Safe'n'Sec

Product line 3.11

Release notes

Introduction

Purpose

Safe’n’Sec 3.11 product line offers program components kit for deploying information security system. The system is intended for providing software environment integrity of network endpoints and data protection against unauthorized access by maintenance staff or violators.

The following modules are included in the product line:

- Safe’n’Sec Service Center is composed of:
  - Safe’n’Sec Server - server component;
  - Safe’n’Sec Admin Console - management console.
- Safe’n’Sec ATM Client / Endpoint Client / SClient / SysWatch Personal (hereafter referred to as «Safe’n’Sec SysWatch») - client components of proactive protection of self-service devices, corporate network workstations, servers and personal computers correspondingly;
- Safe’n’Sec DLP Client - client component of monitoring and data collection of user activity.

This document presents main changes and new capabilities included in the 3.11 version.

3.11 version

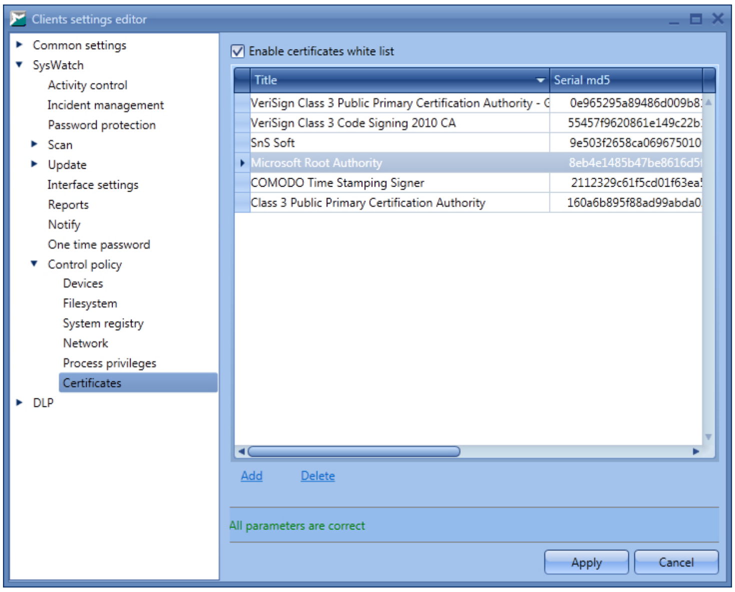
Improvements and new features:

Bug fixes:

Improvements and new features

Configuring certificate white list remotely

In Safe'n'Sec Service Center 3.11 it's become possible to manage the certificate white list that is used by the Safe'n'Sec SysWatch client module for controlling installers execute by their digital signature.



☑ Enable certificates white list

Title	Serial md5
VeriSign Class 3 Public Primary Certification Authority - G	0e965295a89486d009b8
VeriSign Class 3 Code Signing 2010 CA	55457f9620861e149c22b
SnS Soft	9e503f2658ca069675010
Microsoft Root Authority	8eb4e1485b47be8616d5
COMODO Time Stamping Signer	2112329c61f5cd01f63ea
Class 3 Public Primary Certification Authority	160a6b895f88ad99abda0

