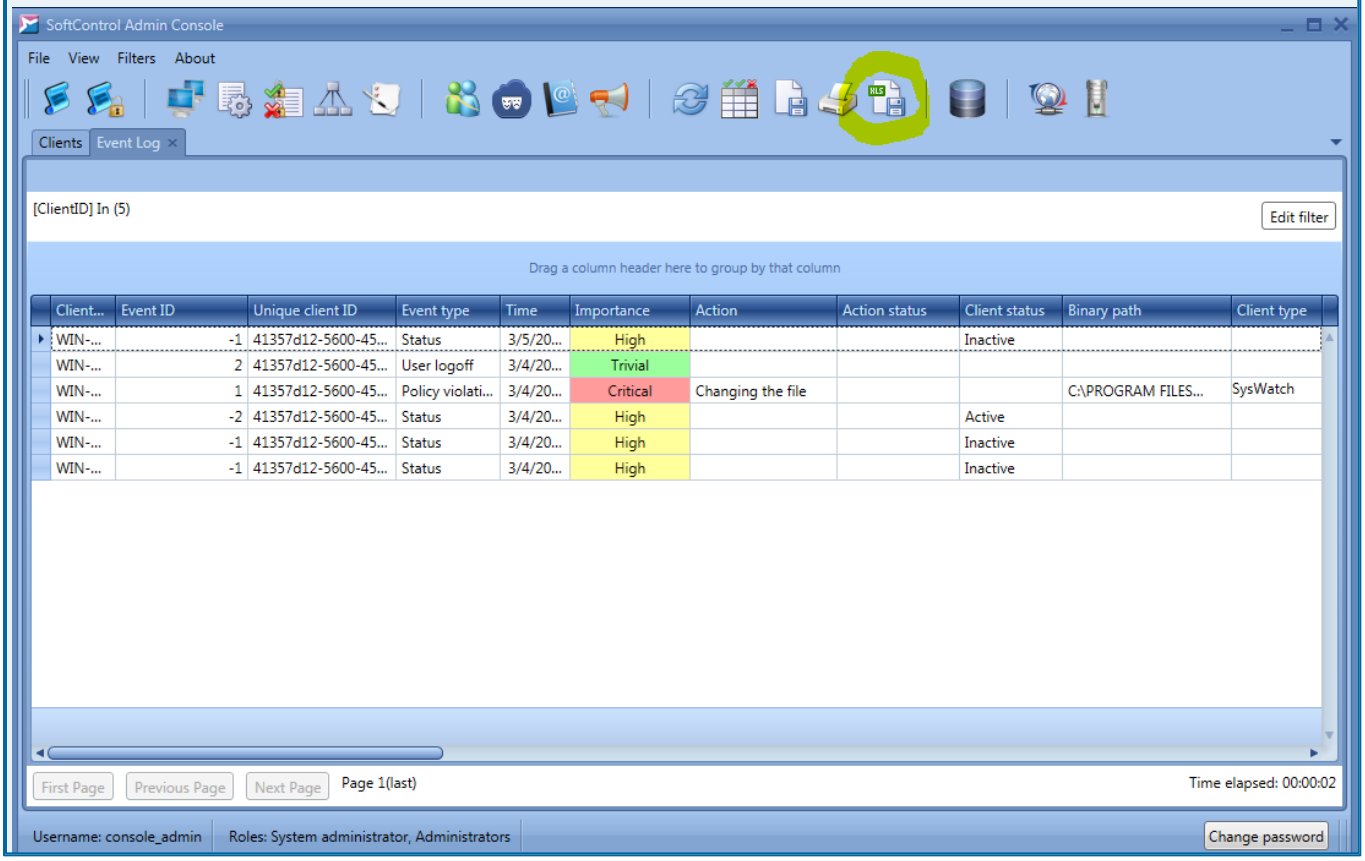
10.9	Create and run the task for antivirus scanning on device 1. (This operation can be optional if it is important to save traffic on the end-point device.)	❑ SoftControl Admin Console displays SoftControl SysWatch client's state in the **Info** column as **Scan – Finished**.	Antivirus scanning task is created and executed in line with antivirus database updating.
10.10	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.
10.11	Get logs of operation of device 1 on the server.		It is strongly advised to reload device 1 during the logging period. The logging period shall amount to one workday.
10.12	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 and select **Show log**.



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

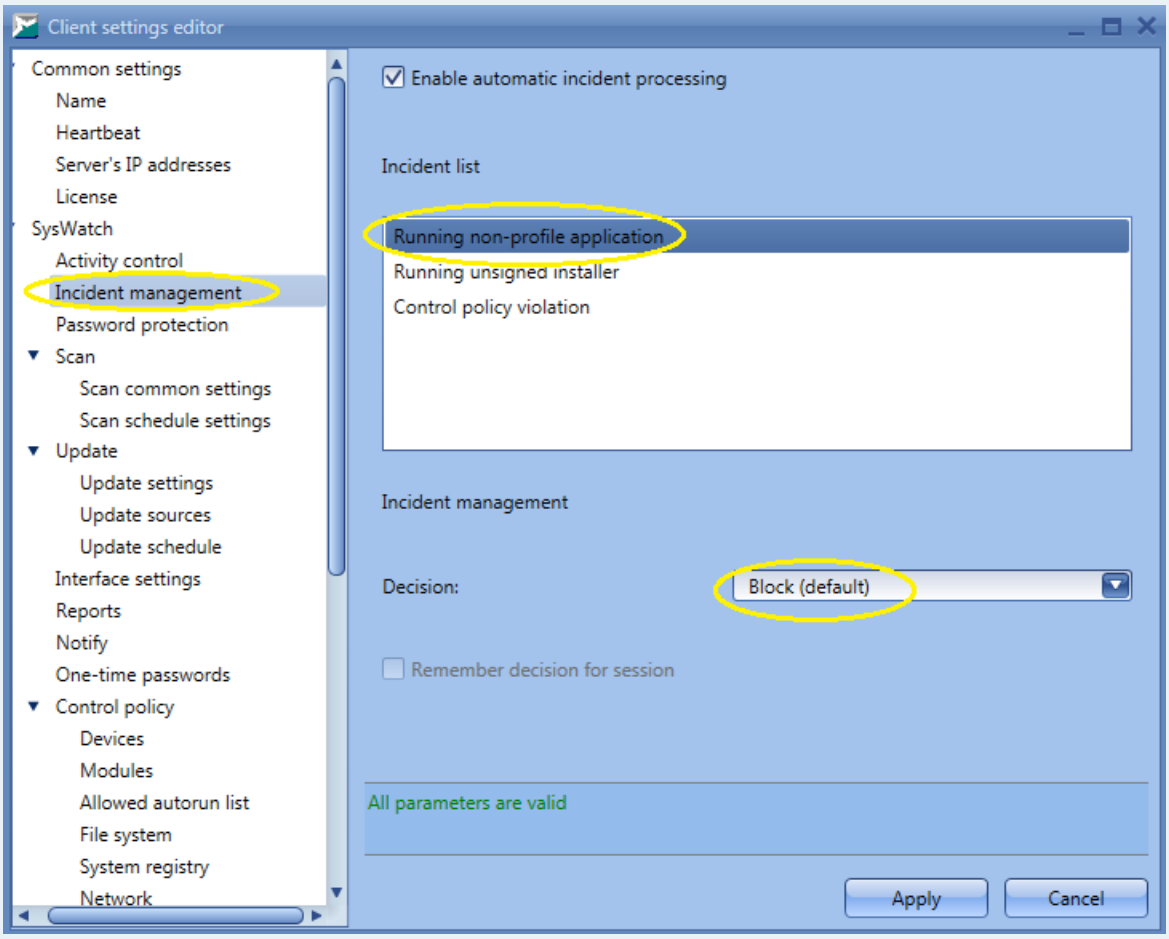
Then click on  icon (**Export to Excel**) and save the file.

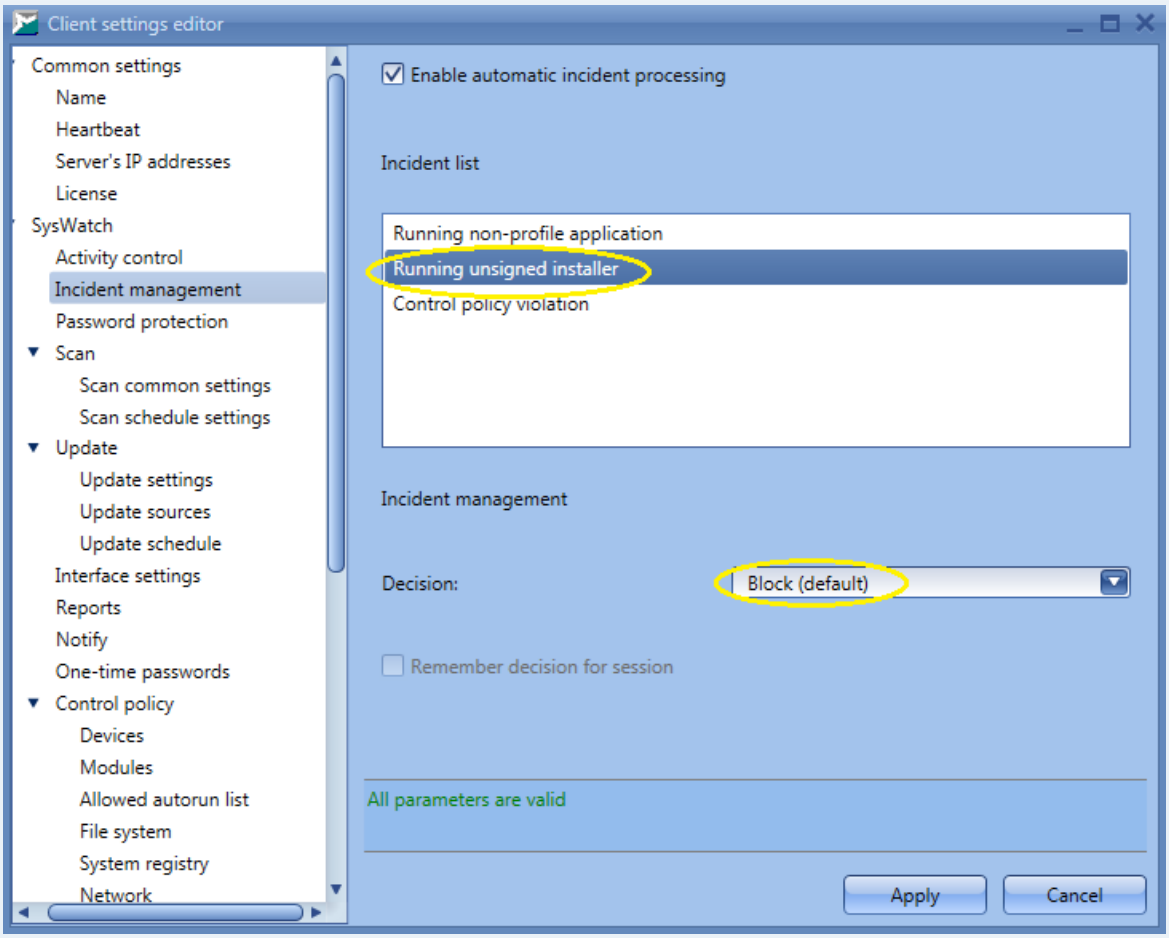


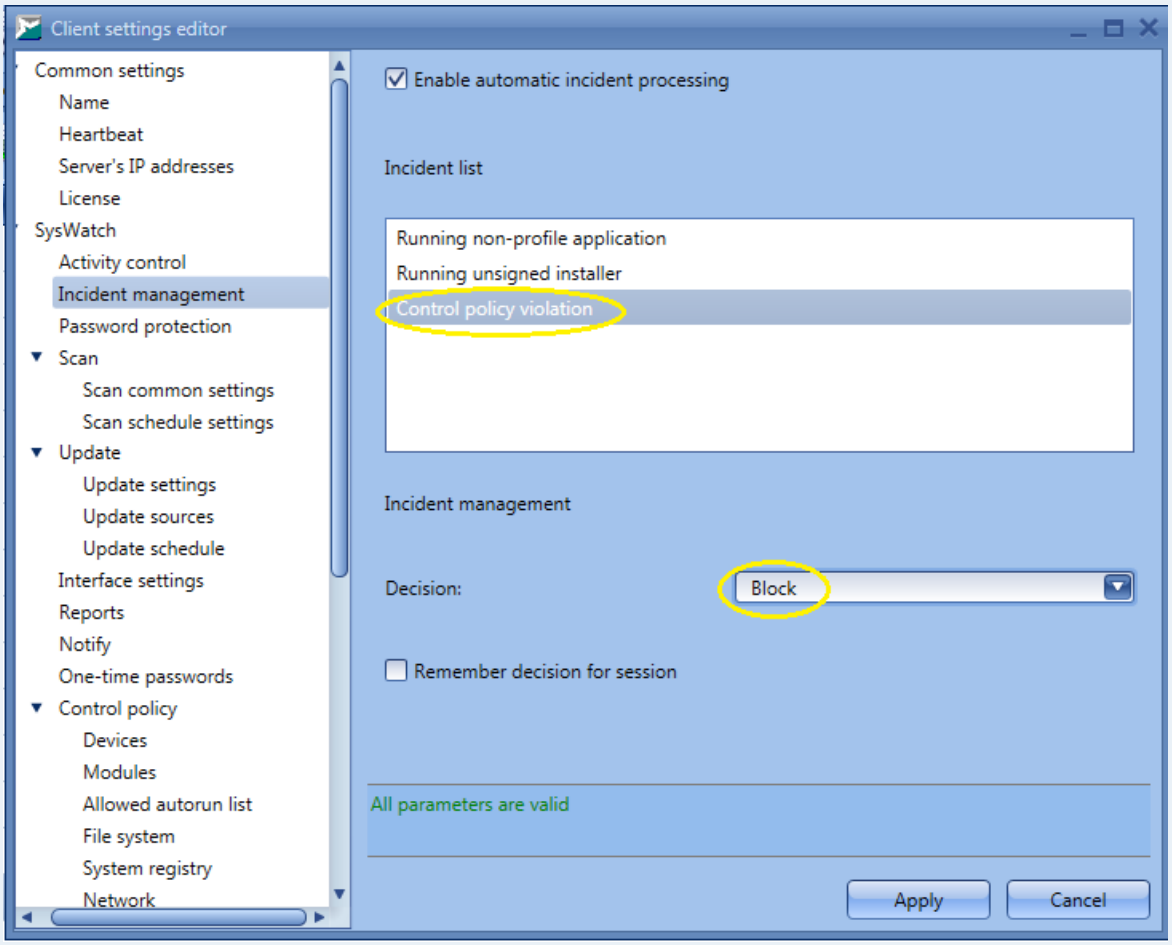
2.3.4 How to create group control policies. Examples

Table 11. Examples of creating group control policies

No.	Action	Expected outcome	Comment
11.1	Switch the client device from auditing to the operational 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 <%SC%_SERVER>:			


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
Enable automatic incident processing
Incident list
Running non-profile application
Running unsigned installer
Control policy violation
Incident management
Decision:
Block (default)
Remember decision for session
All parameters are valid
Apply
Cancel

