



SoftControl

DLP 5.0.18

Testing procedure

Dear user!

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

COPYRIGHT

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

All the names used throughout this document are trademarks of its respective owners.

LIABILITY LIMIT

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

Safe'N'Sec Corporation, 2019

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. Introduction	4
2. Preparing the test bench	5
3. Test Cases	6
3.1 Monitoring the file system.....	6
3.2 Monitoring the registry.....	7
3.3 Keylogging.....	9
3.4 Monitoring external devices.....	9
3.5 Recording video.....	10
4. Customer support	11

1. Introduction

SoftControl DLP Client is designed to control the actions of the corporate network users and to provide company's information security by means of protection against insider incidents. SoftControl DLP Client collects data about users' activity, which allows the security service to monitor how staff accesses the information that represents the trade secret and other confidential data. The obtained reports can be used to perform backward analysis of the data leaks protection, to monitor the efficiency of the working time, etc.

This document describes how to test the installed software.

2. Preparing the test bench

You need two computers for the testing. They can be either physical or virtual machines, and should have USB ports. The computers should be able to connect to each other through the network. Install SoftControl Service Center on the first computer ('the server'; see 'SoftControl Service Center administrator's guide'). Install SoftControl DLP Client on the second computer ('the client computer'; see 'SoftControl DLP Client installation guide'). Connect SoftControl DLP Client to SoftControl Service Center.

3. Test Cases

To perform each test:

- create the objects specified in the *Description* column, on the client computer;
- create organization unit settings in SoftControl Admin Console; the settings should include the appropriate rule;
- apply the settings you created;
- perform the operations on the client computer;
- view the client application's log in SoftControl Admin Console.

Tick off **Collect data** in the **Collect data** section of the **DLP** category for all settings.

3.1 Monitoring the file system

In the settings of the **Log** tab in SoftControl Admin Console, add the **File path** and **Access mask** columns, or enable the required filter: **Filters** → **DLP Events Filters** → **File**.

Table 1. Testing the file system monitoring

Description	Expected result
Monitoring Read operation for a file	
1) Create a C:\file1.txt file. 2) Specify the file monitoring rule: set the path (C:\file1.txt) and tick off Read . Apply the settings. 3) Open the file with <i>Notepad.exe</i> .	The log should contain a string that has C:\file1.txt in the File path column, and Read in the Access mask column.
Complete file and folder monitoring	
1) Create a rule to monitor the C:\file2.txt file that does not exist yet: specify the path (C:\file2.txt) and tick of all checkboxes except for Shadow copy and Video recording . 2) Create a rule to monitor the C:\dir1 directory that does not exist yet. Specify the path (C:\dir1\#**) and tick off all checkboxes except for Shadow copy and Video recording . 3) Apply the settings. <u>Note:</u> SoftControl DLP Client does not monitor objects that have been re-named. 4) Create a C:\file2.txt file. Open it, write something in it and save it. Re-name the file. Modify it once more. Change the name of the file to the original one. Modify the file, then remove it. Create the file once more.	The log should contain a string for each of the operations. The strings should contain C:\file2.txt in the File path column and Create , Read , etc. in the Access mask column. The same entries should appear for the operations with the C:\dir1 directory. Make sure that after you rename file2.txt and dir1, the operations with the file and the directory do not appear in the log. Make sure that after you change the names of the file and the

Description		Expected result
5) Create a <i>C:\dir1</i> directory. Create a <i>C:\dir1\file3.txt</i> file in this directory. Open the file, write something in it and save it. Rename the file, then remove it. Change the name of the directory to <i>dir12</i> . Create a <i>C:\dir12\newfile.txt</i> file. Change the name of the directory to the original one (<i>dir1</i>). Modify the <i>C:\dir1\newfile.txt</i> file.		directory to the original ones, the events appear in the log again.
Monitoring file system objects with shadow copying		
1	1) In the Observation → Shadow copy section of the DLP category, tick off Enable shadow copy . Leave the Local path to save copies of files field empty. This way, the copies are saved to <i>C:\Program Files\SafenSoft\DLP Client\Backups\</i> . 2) Create the <i>C:\file4.txt</i> and <i>C:\file5.txt</i> files on the client computer. Specify the rules to monitor these files: set the paths (<i>C:\file4.txt</i> and <i>C:\file5.txt</i>), tick off Change and Shadow copy for the first rule, and Delete and Shadow copy for the second rule. 3) Apply the settings. 4) Modify both files. Make sure that a single <i>.bkp</i> file appears in the directory with the backup copies. 5) Remove both files.	When you modify both files, the entry about the modification of <i>file4.txt</i> appears in the log. Clicking the pink field in this entry opens the backup copy. Similarly, when you remove both files, only the entry about <i>file5.txt</i> appears in the log.
2	In the Observation → Shadow copy section of the DLP category, enter <i>C:\copies\</i> to the Local path to save copies of files field. Repeat the first test and make sure that the copies now appears in the specified directory.	

3.2 Monitoring the registry

In the settings of the **Log** tab in SoftControl Admin Console, add the **Registry path** and **Access mask** columns, or enable the required filter: **Filters** → **DLP Events Filters** → **Registry**.