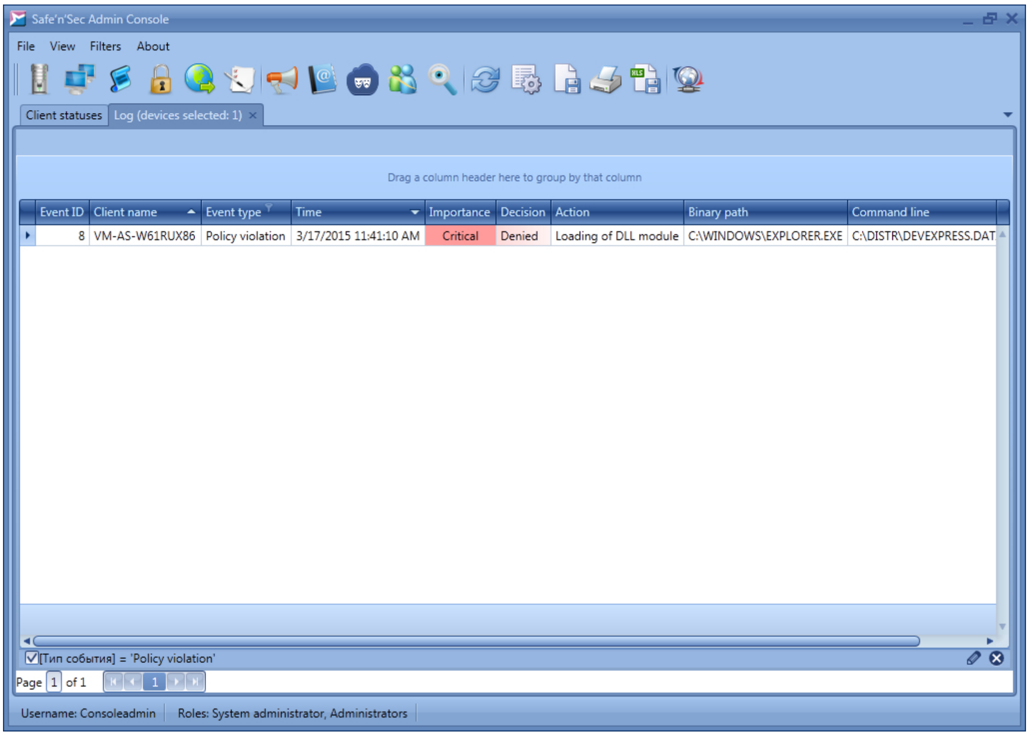
All parameters are correct

Figure 1. Certificate white list

The list is set up in a client configuration and similarly to working locally via Safe'n'Sec SysWatch interface (fig. 1). In that way you can elaborate and apply common policy for controlling certificates for each organizational unit (all organizational units).

Logs of blocking DLL

Logging of the existing Safe'n'Sec SysWatch feature on controlling DLL modules is realized in the 3.11 version. Entry about blocking modules event is written both in local Safe'n'Sec SysWatch text reports and available to an administrator as single event in the Safe'n'Sec Admin Console management console (fig. 2).


Safe'n'Sec Admin Console
File
View
Filters
About
Client statuses
Log (devices selected: 1)
Drag a column header here to group by that column

Event ID	Client name	Event type	Time	Importance	Decision	Action	Binary path	Command line
8	VM-AS-W61RUX86	Policy violation	3/17/2015 11:41:10 AM	Critical	Denied	Loading of DLL module	C:\WINDOWS\EXPLORER.EXE	C:\DISTR\DEVEXPRESS.DAT

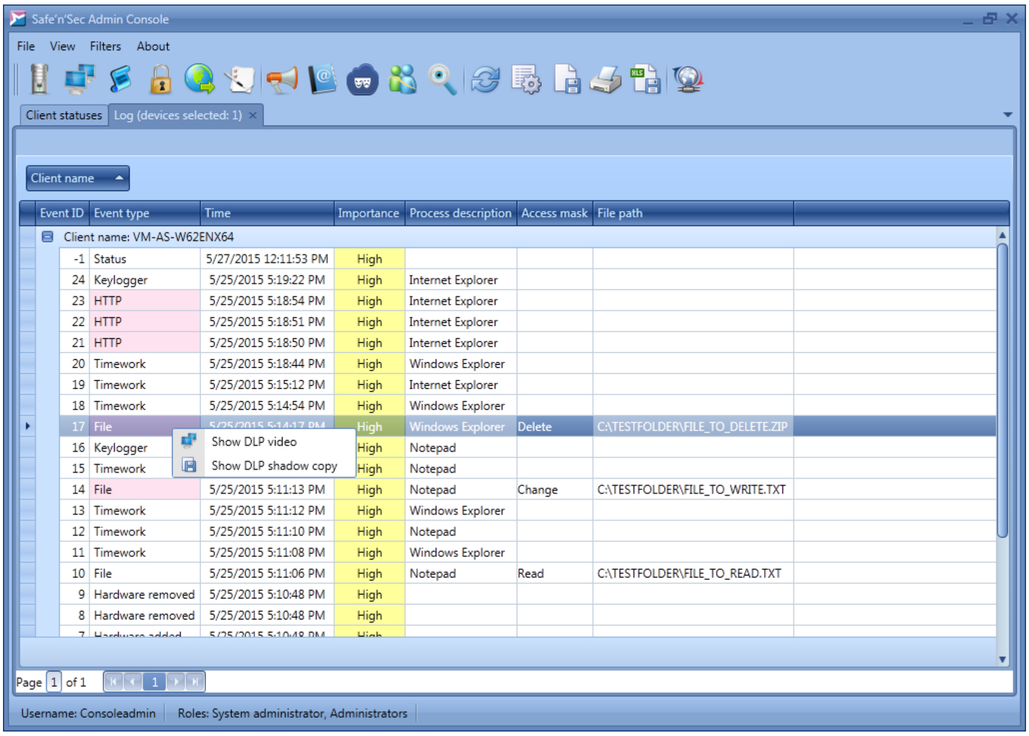
☑[Тип события] = 'Policy violation'