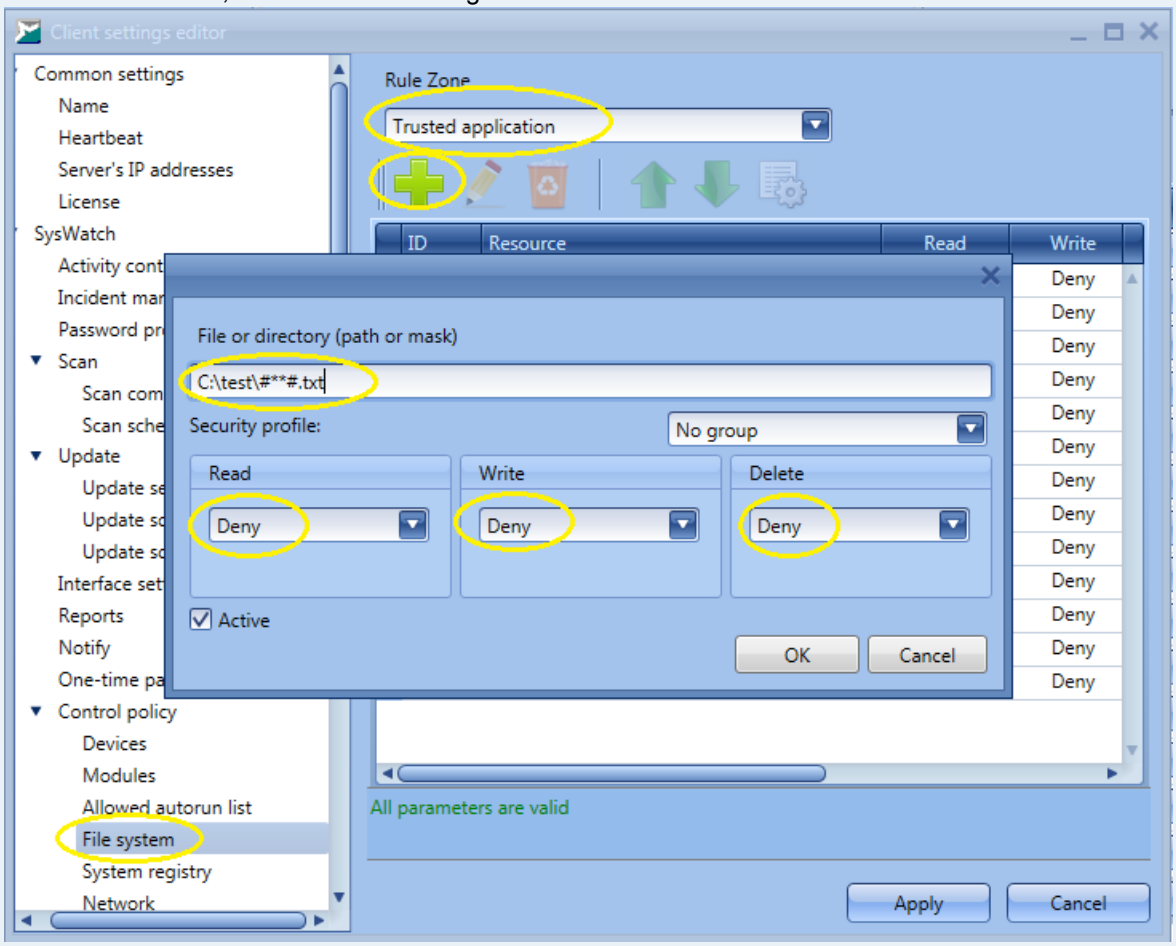

Client settings editor
Common settings
Name
Heartbeat
Server's IP addresses
License
SysWatch
Activity control
Incident management
Password protection
Scan
Scan common settings
Scan schedule settings
Update
Update settings
Update sources
Update schedule
Interface settings
Reports
Notify
One-time passwords
Control policy
Devices
Modules
Allowed autorun list
File system
System registry
Network
Enable automatic incident processing
Incident list
Running non-profile application
Running unsigned installer
Control policy violation
Incident management
Decision:
Block (default)
Remember decision for session
All parameters are valid
Apply
Cancel

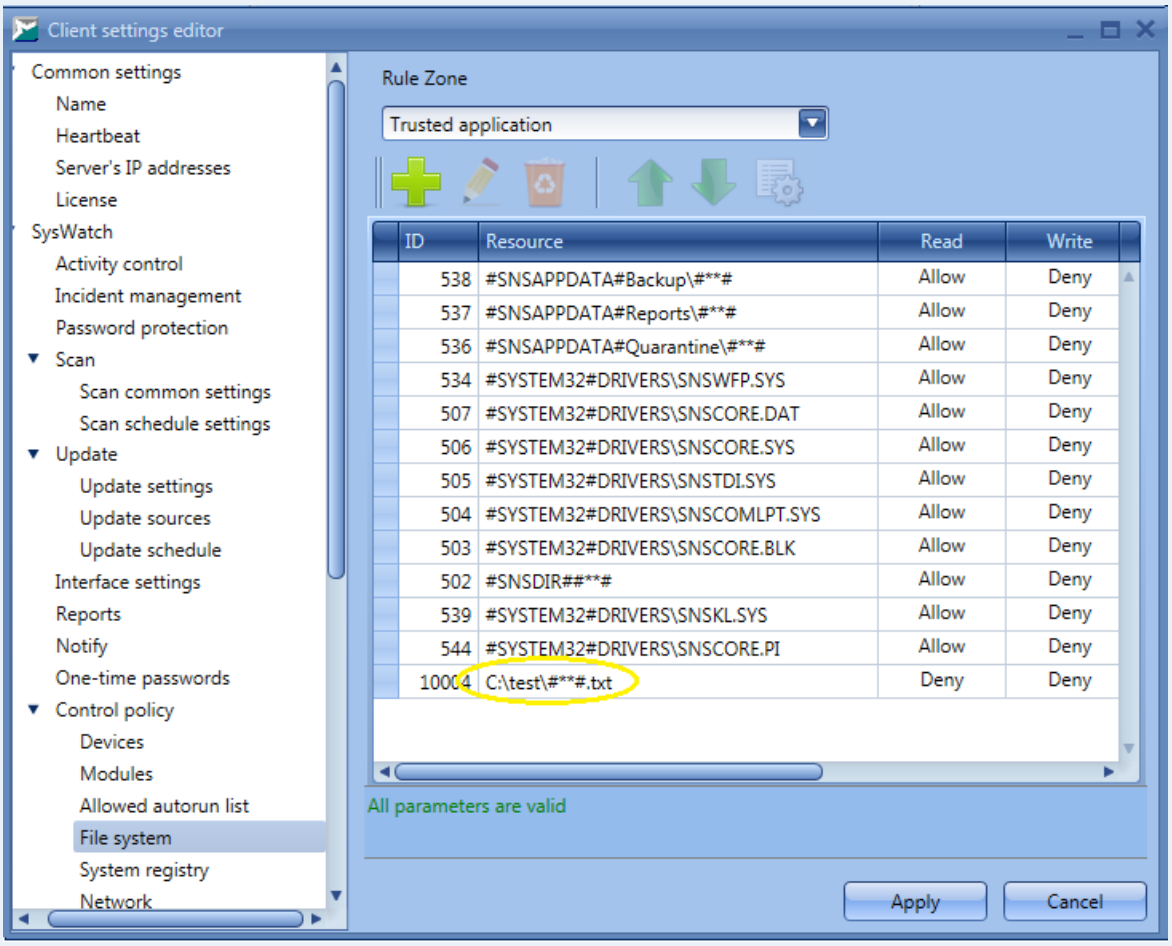


Once you finish editing the client settings, save them under a new name and apply to the organizational unit which the device belongs to.

11.2	Create rules in control policies and test their performance. Each control zone shall be covered.		
11.3	Test rules in control policies for the file system.		
11.4	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 denies reading, removing, and writing for *C:\test*.txt* file resource and applied to all trusted applications.	

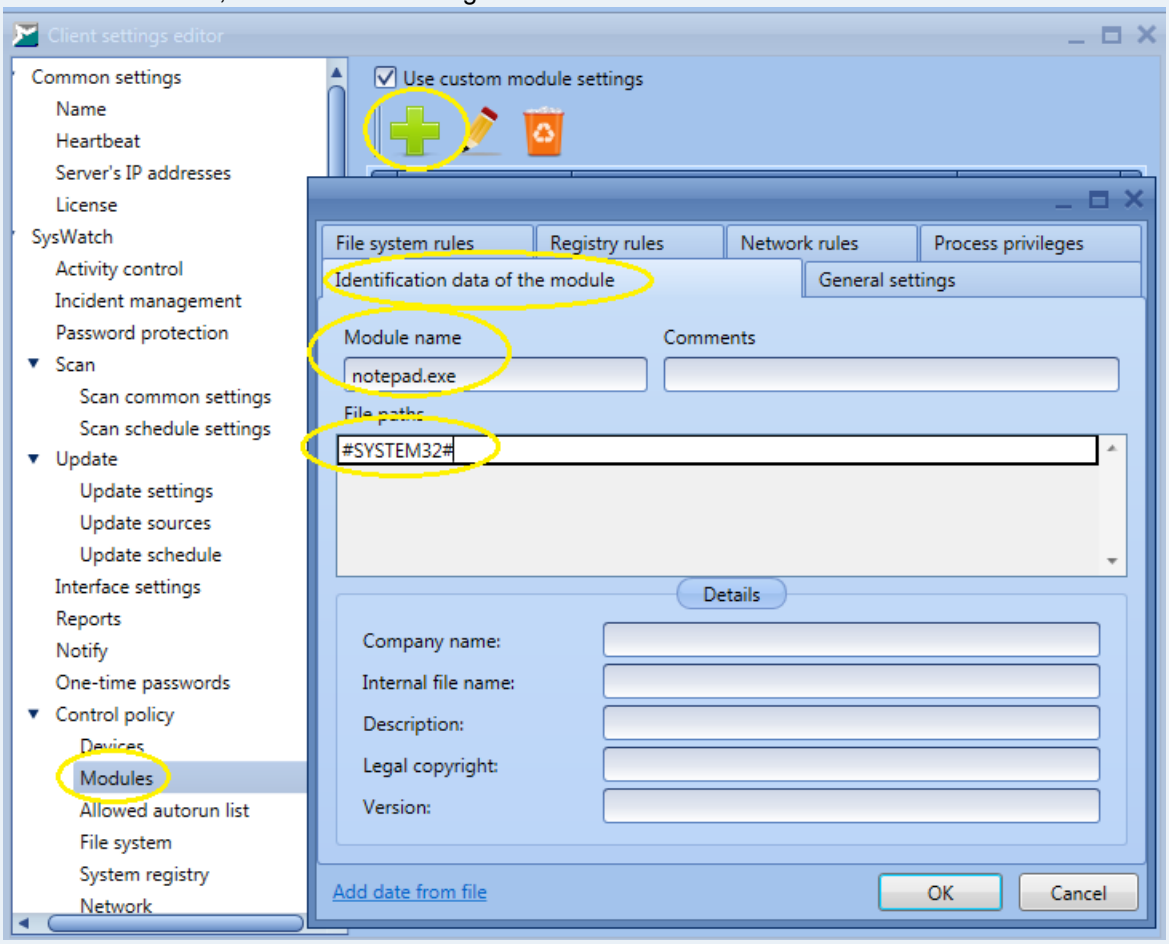
* In order to create the rule, edit the client settings:

