SoftControl Service Center 6.0.98

Руководство администратора

Уважаемый пользователь!

ООО «АРУДИТ СЕКЬЮРИТИ» благодарит Вас за то, что выбрали продукт SoftControl Service Center. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl Service Center будет Вам полезен.

АВТОРСКИЕ ПРАВА

Материалы, приведенные в настоящем документе, являются собственностью ООО «АРУДИТ СЕКЬЮРИТИ» и могут быть использованы только для личных целей приобретателя продукта. Запрещается воспроизведение отдельных частей документа, внесение правок, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения компании и ссылки на источник.

Наименования и товарные знаки, приведённые в документе, являются собственностью своих законных владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Содержание данного документа может изменяться без предварительного уведомления. ООО «АРУДИТ СЕКЬЮРИТИ» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.

ООО «АРУДИТ СЕКЬЮРИТИ», 2021 г.

Почтовый адрес: 127106,Россия,Москва Нововладыкинский проезд, дом 8, стр. 3 ООО «АРУДИТ СЕКЬЮРИТИ»

Телефон: +7 (499) 201-55-12

Электронная почта: Общие вопросы и предложения: support@sns-control.ru Коммерческие вопросы: sales@sns-control.ru Веб-сайт компании: http://www.sns-control.ru

Содержание

1.	Введение	6
	1.1 Назначение	6
	1.2 Условные обозначения и термины	6
	1.2.1 Обозначения	6
	1.2.2 Сокращения	7
	1.2.3 Глоссарий	7
2.	Требования к аппаратному и программному обеспечению	9
	2.1 Системные требования SoftControl Server	9
	2.2 Системные требования SoftControl Admin Console	9
3.	Установка и настройка компонентов SoftControl Service Center	11
	3.1 Установка SoftControl Server и SoftControl Admin Console	11
	3.1.1 Обычная установка	11
	3.1.2 Полная установка	14
	3.1.3 Выборочная установка	
	3.2 Настройка сервера	21
	3.3 Регистрация клиентских приложений	27
	3.4 Подключение к серверу из консоли управления	27
4.	Централизованное управление СИБ	30
	4.1 Интерфейс SoftControl Admin Console	
	4.2 Порядок работы	
	4.3 Управление доступом на основе ролей	
	4.3.1 Роли	
	4.3.2 Пользователи	
	4.3.3 События безопасности сервера	
	4.4 Клиенты	
	4.4.1 Управление процессом регистрации	
	4.4.2 Перемещение в подразделения	
	4.5 Подразделения	
	4.5.1 Управление подразделениями	
	4.5.2 Генерация одноразовых паролей	
	4.6 Настройка клиентских приложений	
	4.6 Настройка клиентских приложений 4.6.1 Общие настройки	59 62
	 4.6 Настройка клиентских приложений	
	 4.6 Настройка клиентских приложений. 4.6.1 Общие настройки	

4.7 Профили безопасности	
4.8 Задачи	
4.8.1 Сбор профиля	
4.8.2 Антивирусное сканирование	
4.8.3 Обновление	
4.8.4 Выполнение команд на клиенте и обмен файлами с клиентом	
4.8.4.1 Создание задачи	
4.8.4.2 Описание работы команд	
4.8.4.5 Результаты выполнения команд	
4.9 TIPOCMOTP OTGETOB	
4.9.1 OTHETE SOFCONTROL DLP Client	
493 Отчеты SoftControl SvsCmd	155
4.9.4 Интегрированный лог событий	
4.9.5 Фильтрация событий	
4.9.6 Запросы к базе данных	
4.9.7 Печать и экспорт в файлы отчётов	
4.9.8 Резервное копирование отчетов	
4.9.9 Оправка сообнии по протоколу Sysiog	
4.10 Onobemeend 0 coobinast	
4.10.1 КОНТАКТЫ 4.10.2 Нотификации	
4 11 Снимки конфигурации	178
4 11 1 Снимки	179
4.11.2 Задачи снимков	
5. Обновление компонентов СИБ	185
5.1 Настройка обновления программных модулей	
5.2 Настройка обновления антивирусных баз	
5.3 Обновление SoftControl Server и SoftControl Admin Console в ручном реж	киме191
5.4 Обновление клиентских компонентов	
6. Удаление компонентов SoftControl Service Center	195
7. Диагностика проблем	199
8. Техническая поддержка	203
9. Приложение	204
9.1 Установка и настройка PostgresQL 9.5	
9.2 Установка и настройка Microsoft® SQL Server® 2008	
9.3. Лобавление компонента Desktop Experience	200

230
230
232
233
234
234
236
237
239
242
242

1. Введение

1.1 Назначение

SoftControl Service Center («Сервисный Центр») представляет собой набор инструментов администрирования для управления системой информационной безопасности, обеспечивающей сохранение целостности программной среды конечных точек сети, защиту от несанкционированного доступа к данным со стороны персонала или злоумышленников, а также мониторинг активности пользователей. В состав Сервисного Центра входят следующие компоненты:

- SoftControl Server серверный компонент;
- SoftControl Admin Console консоль управления.

SoftControl Service Center поддерживает работу со следующими клиентскими компонентами:

- SoftControl ATM Client / Endpoint Client / SClient (далее по тексту SoftControl SysWatch) – клиентские компоненты проактивной защиты устройств самообслуживания, рабочих станций корпоративной сети и серверов соответственно;
- SoftControl DLP Client клиентский компонент мониторинга и сбора данных;
- SoftControl SysCmd клиентский компонент для выполнения команд на удаленном компьютере и обмена с ним файлами;
- SoftControl DeCrypt клиентский компонент для шифрования системных дисков устройств самообслуживания, рабочих станций корпоративной сети и серверов.

1.2 Условные обозначения и термины

1.2.1 Обозначения

Условные обозначения, применяемые в данном документе, приведены в табл. 1.

Пример обозначения	Описание
1	Важная информация.
Условие	Условие выполнения, примечание, пример.
Обновить	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов

Таблица 1. Условные обозначения

	программного интерфейса.
	– термины (определения);
Политика контроля	– имена файлов и других объектов;
	– тексты сообщений, выводимых пользователю.
C:\Program Files\SoftControl	Пути к файлам, каталогам, ключам системного реестра.
%windir%\system32 \msiexec.exe /i	Фрагменты программного кода, командных и конфигурационных файлов.
<каталог установки SoftControl Service Center	Поля для замены функциональных названий фактическими значениями.
<u>Приложение</u> (6)	Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса).

1.2.2 Сокращения

В данном документе употребляются без расшифровки следующие сокращения:

- ✤ БД база данных;
- ◆ ГИП графический интерфейс пользователя;
- ОЗУ оперативное запоминающее устройство;
- OC операционная система;
- ПО программное обеспечение;
- СИБ система информационной безопасности;
- СУБД система управления базами данных;
- ✤ ЦП центральный процессор;
- ✤ ЭЦП электронная цифровая подпись.

1.2.3 Глоссарий

Таблица 2. Глоссарий

Термин	Пояснение
	Комплекс мер по предотвращению вредоносных воздействий, основанный
проактивная защита	на превентивных технологиях.
Превентивные технологии	Передовые технологии защиты данных, в основе которых лежит анализ активности на компьютере пользователя: действий любых приложений, служб операционной системы, действий пользователя, активности извне и т.д. В отличие от реактивных технологий, на которых построены такие средства защиты, как антивирусы и персональные сетевые экраны, превентивные технологии анализируют не код объекта, а отслеживают потенциально опасные действия, выполняемые им. Следовательно, инструменты проактивной защиты не требуют наличия и постоянного обновления баз вредоносного кода, что является необходимым для традиционных средств защиты.
Реактивные (сигнатурные)	Метод работы антивирусного программного обеспечения и систем
технологии	обнаружения вторжений, при котором программа в процессе анализа

	объекта обращается к базе данных известных вирусов и проверяет соответствие какого-либо участка кода просматриваемого объекта известному коду (сигнатуре) вируса в базе данных.
Политика контроля	Целостный набор правил контроля активности .
Правило контроля активности	Набор условий, определяющих действие приложения и реакцию на него SoftControl SysWatch.
Профиль системы	База данных, хранящаяся локально на клиентском хосте и содержащая контрольные суммы исполняемых модулей. Профиль системы создается в результате автоматической настройки SoftControl SysWatch (операция сбора профиля).
Приложение в профиле	Приложение, контрольная сумма которого есть в профиле системы.
Отслеживаемое приложение	Приложение, факт запуска которого SoftControl SysWatch обнаружил на клиентском хосте в процессе работы с момента установки.
Доверенное приложение	Отслеживаемое приложение из доверенной зоны выполнения.
Ограниченное приложение	Отслеживаемое приложение из ограниченной зоны выполнения.
Запрещенное приложение	Отслеживаемое приложение из запрещенной зоны выполнения . SoftControl SysWatch запрещает запуск таких приложений на клиентском хосте.
Зона выполнения (доверенная, ограниченная, запрещенная)	Отдельная политика контроля, применяемая к подмножеству отслеживаемых приложений. Всего на каждом клиентском хосте имеется 3 зоны выполнения: доверенная, ограниченная, запрещенная. Любое отслеживаемое приложение принадлежит к одной из этих трех зон выполнения.
Инсталлятор	Приложение, которое SoftControl SysWatch эвристически определил как программу, предназначенную для установки других программ, или которое пользователь пометил как инсталлятор. Инсталлятор имеет особые привилегии по запуску (см. ниже «Режим обновления ПО»).
Режим обновления ПО	Режим запуска приложения, при котором происходит помещение в профиль системы самого приложения и всех созданных или измененных им РЕ- файлов. Дочерние процессы данного приложения наследуют режим обновления ПО.
V.I.P.O. (Valid Inside Permitted Operations)	Учетная запись пользователя с ограниченными правами (ограниченный набор системных привилегий, отсутствие доступа к системным объектам). Служит для организации песочницы при запуске приложений и обеспечивает дополнительную защиту от потенциальных вредоносных воздействий приложений, которым нельзя полностью доверять. Запуск с использованием учетной записи V.I.P.O. можно устанавливать только для ограниченных приложений.
Роль	Совокупность прав пользователя на использование отдельных функций SoftControl Admin Console.
РЕ-файл	Исполняемый файл в формате PE (Portable Executable). Данный формат используется в операционных системах семейства Microsoft® Windows® для исполняемых файлов (EXE), динамических библиотек (DLL) и некоторых других типов файлов.
Клиентский хост	Средство вычислительной техники (рабочая станция, сервер, терминал самообслуживания), на котором установлен SoftControl SysWatch.

2. Требования к аппаратному и программному обеспечению

2.1 Системные требования SoftControl Server

Таблица 3. Минимальные системные требования

ос	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			
Microsoft® Windows® 7 (SP1) 32-разрядная/64-разрядная Microsoft® Windows® 8, 32-разрядная/64-разрядная			
Microsoft® Windows® 8.1 32-разрядная/64-разрядная			
Microsoft® Windows® 10 32-разрядная/64-разрядная			100 МБ
Серверные операционные системы:	3 ГГц	4 ГБ	дополнительно
Microsoft® Windows® Server 2008 (SP2) 32-разрядная/64- разрядная			4 Г В в случае установки встроенной СУБЛ
Microsoft® Windows® Server 2008 R2 64-разрядная			вопростной сувд
Microsoft® Windows® Server 2012 64-разрядная			
Microsoft® Windows® Server 2012 R2 64-разрядная			
Microsoft® Windows® Server 2016 64-разрядная			
Microsoft® Windows® Server 2019 <i>64-разрядная</i>			

Дополнительные требования:

- Требуется Microsoft® .NET Framework 4.5.
- Поддерживаемые СУБД: PostgreSQL® 9.5, Microsoft® SQL Server® 2008, SQL Server® 2012, SQL Server® 2014 SP1, SQL Server® 2016, SQL Server® 2017.
- Для работы SQL Server® 2014 SP1 или SQL Server® 2012 на Windows Server 2008 R2 в ОС должен быть установлен пакет обновления SP1.
- Для серверных операционных систем поддерживаются только варианты установки ОС с рабочим столом.

2.2 Системные требования SoftControl Admin Console

ос	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			
Microsoft® Windows® 7 (SP1) 32-разрядная/64-разрядная	З ГГц	4 ГБ	100 МБ
Microsoft® Windows® 8 32-разрядная/64-разрядная			
Microsoft® Windows® 8.1 32-разрядная/64-разрядная			

Требования к аппаратному и программному обеспечению

Microsoft® Windows® 10 32-разрядная/64-разрядная
Серверные операционные системы:
Microsoft® Windows® Server 2008 (SP2) <i>32-разрядная/64- разрядная</i>
Microsoft® Windows® Server 2008 R2 64-разрядная
Microsoft® Windows® Server 2012 64-разрядная
Microsoft® Windows® Server 2012 R2 64-разрядная
Microsoft® Windows® Server 2016 <i>64-разрядная</i>
Microsoft® Windows® Server 2019 64-разрядная

Дополнительные требования:

- Microsoft® .NET Framework 4.5.
- Для серверных операционных систем поддерживаются только варианты установки ОС с рабочим столом с установленным компонентом Desktop Experience.

3. Установка и настройка компонентов SoftControl Service Center

В настоящем разделе приведена информация по <u>установке</u>⁽¹¹⁾ серверного компонента SoftControl Server («сервера») и консоли управления SoftControl Admin Console, <u>настройке</u>⁽²¹⁾ SoftControl Server при первом <u>запуске</u>⁽²⁷⁾ SoftControl Admin Console, а также даны указания по <u>регистрации клиентских приложений</u>⁽²⁷⁾.

3.1 Установка SoftControl Server и SoftControl Admin Console

Возможны следующие варианты развертывания SoftControl Service Center:

- <u>обычная</u>⁽¹¹⁾: установка компонентов продукта без встроенной СУБД;
- полная (14): установка компонентов продукта и встроенной СУБД;
- выборочная⁽¹⁸⁾: установка выбранных пользователем компонентов.