Page 1 of 1
1
Username: Consoleadmin
Roles: System administrator, Administrators

Figure 2. Log entry about blocking DLL

Recording video at incidents occuring

The Safe'n'Sec DLP Client module of data collection of the 3.11 version allows to capture screenshots at the moment an incidents occure (performing actions over observable objects). Frames are transferred to the Safe'n'Sec Service Center server and stored in its database centrally. The sequence of the frames can be played as a video record by an administrator via the Safe'n'Sec Admin Console management console. Video record is invoked by context menu of the corresponding event in Safe'n'Sec DLP Client logs (fig. 3, 4).



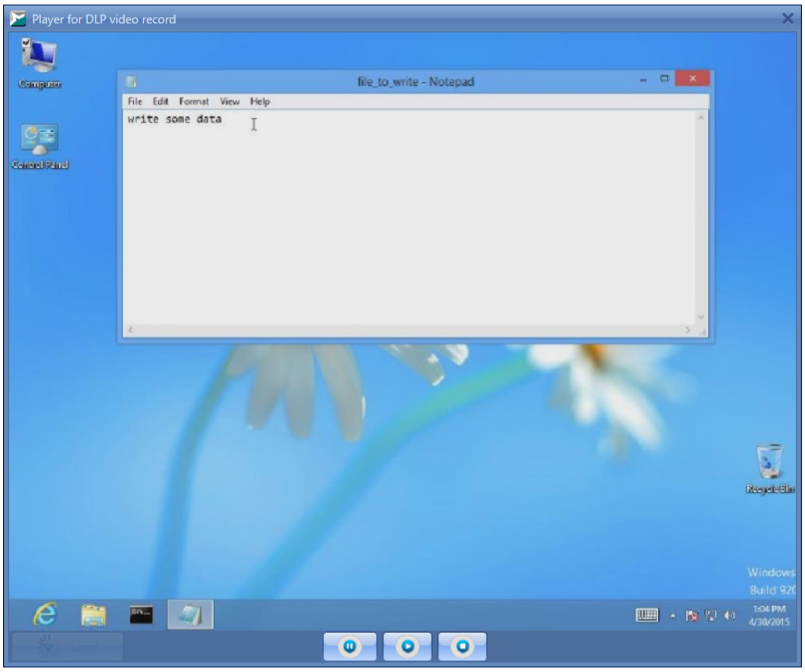
Client name: VM-AS-W62ENX64

Event ID	Event type	Time	Importance	Process description	Access mask	File path
-1	Status	5/27/2015 12:11:53 PM	High			
24	Keylogger	5/25/2015 5:19:22 PM	High	Internet Explorer		
23	HTTP	5/25/2015 5:18:54 PM	High	Internet Explorer		
22	HTTP	5/25/2015 5:18:51 PM	High	Internet Explorer		
21	HTTP	5/25/2015 5:18:50 PM	High	Internet Explorer		
20	Timework	5/25/2015 5:18:44 PM	High	Windows Explorer		
19	Timework	5/25/2015 5:15:12 PM	High	Internet Explorer		
18	Timework	5/25/2015 5:14:54 PM	High	Windows Explorer		
17	File	5/25/2015 5:14:17 PM	High	Windows Explorer	Delete	C:\TESTFOLDER\FILE_TO_DELETE.ZIP
16	Keylogger		High	Notepad		
15	Timework		High	Notepad		
14	File	5/25/2015 5:11:13 PM	High	Notepad	Change	C:\TESTFOLDER\FILE_TO_WRITE.TXT
13	Timework	5/25/2015 5:11:12 PM	High	Windows Explorer		
12	Timework	5/25/2015 5:11:10 PM	High	Notepad		
11	Timework	5/25/2015 5:11:08 PM	High	Windows Explorer		
10	File	5/25/2015 5:11:06 PM	High	Notepad	Read	C:\TESTFOLDER\FILE_TO_READ.TXT
9	Hardware removed	5/25/2015 5:10:48 PM	High			
8	Hardware removed	5/25/2015 5:10:48 PM	High			
7	Hardware added	5/25/2015 5:10:48 PM	High			