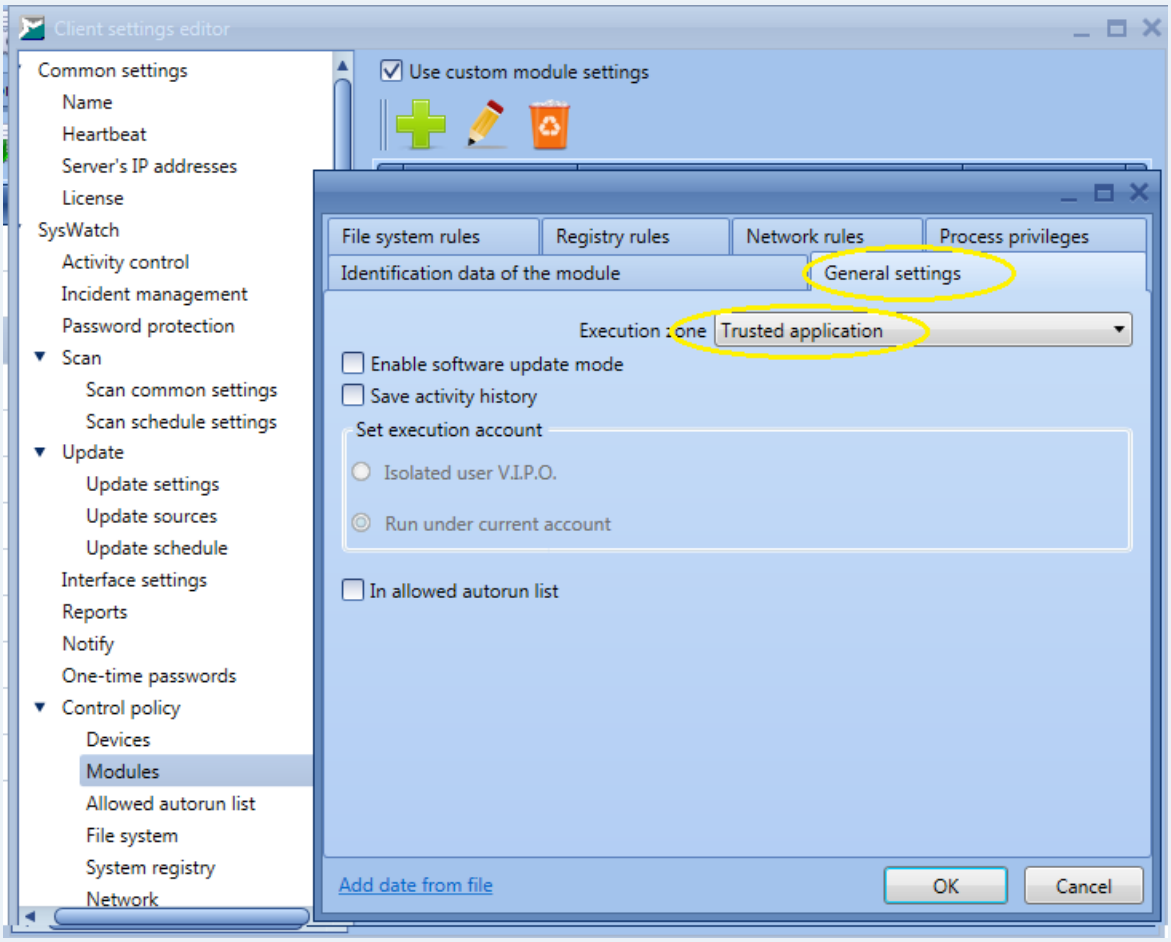


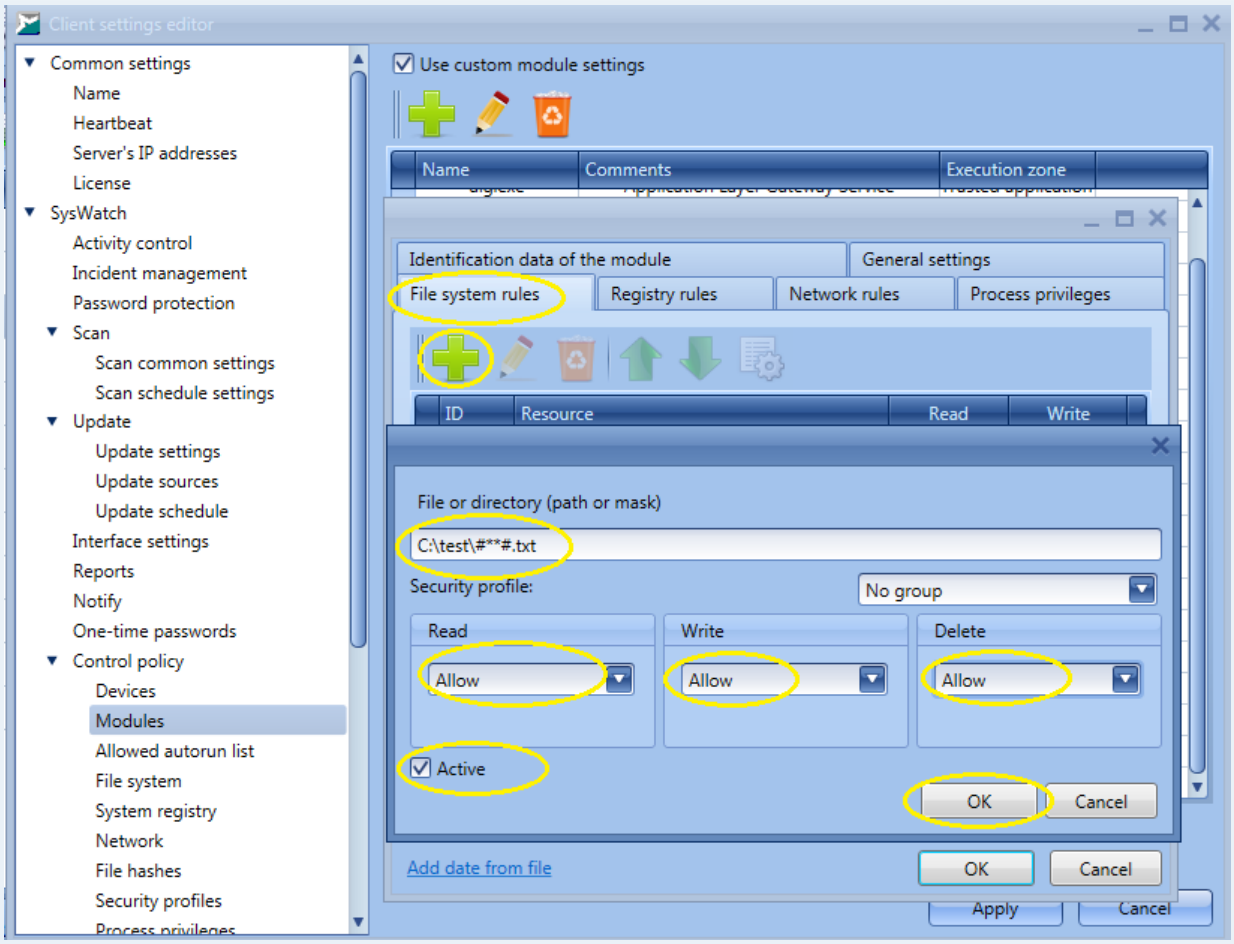


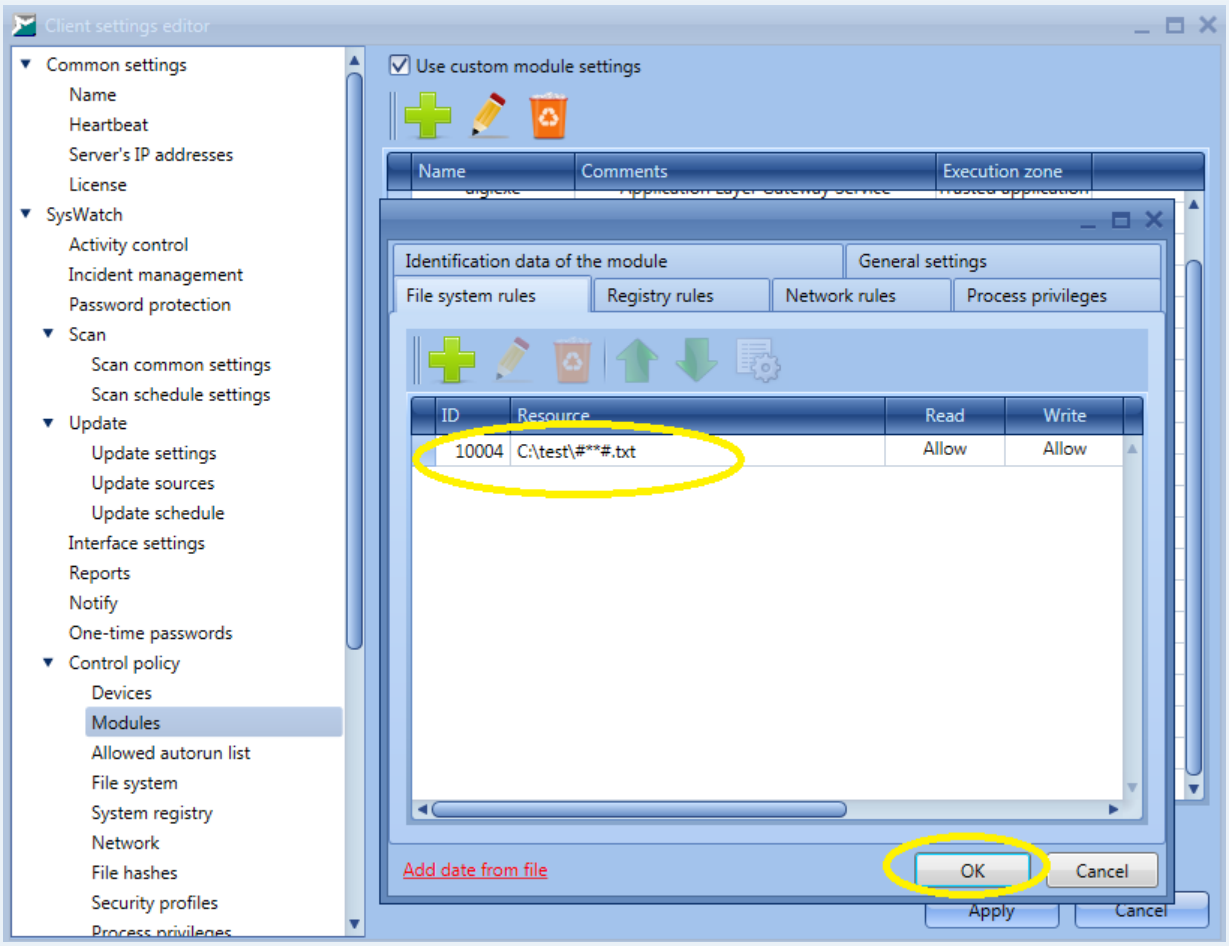
11.5	Create a rule in **Modules** section for *Notepad.exe* that allows reading, writing, and removing of text files in *C:\test\.**	❑ A rule has been created for reading, deleting, and writing of *C:\test\[any_path\name].txt* file resource for *Notepad.exe*	

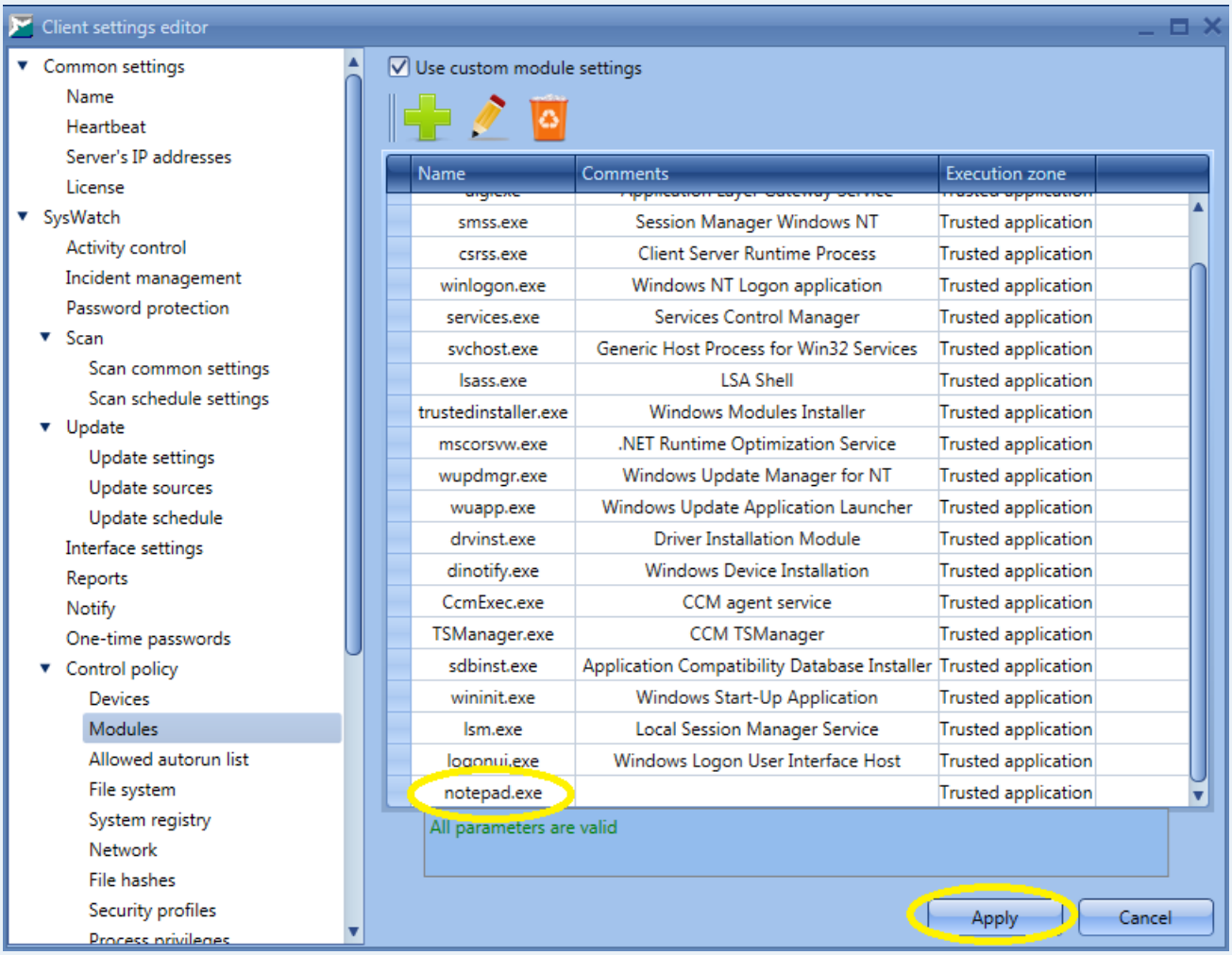
* In order to create the rule, edit the client settings:




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 : one
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
Add date from file
OK
Cancel

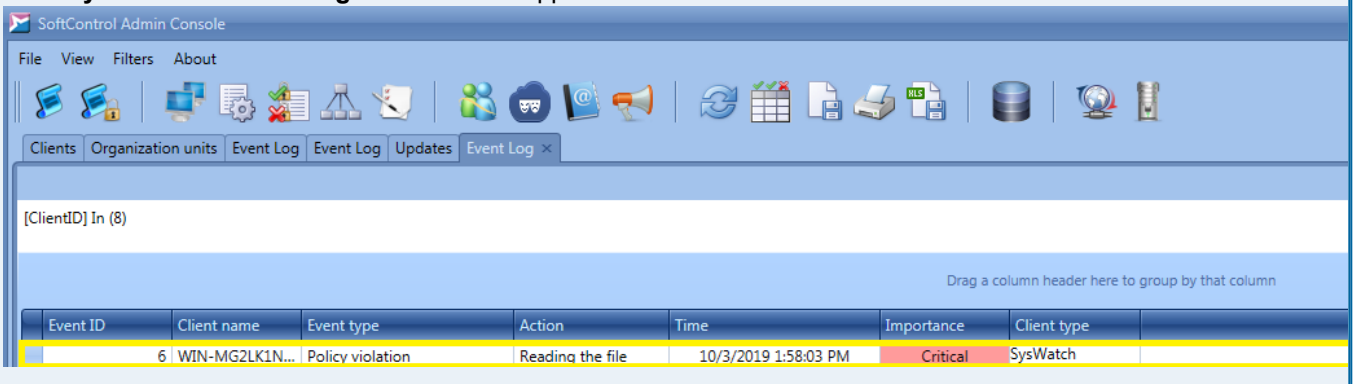

Client settings editor
Common settings
Name
Heartbeat
Server's IP addresses
License
SysWatch
Activity control
Incident management
Password protection
Scan
Scan common settings
Scan schedule settings
Update
Update settings
Update sources
Update schedule
Interface settings
Reports
Notify
One-time passwords
Control policy
Devices
Modules
Allowed autorun list
File system
System registry
Network
File hashes
Security profiles
Process privileges
Use custom module settings
Name
Comments
Execution zone
Identification data of the module
General settings
File system rules
Registry rules
Network rules
Process privileges
ID
Resource
Read
Write
File or directory (path or mask)
C:\test\#**#.txt
Security profile:
No group
Read
Write
Delete
Allow
Allow
Allow
Active
OK
Cancel
Add date from file
OK
Cancel
Apply
Cancel


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
File hashes
Security profiles
Process privileges
Use custom module settings
Name
Comments
Execution zone
Identification data of the module
General settings
File system rules
Registry rules
Network rules
Process privileges
ID
Resource
Read
Write
10004
C:\test\#**#.txt
Allow
Allow
Add date from file
OK
Cancel
Apply
Cancel



11.6	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.	

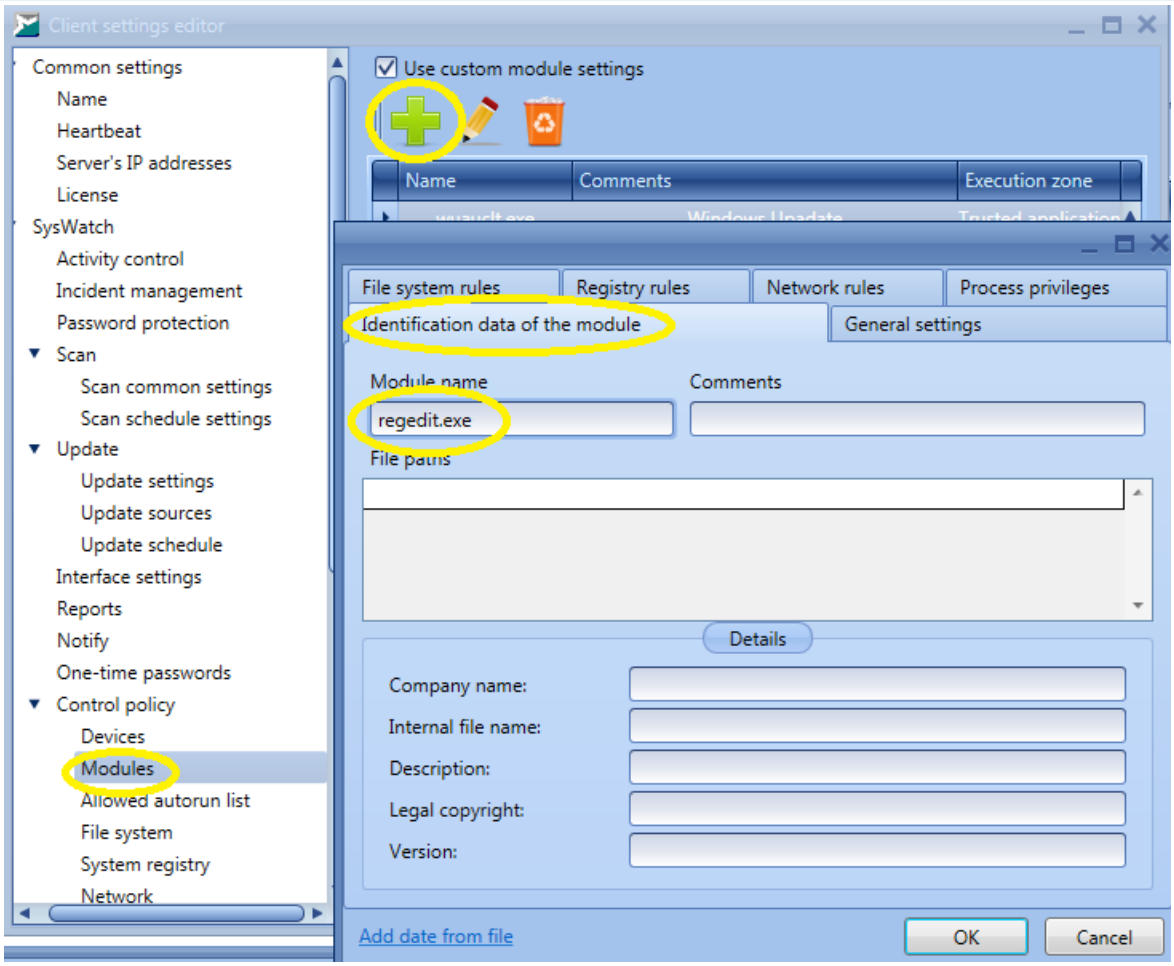
* **Policy violation – Reading the file** event appears in SoftControl Admin Console:

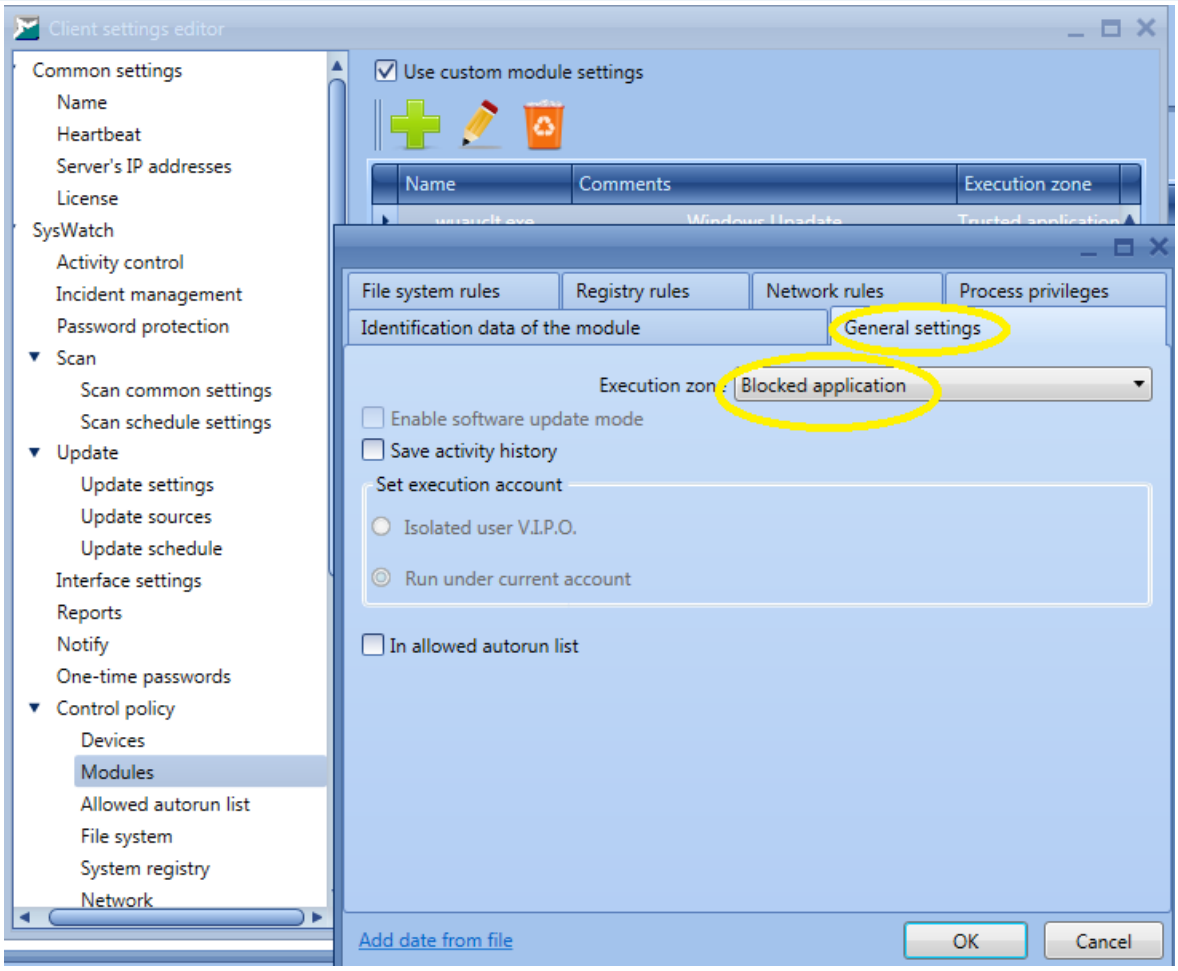


11.7	Check the rules in control policies for modules.		

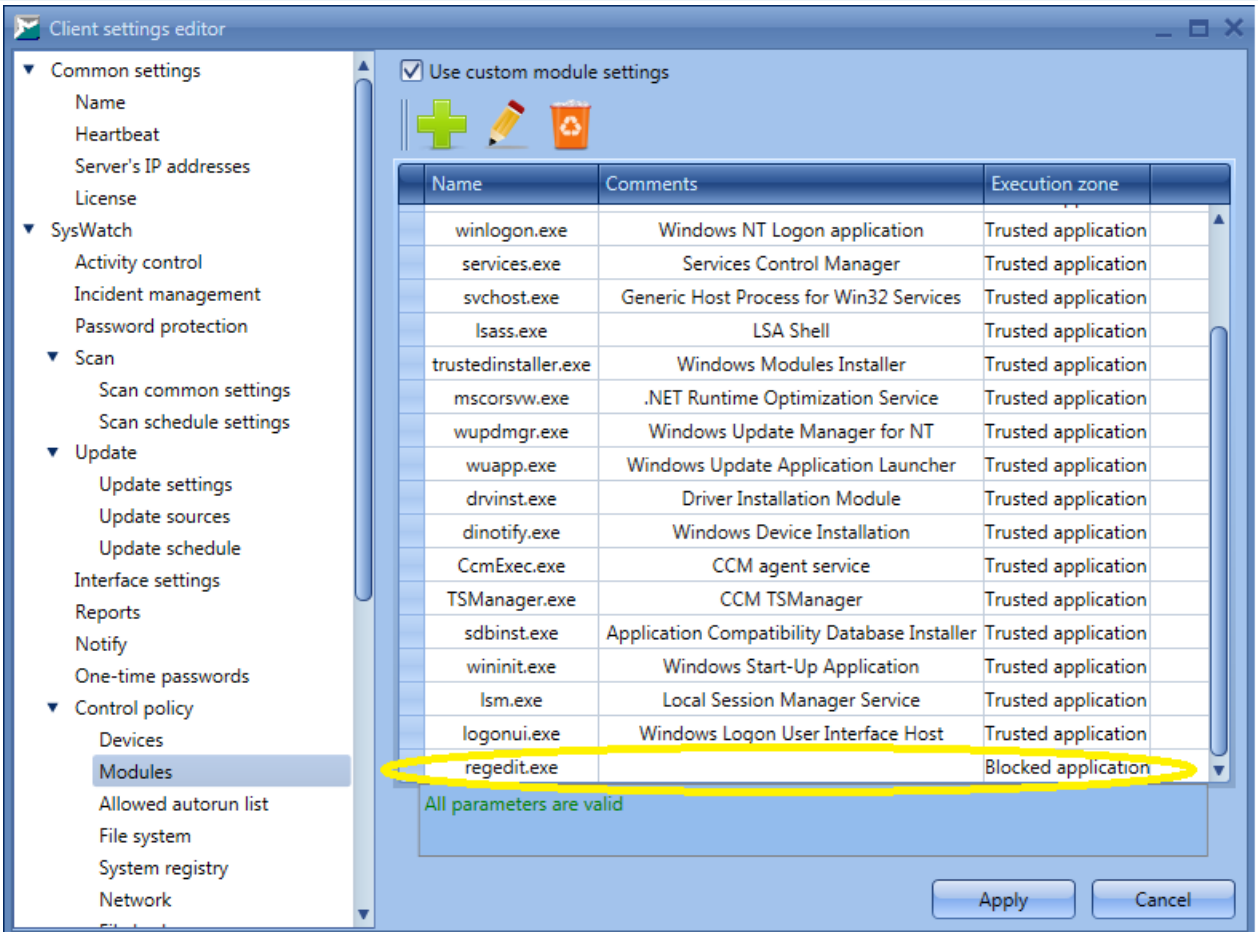
11.8	In **Modules** section, create a rule that blocks the Windows registry editor.*	❑ A setting for blocking *regedit.exe* has been created through **Control policy – Modules**	To create a rule for blocking the Windows registry editor, add *regedit.exe* to the list of private settings for modules and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

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


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
Name
Comments
Execution zone
File system rules
Registry rules
Network rules
Process privileges
Identification data of the module
General settings
Module name
regedit.exe
Comments
File paths
Details
Company name:
Internal file name:
Description:
Legal copyright:
Version:
Add date from file
OK
Cancel

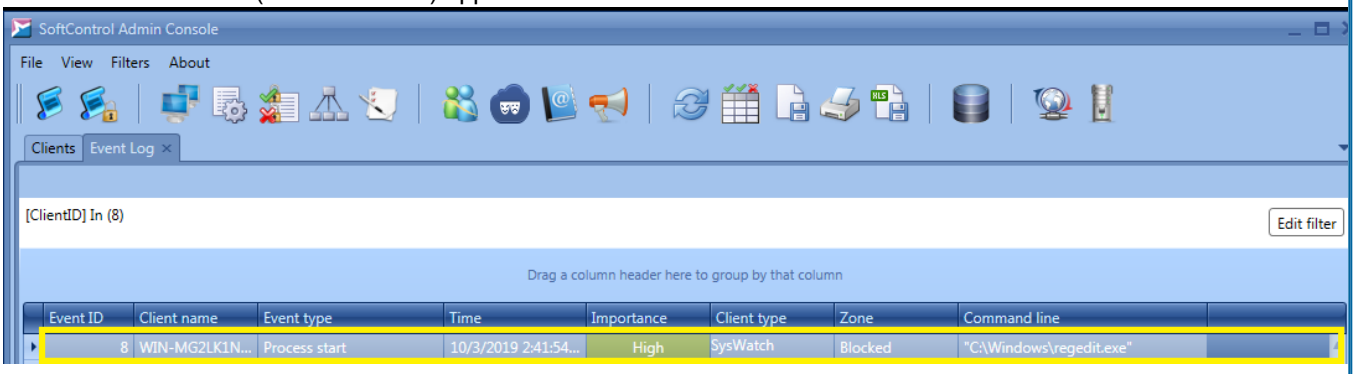


Once you save the settings, a new line will appear in **Control policy – Modules** section:



11.9	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.

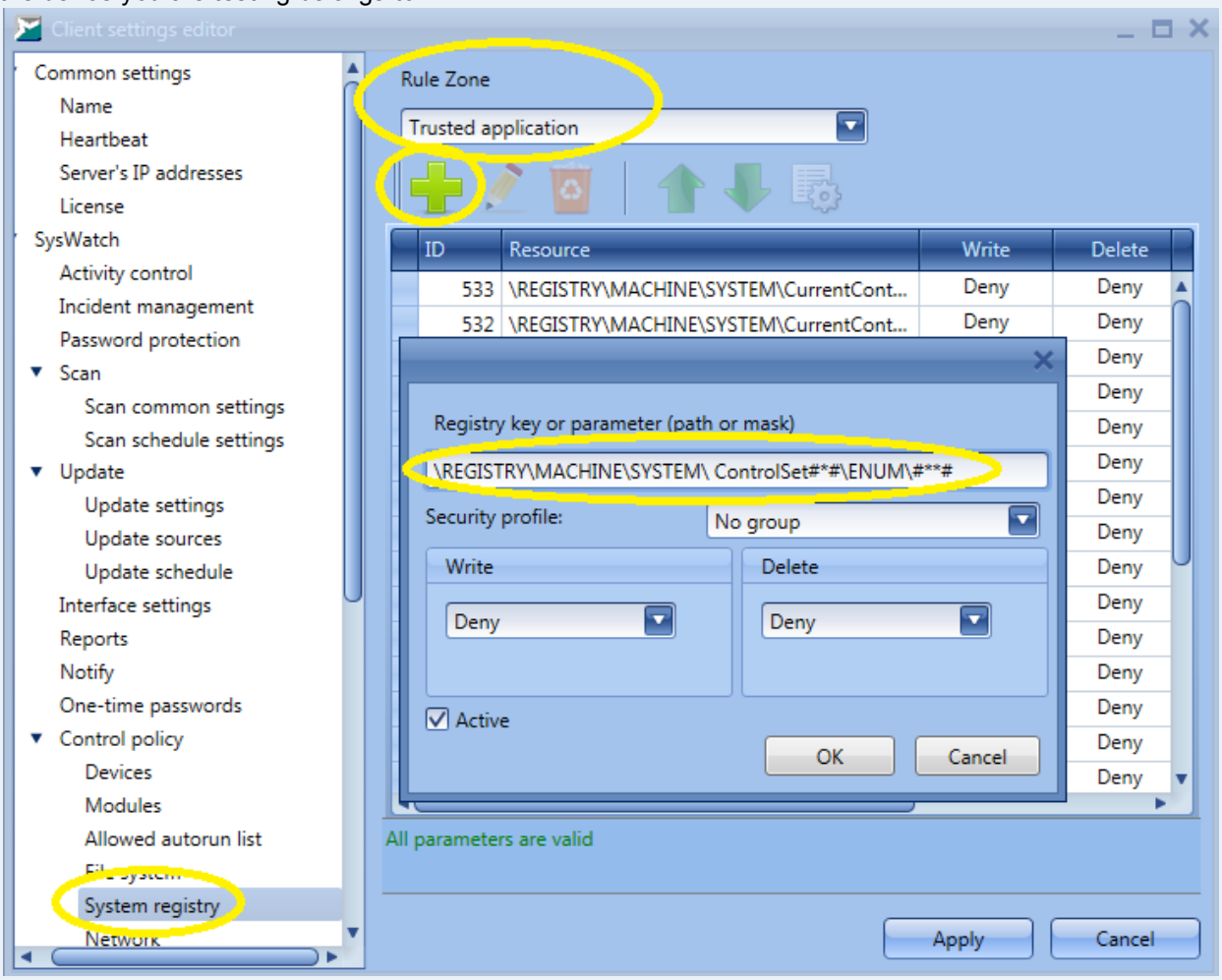
* **Process start** event (**Blocked** zone) appears in SoftControl Admin Console:

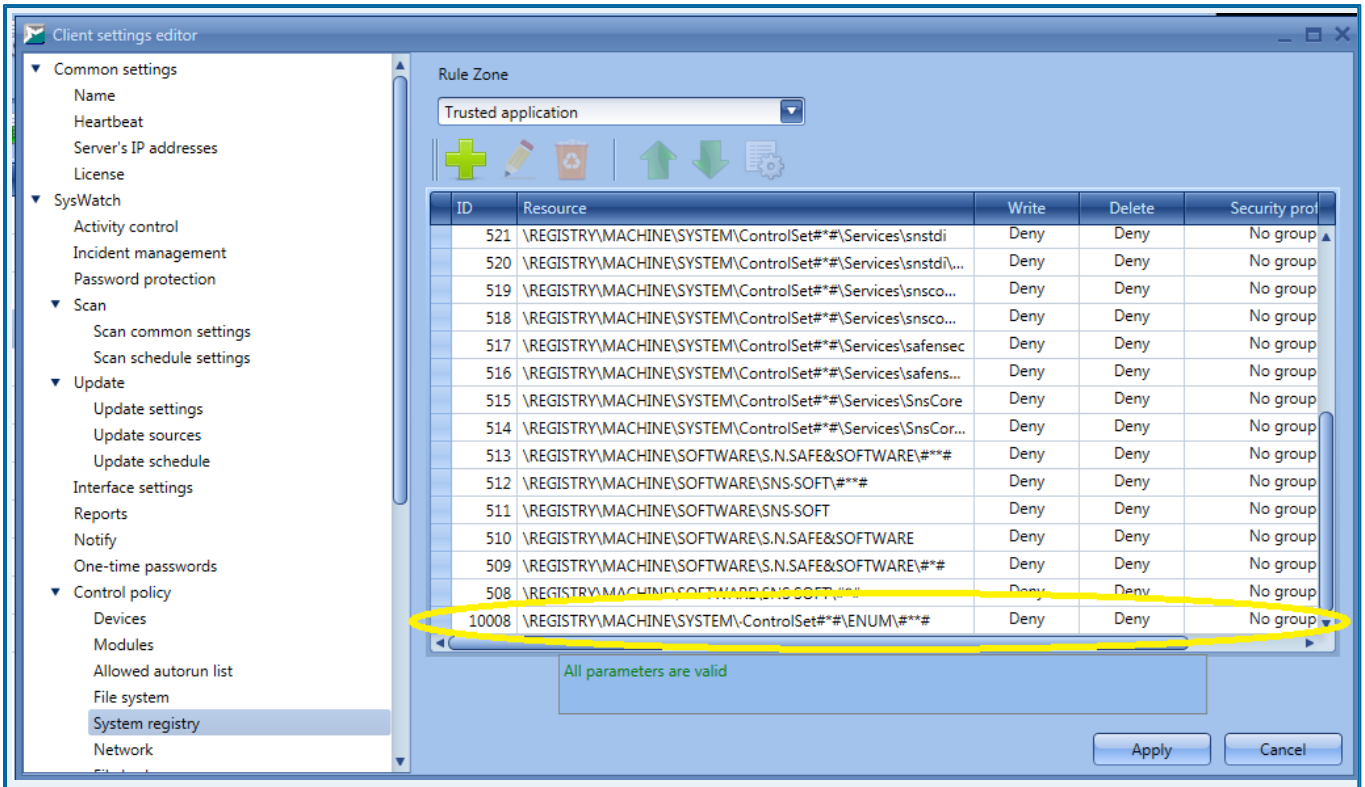


11.10	Test rules on control policies for the system registry.		

11.11	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.