Если в сетевом доступе имеется настроенная СУБД или если ее планируется установить отдельно, выберите вариант обычной установки. Информация по отдельной установке СУБД дана в приложении²⁰⁸.

Для наиболее быстрого развертывания и настройки выберите вариант полной установки; в этом случае все необходимые действия, включая установку входящей в инсталлятор СУБД, выполняются установщиком SoftControl Service Center автоматически. В пакет установки SoftControl Service Center входит бесплатная СУБД Microsoft® SQL Server® 2014 Express SP1, обладающая всей необходимой функциональностью для работы сервера.

Если предпочтительно устанавливать серверный компонент, СУБД и консоль управления на разные компьютеры, используйте выборочную установку.

3.1.1 Обычная установка

- 1) Запустите установочный пакет Service. Center. msi.
- 2) В окне Установка SoftControl Service Center нажмите на кнопку Далее (рис. <u>Запуск</u> программы установки⁽¹¹⁾).



Рисунок 1. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного** соглашения и нажмите на кнопку **Далее** (рис. <u>Лицензионное соглашение</u>⁽¹²⁾).

ИЦЕНЗИОННОЕ СОГЛАШЕНИЕ . Предмет соглашения Настоящее лицензионное соглашение (далее Соглашение) является оридическим документом, заключаемым между ООО « АРУДИТ ЕКЬЮРИТИИ» (далее - Правообладатель) и Вами, физическим или оридическим лицом (далее - Пользователь), правомерно владеющим кземпляром программного продукта группы "SoftControl" (далее - Программный продукт).					0.0
. Предмет соглашения lacтоящее лицензионное соглашение (далее Соглашение) является ppидическим документом, заключаемым между ООО « АРУДИТ EKЬЮРИТИ » (далее - Правообладатель) и Вами, физическим или ppидическим лицом (далее - Пользователь), правомерно владеющим иземпляром программного продукта группы "SoftControl" (далее - lporpаммный продукт). станавливая, копироя, загружая или иным образом используя ¥	ПИЦЕНЗИОННОЕ СС	оглашение			^
Пастоящее лицензионное соглашение (далее Соглашение) является оридическим документом, заключаемым между ООО « АРУДИТ ЕКЬЮРИТИ » (далее - Правообладатель) и Вами, физическим или оридическим лицом (далее - Пользователь), правомерно владеющим изземпляром программного продукта группы "SoftControl" (далее - Программный продукт). Станавливая, копироя, загружая или иным образом используя у	1. Предмет согла	шения			
	оридическим док	ументом, заклю	чаемым межд	y OOO « AF	рудит

4) Выберите тип установки **Обычная**, нажав на соответствующую кнопку (рис. <u>Типы</u> установки ⁽¹²⁾).

😸 Установка SoftControl Service Center	_ • •
Выберите тип установки Укажите наиболее подходящий тип установки	SoftControl
Обычная Устанавливает самые распространенные компоненть Рекомендуется для большинства пользователей. Выборочная Позволяет выбирать для установки отдельные комп их местонахождение. Рекомендуется для опытных п Подная Устанавливает все компоненты программы. Этот вар больше всего места на диске.	і программ. оненты и задавать ользователей. иант требует
<u>Н</u> азад Дал	отмена

Рисунок 3. Типы установки

5) Нажмите на кнопку Установить (рис. Готовность к установке 13).

😸 Установка SoftControl Service Center	
Все готово к установке SoftControl Service Center	SoftControl
Нажмите кнопку "Установить", чтобы начать установку. Наж чтобы проверить или изменить параметры установки. Нажмит чтобы выйти из мастера.	мите кнопку "Назад", ге кнопку "Отмена",
<u>Н</u> азад 😵 Установ	вить Отмена

Рисунок 4. Готовность к установке

6) Дождитесь окончания процесса установки (рис. Процесс установки 13).

😸 Установка SoftControl Service Center	_ • •
Установка SoftControl Service Center	SoftControl
Подождите, пока мастер установки устанавливает SoftCon	trol Service Center.
Состояние: Копирование новых файлов	
<u>Н</u> азад	<u>Да</u> лее Отмена

Рисунок 5. Процесс установки

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. <u>Завершение установки</u>⁽¹⁴⁾).



Рисунок 6. Завершение установки

3.1.2 Полная установка

- 1) Запустите установочный пакет Service. Center. msi.
- 2) В окне Установка SoftControl Service Center нажмите на кнопку Далее (рис. <u>Запуск</u> программы установки⁽¹⁴⁾).



Рисунок 7. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее** (рис. Лицензионное соглашение⁽¹⁵⁾).

👹 Установка SoftControl Service Center	_			×
Лицензионное соглашение Внимательно прочитайте следующее лицензионное соглашение	So	ftC	Cont	trol
лицензионное соглашение 1. Предмет соглашения				^
Настоящее лицензионное соглашение (далее Соглаше юридическим документом, заключаемым между ООО ТЕХНОЛОДЖИ» (далее - Правообладатель) и Вами, фр юридическим лицом (далее - Пользователь), правомер экземпляром программного продукта группы "SoftCor Программный продукт). Устанавливая, копируя, загружая или иным образ	:ние) «П 13иче 10 вл 1trol" 0м	явл РОТЕН ским адек (дал испол	яется КШЕН ощим ощим лее - льзуя	~
☑ Я принимаю условия лицензионного соглашения				
Печать Назад Дале	e		Отмен	на
Рисунок 8. Лицензионное согла	ше	ни	е	

4) Выберите тип установки **Полная**, нажав на соответствующую кнопку (рис. <u>Типы</u> установки ⁽¹⁵⁾).

岃 Установка SoftControl Service Center	- • -
Выберите тип установки Укажите наиболее подходящий тип установки	SoftControl
Обычная Устанавливает самые распространенные компоненть Рекомендуется для большинства пользователей. Выборочная Позволяет выбирать для установки отдельные компо их местонахождение. Рекомендуется для опытных по Подная Устанавливает все компоненты программы. Этот вар больше всего места на диске.	і программ. оненты и задавать ользователей. иант требует
<u>Н</u> азад Дал	ее Отмена

Рисунок 9. Типы установки

5) Нажмите на кнопку Установить (рис. Готовность к установке 16).

😸 Установка SoftControl Service Center	
Все готово к установке SoftControl Service Center	SoftControl
Нажните кнопку "Установить", чтобы начать установку. Наж чтобы проверить или изменить параметры установки. Нажнит чтобы выйти из мастера.	чите кнопку "Назад", 'е кнопку "Отмена",
<u>Н</u> азад 🕅 😵 Установ	вить Отмена

Рисунок 10. Готовность к установке

6) Дождитесь окончания процесса установки (рис. Процесс установки 16).

😸 Установка SoftControl Service Center	
Установка SoftControl Service Center	SoftControl
Подождите, пока мастер установки устанавливает SoftCont	rol Service Center.
Состояние: Копирование новых файлов	
<u>Н</u> азад	<u>Да</u> лее Отмена

Рисунок 11. Процесс установки

7) После появления сообщения Установка SoftControl Service Center завершена нажмите на кнопку Готово, чтобы начать установку Microsoft® SQL Server® 2014 Express SP1 (рис. <u>Завершение установки SoftControl Service Center</u>¹⁷).



Рисунок 12. Завершение установки SoftControl Service Center

8) Дождитесь окончания установки Microsoft® SQL Server® 2014 Express SP1 и нажмите на кнопку **OK** (рис. <u>Завершение установки</u>¹⁷).



Рисунок 13. Завершение установки

3.1.3 Выборочная установка

- 1) Запустите установочный пакет Service. Center. msi.
- 2) В окне Установка SoftControl Service Center нажмите на кнопку Далее (рис. <u>Запуск</u> программы установки⁽¹⁸⁾).



Рисунок 14. Запуск программы установки

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного** соглашения и нажмите на кнопку **Далее** (рис. <u>Лицензионное соглашение</u>⁽¹⁸⁾).

	· · · · · · · · · · · · · · · · · · ·	$\cap - ((\cap + - + - + + - + + - + + + - +$	\mathbf{O}
กลนดะหล II นลกท		Sotti optrol	Service Center

Знимательно прочитайте следующее лицензионное соглашение SoftCc	onti
ИЦЕНЗИОННОЕ СОГЛАШЕНИЕ	^
. Предмет соглашения Іастоящее лицензионное соглашение (далее Соглашение) являе уридическим документом, заключаемым между ООО «ПРОТЕКШ ЕХНОЛОДЖИ» (далее - Правообладатель) и Вами, физическим и оридическим лицом (далее - Пользователь), правомерно владеющ иземпляром программного продукта группы "SoftControl" (дален Программный продукт). Станавливая, копируя, загружая или иным образом исполь	тся ІЕН им ≥ -
Я принимаю условия лицензионного соглашения	

Рисунок 15. Лицензионное соглашение

4) Выберите тип установки **Выборочная**, нажав на соответствующую кнопку (рис. <u>Типы</u> <u>установки</u>⁽¹⁹⁾).

😸 Установка SoftControl Service Center	
Выберите тип установки Укажите наиболее подходящий тип установки	SoftControl
Обычная Устанавливает самые распространенные компоненты Рекомендуется для большинства пользователей. Выборочная Позволяет выбирать для установки отдельные компо их местонахождение. Рекомендуется для опытных по	программ. менты и задавать льзователей.
Подная Устанавливает все компоненты программы. Этот вари больше всего места на диске.	ант требует
<u>Н</u> азад Дале	ее Отмена

Рисунок 16. Типы установки

5) Настройте конфигурацию установки компонентов (рис. <u>Конфигурация установки</u> <u>компонентов</u>⁽²⁰⁾): нажмите на пиктограмму у компонента, который не требуется устанавливать, и в выпадающем меню выберите опцию Компонент будет полностью недоступен (рис. <u>Опции установки компонента</u>⁽²⁰⁾). Для устанавливаемого компонента должна быть выбрана опция Будет установлен на локальный жесткий диск (рис. <u>Опции установки компонента</u>⁽²⁰⁾). При необходимости измените путь установки по умолчанию, нажав на кнопку Обзор. С помощью кнопки Использование диска можно просмотреть суммарный размер устанавливаемых компонентов и доступное место на

жестком диске. После того как все установки завершены, нажмите на кнопку Далее.

🗒 Установка SoftControl Service Center	- • •			
Выборочная установка Укажите конфигурацию установки компонентов.	SoftControl			
Для изменения параметров установки какого-либо компонента щелкните соответствующий значок в расположенном ниже дереве.				
SoftControl Server SoftControl Server 20 SoftControl Admin Console	rver			
Для компонен- на жестком ді подкомпонент подкомпонент на жестком ді	нта требуется 29МБ иске. Выбрано тов: 0 из 1. Для тов требуется 0КБ иске.			
Mecтоположе C:\Program Files (x86)\SafenSoft\Service Обзор Center\Server\				
Сброс Использование диска Назад И	Далее Отмена			

Рисунок 17. Конфигурация установки компонентов



6) Выберите опцию Добавить необходимые порты в исключения Брандмауэра Windows для автоматического добавления порта связи между SoftControl Admin Console и SoftControl Server в исключения брандмауэра (рис. Опция добавления порта в исключения брандмауэра⁽²⁰⁾). В обратном случае будет необходимо произвести эту операцию вручную (по умолчанию используется порт 8080). Для продолжения установки нажмите на кнопку Далее.



Рисунок 19. Опция добавления порта в исключения брандмауэра

7) В случае выбора установки SoftControl Admin Console и/или SoftControl Server без встроенной СУБД повторите действия 5-7 для <u>обычной установки⁽¹³⁾</u>. Если устанавливается SoftControl Server с подкомпонентом *Microsoft SQL Server*® 2014 *Express SP1*, повторите действия 5-8 для полной установки⁽¹⁶⁾.

3.2 Настройка сервера

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В случае несконфигурированного сервера в появившемся окне введите IP-адрес компьютера с установленным SoftControl Server в поле **Адрес сервера** (допускается указывать зарезервированное имя *localhost*, если SoftControl Server и SoftControl Admin Console установлены на одном компьютере) и нажмите на кнопку **Применить** (рис. Первый запуск SoftControl Admin Console⁽²¹⁾).

🔀 Авторизация		×
Адрес сервера:	localhost	Изменить
Имя пользователя:		
Пароль:		
	Приме	Отмена

Рисунок 20. Первый запуск SoftControl Admin Console

В диалоговом окне с предложением создания первичной конфигурации сервера выберите **Да** (рис. <u>Предложение запуска мастера настройки</u>⁽²²⁾).



Рисунок 21. Предложение запуска мастера настройки

В окне мастера настройки сервера в разделе **База данных** задаются параметры подключения к СУБД и имя БД, которая будет использоваться серверным компонентом SoftControl Server. Введите следующие параметры (в скобках указаны значения по умолчанию для PostgreSQL):

- SQL Provider тип СУБД (PostgreSQL);
- Сервер СУБД сетевой адрес (имя) сервера СУБД (localhost);
- Порт номер порта для работы сервера (5432);
- Имя базы данных имя БД на сервере СУБД (tpsecure);
- Пользователь имя пользователя на сервере СУБД (postgres);
- Пароль пароль пользователя на сервере СУБД.

Mастер настройки сервера	ĸ
База данных	
SQL провайдер:	٦
PostgreSQL	
Сервер СУБД:	
localhost	
Порт:	
5432	
Имя базы данных:	
tpsecure	
Пользователь:	
postgres	
Пароль:	
•••••	
Проверить соединение	
Хост клиентов	
Пользователь	
	1
Значения всех параметров корректны	
Настроить Отмена	

Рисунок 22. Настройка подключения к СУБД PostgreSQL

🚩 Мастер настройки сервера	×		
База данных			
SQL провайдер:			
MSSQL			
Сервер СУБД:			
localhost\SQLTPS			
Имя базы данных:			
safensoft.tpsecure			
Тип авторизации:			
Авторизация SQL Server			
Пользователь:			
Пароль:			
Проверить соединение			
Хост клиентов			
Пользователь			
	Настроить Отмена		
Рисунок 23. Настройка подключения к СУБД MS SQL			

Server

Для проверки соединения с СУБД и корректности данных учетной записи нажмите на кнопку **Проверить соединение**. Если БД с указанным именем не существует, то она будет создана на сервере СУБД по окончании работы мастера настройки.