Page 1 of 1

Username: Consoleadmin | Roles: System administrator, Administrators

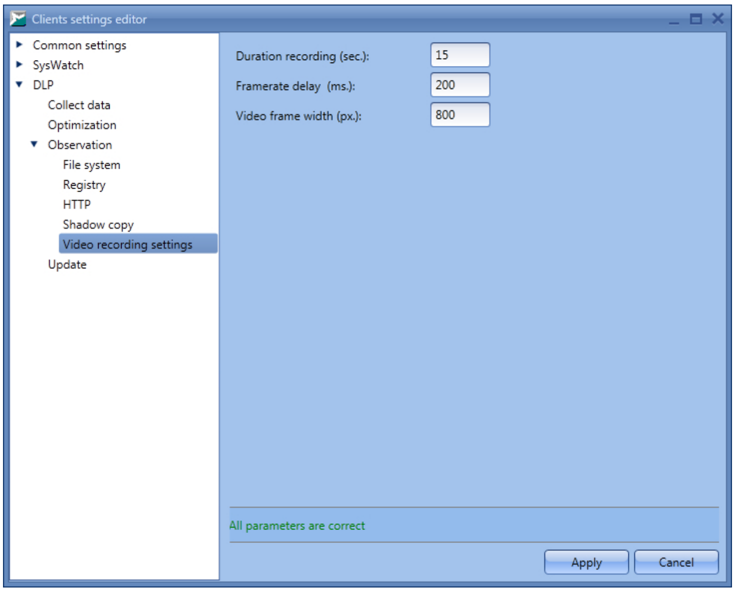
Figure 3. The "Log" tab for the Safe’n’Sec DLP Client component



write some data

Figure 4. Safe’n’Sec DLP Client video player

Saving screenshots settings are available to an administrator in the client module configuration (fig. 5).



Duration recording (sec.): 15

Framerate delay (ms.): 200

Video frame width (px.): 800

All parameters are correct

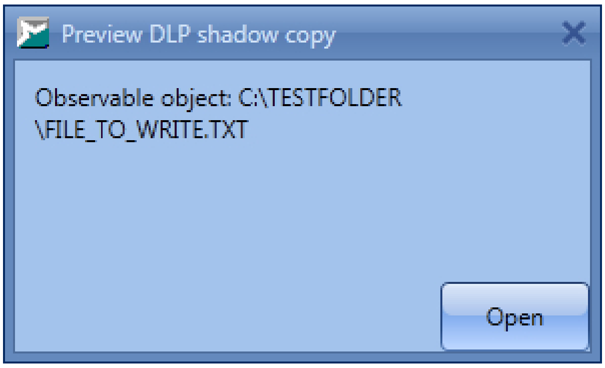
Figure 5. Video recording settings

The following observable events can be watched with the help of the screenshots capture:

- reading file system / system registry objects;
- creating file system / system registry objects;
- changing file system / system registry objects;
- renaming file system / system registry objects;
- deleting file system / system registry objects;
- transferring data via network.

Accessing shadow copies remotely

In Safe’n’Sec Service Center 3.11 it's become possible to remotely access shadow copies of observable objects that is saved by the Safe’n’Sec DLP Client modules.