To perform the test, you need to have administrator privileges on the client computer, or simply rights to modify the registry. The registry root keys in the path specified in the rules should be assigned as follows.

Table 2. Specifying the paths in the registry

Registry key	Assigned in the SoftControl DLP Client rules as
<i>HKEY_CLASSES_ROOT</i>	<i>\REGISTRY\MACHINE\SOFTWARE\CLASSES\</i>
<i>HKEY_LOCAL_MACHINE</i>	<i>\REGISTRY\MACHINE\</i>
<i>HKEY_CURRENT_USER</i>	<i>\REGISTRY\USER\<SID>\</i> for the user with the specified security identifier (<SID>)

Registry key	Assigned in the SoftControl DLP Client rules as
HKEY_USERS	\REGISTRY\USER\

Table 3. Testing the registry monitoring

Description	Expected result
Monitoring a registry key	
1) Create a rule for the registry: Specify the path (\REGISTRY\MACHINE\SYSTEMKey1) and tick off all checkboxes except for Shadow copy and Video recording . Apply the settings. 2) Create the HKEY_LOCAL_MACHINE\SYSTEMKey1\ key. Create the VALUE1 parameter of an arbitrary type with any value. Modify its value. 3) Create the Subkey1 subkey and the VALUE2 parameter in it. Modify the value of the parameter. 4) Rename Key1. Change its name to the original one.	The log in SoftControl Admin Console should contain operations for Key1 and VALUE1, but not for Subkey1 and VALUE2.
Monitoring a key and all included objects in the registry	
1) Create a rule for the registry and specify the path (\REGISTRY\MACHINE\SYSTEMKey2\###). The ### mask means that all included objects, not just the key, are under observation. Tick off all checkboxes except for Shadow copy and Video recording . 2) Apply the settings. 3) Create the HKEY_LOCAL_MACHINE\SYSTEMKey2\ key. Create the VALUE3 parameter of an arbitrary type with any value. Modify its value. 4) Create the Subkey2 subkey and the VALUE4 parameter in it. Modify the value of the parameter.	For Key2, all operations with the key and its subkeys and parameters appear in the log.
Monitoring the registry objects with shadow copying	
1) In the Observation → Shadow copy section of the DLP category, tick off Enable shadow copy . Leave the Local path to save copies of files field empty. This way, the copies are saved to C:\Program Files\SafenSoft\DLP Client\Backups\ 2) Create the HKEY_LOCAL_MACHINE\SYSTEMKey3 key and the VALUE5 parameter in it. 3) Create a rule for the registry and specify the path (\REGISTRY\MACHINE\SYSTEMKey3\###). Tick off the Change , Delete and Shadow copy checkboxes. 4) Apply the settings. 5) Modify the value of VALUE5. Make sure that the exported key	When you modify VALUE5, the entry about the modification of the key appears in the log. Clicking the pink field in this entry opens the backup copy. After you remove the key, one more entry with the second value (VALUE5) appears in the log.

Description	Expected result
(HKEY_LOCAL_MACHINE\SYSTEM\Key3) with the old value (VALUE5) appears in the directory with the backup copies. 6) Remove the key. Make sure that a copy of the key has been saved. 7) In the Observation → Shadow copy section of the DLP category, enter C:\copies\ to the Local path to save copies of files field. Repeat the first test and make sure the copies now appear in the specified directory.	

3.3 Keylogging

Table 4. Testing the keylogger

Description	Expected result
1) In the settings of the Log tab in SoftControl Admin Console, add the Keylogger data column, or enable the required filter: Filters → DLP Events Filters → Keylogger. Tick off Enable keylogger on the Collect data tab of the organization unit settings. 2) Apply the settings. 3) On the client computer, enter some text in various programs, for example, <i>Notepad.exe</i>, command line prompt, or Search in the Start menu.	The log in SoftControl Admin Console should contain entries with the entered text, in the Keylogger data field.

3.4 Monitoring external devices

To perform this test, you need a USB drive.

Table 5. Testing the connection of a USB drive

Description	Expected result
1) In the settings of the Log tab in SoftControl Admin Console, add the Device class and Device description columns. Tick off USB control on the Collect data tab of the organization unit settings. 2) Apply the settings. 3) Connect the USB drive. 4) Disconnect the USB drive.	The log should contain entries that the device has been connected and disconnected. The device type should appear in the Device class field; its name should appear in the Device description field.

3.5 Recording video

This testing checks how the file system objects are monitored with the help of video recording.

Table 6. Testing video recording

Description	Expected result
1) Create the C:\file10.txt file on the client computer. Create a rule to monitor it: specify the path (C:\file10.txt) and tick off Read , Change and Video recording . 2) Apply the settings. Modify the file. 3) In the Observation → Shadow copy section of the DLP category, set Recording duration to 15 sec, Frame rate delay to 500 ms, and Video frame width to 640 pixels. Repeat the first test.	When you modify the file, the entry about the modification of <i>file10.txt</i> appears in the log. Right-clicking the pink field in this entry opens a 15-sec video of the event.

4. Customer support

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