В разделе **Хост клиентов** определяются параметры подключения клиентских приложений к серверу (рис. <u>Настройка подключения клиентских приложений к серверу</u>⁽²⁴⁾).

🔀 Мастер настройки сервера 🛛 🗙					
База данных					
Хост клиентов					
Список IP адресов с	Список IP адресов сервера				
Введите новое значение:					
	Добавить в список				
172.16.16.5					
VM-AS-W61RUX86					
	Удалить из списка				
Порт сервера:					
8000					
Лобавить порт в исключения брандмаузра					
Дооавить порт в исключения орандмауэра					
Пользователь					
Значения всех параметров корректны					
	Настроить Отмена				
	Inderpointe Conventa				

Рисунок 24. Настройка подключения клиентских приложений к серверу

По умолчанию для связи с сервером используется его текущий IP-адрес и порт 8000 протокола ТСР. Возможно также осуществлять взаимодействие клиентских приложений с сервером по нескольким резервным каналам. Данная функция реализуется путем задания всех IP-адресов или имен (DNS, NetBIOS), по которым сервер доступен для клиентских приложений. В этом случае клиентский компонент осуществляет поочередное подключение по каждому из адресов до первой успешной обработки запроса, после чего связь с сервером устанавливается по данному адресу. Если подключиться ни по одному из адресов не удалось, то клиентский компонент повторяет перебор адресов по истечении интервала обращения к серверу. Чтобы добавить адрес в перечень, введите новое значение в соответствующем поле и нажмите на кнопку Добавить в список. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку Удалить из списка. В поле Порт сервера укажите порт связи клиентских приложений с сервером (в случае установки SoftControl Server и SoftControl Admin Console на один компьютер данный порт не должен совпадать с портом связи SoftControl_Server и SoftControl Admin Console⁽²⁸⁾). Установите флажок Добавить порт в исключения Брандмауэра Windows в том случае, если исключение на выбранный порт отсутствует в брандмауэре.

Настоятельно рекомендуется указывать имя сервера в списке адресов, чтобы приложения СВЯЗИ С сервером клиентские не теряли даже в случае автоматической IP-адреса. Если это смены его все же произошло, воспользуйтесь указаниями по восстановлению связи 233.

В разделе **Пользователь** создайте учетную запись первого пользователя, введя **Имя пользователя**, **Пароль** и **Подтверждение пароля** (рис. <u>Создание пользователя</u>⁽²⁶⁾). Данный пользователь будет иметь права администратора.

<u>Примечание</u>. В дальнейшем пароль пользователя можно будет сменить, нажав на кнопку Смена пароля в правом нижнем углу SoftControl Admin Console на любой открытой вкладке (см. раздел <u>Пользователи</u>⁴⁰).

Мастер настройки сервера
База данных
Хост клиентов
Пользователь
Имя пользователя:
Console_admin
Пароль:
•••••
Подтверждение пароля:
•••••
Настроить Отмена

Рисунок 25. Создание пользователя

После того как все настройки введены, нажмите на кнопку **Настроить**. В случае успешного создания конфигурации отобразится соответствующее уведомление (рис. Успешное создание конфигурации²⁶).



Рисунок 26. Успешное создание конфигурации

В <u>окне авторизации ⁽²⁷⁾</u> используйте данные созданной учетной записи для подключения к серверу SoftControl Server.

3.3 Регистрация клиентских приложений

После того как сервер прошел <u>первичную настройку</u>⁽²¹⁾, на компьютере с установленным SoftControl Server формируется зашифрованный конфигурационный файл по следующему пути:

C:\ProgramData\SafenSoft\ClientSettings.xmlc

Данный файл содержит параметры подключения клиентских приложений к серверу, а также <u>общий клиентский сертификат</u>²³⁰, используемый по умолчанию для установления безопасного соединения. Для регистрации в SoftControl Service Center необходимо применить указанный файл на устройствах с предварительно установленными по документации клиентскими приложениями.

В режиме ожидания регистрации соединение с сервером осуществляется с использованием общего клиентского сертификата, при этом не происходит передача данных от клиента к серверу. Взаимодействие осуществляется в штатном режиме после перехода клиентского компонента в <u>статус</u>⁽⁴⁵⁾ **Активен**.

Подробные действия по применению файла описаны в документах «Руководство пользователя SoftControl ATM Client / Endpoint Client / SClient» и «Руководство по установке SoftControl DLP Client» для соответствующих компонентов.

3.4 Подключение к серверу из консоли управления

Для запуска консоли управления откройте ярлык SoftControl Admin Console на рабочем столе. В окне Авторизация введите Адрес сервера, Имя пользователя и Пароль, выберите Токен и введите его PIN-код (рис. <u>Авторизация пользователя в SoftControl</u> Admin Console²⁷).

🚩 Авторизация		×
Адрес сервера:	localhost Измените	•
Имя пользователя:	console_admin	
Пароль:	•••••	
	Применить Отмена	

Рисунок 27. Авторизация пользователя в SoftControl Admin Console

Нажмите на кнопку Применить, чтобы подключиться к серверу SoftControl Server.

При аутентификации пользователя на сервере создается сессия, имеющая уникальный идентификатор. Вся работа пользователя с консолью управления осуществляется в рамках данной сессии, при этом с постоянной периодичностью проверяется наличие соединения между сервером и консолью управления. Если консоль управления недоступна для сервера более чем 2 минуты, то текущая сессия прекращается.

Для связи между SoftControl Admin Console и SoftControl Server по умолчанию используется порт 8080 протокола TCP. Если по какой-либо причине данный порт использовать не удается, измените его значение в файлах конфигурации серверного компонента и консоли управления.
Файл конфигурации сервера расположен по следующему пути:
С:\ProgramData\SafenSoft\Server.Config.xml
Значение порта задается в атрибуте *Port* элемента *WebApiHost*.
Файл конфигурации консоли управления расположен по следующему пути:
C:\ProgramData\SafenSoft\SafenSoft.Enterprise.Console.exe.Config
Значение порта задается в следующем участке файла:

<databases></databases>		
<elements></elements>		
<add <="" name="<номер порта>" th=""><th>lastconnection="" /></th><th></th></add>	lastconnection="" />	

При первом подключении с использованием токена SoftControl Service Center выводит сообщение о необходимости привязки учетной записи пользователя к токену (см. рис. <u>ниже⁽²⁸⁾</u>). Нажмите на кнопку **Да**, чтобы войти в систему и приступить к <u>централизованному управлению СИБ⁽³⁰⁾</u>.



Рисунок 28. Сообщение о привязке учетной записи к токену.

Вы можете поменять токен, к которому была привязана учетная запись, в окне авторизации (см. <u>выше⁽²⁷⁾</u>) или на любой открытой вкладке SoftControl Admin Console, нажав на кнопку **Смена токена** в правом нижнем углу.

Если число попыток подключения превышает заданное значение (5 по умолчанию), учетная запись пользователя блокируется. Значение выставляется в конфигурационном файле сервера с помощью параметра *PasswordAttempts*. Время действия блокировки (в секундах) задается с помощью параметра *LockForSeconds*. Разблокировать учетную запись может только системный администратор.

Кроме того, учетная запись блокируется, если она не использовалась в течение 45 дней (кроме пользователей с ролью Системный администратор).

Если в течение 5 минут пользователь не совершал никаких действий, его сеанс блокируется. Для возобновления работы необходимо авторизоваться повторно.

4. Централизованное управление СИБ

Удаленное централизованное управление клиентскими приложениями SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd осуществляется из консоли управления SoftControl Admin Console на базе сервисных функций, предоставляемых серверным компонентом SoftControl Server.

Данный раздел посвящен работе с SoftControl Admin Console и предназначен для администраторов системы информационной безопасности (далее по тексту – «СИБ») на основе SoftControl Service Center.

4.1 Интерфейс SoftControl Admin Console

Интерфейс консоли управления SoftControl Admin Console состоит из главного окна программы, в котором имеются следующие вкладки:

- <u>Лог событий ¹⁴³</u>;
- <u>События безопасности⁽⁴²⁾;</u>
- Интегрированный лог событий⁽¹⁵⁷);
- <u>Клиенты</u>⁴⁵;
- Настройки клиентов⁵⁹;
- Профили безопасности¹²⁵;
- Подразделения⁵³;
- <u>Задачи</u>¹²⁷;
- Пользователи⁽³⁷⁾;
- Роли³⁵;
- Контакты¹⁷⁰;
- Управление нотификациями⁽¹⁷¹⁾;
- <u>Обновлен</u>ия¹⁸⁵;
- Снимки конфигурации¹⁷⁸

Перечисленным выше вкладкам соответствуют графические кнопки, расположенные в верхней части главного окна SoftControl Admin Console под основным меню. Кроме того, вкладки <u>Клиенты⁴⁵</u>, <u>Лог событий¹⁴³</u>, <u>События безопасности⁴²</u>, <u>Интегрированный лог событий¹⁵⁷</u>, <u>Подразделения⁵³</u>, <u>Настройки клиентов⁵⁹, <u>Профили безопасности¹²⁵</u>, <u>Задачи</u>¹²⁷, <u>Контакты¹⁷⁰</u> и <u>Управление нотификациями¹⁷¹</u> имеют свои графические кнопки,</u>

область действия которых распространяется только на данные вкладки. Основные кнопки SoftControl Admin Console описаны в табл. 5.

Таблица 5. Элементы у	правления SoftControl Admin Console
-----------------------	-------------------------------------

Кнопка	Название	Описание	Горячие клавиши
8	Лог событий	Вызов вкладки Лог для всех клиентских компонентов.	
S	События безопасности	опасности Вызов вкладки События безопасности.	
	Интегрированный лог событий	Вызов вкладки Интегрированный лог событий	
1	Клиенты	Вызов вкладки Клиенты .	F4
1	Настройки клиентов	Вызов вкладки Настройки клиентов .	
	Профили безопасности	Вызов вкладки Профили безопасности .	
杰	Подразделения	Вызов вкладки Подразделения .	
	Задачи	Вызов вкладки Задачи .	
	Пользователи	Вызов вкладки Пользователи .	
88	Роли	Вызов вкладки Роли .	
@	Контакты	Вызов вкладки Контакты .	
-	Управление нотификациями	Вызов вкладки Нотификации .	
2	Обновить	Обновление информации в текущей вкладке.	F5
	Выбрать колонки	Изменение состава полей таблицы текущей вкладки.	F6
	Сохранить настройки вида	Сохранение выбранного набора колонок в качестве пользовательского фильтра. Применима только к вкладке Лог .	F2
4	Печать	Вывод текущего списка устройств или выборки событий на печать.	Ctrl + P
	Экспорт в Excel	Экспорт текущего списка устройств или выборки событий в файл формата XLSX (Microsoft® Excel®).	Ctrl + E
	Снимки конфигурации Вызов вкладки Снимки конфигурации		
1	Обновления	Вызов вкладки Обновления .	
	Сервер	Вызов настроек соединения с сервером.	

Часть функций, вызываемых с помощью основных кнопок, доступны также из главного

меню программы.

В нижней части окна отображается строка с именем текущего пользователя и его ролями.

В главном окне SoftControl Admin Console дополнительно возможны следующие действия:

Настройка соединения с сервером

Если необходимо просмотреть или изменить параметры соединения консоли управления и сервера во время работы SoftControl Admin Console, нажмите на кнопку **Сервер**.

Окно настроек подключения аналогично окну <u>авторизации⁽²⁷⁾</u>, открываемому при запуске SoftControl Admin Console.

Настройка интерфейса

Для изменения настроек интерфейса SoftControl Admin Console в основном меню выберите пункт **Вид** → **Настройки**.

По умолчанию язык интерфейса SoftControl Admin Console выбирается при первом запуске программы исходя из региональных настроек ОС. Для изменения языка в окне **Настройка интерфейса** выберите требуемый вариант из выпадающего списка (рис. <u>Настройка интерфейса</u>⁽³²⁾):

- ru-RU русский;
- en-US английский (США).

Чтобы изменения вступили в силу, необходимо перезапустить программу.

Установите флажок Запускать только один экземпляр консоли, если необходимо запретить возможность одновременного запуска нескольких экземпляров SoftControl Admin Console.

В поле **Размер страницы событий** задается максимальное количество событий, которое должно отображаться на одной странице вкладки <u>Лог</u>¹⁵⁹.

Централизованное управление СИБ



Рисунок 29. Настройка интерфейса

- Просмотр информации о программе
- В главном меню выберите пункт О программе.

4.2 Порядок работы

При администрировании СИБ на основе SoftControl Service Center из консоли управления SoftControl Admin Console рекомендуется придерживаться следующего порядка работы для снижения временных затрат и повышения продуктивности работы:

- 1) Откройте консоль управления SoftControl Admin Console, выполните подключение к серверу SoftControl Server²⁷.
- 2) На вкладке Роли при необходимости создайте дополнительные роли⁽³⁵⁾ и назначьте <u>учетным записям⁽³⁷⁾</u> пользователей роли с выбранными разрешениями. С помощью вкладки События безопасности производите <u>учет действий пользователей⁽⁴²⁾</u> через консоль управления.
- 3) На вкладке **Клиенты** <u>подтвердите</u>⁵⁰ или <u>отклоните</u>⁵¹ запросы на регистрацию от клиентских приложений, установленных на защищаемых устройствах.
- 4) После формирования рабочей области из необходимых устройств перейдите на вкладку Настройки клиентов и <u>создайте необходимые конфигурации</u>⁶⁰, которые будут применяться для клиентских приложений.
- 5) После создания клиентских настроек перейдите на вкладку **Подразделения** и <u>создайте подразделения</u>⁽⁵⁵⁾ (группы) по какому-либо принципу для распределения в них зарегистрированных компонентов на клиентских хостах. При создании подразделений выполните их <u>привязку к определенным</u> <u>конфигурациям</u>⁽⁵⁶⁾.