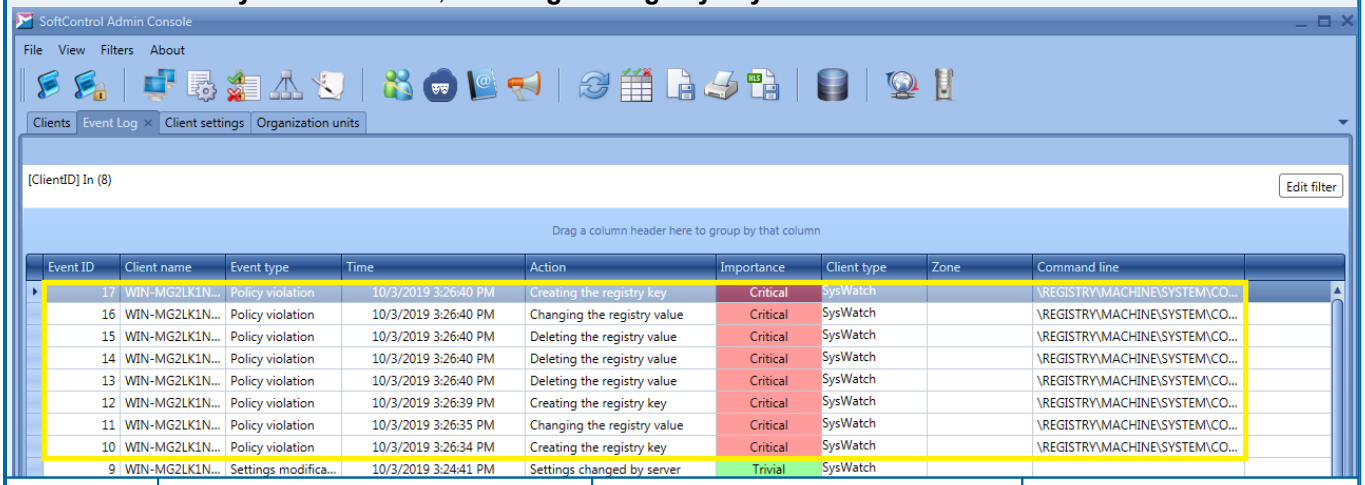
* In order to create a rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to.





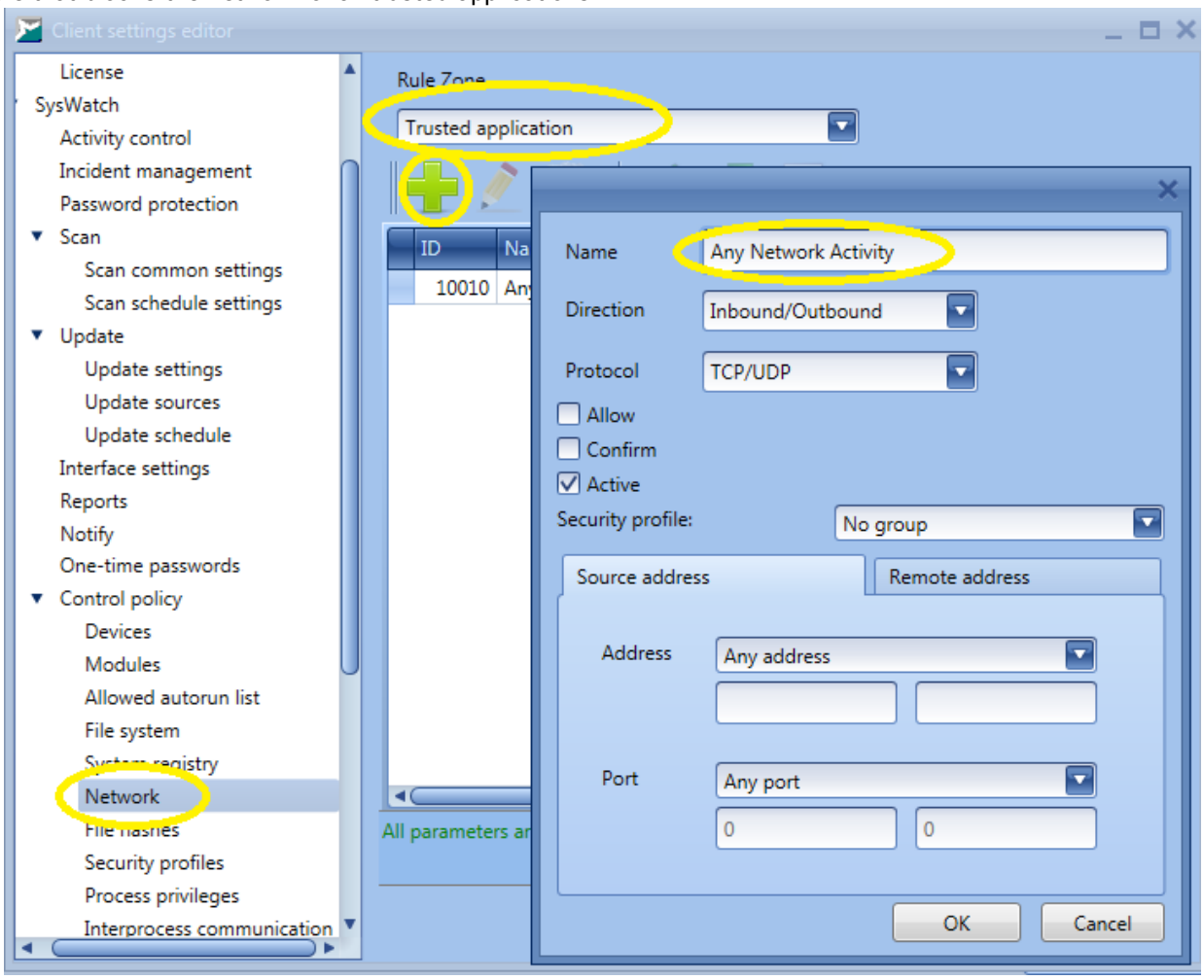
11.12	Make an attempt to connect a new USB drive (which has not been previously connected to the host) to the device you are testing.	❑ The USB drive does not connect to the device. You get a message that drivers for the USB drive have not been installed.	In the device logs on SoftControl Server, you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

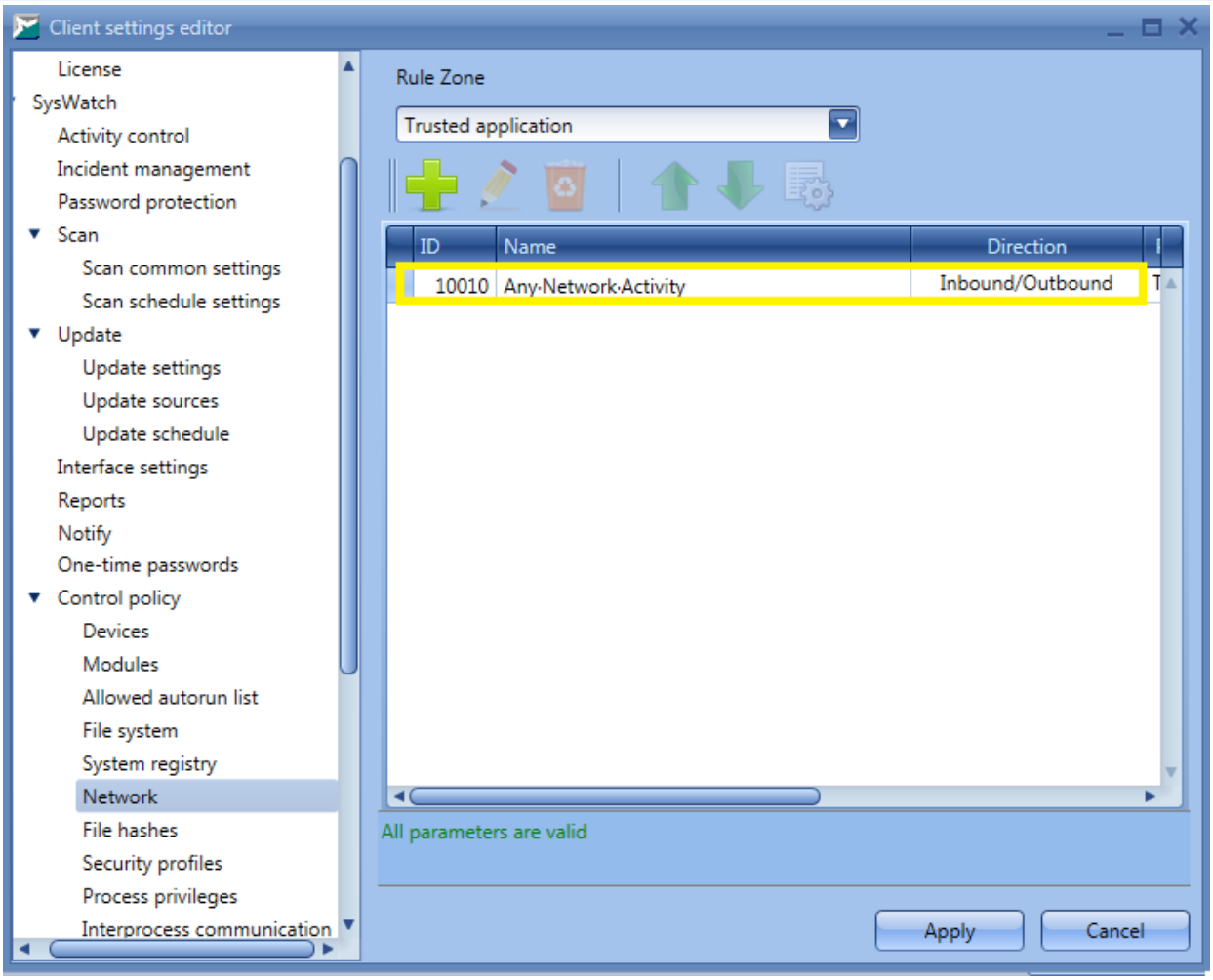
*You can see **Policy violation** event, **Creating the registry key** action in SoftControl Admin Console:



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

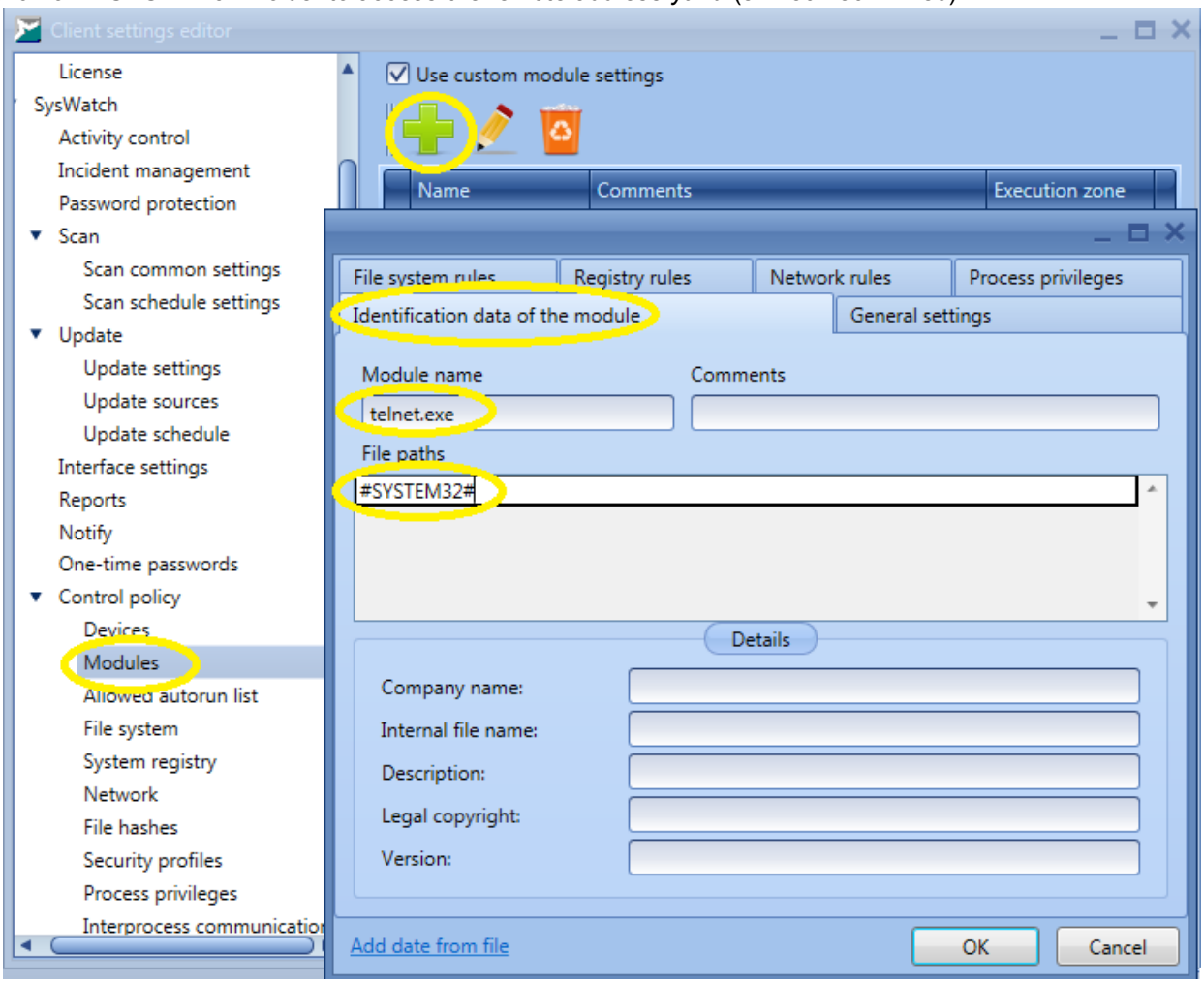
* In order to create the rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to. Find below the instructions on how to create the **Any Network Activity** rule that blocks the network for all trusted applications:

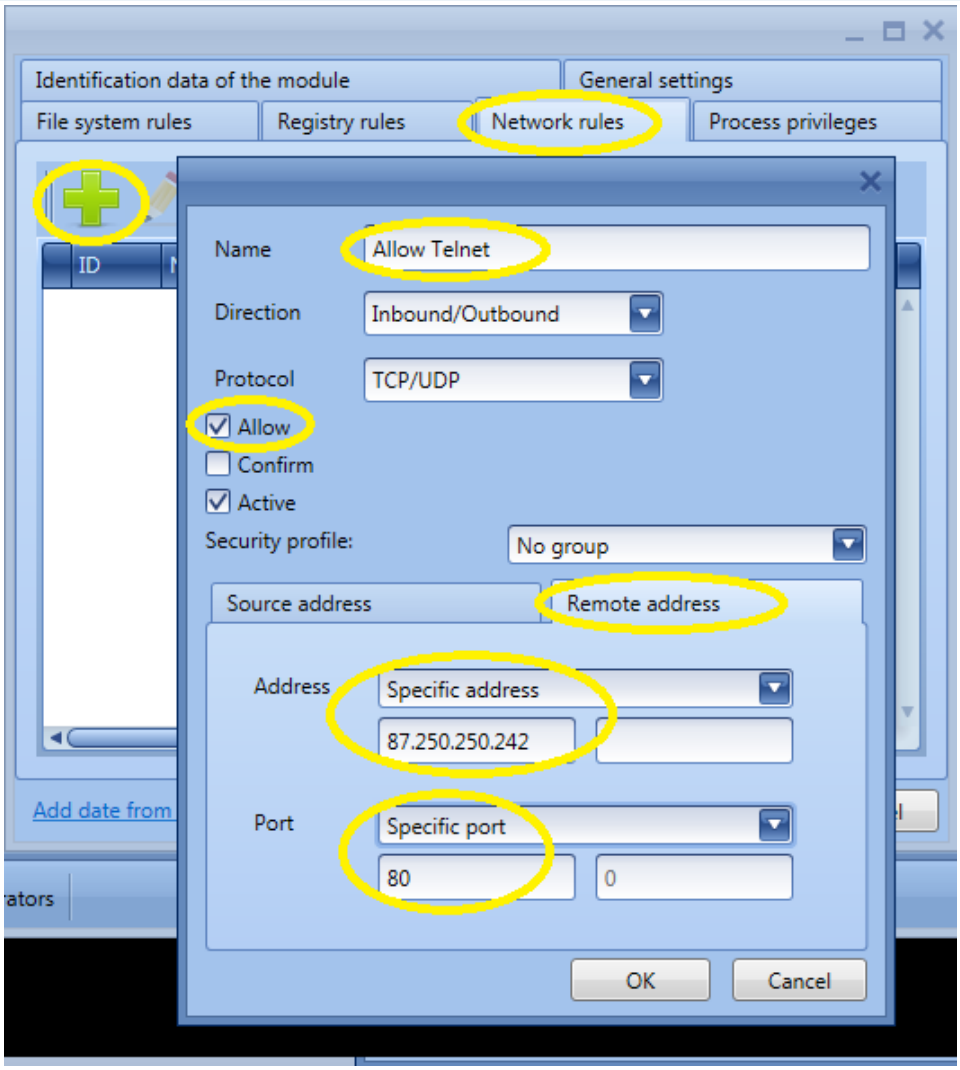


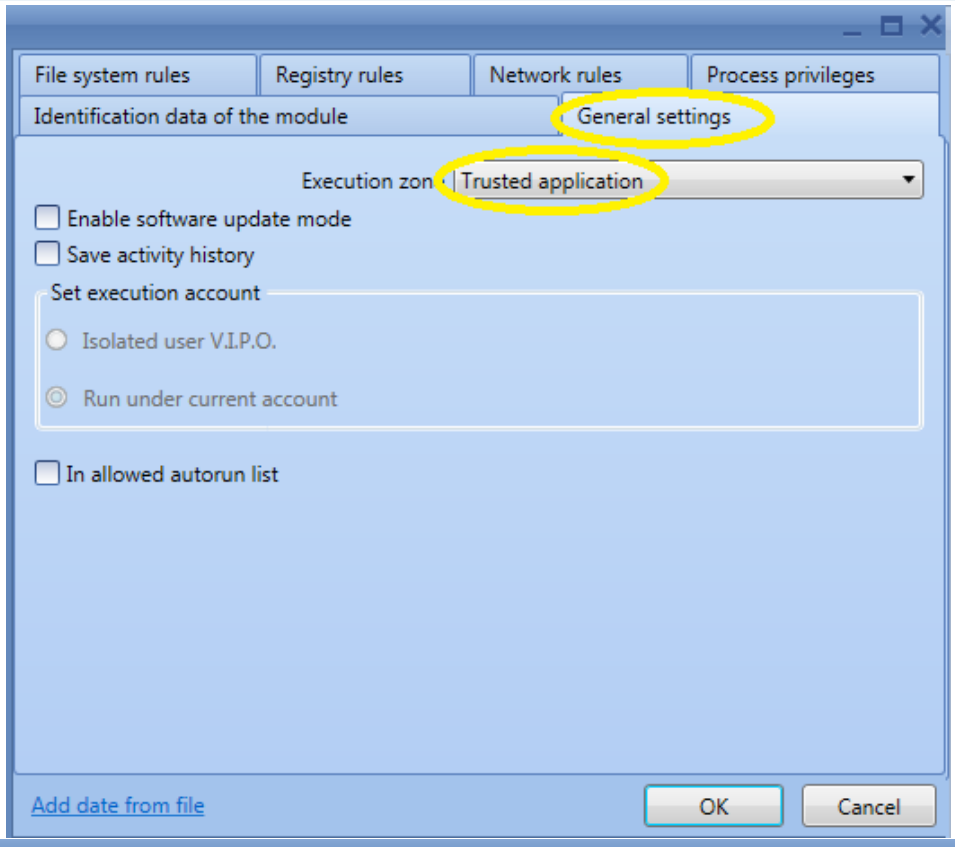


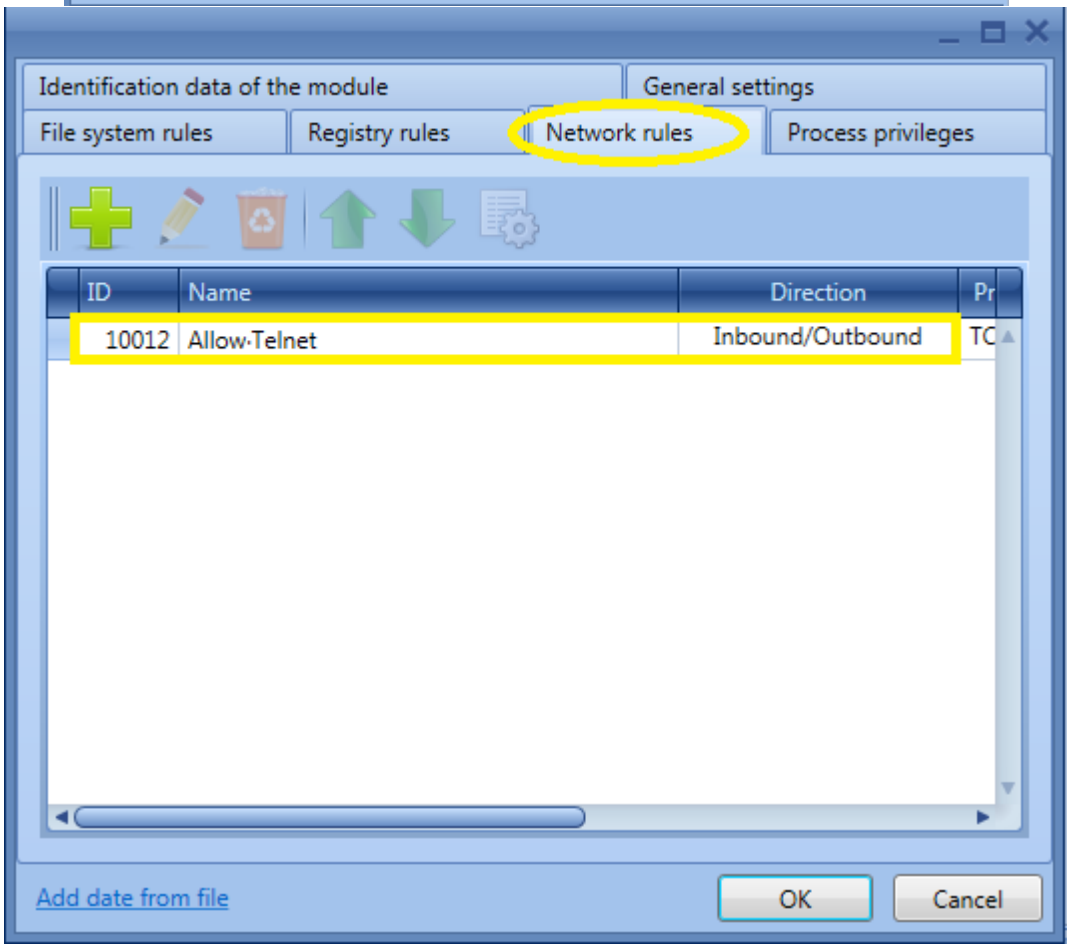
11.15	Create a rule that allows the *Telnet* application (*C:\windows\system32\telnet.exe*) to access *ya.ru* (87.250.250.242:80).*	❑ A rule that allows *Telnet* application (*C:\windows\system32\telnet.exe*) to access *ya.ru* (87.250.250.242:80) has been created.	

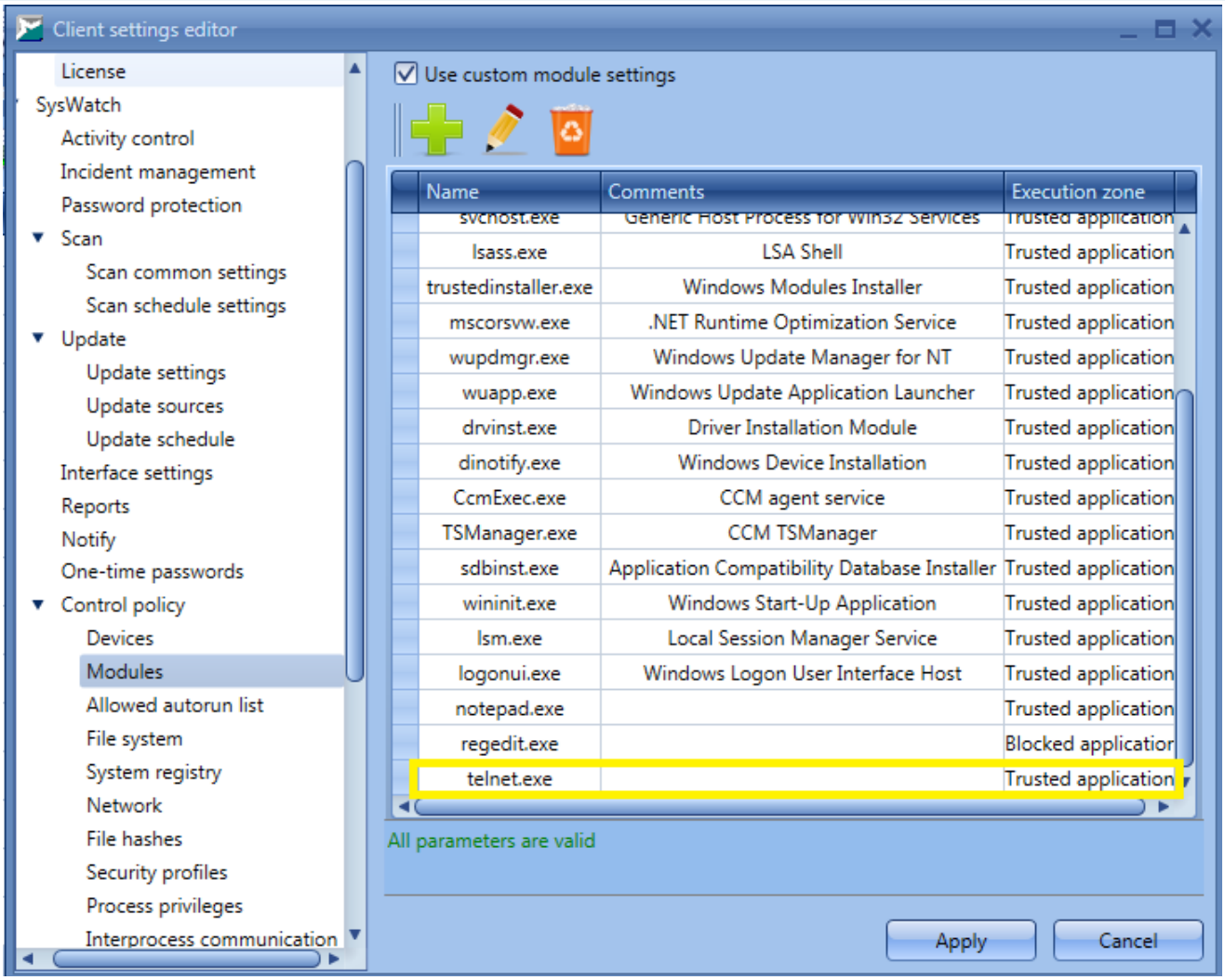
* In order to create the rule, edit the client settings, save them under a new name, and apply to the organizational unit that the device you are testing belongs to. Find below the instructions on how to create a rule that allows *telnet.exe* from *#SYSTEM32#* folder to access the remote address *ya.ru*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




Identification data of the module
General settings
File system rules
Registry rules
Network rules
Process privileges
ID
Add date from
ators
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
OK
Cancel

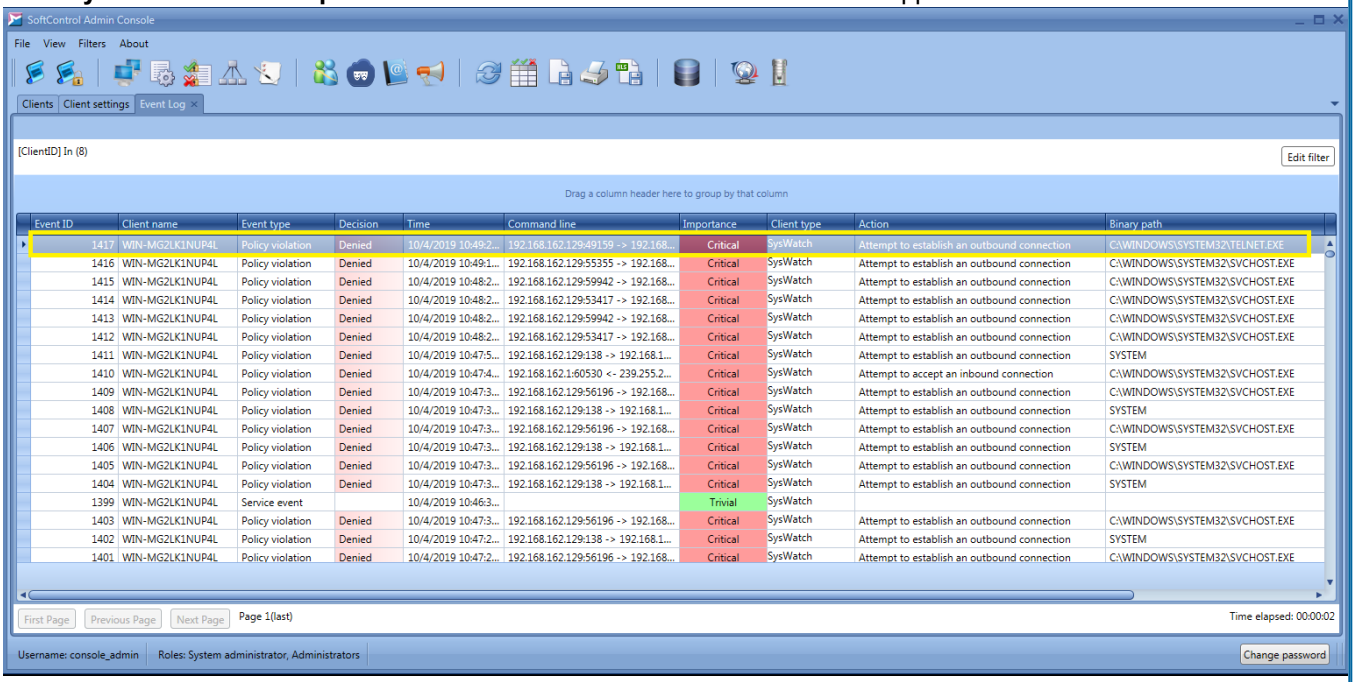

File system rules
Registry rules
Network rules
Process privileges
Identification data of the module
General settings
Execution zon
Trusted application
Enable software update mode
Save activity history
Set execution account
Isolated user V.I.P.O.
Run under current account
In allowed autorun list
Add date from file
OK
Cancel


Identification data of the module
General settings
File system rules
Registry rules
Network rules
Process privileges
ID
Name
Direction
Pr
10012
Allow-Telnet
Inbound/Outbound
TC
Add date from file
OK
Cancel



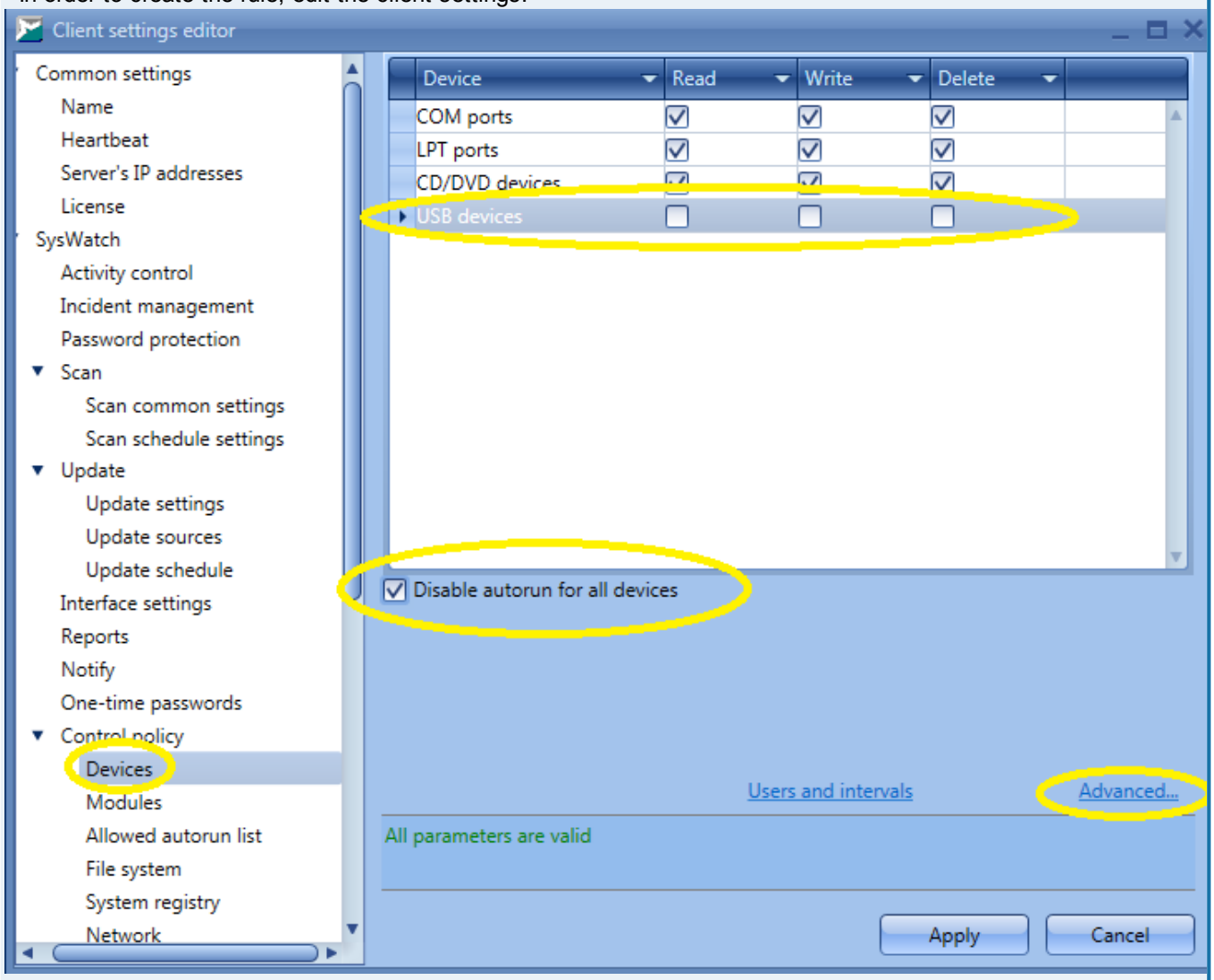
11.16	Make an attempt to access *ya.ru* (87.250.250.242:80) and 192.168.1.180:8000 (a random address is given for example) by *telnet.exe*.	❑ Connection to 87.250.250.242:80 has been established successfully. Connection to 192.168.1.180:8000 has not been established.	In the device logs on SoftControl 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:

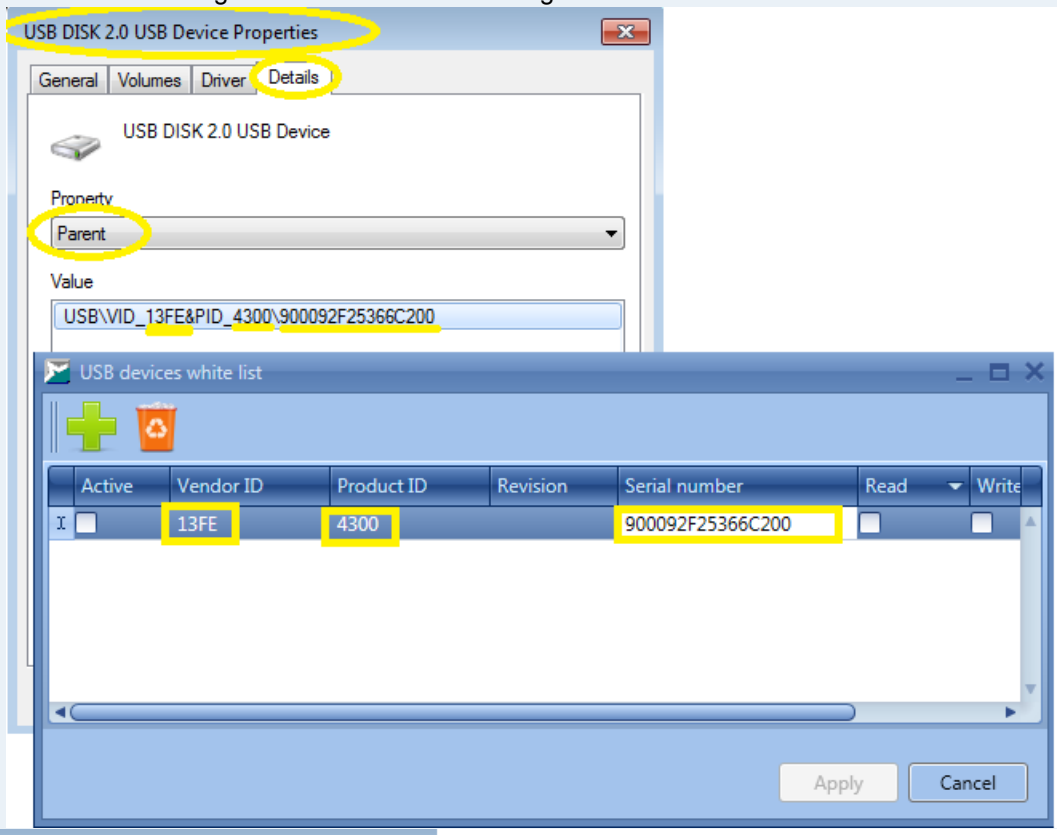


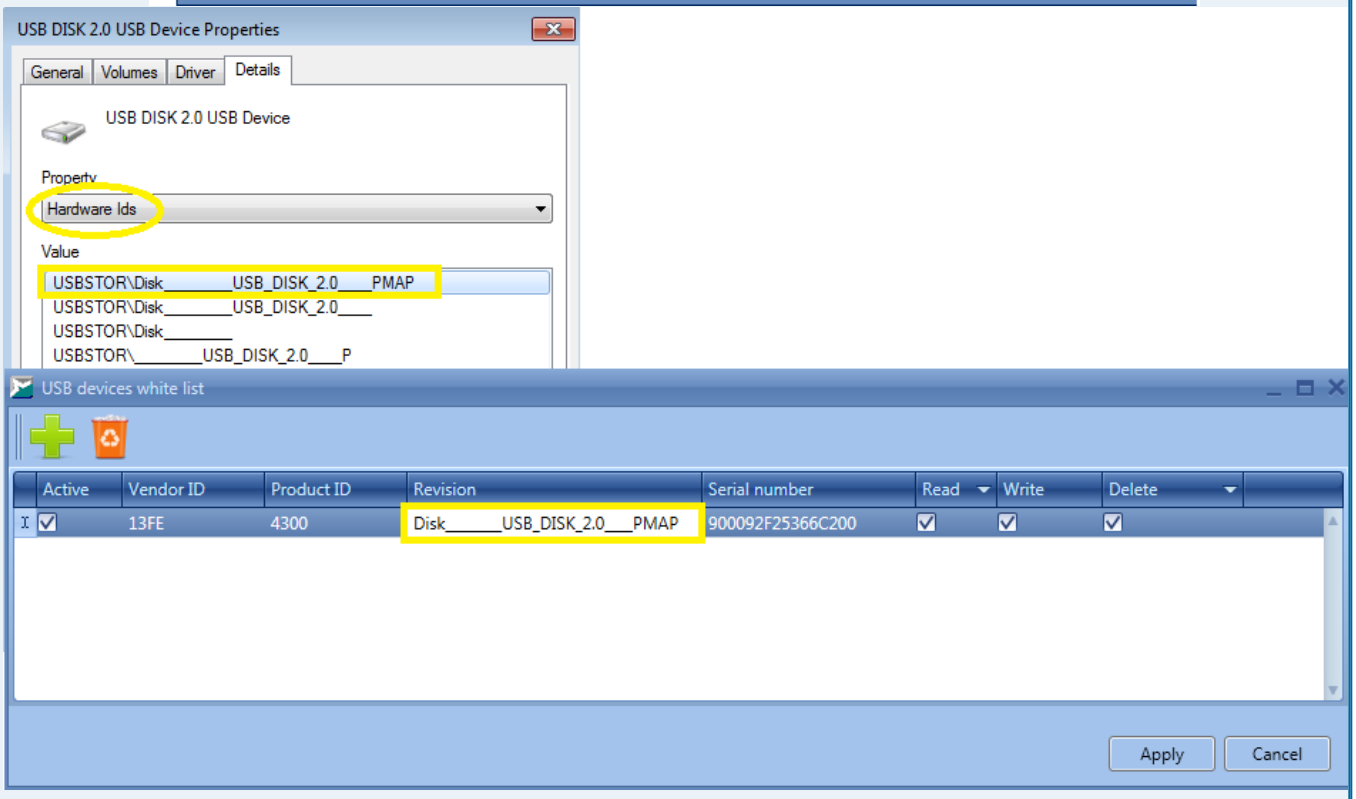
11.17	Test rules in control policies for the devices.		
11.18	Create a rule that blocks access to the file system for USB drives. Also create a whitelist and include a trusted USB device in it.*	❑ Access to the file system is forbidden to all USB drives except the ones in the whitelist.	

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



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

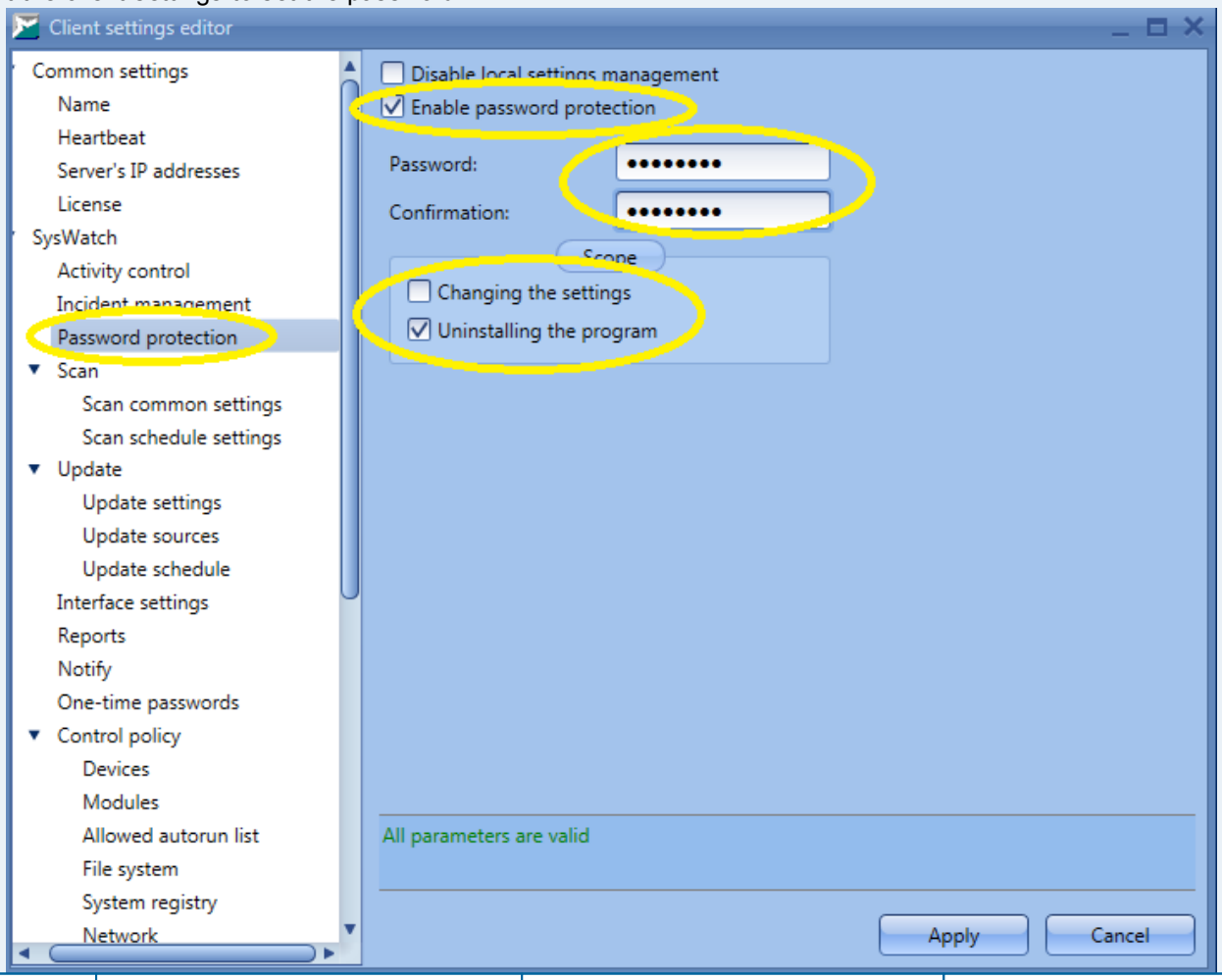




Once you create the rules, save them under a new name and apply to the organizational unit to which the device you are testing belongs.

11.19	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.	
11.20	Test rules in control policies for **Password protection** self-protection functionality.		
11.21	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, and delete the SoftControl SysWatch client module.	

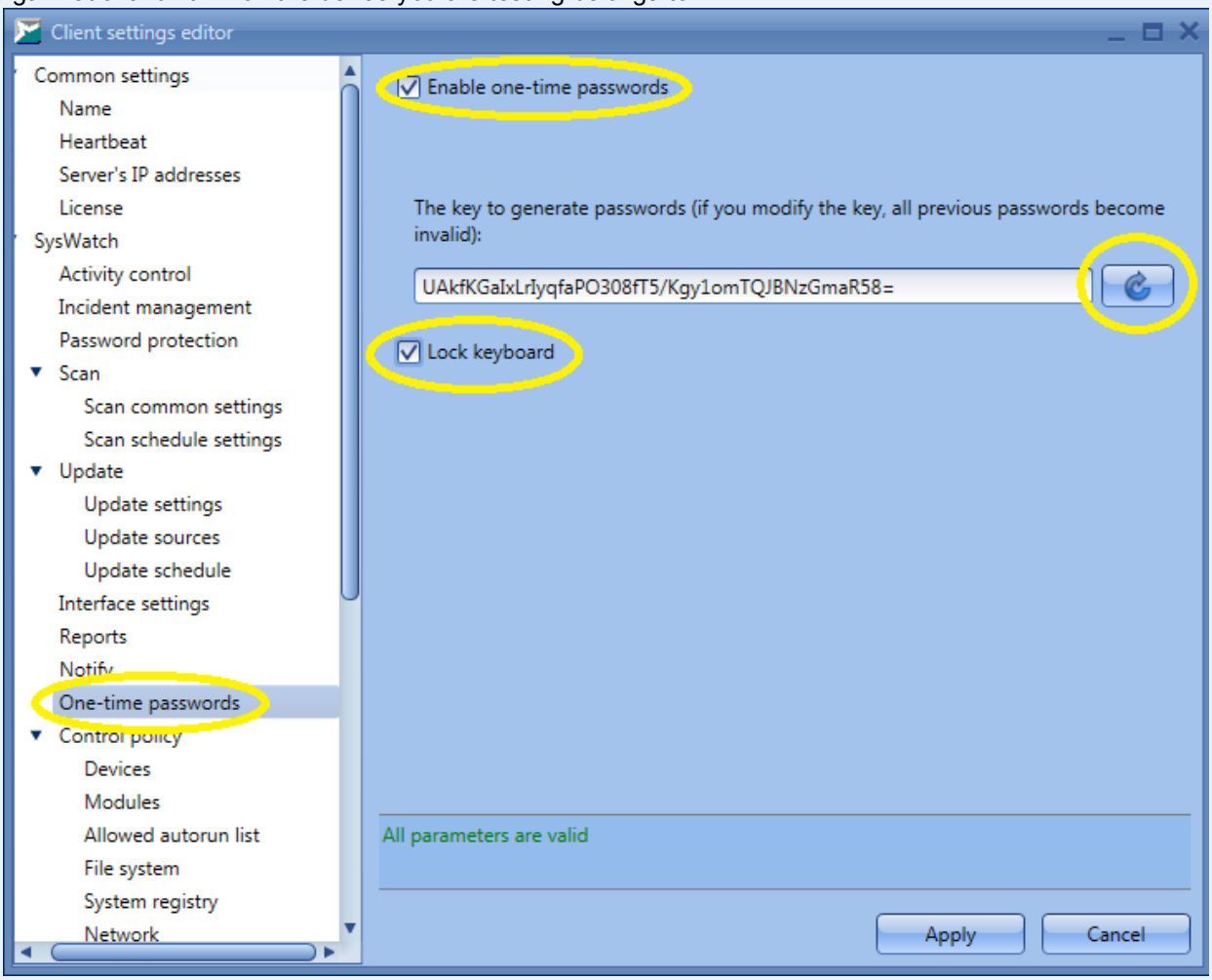
* Edit the client settings to set the password:



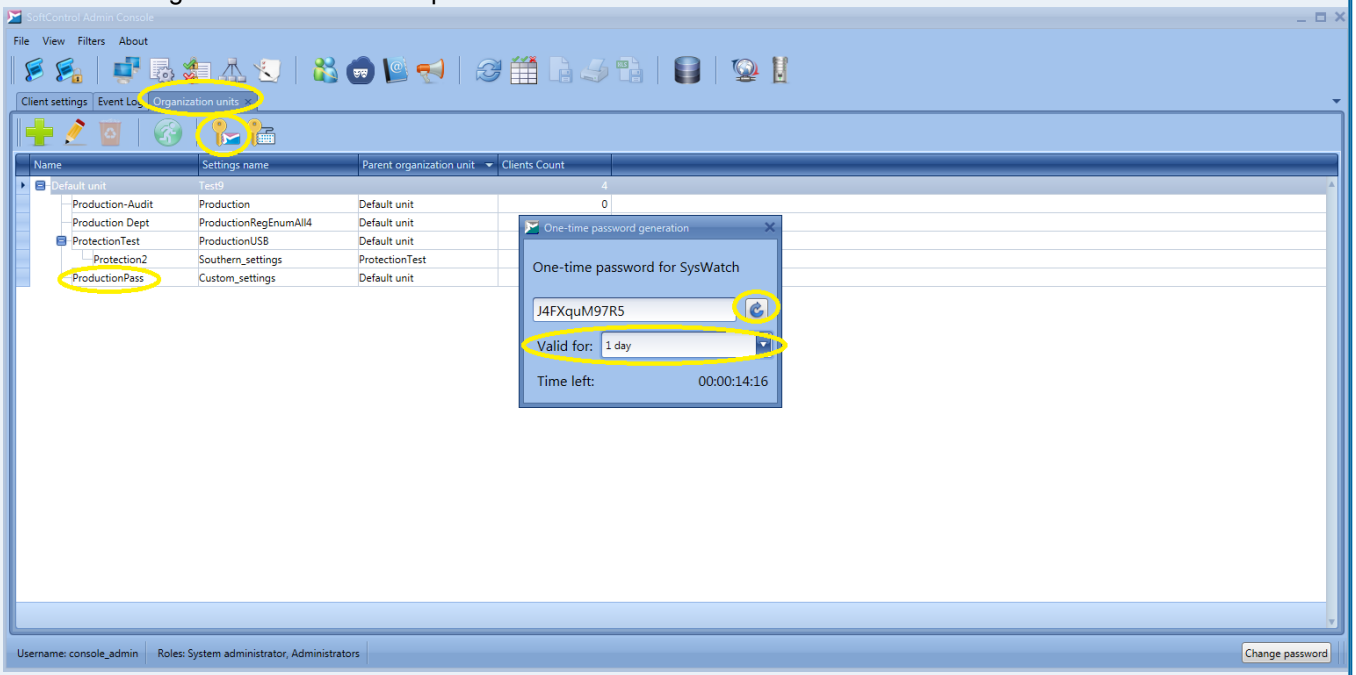
11.22	Check access to GUI, make an attempt to delete the SoftControl SysWatch client module.	❑ You can't access GUI without the password. When you try to delete the SoftControl SysWatch client module, you are requested to enter the password.	
11.23	Test rules in control policies for one-time (temporary) passwords.		

11.24	Activate use of one-time (temporary) passwords for access to GUI of the SoftControl SysWatch client module and keyboard blocking.*	❑ One-time passwords and key-board 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 Con-sole shall not be greater than validity time of the password. Otherwise, the password access to GUI of the SoftControl SysWatch client module (and to key-board unblocking) will not function.

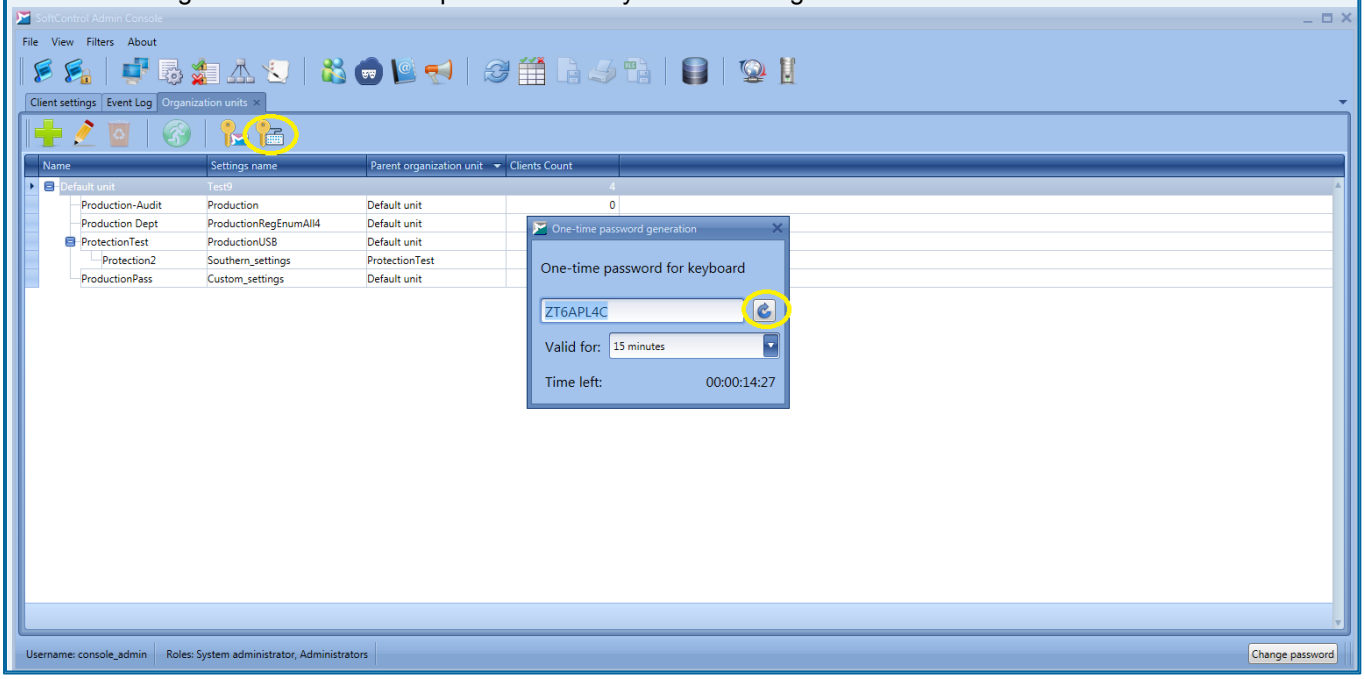
* In order to activate use of one-time passwords, edit the client settings, save them under a new name and apply to the organizational unit which the device you are testing belongs to:



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

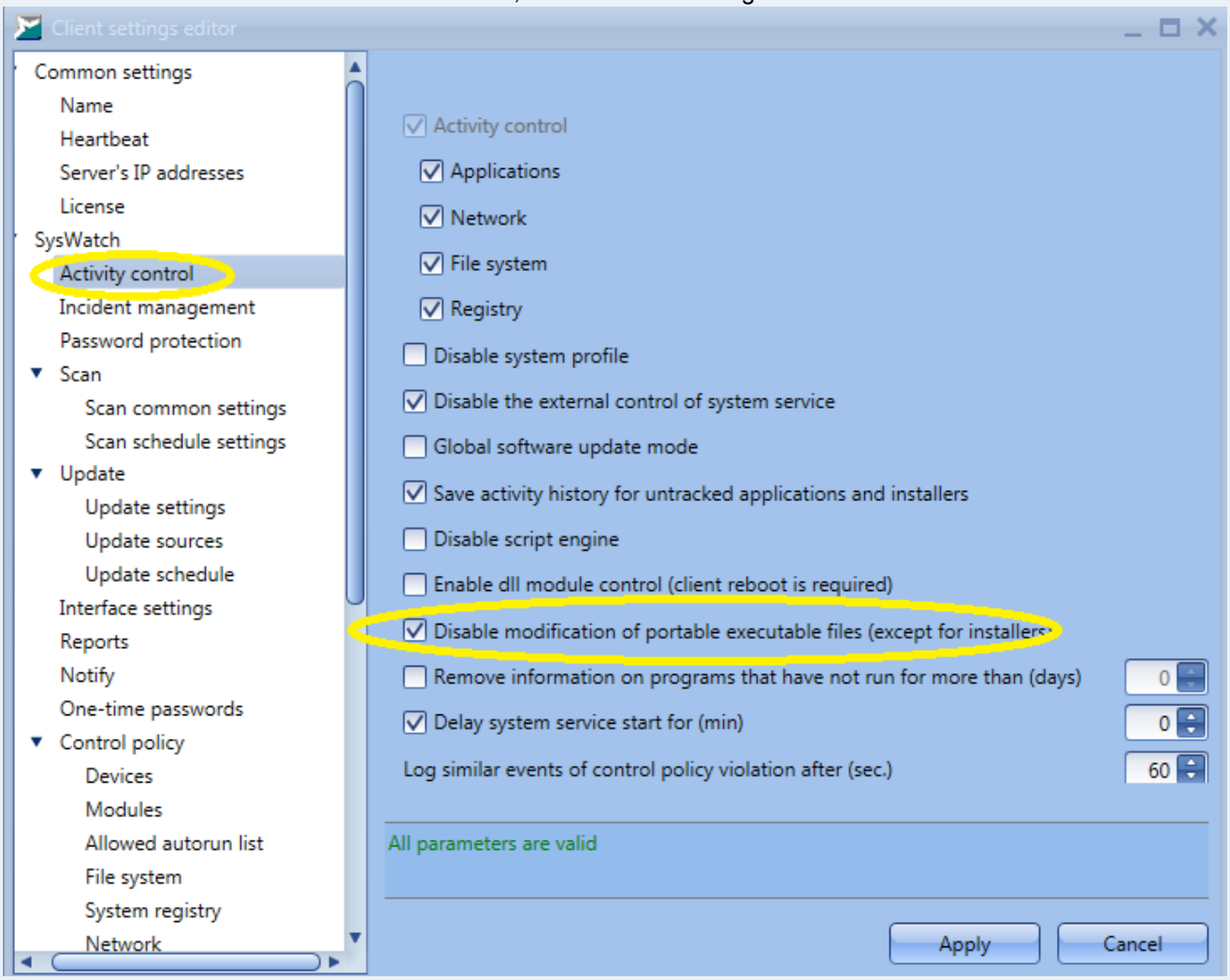


Do the following to create a one-time password for keyboard blocking:



11.25	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 the password, use lowercase letters.
11.26	Test rules in control policies for prohibition of PE files modification.		
11.27	Forbid modification of PE files to all but trusted installers.*	❑ PE files modification is now forbidden.	

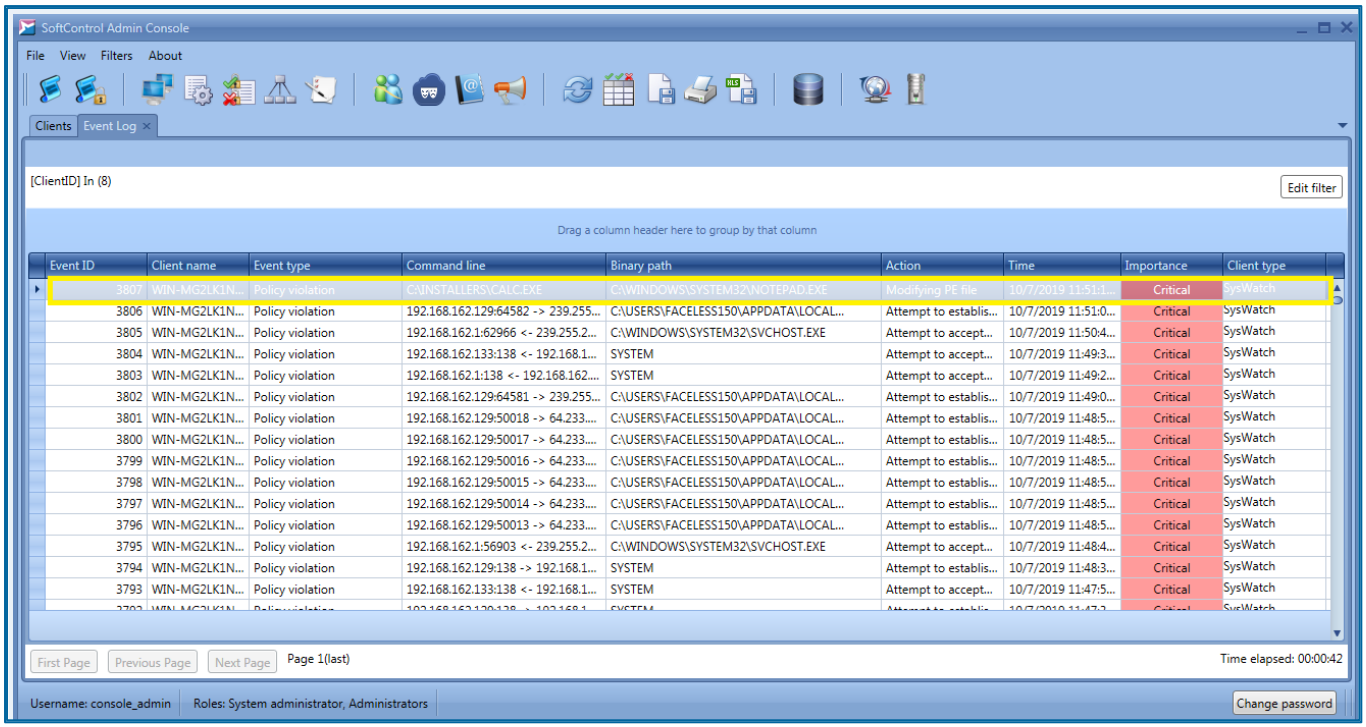
* In order to forbid modification of executable files, edit the client settings:



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.

11.28	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:


SoftControl Admin Console
File View Filters About
Clients Event Log
[ClientID] In (8)
Edit filter
Drag a column header here to group by that column
Event ID | Client name | Event type | Command line | Binary path | Action | Time | Importance | Client type
3807 WIN-MG2LK1N... Policy violation C:\INSTALLERS\CALC.EXE C:\WINDOWS\SYSTEM32\NOTEPAD.EXE Modifying PE file 10/7/2019 11:51:1... Critical SysWatch
3806 WIN-MG2LK1N... Policy violation 192.168.162.129:64582 -> 239.255... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:51:0... Critical SysWatch
3805 WIN-MG2LK1N... Policy violation 192.168.162.1:62966 <- 239.255.2... C:\WINDOWS\SYSTEM32\SVCHOST.EXE Attempt to accept... 10/7/2019 11:50:4... Critical SysWatch
3804 WIN-MG2LK1N... Policy violation 192.168.162.133:138 <- 192.168.1... SYSTEM Attempt to accept... 10/7/2019 11:49:3... Critical SysWatch
3803 WIN-MG2LK1N... Policy violation 192.168.162.1:138 <- 192.168.162.... SYSTEM Attempt to accept... 10/7/2019 11:49:2... Critical SysWatch
3802 WIN-MG2LK1N... Policy violation 192.168.162.129:64581 -> 239.255... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:49:0... Critical SysWatch
3801 WIN-MG2LK1N... Policy violation 192.168.162.129:50018 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3800 WIN-MG2LK1N... Policy violation 192.168.162.129:50017 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3799 WIN-MG2LK1N... Policy violation 192.168.162.129:50016 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3798 WIN-MG2LK1N... Policy violation 192.168.162.129:50015 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3797 WIN-MG2LK1N... Policy violation 192.168.162.129:50014 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3796 WIN-MG2LK1N... Policy violation 192.168.162.129:50013 -> 64.233.... C:\USERS\FACELESS150\APPDATA\LOCAL... Attempt to establis... 10/7/2019 11:48:5... Critical SysWatch
3795 WIN-MG2LK1N... Policy violation 192.168.162.1:56903 <- 239.255.2... C:\WINDOWS\SYSTEM32\SVCHOST.EXE Attempt to accept... 10/7/2019 11:48:4... Critical SysWatch
3794 WIN-MG2LK1N... Policy violation 192.168.162.129:138 -> 192.168.1... SYSTEM Attempt to establis... 10/7/2019 11:48:3... Critical SysWatch
3793 WIN-MG2LK1N... Policy violation 192.168.162.133:138 <- 192.168.1... SYSTEM Attempt to accept... 10/7/2019 11:47:5... Critical SysWatch
First Page Previous Page Next Page Page 1(last)
Time elapsed: 00:00:42
Username: console_admin Roles: System administrator, Administrators
Change password

3. Customer support

If you have any questions concerning the installation, setting up and operation of TPSecure 5.0.18, please contact our customer support by e-mail support@safensoft.com.