



SoftControl

Product line 4.4.12

Release notes

Introduction

Purpose

The 4.4.12 product line by Safe'N'Sec Corporation offers a set of program components for deploying the information security system. The system is designed to provide the integrity of the software environment of the network endpoints and to protect data against unauthorized access by maintenance staff or violators.

The following modules are included in the product line.

- SoftControl Service Center that consists of:
 - SoftControl Server, the server component;
 - SoftControl Admin Console, the management console.
- SoftControl ATM Client / Endpoint Client / SClient / SysWatch, the client components for proactive protection of self-service devices, corporate network workstations, servers, and personal computers, respectively;
- SoftControl DLP Client, the client component designed to monitor and collect data about the user's activity.

This document presents the main changes and new features included in version 4.4.12.

SoftControl Service Center

Improvements and new features:

1. Control activity rules for certain applications can be created in SoftControl Admin Console and then applied on client hosts with installed SoftControl SysWatch. The feature is disabled by default. To enable it, tick off **Use personal modules settings** in the **Client settings editor** window in SoftControl Admin Console.
2. Increased password security for SoftControl Service Center database and SoftControl SysWatch client components.
3. Improved signature algorithm for the configuration file that is used to update the components.
4. Updated versions of the third-party components (OpenSsl, etc.) used by SoftControl, in order to fix known vulnerabilities in these components.
5. Some options and buttons are updated.

Bug fixes:

1. The events in the data base were duplicated if they had associated notifications.
2. SoftControl Admin Console update error if the console and SoftControl Server have been installed on different computers.
3. Error that occurred when creating personal modules settings in SoftControl Admin Console and trying to apply them on client hosts with SoftControl SysWatch.
4. Fixed logic of decision making in case of a conflict between incident management settings and activity control rules for certain applications. Incident management settings now take precedence over activity control rules.

Fix:

Fixed in version 4.4.12.

SoftControl Admin Console

Improvements and new features:

1. Supported flags for files on the **Profile information for...** tab. The flags indicate whether a file was added to the profile by an installer or during profile gathering.
2. Sorting the client hosts by name is supported when creating a task.
3. Event logs are now more detailed and easier to understand. This includes improved format for

the information displayed in the **Action** field on the **Log** tab.

4. Improved logic for creating system reports. The groups of events are now called 'Threats' and 'Services and unsuspecting applications'. In the former case, SoftControl Admin Console logs control policy violations and the start of suspicious processes. In the latter case, SoftControl Admin Console logs service events and the start of unsuspecting processes.

Bug fixes:

1. Error when requesting detailed profile data (the **Profile information for...** tab) if the profile has not been created on the client host yet. An empty file is provided in this case.
2. The **Profile information for...** tab did not display all the files from the profile.
3. Error that occurred when different users were working with SoftControl Admin Console.
4. Error in the SoftControl Admin Console interface when creating control policy rules for certain applications.

Fix:

Fixed in version 4.4.12.

SoftControl Server

Bug fixes:

Error that occurred when updating common client certificate.

Fix:

Fixed in version 4.4.12.

SoftControl SysWatch

Improvements and new features:

1. Event logs are now more detailed and easier to understand. In particular, the report indicates whether an application is in the profile; whether it is a tracked application; if an installer has a valid digital signature; if global software update mode is enabled, and so on.
2. Improved format for the scan reports.
3. Improved logic for creating system reports. The groups of events are now called 'Threats' and 'Services and unsuspecting applications'. In the former case, SoftControl SysWatch logs control policy violations and the start of suspicious processes. In the latter case, SoftControl SysWatch logs service events and the start of unsuspecting processes.
4. 'Limited user' account cannot be assigned for trusted applications any more.
5. Increased password security for SoftControl SysWatch client components.
6. Fixed vulnerability associated with the msixexec installer. Executing the msixexec system installer from a folder other than %SYSTEM32% is blocked.
7. Fixed vulnerability in dll blocking algorithm (CVE-2018-5718). This vulnerability allowed local users to cause a denial of service (BSOD) or modify kernel-mode memory by loading a forged dll into a user-mode process. Fixed for versions starting from 4.4.1. Vulnerability occurs for versions earlier than 4.4.1.
8. Improved message that is displayed when processes are blocked after they are terminated.
9. Updated glossary that is used in the software. In particular, 'installation mode' is changed to 'software update mode', 'unknown installer' is changed to 'unsigned installer', and 'unknown application' is changed to 'non-profile application'. Some options and buttons are updated.
10. Updated user guides. This includes improved description of how SoftControl SysWatch works.

Bug fixes:

1. Invalid processing of the damaged file that contains the list of objects from the profile.
2. A number of errors in thread synchronization and in OS interaction. As a result, SoftControl SysWatch operation has improved. (Before the fix, OS hang and BSOD as well as false blocking by SoftControl SysWatch sometimes occurred.)
3. Invalid processing of the control policy violation incidents. (An operation was blocked even though it was allowed in the settings.)
4. Error that prevented the users from deleting files in the profile.

5. Error when saving the file with the system profile.
6. The user can now neither add a file to the profile nor delete a file from the profile if the **Use system profile** option is deselected or activity control for applications is disabled.
7. An application status displayed in the **Profile** column in the **Tracked applications** window did not correspond to the actual application status.

Fix:

Fixed in version 4.4.12.

SoftControl DLP Client

Bug fixes:

A number of errors in thread synchronization and in OS interaction. As a result, SoftControl DLP Client operation has improved. (Before the fix, OS hang and BSOD sometimes occurred.)

Fix:

Fixed in version 4.4.12.

Customer support

If you have any questions concerning the installation, setting up and operation of Safe'N'Sec Corporation products, please contact our customer support by e-mail support@safensoft.com.