Централизованное управление СИБ

- 6) На вкладке **Клиенты** <u>переместите клиентские компоненты</u>⁽⁵²⁾ в созданные подразделения.
- 7) На вкладке **Задачи** создайте необходимые <u>задачи ¹²⁷</u> для клиентских приложений.
- 8) Перейдите на вкладку **Лог** и приступите к <u>просмотру отчетов клиентских</u> компонентов¹⁴³.
- 9) Дополнительно можно <u>настроить оповещения</u>⁽¹⁷¹⁾ об определенных событиях, которые будут отправляться на электронные почтовые ящики заданных <u>адресатов</u>⁽¹⁷⁰⁾, а также <u>экспортировать и вывести на печать</u>⁽¹⁶⁷⁾ необходимые данные.

4.3 Управление доступом на основе ролей

В SoftControl Service Center реализована подсистема управления доступом на основе ролей (*RBAC* – Role Based Access Control). Данная подсистема позволяет производить разграничение доступа <u>пользователей</u>³⁷ к различным функциям Сервисного Центра в зависимости от делегированной им <u>роли</u>³⁵.

Через SoftControl Admin Console осуществляется контроль действий пользователей с помощью регистрации событий безопасности сервера⁽⁴²⁾.

4.3.1 Роли

Вкладка **Роли** позволяет управлять ролями и настраивать разрешения для них (рис. <u>Вкладка «Роли»</u>³⁵).

SoftControl Admin Console			_ = ×
Файл Вид Фильтры Инструменты Опрограмме			
🖻 🛸 🍢 🚅 💀 🏩 🚣 😒 👗 🧰 🖳	ا 🎬 🕄 🖌 ا		
Клиенты Роли ×			
Добавить новую роль			1
		,	
Системный администратор		4	
Включает все имеющиеся разрешения			
		-	
Наблюдатель	<u>Удалить роль</u>		
Просматривать существующие контакты	<u>Удалить разрешение</u>		
Просматривать события от клиентов	<u>Удалить разрешение</u>		
Просматривать существующие нотификации	<u>Удалить разрешение</u>		0
Просматривать существующие подразделения	<u>Удалить разрешение</u>		
Добавлять комментарии к клиентам	<u>Удалить разрешение</u>		
Просматривать существующие настройки клиентов	<u>Удалить разрешение</u>		
Просматривать ранее созданные задачи	<u>Удалить разрешение</u>		
Просматривать настройки и историю обновлений	<u>Удалить разрешение</u>		
Применять настройки подразделения, если они были изменены локально	Удалить разрешение]	
Просматривать существующие роли	Удалить разрешение		
Входить в Admin Console	<u>Удалить разрешение</u>		•
Имя пользователя: admin Роли: Системный администратор, Администраторы			Смена пароля

Рисунок 30. Вкладка «Роли»

Роли на вкладке представлены в виде таблиц, в первой строке которой указано имя роли, а в последующих – права на выполнение определенных операций в консоли управления (разрешения).

SoftControl Service Center включает в себя две предустановленные роли:

- Системный администратор позволяет осуществлять доступ ко всей функциональности консоли управления. Рекомендуется для опытных пользователей/администраторов безопасности.
- Наблюдатель дает права на просмотр основной части информации, включая все данные по работе с клиентскими приложениями. Рекомендуется для операторов, ведущих мониторинг инцидентов безопасности на клиентских хостах.

Помимо этого, можно создать новые роли с собственным набором разрешений. Ниже описаны действия с ролями, выполняемые на данной вкладке:

Создание роли

Чтобы добавить роль, нажмите на кнопку **Добавить новую роль** (рис. <u>Вкладка</u> <u>«Роли»</u>³⁵). В появившемся окне укажите **Имя роли** и нажмите на кнопку **ОК** (рис. Создание новой роли³⁶).

🔀 Новая ро.		_ = ×
Имя роли:	Инженер сервисной службы	
	ОК	Отмена

Рисунок 31. Создание новой роли

Новая роль будет добавлена в конец списка ролей. Далее задайте <u>разрешения</u>³⁶ для нее.

Редактирование разрешений

Чтобы добавить разрешения к роли, нажмите на кнопку **Добавить разрешение** после таблицы с данной ролью. В появившемся окне отметьте необходимые разрешения и нажмите на кнопку **ОК** (рис. <u>Добавление разрешений</u>³⁶).

Чтобы удалить разрешение, нажмите на ссылку **Удалить разрешение** в соответствующей строке таблицы с ролью (рис. <u>Вкладка «Роли»</u>³⁵).

5	🖌 Добавить разрешение	_ 🗆 ×
	Выберите разрешения:	
	Генерировать основанные на времени одноразовые пароли	
	Задавать настройки SMTP-протокола для нотификаций	
	Изменять настройки SMTP-протокола для нотификаций	
	Изменять настройки обновлений	
	Изменять статусы клиентов: подтверждать, отклонять	
	Изменять существующие аккаунты	
	Изменять существующие контакты	
	Изменять существующие нотификации	
	Изменять существующие подразделения	
	Изменять существующие роли	
	Обновлять клиентские сертификаты	
	🔲 Операции теневого копирования	
	Отменять выполняющиеся задачи	
	Перемещать клиентов в другое подразделение	
	Применять частные настройки к клиентам	
	Проверять доступные обновления	
	Просматривать лог событий безопасности	
	Просматривать настройки SMTP-протокола для нотификаций	
	Создавать новые задачи для клиентов	
	Создавать новые контакты	•
Ĺ		

Рисунок 32. Добавление разрешений
🗢 Удаление роли

Для удаления роли нажмите на ссылку **Удалить роль** в строке таблицы с именем роли (рис. Вкладка «Роли»³⁵) и подтвердите удаление в диалоговом окне.

Удаление ролей, которые присвоены имеющимся пользователями (см. раздел <u>ниже³⁷)</u>, невозможно.

4.3.2 Пользователи

На вкладке **Пользователи** производится управление учетными записями пользователей и назначение ролей для них (рис. <u>Вкладка «Пользователи»</u>³⁷).

۲	SoftControl Admin Console								
Φ	айл Вид Фи	льтры И	Инструменты (О программе					
	ا 🛃 🦻		📫 🔯	🏚 🛦 🝤 📗	👪 💼 📔 🐔	3	64 ° 6		
	Клиенты Пол	зователи	×						
	1		8						
	Подразделен	ие Имя	🕶 Роли	Разрешённые клиенты	Связан с пользователем W	indows Количество п	араллельных сессий		
	По умолчани	o user	2 Показать)					
	По умолчани	o admi	in Показать						
L									▼
ŀ	Імя пользовате	ля: admin	Роли: Систен	иный администратор, Адм	инистраторы				Смена пароля

Рисунок 33. Вкладка «Пользователи»

Основные операции с учетными записями пользователей осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 6.

Кнопка	Название	Описание
	Добавить	Создание новой учетной записи.
<u> </u>	Редактировать	Редактирование свойств выбранной учетной записи.

Таблица 6. Элементы управления вкладки «Пользователи»

Кнопка	Название	Описание
0	Удалить	Удаление выбранных учетных записей.
3	Переместить	Переместить выбранного пользователя в другое подразделение.

Перечень полей вкладки приведен в табл. 7.

Таблица 7. Поля вкладки «Пользователи»

Поле	Описание
Подразделение	Подразделение, к которому приписан данный пользователь.
Имя	Имя пользователя.
Роли	Роли, присущие пользователю.

Основные действия, выполняемые на данной вкладке:

Создание учетной записи

Чтобы добавить новую учетную запись, нажмите на кнопку **Добавить** (рис. <u>Вкладка</u> <u>«Пользователи»</u>⁽³⁷⁾). В появившемся окне укажите **Имя** пользователя, введите **Пароль** учетной записи и его **Подтверждение**. Укажите необходимые **Роли** для создаваемого пользователя и нажмите на кнопку **Применить** (рис. <u>Создание</u> <u>учетной записи</u>⁽³⁸⁾). Минимальная длина пароля задается в настройках SoftControl Server. Для этого в файле конфигурации сервера (C:\ProgramData\SafenSoft \Server.Config.xml) следует выставить требуемое значение для параметра MinPasswordLength.

🔀 Новый пользователь	×						
Имя	Роли						
console_user	🔲 Системный администратор 🔺						
Пароль	✓ Наблюдатель						
•••••	Инженер						
Подтверждение	v						
•••••	🗌 Аккаунт заблокирован						
Пароль действителен до: Не ог	раничено						
📄 Временный пользователь. Б	удет заблокирован: 05.02.2021 8:16						
Поль	зователь Windows						
Пользователь не задан							
Режим входа в Windows							
Вход только через SoftCo	ontrol						
 Возможен вход через Wi 	indows						
Значения всех параметров корректны							
	Применить Отмена						

Рисунок 34. Создание учетной записи

Область **Пользователь Windows** зарезервирована для будущего использования. Связанная с ней функциональность в текущей версии не реализована.

Все новые учетные записи автоматически помещаются в подразделение **По умолчанию**. Вы можете <u>переместить</u>⁽⁴¹⁾ выбранную учетную запись в другое подразделение.

В зависимости от <u>роли⁽³⁵⁾</u>, пользователь имеет доступ к информации в текущем подразделении и во всех дочерних подразделениях и не имеет доступа к информации в родительских подразделениях.

Вы также можете сделать учетную запись временной, выставив галочку Временный пользователь и указав дату блокировки.

Редактирование учетной записи

Чтобы изменить свойства учетной записи, нажмите на кнопку **Редактировать** (рис. <u>Вкладка «Пользователи»</u>³⁷).

В появившемся окне измените Имя пользователя и/или измените Роли в соответствующей области, после чего нажмите на кнопку Применить

(рис. <u>Редактирование учетной записи</u>⁽⁴⁰⁾). Пароль при этом останется без изменений. Если требуется сменить пароль, то введите новый **Пароль** в одноименном поле и его **Подтверждение**.

🔀 Редактирование пользователя	×						
Имя	Роли						
console_user	Системный администратор						
Пароль	🗹 Наблюдатель						
Пароль	Инженер						
Подтверждение	v .						
Подтверждение пароля	Аккаунт заблокирован						
Пароль действителен до: Не огран	ичено						
Временный пользователь. Буде	ет заблокирован: 25.02.2021 8:08						
Пользое	затель Windows						
DESKTOP-63KNC18\eelagina							
Режим входа в Windows	rol						
 Возможен вход через Wind 	ows						
Значения всех параметров корректны							
Применить Отмена							

Рисунок 35. Редактирование учетной записи

Кроме того, любой пользователь может сменить свой пароль в окне, которое появляется при нажатии на кнопку **Смена пароля** в правом нижнем углу SoftControl Admin Console (см. рис. <u>Вкладка «Пользователи»</u>⁽³⁷⁾). Кнопка доступна на любой открытой вкладке.

🔀 Смена пароля для admin 🛛 🗙 🗙
Старый пароль:
Пароль
Новый пароль:
Пароль
Подтверждение:
Подтверждение пароля
Применить Отмена

Рисунок 36. Смена пароля пользователя

В появившемся окне (рис. <u>Смена пароля пользователя</u>⁽⁴⁰⁾) необходимо ввести старый **Пароль**, **Новый пароль** и его **Подтверждение** и нажать на кнопку **Применить**.

При смене пароля администратор может ограничить срок его действия. Для этого в файле конфигурации сервера (C:\ProgramData\SafenSoft\Server.Config.xml) следует требуемое выставить значение (количество дней) для параметра PasswordValidDays (по умолчанию 60 дней; 0 означает, что время действия пароля не ограничено). Минимальное время действия задается с помощью параметра MinPasswordPeriodDays и не может быть больше значения, установленного для параметра *PasswordValidDays*. Кроме того, можно выставить запрет на использование определенного числа старых паролей (от 1 до 10; параметр ForbidOldPasswordCount).

Если учетную запись необходимо заблокировать, выставите галочку **Аккаунт заблокирован** (рис. Редактирование учетной записи⁴⁰).

▽ Удаление учетной записи

Для удаления учетной записи выберите ее, нажмите на кнопку **Удалить** (рис. <u>Вкладка «Пользователи»</u>⁽³⁷⁾) и подтвердите удаление в диалоговом окне. <u>Примечание</u>. После удаления учетной записи создать новую учетную запись с таким же именем можно не ранее, чем через 3 года.

Перемещение учетной записи

Для перемещения учетной записи выберите ее, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое надо переместить данного пользователя (рис. Перемещение учетной записи⁽⁴¹⁾).

🔀 Подразделения	×
Выберите подразделение:	
Production-Audit	
Применить Отмена	
Рисунок 37. Перемещение учетн записи	юй

4.3.3 События безопасности сервера

Консоль управления позволяет фиксировать операции, производимые пользователями, для дальнейшего анализа на вкладке **События безопасности** (рис. <u>Вкладка «События</u> <u>безопасности»</u>⁽⁴³⁾).

Полный перечень полей вкладки приведен в таблице ниже.

Поле	Описание
	Уникальный идентификатор клиентского приложения (только для типов
Guid клиента	событий Подтверждение клиента, Отклонение клиента, Удаление клиента,
	Перемещение клиента в другое подразделение).
	Тип зарегистрированного события:
	• Начало сессии;
	• Конец сессии;
	• Роль создана;
	• Роль удалена;
	 К роли добавлены разрешения;
	 Удалено разрешение у роли;
	 Была создана учетная запись;
	 Учетная запись была изменена;
	 Учетная запись была удалена;
	• Подтверждение клиента;
	• Отклонение клиента;
	• Удаление клиента;
	 Запрос на изменение сертификата клиента;
	 Новый сертификат назначен клиенту;
	 Перемещение объекта в другое подразделение;
	 Создано новое подразделение;
	• Подразделение было удалено;
	• Создание новых настроек;
	 Изменение настроек для подразделения;
	• Применение частных настроек;
	 Удалены настройки;
	 Назначены настройки подразделения;
	• Создание задачи;
	• Отмена задачи;
	• Создан контакт;
	• Контакт изменен;
	• Контакт был удален;
	 Была создана нотификация;
	 Нотификация была изменена;
	 Нотификация была удалена;
	 Неавторизованный запрос;
	 Недостаточно прав на выполнение запроса;
	 Ошибка обработки запроса.