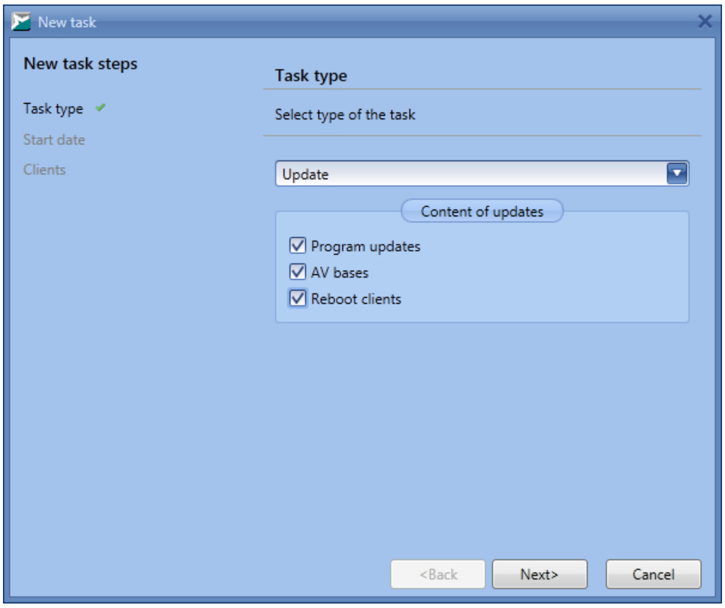
Observable object: C:\TESTFOLDER
\FILE_TO_WRITE.TXT

Figure 6. Shadow copy of observable object

Backup copy of changed observable object is available to an administrator in Safe'n'Sec Admin Console by invoking context menu of the corresponding event in Safe'n'Sec DLP Client logs (fig. 3, 6).

Centralized updating of client modules on demand

New feature is available in the Safe'n'Sec Service Center of the 3.11 version that expands capabilities of centralized updating of the client modules. Now besides remote updating via scheduling, Safe'n'Sec Admin Console administrator has capability to remote updating on demand via new corresponding type of the task. As task options you can select components to update and also choose whether client devices will be rebooted forcibly after update (fig. 7).


New task

New task steps

Task type ✓
Start date
Clients

Task type

Select type of the task

Update

Content of updates

☑ Program updates
☑ AV bases
☑ Reboot clients

Figure 7. Update task options

New installers of Safe'n'Sec SysWatch and Safe'n'Sec DLP Client

New installers have been applied in the Safe'n'Sec SysWatch and Safe'n'Sec DLP Client modules of the 3.11 version. This provides multilingual installation of components and simplified update routine for end users. Along with that, installers develop process and their support was made easier. Server and client components installers designed in one technology allow to organize homogeneous and logical structure on the Safe'n'Sec update server.

Bug fixes

Safe’n’Sec SysWatch: incomplete merge of policies from SC and local policies

Part of local policies (custom rules) weren't deleted when rules received from Safe’n’Sec Service Center are applied on Safe’n’Sec SysWatch.

Fix:

The defect has been eliminated in the 3.11 version. Merge of policies from Safe’n’Sec Service Center and local policies is correct.

Safe’n’Sec SysWatch: hashing error when application has incorrect PE format

It was established that Safe’n’Sec SysWatch driver doesn't calculate hash sum of an executable file that have incorrect PE format. As a result, launch of such applications has been blocked in all cases.

Fix:

The character has been eliminated in the 3.11 version. Executable files with incorrect PE format are processed by driver in regular mode.

Safe’n’Sec Service Center: removing client from database error

Error has been appeared in the Safe’n’Sec Admin Console management console at deleting the Safe’n’Sec SysWatch client modules from the Safe’n’Sec Service Center database in a case of big amount of accumulated events in logs (250 000 entries and more).

Fix:

Algorithm for removing the client modules from the database has been optimized in the 3.11 version to avoid such mistakes.

Safe’n’Sec Service Center: management console crashing at all file system policies deleting

Safe’n’Sec Admin Console has crashed in a case of deleting all rules from the file system control policy in Safe’n’Sec SysWatch configuration.

Fix:

The defect has been eliminated in the 3.11 version.

Customer support

If you have any questions concerning the Safe’n’Sec products installation, setting up and operation, please contact our round-the-clock customer support by e-mail support@safensoft.ru.