Таблица 8. Поля вкладки «События безопасности»

Поле	Описание
Тип задачи	Тип задачи (только для типов событий Создание задачи , Отмена задачи).
Сообщение об ошибке	Сообщение об ошибке во время обработки запроса.
Причина ошибки авторизации	Причина невозможности авторизации на сервере (только для типа события Неавторизованный запрос).
ID задачи	Порядковый номер задачи (только для типов событий Создание задачи , Отмена задачи).
Номер порта запроса	Порт компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.
URI запроса	Полный URI запроса консоли управления SoftControl Admin Console, который был отправлен на сервер.
Имя подразделения	Подразделение, в которое перемещен установленный клиентский компонент (только для типов событий Перемещение клиента в другое подразделение , Создано новое подразделение, Подразделение было удалено).
Разрешения роли	Перечисление добавленных (для типа события К роли добавлены разрешения) или удаленных (для типа события Удалено разрешение у роли) разрешений роли.
ID сессии	Контрольная сумма идентификатора сессии, с которой ассоциировано событие.
Имя аккаунта	Имя учетной записи пользователя (только для типов событий Была создана учетная запись, Учетная запись была изменена, Учетная запись была удалена).
Имя роли	Имя роли (только для типов событий Роль создана, Роль удалена, К роли добавлены разрешения, Удалено разрешение у роли).
Имя пользователя	Имя пользователя, с которым ассоциировано данное событие.
Имя нотификации	Имя оповещения (только для типов событий Была создана нотификация , Нотификация была изменена, Нотификация была удалена).
Имя настроек	Имя конфигурации клиентских приложений (только для типов событий Создание новых настроек, Изменение настроек для подразделения, Удалены настройки).
Имя контакта	Имя адресата получателя оповещений (только для типов событий Создан контакт, Контакт был изменен, Контакт был удален).
Время возникновения	Дата и время возникновения события.
Время создания настроек	Время создания настроек клиентских приложений на сервере (только для типа события Создание новых настроек).
Имя клиента	Имя клиентского хоста (только для типов событий Подтверждение клиента, Отклонение клиента, Удаление клиента, Запрос на изменение сертификата клиента, Новый сертификат назначен клиенту, Перемещение клиента в другое подразделение).
IP адрес запроса	IP-адрес компьютера с установленной консолью управления SoftControl Admin Console, от которой пришел запрос на сервер.

SoftControl Admin Console							_ = ×			
Файл Вид Фильтры Инструменты Опрограмме										
S Sa 🍕 🚅 💀 🏂 📐 😒 👪 📾 🔛 🥪 🗎 🕼 🎜 🎬 😜 😰 🗓										
Клиенты События безопасно	Клиенты События безопасности ×									
		Перетяните сю	да мышкой заголовок ко	лонки для группировки	данных по ней					
Время возникновения	Тип события	ID сессии Имя пользоват	геля IP-адрес запроса	Номер порта запрос	a URI запроса					
20.02.2021 14:01:51 +03:00	Начало сессии	ef6a1d9f11Iadmin					A			
20.02.2021 14:00:32 +03:00	Конец сессии	15800c7e6cadmin								
20.02.2021 13:51:55 +03:00	Начало сессии	15800c7e6cadmin								
20.02.2021 12:56:08 +03:00	Подтвержден	65590f67deadmin	:1	49454	https://loc					
20.02.2021 12:55:05 +03:00	Начало сессии	65590f67deadmin								
20.02.2021 12:52:32 +03:00	Конец сессии	7e052d346(admin								
20.02.2021 12:08:59 +03:00	Вручную выбр	7e052d346(admin	:1	49477	https://loc					
20.02.2021 12:06:57 +03:00	Изменение на	7e052d346(admin	:1	49472	https://loc					
20.02.2021 12:06:42 +03:00	Создание нов	7e052d346ladmin	:1	49470	https://loc					
20.02.2021 12:05:07 +03:00	Вручную выбр	7e052d346ladmin	:1	49466	https://loc					
20.02.2021 12:04:58 +03:00	Вручную сген	7e052d346íadmin	:1	49466	https://loc					
20.02.2021 12:04:27 +03:00	Начало сессии	7e052d346íadmin								
20.02.2021 11:58:33 +03:00	Конец сессии	4a109733ctadmin					Ŭ			
20.02.2021 14:06:03 +03:00	Начало сессии	4a109733ctadmin								
20.02.2021 13:54:29 +03:00	Начало сессии	7c03d7ae44admin								
Первая страница Предыду	/щая страница	Следующая страница	Страница №1 (последн	няя)			Прошло времени: 00:00:01			
Имя пользователя: admin Роли: Системный администратор, Администраторы Смена пароля										

Рисунок 38. Вкладка «События безопасности»

С данными в таблице можно работать с помощью фильтрации или создания запросов к базе данных. Эти операции подробно описаны в разделах <u>Фильтрация событий</u>⁽¹⁵⁹⁾ и <u>Запросы к базе данных</u>⁽¹⁶⁵⁾.

Также на этой вкладке можно выполнить следующие действия:

Изменение состава колонок

Если необходимая колонка отсутствует в заголовке таблицы, то для добавления нового поля нажмите кнопку **Выбрать колонки** и перетащите требуемое поле из окна **Выбор колонок** (рис. <u>Выбор колонок</u>⁴⁴) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно **Выбор колонок**, либо за пределы заголовка таблицы.



Рисунок 39. Выбор колонок

🗢 Группировка данных

Информация на вкладке может группироваться по всем полям (категориям), кроме поля **Время возникновения**, для удобства просмотра. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. <u>Вкладка «События</u> <u>безопасности»</u>⁽⁴³⁾). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

4.4 Клиенты

Вкладка **Клиенты** служит для управления регистрацией клиентских приложений, перемещением их в подразделения, отслеживания статуса и получения информации о хостах, на которых они установлены (рис. <u>Вкладка «Клиенты»</u>⁴⁶).

Основные операции с клиентскими компонентами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 9.

Кнопка Название		Описание	Горячие клавиши
0	Удалить	Удаление выбранных клиентских компонентов из БД.	Delete
~	Одобрить	Одобрение регистрации клиентского компонента на сервере.	

×	Отклонить	Отклонение регистрации клиентского компонента на сервере.	
	Переместить	Перемещение выбранных клиентских компонентов в другое подразделение.	
Real O	Сертификат	Обновление индивидуального сертификата клиентского компонента.	
8	Лог событий	Вызов вкладки Лог для выбранных компонентов.	

	Soft	Control Admin Cor	nsole												_ 🗆 X
Φ;	Райл Вид Фильтры Инструменты Опрограмме														
						Перетяните	е сюда мышкой за	аголовок колонки	для группировки ,	данных по ней					
	ID	Подразделение	Имя	Тип клиента	Тип настроек	Версия продукта	Статус	Информация		Изменён	ІР-адрес	DNS	Кол-во дней до	Состояние настроек	Срок
Þ	1	По умолчанию	DESKTOP-63K	SysCmd	Настройки под		Активен	Наблюдение Обновление	Частично Нет информаци	01.02.2021 17:00:26	192.16				2
	2	По умолчанию	DESKTOP-63K	SysWatch	Настройки под	6.0.58.0	Активен	Защита Сканирование Профиль Обновление	<mark>Включено</mark> Нет информаци Нет информаци Нет информаци	01.02.2021 16:59:30	192.16	DE	30	Применены успе	2
															_
И	мяп	ользователя: adm	in Роли: Систе	мный админи	стратор, Админ	истраторы								Смена паро	оля

Рисунок 40. Вкладка «Клиенты»

Полный перечень полей вкладки приведен в табл. 10.

Таблица 10. Поля вкладки «Клиенты»

Поле	Описание					
ID	Торядковый номер клиентского хоста.					
Подразделение	одразделение, к которому принадлежит клиентский компонент.					
Имя	Имя клиентского хоста.					
Тип клиента	 Тип установленного клиентского компонента на данном клиентском хосте: SysWatch – компонент проактивной защиты (SoftControl ATM Client / Endpoint Client / SClient); DLP – компонент сбора данных (SoftControl DLP Client); SysCmd - компонент удаленного выполнения команд и обмена файлами (SoftControl SysCmd). 					
Тип настроек	 Тип конфигурации клиентского компонента: Настройки подразделения – настройки, общие для подразделения, которому принадлежит клиентский компонент; Частные настройки – настройки, индивидуальные для клиентского компонента, 					

	независимо от подразделения;			
	 Локальные настройки – настройки, измененные локально для клиентского компонента типа SysWatch. 			
Версия продукта	Версия установленного клиентского компонента. Если версия компонента ниже версии SoftControl Admin Console, данная ячейка подсвечивается красным цветом, если выше – оранжевым.			
	 Возможные статусы, отражающие текущее состояние клиентского компонента: Ожидает решения: от клиентского приложения получен запрос на регистрацию, ожидается решение администратора. Одобрен: запрос на регистрацию от клиентского приложения одобрен администратором. Отклонен: запрос на регистрацию от клиентского приложения отклонен 			
Статус	 администратором. Активен: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу⁶³, зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером. Остановлен: за последний отрезок времени, равный удвоенному значению интервала обращения клиента к серверу⁶³, не зафиксирован факт установки связи зарегистрированного клиентского приложения с сервером. 			
	 Дополнительная информация по состоянию клиентского компонента. Для компонента типа SysWatch имеет следующие показатели: Защита – статус проактивной защиты. Включено: защита включена по всем областям контроля; Отключено: защита отключена по всем областям контроля; Частично: защита включена по части областей контроля; Частично: защита включена по части областей контроля; Сканирование – статус последней по времени задачи антивирусного сканирования. Профиль – статус последней по времени задачи сбора профиля (автоматической настройки). Выполняется: задача находится в процессе выполнения; Остановлено: задача остановлена пользователем; Завершено: задача успешно завершена; Ошибка: возникла ошибка в процессе запуска или завершения задачи 			
Информация	 Статус Нет информации для операций Сканирование, Профиль и Обновление означает, что указанные действия не производились с момента регистрации клиентского приложения на сервере. Для компонента типа DLP имеет следующие показатели: Наблюдение – статус активности наблюдения. Включено: наблюдение включено по всем областям сбора данных (не включает в себя подкатегорию съемных носителей); Отключено: наблюдение отключено по всем областям сбора данных; Частично: наблюдение включено по всем областям сбора данных; Информация по обновлению присутствует у всех типов клиентов: Обновление – статус последнего по времени обновления компонента. Установлено: обновление было успешно установлено; Не найдено: обновления для компонента не найдены; Перезагрузить: необходима перезагрузка клиентского хоста для завершения обновления. 			
Изменен	Время регистрации последнего события выбранным клиентским компонентом			
IP адрес	IР-адрес клиентского хоста.			
п адроо	п адрестоноптоного лоста.			

DNS	Сетевое имя клиентского хоста в рабочей группе либо доменной сети.					
Количество дней до	Количество дней, оставшихся до истечения срока действия текущего лицензионного					
окончания лицензии	люча клиентского приложения.					
Состояние настроек	Статус применения настроек клиентского приложения, полученных им со стороны сервера SoftControl Server. Обновляется динамически при каждом изменении настроек через консоль управления SoftControl Admin Console. Возможные состояния: • применены успешно; • ожидание ответа; • ошибка применения; • локальные настройки; • нет информации.					
Срок действия	Дата, до которой действителен индивидуальный сертификат клиентского					
сертификата	приложения.					
Комментарий	Поле для ввода комментария к выбранному клиентскому компоненту.					
Уникальный ID	Уникальный идентификатор клиентского компонента, который автоматически					
устройства	присваивается ему при первом обращении к серверу SoftControl Server.					
Статус постоянного соединение с Сервисным Центром (см. раздел Общие настройки ⁽⁶³⁾ • Активен: постоянное соединение с SoftControl Service Center вклю • Остановлен: постоянное соединение с SoftControl Service Center общие настройки						
Запретить локальное управление настройками	Индикатор управления настройками клиентских хостов. Галочка в данном поле означает, что управлять настройками можно только через SoftControl Service Center. Включение и отключение данной опции осуществляется через настройки клиентских приложений (см. раздел <u>Настройки SoftControl SysWatch</u> ⁷⁴).					

Основные действия, выполняемые на данной вкладке:

- управление процессом регистрации⁽⁵⁰⁾;
- перемещение в подразделения⁽⁵²⁾;
- управление списком файлов, разрешенных к запуску⁽⁵²⁾.

Дополнительные действия, возможные на данной вкладке:

Работа с несколькими компонентами

Вкладка позволяет работать как с одним, так и с несколькими клиентскими компонентами. Для выполнения действий над несколькими компонентами выберите их с помощью одного из способов выделения и произведите требуемые действия:

- выделение нескольких произвольных компонентов: зажмите клавишу Ctrl на клавиатуре и выделите требуемые компоненты;
- выделение диапазона компонентов: выберите первый компонент диапазона, зажмите клавишу Shift на клавиатуре и выберите последний компонент

диапазона.

Группировка данных

Информация на вкладке может группироваться по определенным полям для удобства отображения. Полями, по которым возможно произвести группировку (категориями), являются Подразделение, Тип клиента, Тип настроек, Версия продукта, Статус, IP адрес, DNS, Количество дней до окончания лицензии, Состояние настроек и Комментарий. Для группировки по указанным категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки (рис. <u>Вкладка «Клиенты»</u>⁽⁴⁶⁾). Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

Просмотр журналов

Для открытия вкладки <u>Лог событий ⁽¹⁴³⁾</u> со списком событий выделите требуемые компоненты и выполните одно из следующих действий:

- нажмите на кнопку **Лог событий** в группе кнопок вкладки (рис. <u>Вкладка</u> «Клиенты»⁽⁴⁶⁾);
- вызовите контекстное меню нажатием правой кнопки мыши на списке компонентов и выберите команду **Показать события**.

При открытии списка событий в заголовке вкладки <u>Лог¹⁴³</u> отображается количество выбранных компонентов (рис. <u>Вкладка «Клиенты»</u>⁴⁶).

Просмотр данных профиля

Выделите нужный профиль и вызовите контекстное меню нажатием правой кнопкой мыши. Выберите команду **Просмотр данных профиля**. Откроется вкладка **Данные профиля** со списком хэш-сумм, включенных в выбранный профиль. При необходимости настройте фильтр для отображения нужных записей. Внизу находится гиперссылка **Экспортировать выборку в файл**. Нажмите ее, чтобы создать файл XML с записями, соответствующими заданным настройкам фильтра. Также вы можете удалить записи или скопировать нужные контрольные суммы, вызвав контекстное меню нажатием правой кнопкой мыши.

SoftControl Admin Console _ C × Зайл Вид Фильтры Инструменты О программе Soft Sea						
Время последнего обновления: 2/2/2021 10:44:16 АМ Запросить обновление						
 Показывать записи за период: Имя файла содержит: Путь к файлу содержит: 	Показывать записи за период: 01.02.2021, 12:38:07 02.02.2021, 10:16:56 Имя файла содержит: Путь к файлу содержит:					
Хэш-сумма файла	Имя файла	Размер файла	Время добавления	Путь к файлу		
• E0E7F59E8D567E1D1FD0D94BA19	PRESENTATIONNATIVE_V0400.DLL	789736	02.02.2021 10:16:22	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
A4F648B9BC8F2A539F3FBAC551E	SOS.DLL	716432	02.02.2021 10:16:24	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
C65EBFE5B073F329AE3A8470FFF	WEBENGINE4.DLL	511664	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
CB109C45DDEA2CF98F6DC79EAB	WEBENGINE.DLL	24744	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
AC9D84467DC2A47B24AC76577E	WMINET_UTILS.DLL	42168	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
2730647614998B0E43E64C9288F6	WORKFLOWSERVICEHOSTPERFOR	87328	02.02.2021 10:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
ECA0A070F7C88A3A4D29FF9E5A	WPFGFX_V0400.DLL	1691824	02.02.2021 10:16:42	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
224C713088986C73E0693C76A39	PRESENTATIONCORE.DLL	3485536	02.02.2021 10:16:47	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
B04D79AF7A93B0A23C318DEAEC	SYSTEM.DATA.DLL	3332784	02.02.2021 10:16:54	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
	SYSTEM.WEB.DLL	5376680	02.02.2021 10:16:55	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
0D8EE35F77ED0A3A8E131A4A6C						
0D8EE35F77ED0A3A8E131A4A6C D99D64F39A52B4F3DAD2990690	PRESENTATIONHOST.EXE	244224	02.02.2021 10:16:56	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
ОВВЕЕЗ5F77ED0A3A8E131A4A6С D99D64F39A52B4F3DAD2990690 «С Страница 423 из 423	PRESENTATIONHOST.EXE 20 421 422 423 €) Экс	244224 портировать выбо	02.02.2021 10:16:56 орку в файл	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		

Рисунок 41. Вкладка «Данные профиля»

4.4.1 Управление процессом регистрации

Управление процессом регистрации включает в себя следующие действия:

✓ Подтверждение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Одобрить** (рис. Вкладка «Клиенты»⁴⁶).

Поле Статус после подтверждения регистрации выбранных клиентов изменяет свое состояние на Одобрен.

При следующем получении запроса от клиентского компонента происходит проверка его <u>сертификата</u>²³⁰: если он общий, то серверный компонент SoftControl Server выдает индивидуальный сертификат для авторизации на сервере. При следующем обращении клиентского компонента (с индивидуальным сертификатом) его статус изменяется на **Активен**. С этого момента клиентский компонент считается введенным в эксплуатацию: между сервером и клиентом установлен безопасный зашифрованный канал связи.

Отклонение регистрации

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Ожидает решения**, и нажмите на кнопку **Отклонить** (рис. <u>Вкладка «Клиенты»</u>⁽⁴⁶⁾). Поле **Статус** после отклонения регистрации выбранных клиентов изменяет свое состояние на **Отклонен**, и их дальнейшее взаимодействие с сервером

прекращается.

После отклонения регистрации повторную попытку можно совершить только следующим образом:

1) Удалите клиентские компоненты из БД с помощью кнопки Удалить.

2) Повторите процедуру регистрации на сервере с общим сертификатом²³⁰.

Обновление клиентского сертификата

Выберите в списке требуемые клиентские компоненты, находящиеся в состоянии **Активен** или **Остановлен**, и нажмите на кнопку **Сертификат** (рис. <u>Вкладка</u> «Клиенты»⁴⁶).

Поле **Срок действия сертификата** обновляется после следующего обращения клиентского компонента с новым <u>индивидуальным сертификатом</u>²³⁰. При этом использование предыдущего сертификата становится невозможным в связи с его помещением в черный список.

Удаление клиентского компонента из БД

Выберите в списке требуемые клиентские компоненты и нажмите на кнопку Удалить (рис. <u>Вкладка «Клиенты»</u>⁽⁴⁶⁾). При этом не происходит отзыва клиентского <u>сертификата</u>⁽²³⁰⁾ и через интервал обращения клиента к серверу в консоли управления SoftControl Admin Console вновь отобразятся удаленные компоненты в статусе **Ожидает решения**. Для полного вывода клиентских компонентов из эксплуатации необходима следующая последовательность действий:

- 1) Поместите <u>индивидуальный сертификат</u>²³⁰ клиентского компонента в черный список с помощью кнопки **Отклонить**.
- 2) Удалите клиентские компоненты из БД с помощью кнопки Удалить.

4.4.2 Перемещение в подразделения

Для перемещения выбранных клиентских компонентов в другое подразделение, нажмите на кнопку **Переместить** и в появившемся окне выберите из выпадающего списка необходимое подразделение (рис. <u>Выбор подразделения для перемещения компонента</u> ⁽⁵²⁾).

При перемещении клиентских компонентов в другое подразделение их настройки автоматически изменяются на конфигурацию данного подразделения.

🔀 Подразделения	×
Выберите подразделение:	
ProtectionTest	
Применить	Отмена
Рисунок 42. Выбор подра перемещения комп	зделения для юнента

4.4.3 Управление списком разрешенных файлов

SoftControl Admin Console позволяет получить список файлов, разрешенных к запуску на компьютере с установленным клиентским приложением SoftControl SysWatch, и при необходимости отозвать разрешения для выбранных файлов.

Для получения списка файлов щелкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl SysWatch и в контекстном меню выберите команду **Просмотр данных профиля**. Данное действие открывает вкладку **Данные профиля для <имя_клиентского_приложения>** (рис. <u>Вкладка_«Данные профиля для...»</u>⁽⁵²⁾). Для начала сбора профиля нажмите на кнопку **Запросить обновление**. В процессе сбора данных SoftControl Admin Console показывает примерное время до окончания сбора. Список файлов содержит следующую дополнительную информацию: имя файла в момент добавления в список, его контрольная сумма, полный путь, дата добавления, размер, а также флаг, указывающий, был ли файл добавлен в профиль инсталлятором (I) или в процессе сбора профиля (**P**).

🚩 SoftControl Admin Console 📃 🗖 🛛							
Файл Вид Фильтры Инструменты	О программе						
۶ 🖗 🌠 🚅 💀 🤹 🛝 😒 🐹 😁 🕒 🥪 🛗 🕼 🍜 🐘 😜 📗							
Клиенты Данные профиля для DESKTOP-63KNC18 ×							
			Фильтр				
🗌 Показывать записи за период:	01.02.2021, 12:38:07 - 02.0	02.2021, 10:16:56	-				
Имя файла содержит:							
Путь к фаилу содержит:							
	1/140 ต่อนักว	Dogwon doğur	Prous robo				
F0F7E59E8D567E1D1ED0D94B419		789736	02 02 2021 1)-16-22			
A4F648B9BC8F2A539F3FBAC551E	SOS.DLL	716432	02.02.2021 1	0:16:24	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
C65EBFE5B073F329AE3A8470FFF	WEBENGINE4.DLL	511664	02.02.2021 10	0:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
CB109C45DDEA2CF98F6DC79EAB	WEBENGINE.DLL	24744	02.02.2021 10):16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
AC9D84467DC2A47B24AC76577E	WMINET_UTILS.DLL	42168	02.02.2021 1):16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
2730647614998B0E43E64C9288F6	WORKFLOWSERVICEHOSTPERFOR	87328	02.02.2021 10	0:16:41	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
ECA0A070F7C88A3A4D29FF9E5A	WPFGFX_V0400.DLL	1691824	02.02.2021 1	0:16:42	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
224C713088986C73E0693C76A39	PRESENTATIONCORE.DLL	3485536	02.02.2021 10	0:16:47	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
B04D79AF7A93B0A23C318DEAEC	SYSTEM.DATA.DLL	3332784	02.02.2021 1	0:16:54	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
0D8EE35F77ED0A3A8E131A4A6C	SYSTEM.WEB.DLL	5376680	02.02.2021 1	0:16:55	\DEVICE\HARDDISKVOLUME3\WINDOWS.OLD\WINDOWS\WINSXS\X86		
D99D64F39A52B4F3DAD2990690	PRESENTATIONHOST.EXE	244224	02.02.2021 1	0:16:56			
					*		
Страница 423 из 423 🚺 🖬 🛶 4	20 421 422 423 V X Экс	портировать выбо	орку в файл				
Имя пользователя: admin Роли: Системный администратор, Администраторы Смена пароля							

Рисунок 43. Вкладка «Данные профиля для...»

Для просмотра списка файлов за определенный период времени выберите требуемые даты в поле **Фильтр**. Вы также можете указать в фильтре часть имени файла и пути к нему. Для того чтобы отозвать разрешения на запуск для каких-либо файлов, выделите их, используя клавиши **Shift** и **Ctrl**, и в контекстном меню выберите команду **Удалить выбранные**.

4.5 Подразделения

Вкладка **Подразделения** предназначена для группирования клиентских компонентов по территориальному, административному или иному признаку (рис. <u>Вкладка «Подразделения»</u>⁵³). Кроме того, на вкладке производится привязка подразделений к определенным наборам настроек и генерация одноразовых паролей.

🔀 SoftControl Admin Console	_ 0 1
Файл Вид Фильтры Инструменты Опрограмме	
👂 🕵 🕵 📭 🗟 🍙 杰 🝤 🖁	8 💼 🕒 📢 2 🎬 la 🌙 Ta 📳 😰 1
Клиенты Подразделения ×	
1 🕂 🖉 😵 🛼 🐂	
Имя Имя настроек Ведущее подразделение 🕶	Количество клиентов
🗧 По умолчанию По умолчанию	2
Unit South По умолчанию По умолчанию	0
Unit North По умолчанию По умолчанию	0
Имя пользователя: admin Роли: Системный администратор, Админи	истраторы Смена пароля

Рисунок 44. Вкладка «Подразделения»

В программе всегда существует как минимум одно подразделение – **По умолчанию**; его удаление невозможно. Все новые клиентские компоненты автоматически помещаются в данное подразделение. В дальнейшем администратор может создать требуемую иерархическую структуру подразделений (с любым уровнем вложенности), используя кнопку **Переместить**. Каждому подразделению при создании назначается конфигурация (настройки) клиентских приложений.

Основные операции с подразделениями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 11.

Кнопка	Название	Описание
	Добавить	Создание нового подразделения.
2	Редактировать	Редактирование свойств выбранного подразделения.
6	Удалить	Удаление выбранных подразделений.
3	Переместить	Переместить выбранное подразделение в другое. Нельзя перемещать подразделение По умолчанию , а также родительское подразделение в дочернее.
	Одноразовый пароль для SysWatch	Открытие окна генератора одноразовых паролей.

Таблица 11. Элементы управления вкладки «Подразделения»

Кнопка	Название	Описание
1	Одноразовый пароль для разблокировки клавиатуры	Открытие окна генератора паролей для разблокировки клавиатуры на клиентском хосте.

Перечень полей вкладки приведен в табл. 12.

Таблица 12. Поля вкладки «Подразделения»

Поле	Описание
Имя	Наименование подразделения.
Имя настроек	Наименование конфигурации клиентских компонентов, действующее в выбранном
	подразделении.
Ведущее подразделение	Наименование родительского подразделения.

Основные действия, выполняемые на данной вкладке:

- управление подразделениями⁽⁵⁵⁾;
- генерация одноразовых паролей⁽⁵⁷⁾.

4.5.1 Управление подразделениями

Управление подразделениями включает в себя следующие действия:

Создание подразделения

Чтобы добавить новое подразделение, нажмите на кнопку **Создать** (рис. <u>Вкладка</u> <u>«Подразделения»</u>⁽⁵³⁾). В появившемся окне укажите **Имя** подразделения и выберите **Имя настроек** в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. <u>Создание подразделения</u>⁽⁵⁵⁾).

🔀 Параметры подразделения	a	×
Имя:	Северный филиал	1
Имя настроек:	По умолчанию	
Клиенты:		
]
(Применить Отмена)

Рисунок 45. Создание подразделения

Изменение свойств подразделения

Чтобы изменить свойства подразделения, нажмите на кнопку **Редактировать** (рис. Вкладка «Подразделения»⁵³).

В появившемся окне измените **Имя** подразделения и/или выберите другое **Имя** настроек в выпадающем списке, после чего нажмите на кнопку **Применить** (рис. <u>Параметры подразделения</u>⁵⁶). Если данное подразделение содержит компоненты, их перечень отображается в списке **Клиенты**.

🔀 Параметры подразделения	×
Имя:	Северный филиал
Имя настроек:	Settings 1
Клиенты:	
DESKTOP-63KNC18 DESKTOP-63KNC18	
	Применить Отмена

Рисунок 46. Параметры подразделения

Удаление подразделения

Для удаления подразделения выберите его, нажмите на кнопку **Удалить** (рис. <u>Вкладка «Подразделения»</u>⁵³) и подтвердите удаление в диалоговом окне. Все компоненты из удаляемого подразделения будут перемещены в подразделение, которое является для него родительским.

Удаление подразделения По умолчанию невозможно.

Перемещение подразделения

Для перемещения подразделения выберите его, нажмите на кнопку **Переместить** и в появившемся окне укажите подразделение, в которое происходит перемещение (рис. Перемещение подразделения⁵⁶).

	Подраздел Выберите по Production-л	ания дразделение: Audit Применить нок 47. Пере подразделе	Отмен емещение ения	Ha B			
Невозможно пере	местить	подразде.	ление	По	умолчанию,	а	также
	Невозможно пере родительское подра	Годраздел Выберите по Production-/ Рису Невозможно переместить родительское подразделение	Годразделения Выберите подразделение: Production-Audit Применить Рисунок 47. Пере подразделе Невозможно переместить подразде родительское подразделение в дочерне	Годразделения Выберите подразделение: Production-Audit Применить Отмен Рисунок 47. Перемещение подразделения Невозможно переместить подразделение родительское подразделение в дочернее.	Годразделения Выберите подразделение: Production-Audit Применить Отмена Рисунок 47. Перемещение подразделения Невозможно переместить подразделение По родительское подразделение в дочернее.	Подразделения Выберите подразделение: Production-Audit Применить Отмена Рисунок 47. Перемещение подразделения Невозможно переместить подразделение По умолчанию, родительское подразделение в дочернее.	Подразделения Выберите подразделение: Production-Audit Применить Отмена Виберите подразделение Рисунок 47. Перемещение подразделения Невозможно переместить подразделение По умолчанию, а родительское подразделение в дочернее.

4.5.2 Генерация одноразовых паролей

В SoftControl Service Center реализована подсистема защищенной аутентификации на основе алгоритма создания одноразовых паролей. Данный алгоритм обладает высокой криптографической стойкостью и позволяет генерировать пароли, действительные только в течение определенного промежутка времени. Одноразовые пароли могут быть использованы для доступа к ГИП/деинсталлятору клиентского компонента SoftControl SysWatch в случае необходимости (например, если требуется обеспечить однократный доступ к SoftControl SysWatch без раскрытия основного пароля), а также для разблокировки клавиатуры на клиентском хосте.

Для начала работы с генератором одноразовых паролей необходимо, чтобы в текущей конфигурации подразделения была включена и настроена <u>соответствующая опция</u>⁸³.

Генерация одноразовых паролей осуществляется в рамках подразделения: создаваемый пароль применим для всех приложений SoftControl SysWatch, входящих в подразделение. Выберите подразделение и нажмите на кнопку **С** (Одноразовый пароль для SysWatch) или **С** (Одноразовый пароль для разблокировки клавиатуры), чтобы открыть окно генератора (рис. Вкладка «Подразделения»⁵³). В появившемся окне выберите Время действия пароля и нажмите на кнопку **С** (Сгенерировать пароль). Пароль отображается в поле Одноразовый пароль для SysWatch (или Одноразовый пароль для разблокировки клавиатуры); время его жизни – в счетчике Осталось времени в формате *дд:чч:мм:сс* (рис. <u>Окно генерации</u>⁵⁸). По истечении интервала времени жизни нажмите на кнопку **С** еще раз, чтобы сгенерировать новый пароль.

- I) Использование одноразовых паролей для SysWatch рассчитано на применение совместно с основным паролем. Для возможности получения доступа к SoftControl SysWatch на клиентском хосте по одноразовым паролям должна быть включена <u>общая парольная защита</u>⁷³. При запросе пароля в ГИП SoftControl SysWatch необходимо установить флажок Использовать одноразовый пароль.
 - II) В связи с тем, что алгоритм создания одноразовых паролей в качестве параметра принимает время, для его корректной работы необходимо, чтобы время по UTC (т.е. независимо от часового пояса) на компьютере с SoftControl Admin Console и хосте с установленным SoftControl SysWatch было синхронизировано с погрешностью, значительно меньшей времени жизни пароля.

🔀 Генерация одноразового пароля 💦 🔪
Одноразовый пароль для SysWatch
Č
Время действия: 15 минут
Осталось времени: 00:00:00:00

Рисунок 48. Окно генерации пароля для SysWatch

Генерация одноразового пароля
Одноразовый пароль для разблокировки клавиатуры
Время действия: 15 минут
Осталось времени: 00:00:00:00

Рисунок 49. Окно генерации пароля для разблокировки клавиатуры

4.6 Настройка клиентских приложений

Вкладка **Настройки клиентов** содержит список конфигураций (наборов настроек) клиентских приложений (рис. <u>Вкладка «Настройки клиентов»</u>⁵⁹).



Рисунок 50. Вкладка «Настройки клиентов»

В SoftControl Admin Console различаются следующие типы конфигураций:

- настройки подразделения;
- частные настройки;
- локальные настройки (только для SoftControl SysWatch).

По умолчанию все клиентские компоненты после регистрации на сервере получают настройки подразделения. Частные настройки созданы для тех случаев, когда требуется задать для определенного клиентского компонента конфигурацию, отличную от конфигурации подразделения. На вкладке отображается список всех конфигураций, включая частные. Информация по работе с частными настройками приведена <u>ниже</u>⁶¹.

Основные операции с конфигурациями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 13.

Кнопка	Название	Описание
	Добавить	Создание новой конфигурации клиентских компонентов.
<u>/</u>	Редактировать	Редактирование выбранной конфигурации.
0	Удалить	Удаление выбранных конфигураций.
	Импорт	Импортирование конфигурации из XML-файла.
	Экспорт	Экспортирование выбранной конфигурации в XML-файл.

Таблица 13. Элементы управления вкладки «Настройки клиентов»

Перечень полей вкладки приведен в табл. 14.

Таблица 14. Поля вкладки «Настройки клиентов»

Поле	Описание
Имя	Наименование конфигурации клиентских компонентов.
Описание	Описание конфигурации клиентских компонентов.
Созданы	Дата и время создания конфигурации.
Подразделения	Список подразделений, к которым применяется данная конфигурация.

В SoftControl Admin Console представлены следующие категории централизованной настройки клиентских приложений:

- общие настройки⁶²;
- настройки SoftControl SysWatch⁽⁶⁶⁾;
- настройки SoftControl DLP Client⁽¹⁵⁾.
- настройки SoftControl SysCmd¹²⁴.

Основные действия, выполняемые с клиентскими конфигурациями:

Создание конфигурации подразделения

Чтобы добавить новую конфигурацию подразделения, нажмите на кнопку **Добавить** (рис. <u>Вкладка «Настройки клиентов»</u>⁵⁹). В окне **Редактирование** настроек клиентов задайте параметры конфигурации (см. рисунки, начиная с <u>Раздел «Имя и описание»</u>⁶³ и до <u>Настройки расписания обновления</u>¹²⁴). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров.

Создание конфигурации подразделения на основе существующей

Чтобы добавить новую конфигурацию на основе уже существующей, выберите ее и выполните одно из следующих действий:

- нажмите на кнопку **Редактировать** в группе кнопок вкладки (рис. <u>Вкладка</u> «Настройки клиентов»⁵⁹);
- дважды нажмите левой кнопки мыши на конфигурации.

В окне **Редактирование настроек клиентов** измените имя (обязательно) и параметры конфигурации (в случае необходимости) аналогично работе с новой конфигурацией (см. рисунки, начиная с <u>Раздел «Имя и описание»</u>⁶³ и до <u>Настройки расписания обновления</u>¹²⁴). Если внизу окна отображается статус **Значения всех параметров корректны**, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров.

Изменение типа настроек

Чтобы изменить тип настроек клиентского компонента, перейдите на вкладку <u>Устройства и статусы⁽⁴⁵⁾</u>, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите один из пунктов:

• Использовать настройки подразделения:

Назначить клиентскому компоненту настройки подразделения, которому он принадлежит.

• Использовать частные настройки:

Назначить клиентскому компоненту частные настройки.

• Отправить повторно настройки клиенту с локальными настройками:

Назначить клиентскому компоненту SoftControl SysWatch, настройки которого были изменены локально, последнюю конфигурацию, заданную с сервера SoftControl Server.

Использование частных конфигураций

Чтобы добавить новую частную конфигурацию и назначить ее клиентскому компоненту, перейдите на вкладку <u>Клиенты⁴⁵</u>, вызовите контекстное меню требуемого клиентского компонента правой кнопкой мыши и выберите пункт **Использовать частные настройки**. В окне **Выбор частных настроек** нажмите на

кнопку **Добавить** для создания новой частной конфигурации (рис. <u>Управление</u> частными настройками⁶²).

🔀 Выбор частных настроек	×
Список доступных частных настроек:	
Custom_settings_A	Добавить
	Ок Отмена

Рисунок 51. Управление частными настройками

В окне **Редактирование настроек клиентов** задайте параметры конфигурации (см. рисунки, начиная с <u>Раздел «Имя и описание»</u>⁶³ и до <u>Настройки расписания</u> <u>обновления</u>¹²⁴). Если внизу окна отображается статус **Значения всех параметров** корректны, нажмите на кнопку **Применить** для добавления созданной конфигурации; в обратном случае измените некорректные значения параметров. Созданная конфигурация будет добавлена в список частных настроек. Выберите в списке ее или ранее созданную конфигурацию, после чего нажмите на кнопку **ОК** для применения конфигурации к клиентскому компоненту.

Удаление конфигурации

Для удаления конфигурации выберите ее, нажмите на кнопку **Удалить** (рис. <u>Вкладка «Настройки клиентов»</u>⁵⁹) и подтвердите удаление в диалоговом окне.

4.6.1 Общие настройки

Данная категория настроек включает в себя общие параметры конфигурации и настройки взаимодействия клиентских приложений с сервером.

✓ Имя и описание

Имя конфигурации клиентских приложений необходимо для однозначной

идентификации определенного набора настроек, описание конфигурации – для его краткой характеристики.

Чтобы задать **Имя и описание**, в одноименном разделе категории **Общие** настройки введите **Имя** и **Описание** в соответствующих полях (рис. <u>Раздел «Имя</u> и описание»⁶³).

🚩 Редактирование настроек клиенто	08	×
 Общие настройки Имя и описание 	Имя:	Конфигурация 1
Хартбит IP адреса сервера Номер лицензии • SysWatch • DLP • SysCmd	Описание: Основной набор настроек клиентов.	
	Значения всех параметров корректны	Применить Отмена

Рисунок 52. Раздел «Имя и описание»

Имя конфигурации должно быть уникальным и не может совпадать с уже существующими конфигурациями.

⊸ Хартбит

Хартбит, или интервал обращения клиентского приложения к серверу – параметр клиентских компонентов, отвечающий за периодичность установки связи с серверным компонентом SoftControl Server. По умолчанию устанавливается равным 60 с (1 минута).

Редактирование настроек клиентов			_ = ×
 Общие настройки Имя и описание 	Период хартбита (сек.):	30	
хартоит IP-адреса сервера Номер лицензии	Скрыть службу Windows	рвисным центром	
 DLP SysCmd 	Синхронизировать времи с сервером		
	Значения всех параметров корректны		
		Применить	Отмена

Рисунок 53. Раздел «Хартбит»

Для изменения параметра перейдите в раздел **Хартбит** категории **Общие** настройки и установите значение в поле **Период хартбита (сек.)** (рис. <u>Раздел</u> «Хартбит»⁶³).

Выставите галочку **Держать постоянное соединение с Сервисным Центром**, если необходимо поддерживать соединение с SoftControl Service Center в режиме реального времени.

Кроме того, галочку **Держать постоянное соединение с Сервисным Центром** следует выставить, если для компонента SoftControl DLP Client необходимо включить запись видео по требованию. Настройки записи видео см. в разделе <u>Настройки SoftControl DLP Client</u>¹²².

Выставите галочку **Скрыть службу Windows**, если системные службы SoftControl SysWatch (*safensec.exe*), SoftControl DLP Client (*eventsvc.exe*) и SoftControl SysCmd (SysCmd.exe) не должны показываться в оснастке **Службы** ОС Windows.

<u>Примечание</u>: скрытие системных служб не работает на ОС Windows XP.

<u>Примечание</u>: если системные службы скрыты, то управлять ими при помощи средств ОС невозможно.

Выставите галочку Синхронизировать время с сервером для того, что бы SoftControl SysWatch синхронизировал время на клиентском компьютере с временем SoftControl Server.

IP-адреса сервера

Задание адресов сервера для подключения со стороны клиентских приложений производится мастером настройки сервера⁽²⁴⁾.

Для изменения списка адресов перейдите в раздел **IP адреса сервера** категории **Общие настройки** (рис. <u>Раздел «IP адреса сервера»</u>⁶⁵). Чтобы добавить адрес в перечень, введите новое значение IP-адреса или имени в соответствующем поле и нажмите на кнопку **Добавить в список**. Чтобы удалить адрес из перечня, выберите его и нажмите на кнопку **Удалить из списка**.

🔀 Редактирование настроек клиенто	08	×
 Общие настройки Имя и описание Хартбит ІР адреса сервера Номер лицензии SysWatch DLP SysCmd 	Введите новое значение: Добавить в списох 172.16.16.5 VM-AS-W61RUX86 Удалить из списка	
- ,		
	Значения всех параметров корректны Применить Отм	иена

Рисунок 54. Раздел «IP адреса сервера»

✓ Номер лицензии

Лицензионный ключ определяет функциональность клиентских компонентов. По умолчанию устанавливается пробная лицензия сроком действия 30 дней.

Для задания ключа перейдите в раздел **Номер лицензии** категории **Общие** настройки, выберите тип клиентского компонента в выпадающем списке (SysWatch, DLP, DeCrypt, SysCmd), введите ключ в текстовое поле и нажмите на кнопку **Проверить** для проверки лицензии и отображения ее параметров в случае

корректного ключа (рис. <u>Раздел «Номер лицензии»</u>⁽⁶⁶⁾).

🔀 Редактирование настроек клиен		s _ 🗆 X
 Общие настройки 		
Имя и описание		SysWatch BVT5E-NFUQ3-JDMUF-YQ3M
Хартбит		
IP-адреса сервера		Тип лицензии: Коммерческая Срок действия (дней): 30
Номер лицензии		AV_AV4
 SysWatch 		
Контроль активности		
Управление инцидентами		
Защита паролем		
 Сканирование 		
Общие настройки		
Настройки расписания		
 Обновление 		Проверить
Общие настройки		
Источники обновлений	U	
Настройки расписания		
Настройки интерфейса		
Отчеты		
Оповещения		
Одноразовые пароли		
 Политика контроля 		
Устройства		
Модули		опачения всех параметров корректив
Доверенный список автоз		
Файловая система		Применить Отмена
Системный реестр		

Рисунок 55. Раздел «Номер лицензии»

4.6.2 Настройки SoftControl SysWatch

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl SysWatch, аналогичную задаваемой с помощью ГИП SoftControl SysWatch, и политики контроля.

🗢 Контроль активности

В разделе **Контроль активности** категории **SysWatch** установите флажки у требуемых областей контроля (рис. <u>Настройки контроля активности</u>⁶⁶):

• Контроль активности:

- Приложения;
- 🛛 Сеть;
- Файловая система;
- Реестр.



Рисунок 56. Настройки контроля активности

Ниже отметьте необходимые дополнительные опции программы и контроля активности:

Отключить профиль системы:

Отключить контроль исполняемых файлов РЕ на клиентском хосте.

Запретить внешнее управление службой:

Запретить выгрузку системной службы SoftControl SysWatch из ОЗУ клиентского хоста.

Глобальный режим обновления ПО:

Запускать все приложения в режиме установки.

При включении данного режима <u>все</u> приложения запускаются как инсталлятор и добавляются в профиль (режим обучения). Кроме того, в профиль добавляются все изменения в исполняемых файлах PE. Рекомендуется использовать только на «чистых» системах, все ПО для которых устанавливалось с «золотого» образа. Для включения и выключения режима потребуется перезагрузка клиентского хоста.

Сохранять историю активности неотслеживаемых приложений и инсталляторов:

Автоматически включать опции записи истории активности при первом

запуске приложения, отсутствующего в профиле, или инсталлятора без ЭЦП.

• Контролировать выполнение скриптов:

Заблокировать выполнение недоверенных скриптов интерпретаторами (кроме скриптов, подписанных ЭЦП из белого списка сертификатов). Запрещаются следующие процессы:

- wscript.exe (Microsoft ® Windows Based Script Host);

- cscript.exe (Microsoft ® Console Based Script Host);

– java.exe (Java[™] Platform SE binary);

- javaw.exe (Java[™] Platform SE binary);

- javaws.exe (Java™ Web Start Launcher).

Для запрета запуска определенных процессов рекомендуется создавать соответствующие <u>Правила политики контроля</u>⁽⁹²⁾.

<u>Примечание</u>. Если в разделе **Управление инцидентами** для инцидента **Запуск интерпретатора скриптов** выбрано решение **Разрешить**, выполнение скрипта будет разрешено. Событие при этом заносится в лог.

Все интерпетаторы скриптов находятся в системной папке:

Система будет запрещать только процессы, запущенные из системной папки (C:\Windows\System32 или C:\Windows\SysWOW64).

Эта опция активна, только если выбрана опция Контролировать выполнение скриптов.

□ Включить контроль dll-модулей (требуется перезагрузка клиента):

Контроль запуска dll-модулей работает следующим образом. При попытке загрузить dll-библиотеку SoftControl SysWatch проверяет, подписана ли она ЭЦП. Если библиотека подписана и Windows признает ЭЦП действительной, то загрузка библиотеки разрешается (даже если ее нет в профиле). Если у библиотеки отсутствует ЭЦП, SoftControl SysWatch проверяет, есть ли данная библиотека в профиле. Если есть, запуск разрешается; если нет – запрещается.

<u>Примечание 1</u>. Не поддерживается запрет на запуск библиотек, в которых отсутствует точка входа (библиотек, содержащих только ресурсы, без исполняемого кода).

<u>Примечание 2</u>. Если в разделе **Управление инцидентами** для инцидента **Загрузка недоверенной DLL** выбрано решение **Разрешить**, запуск будет

разрешен. Событие при этом заносится в лог.

Контролировать модификацию РЕ-файлов не инсталляторами:

Запретить изменения исполняемых файлов (exe, dll и т.п.) всеми приложениями, кроме работающих в режиме обновления ПО.

<u>Примечание</u>. Если в разделе **Управление инцидентами** для инцидента **Модификация РЕ-файла не инсталлятором** выбрано решение **Разрешить**, изменение исполняемых файлов будет разрешено. Событие при этом заносится в лог.

□ Удалять информацию о приложениях, не запускавшихся более (дней):

Удалять из базы данных SoftControl SysWatch записи о неактивных приложениях, удовлетворяющих заданному условию (число дней без активности).

Отложить запуск системной службы на (мин.):

Установить интервал задержки запуска системной службы SoftControl SysWatch.

Записывать однотипные события нарушения политики контроля после (сек.):

Установить интервал, по истечении которого однотипные события будут записываться в отчет (по умолчанию 60 секунд). События нарушения политики контроля считаются *однотипными* и не вносятся в отчет, если одновременно выполняются следующие условия:

- у событий совпадают:
 - о действия;
 - о исполняемые файлы;
 - о командные строки процессов;
 - о идентификаторы (PID) процессов;
- время, прошедшее с момента добавления предыдущего события, меньше заданного значения.

При этом в локальный файл отчета на клиентском хосте с SoftControl SysWatch добавляется информация о том, сколько однотипных событий было пропущено.

Проверять наличие запущенных модулей после старта SysWatch через (мин.):

Установить интервал задержки после запуска SoftControl SysWatch, после которого начнется проверка наличия модулей, имеющих флаг <u>Должен быть</u> запущенным при старте системы⁽⁹⁰⁾, среди запущенных процессов.

Некоторые модули имеют критическую важность для работы системы. SoftControl Service Center позволяет указать модули, наличие которых необходимо проверять, и задать временной интервал после запуска SoftControl SysWatch, по истечении которого проверяется, запущены ли нужные модули. Если некоторые модули не обнаружены, создается соответствующее событие безопасности.

Проверять наличие запущенных модулей после входа пользователя через (мин.):

Установить интервал задержки после входа пользователя в систему, после которого начнется проверка наличия модулей, имеющих флаг <u>Должен быть</u> <u>запущенным в пользовательской сессии</u>⁽⁹¹⁾, среди запущенных процессов.

Некоторые модули имеют критическую важность для при работе пользователя в системе. SoftControl Service Center позволяет указать модули, наличие которых необходимо проверять, и задать временной интервал после входа пользователя, по истечении которого проверяется, запущены ли нужные модули. Если некоторые модули не обнаружены, создается соответствующее событие безопасности.

Высокий риск отсутствия модулей:

Если отмечено и в ходе проверки среди запущенных процессов не обнаружены модули, имеющие флаги <u>Должен быть запущенным в пользовательской сессии</u> ⁽⁹¹⁾ или <u>Должен быть запущенным при старте системы</u>⁽⁹⁰⁾, то в логе будет сгенерировано событие **Критической**, а не **Высокой** важности.

• Отслеживать наличие отладчика:

Если отмечено и будет обнаружено наличие отладчика ядра в системе или подключение отладчиком к процессу safensec.exe, то в логе будет сгенерировано событие **Критической** важности.

Восстанавливать базу данных после аппаратной перезагрузки:

В случае аппаратной перезагрузки восстановить базу данных из последней

резервной копии. SoftControl SysWatch создает резервную копию базы данных при начале работы, при получении новых настроек с сервера и при локальном изменении настроек.

Включить отправку событий из журналов Windows на сервер:

Передавать на сервер события из журналов Windows (System, Security и Application) на клиентском устройстве.

Управление инцидентами

В разделе Управление инцидентами категории SysWatch установите флажок Включить автоматическую обработку инцидентов и задайте реакцию на инциденты из перечня Список инцидентов в выпадающем списке Решение согласно табл. 15 (рис. <u>Настройки реакции на инциденты</u>⁷¹).

🔀 Редактирование настроек клиентов	8		_ = ×
 Общие настройки 			
Имя и описание		🗹 Включить автоматическую обработку инци	дентов
Хартбит		Список инцидентов	
IP-адреса сервера		Запуск придожения не в профиде	
Номер лицензии		Запуск неполлисанного инсталлятора	
 SysWatch 			
Контроль активности		парушение политики контроля	
Управление инцидентами		запуск интерпретатора скриптов	
Защита паролем		Загрузка недоверенной DLL	
 Сканирование 		Модификация РЕ-файла	
Общие настройки			
Настройки расписания			
 Обновление 			
Общие настройки			
Источники обновлений			
Настройки расписания			
Настройки интерфейса			
Отчеты			
Оповещения			
Одноразовые пароли			
 Политика контроля 		Управление инцидентами	
Устройства		Payrantea	23630////000375
Модули		гешение.	Заблокировать
Доверенный список автозагр			
Файловая система			
Системный реестр		Значения всех параметров корректны	
Сеть			
Хэш-суммы файлов			
Профили безопасности	Ŧ		Применить Отмена

Рисунок 57. Настройки реакции на инциденты

Таблица 15. Возможные действия при инцидентах

Инцидент	Действия						
Запуск приложения не в профиле	• Выполнить в ограниченном режиме Выполнение приложения в изолированной среде (песочнице) под учетной записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом добавления в профиль системы не происходит, а приложение помещается в ограниченную зону. Приложение может загружать дочерние модули, которые также не войдут в профиль системы. Даже если такое приложение является вредоносным и						

Инцидент	Действия
	выполнит установку каких-либо дополнительных компонентов, то их последующая
	загрузка будет предотвращена.
	 Выполнить в ограниченном режиме после проверки
	Запуск приложения в ограниченном режиме, если при антивирусном сканировании
	приложения не найдено вредоносного кода. В обратном случае запуск будет
	заблокирован.
	 Выполнить в режиме обновления ПО
	Выполнение приложения под текущей учетной записью без ограничений. При
	этом приложение и все его дочерние модули помещаются в профиль системы и
	доверенную зону.
	 Выполнить в режиме обновления ПО после проверки
	Запуск приложения в режиме обновления ПО, если при антивирусном
	сканировании приложения не найдено вредоносного кода. В обратном случае
	запуск будет заблокирован.
	• Заблокировать
	Блокировка запуска приложения.
	• Установить
	Выполнение инсталлятора под текущей учетной записью без ограничений. При
	этом после установки приложение и все его дочерние модули помещаются в
	профиль системы и доверенную зону.
	 Установить после проверки
	Запуск инсталлятора в режиме обновления ПО, если при антивирусном
	сканировании установщика не найдено вредоносного кода. В обратном случае
Запуск	запуск будет заблокирован.
неподписанного	• Установить в ограниченном режиме
инсталлятора	выполнение инсталлятора в изолированной среде (песочнице) под учетной
	записью пользователя «V.I.P.O.» с ограниченными привилегиями. При этом
	дооавления в профиль системы не происходит.
	• эстановить в ограниченном режиме после проверки Запуск инстандатора в ограниценном режиме если при антивирусном
	сканировании установщика не найлено вредоносного кода. В обратном случае
	запировании установщика не наидено вреденосного кода. В соратном олу нас
	• Заблокировать
	Блокировка запуска инсталлятора.
	• Разрешить
	Разрешение приложению выполнить лействие совпалающее с условиями
	правила заданной политики контроля.
Нарушение политики	• Разрешить после проверки
	Разрешение приложению выполнить действие, совпадающее с условиями
	правила заданной политики контроля, если при антивирусном сканировании
	приложения не найдено вредоносного кода. В обратном случае действие будет
	запрещено.
Komponn	• Запретить
	Запрет приложению выполнить действие, совпадающее с условиями правила
	заданной политики контроля.
	 Запретить и завершить приложение
	Запрет приложению выполнить действие, совпадающее с условиями правила
	заданной политики контроля, и последующее завершение приложения.
Запуск	• Разрешить
интерпретатора	Разрешение запуска без ограничений.
Инцидент	Действия
---	---
скриптов	• Запретить Запрет запуска.
Загрузка недоверенной DLL	 Разрешить Разрешение загрузки DLL-библиотеки без ограничений. Запретить Запрет загрузки.
Модификация РЕ-файла не инсталлятором	 Разрешить Разрешение модификации РЕ-файла. Запретить Запрет модификации.

Сбросьте флажок **Включить автоматическую обработку инцидентов**, если предполагается делегировать полномочия по обработке инцидентов локальному пользователю SoftControl SysWatch.

▽ Защита паролем

Чтобы установить общий парольный доступ к интерфейсу и/или деинсталлятору SoftControl SysWatch на клиентском хосте, перейдите в раздел **Защита паролем** категории **SysWatch** и установите флажок **Включить защиту паролем** (рис. <u>Настройки парольной защиты</u>⁷³).



Рисунок 58. Настройки парольной защиты

Задайте Пароль и введите его Подтверждение, после чего отметьте области

действия:

П Изменение свойств программы:

Запрос пароля при доступе к ГИП SoftControl SysWatch.

Удаление программы:

Запрос пароля при запуске удаления SoftControl SysWatch.

Выставите флажок **Запретить локальное управление настройками**, если необходимо запретить редактирование настроек SoftControl SysWatch с клиентского хоста. Состояние данной опции будет также отображаться на вкладке Клиенты⁽⁴⁵⁾.

Настройки сканирования

В разделе Сканирование → Общие настройки категории SysWatch настройте опции антивирусной проверки (рис. <u>Общие настройки сканирования</u>⁽⁷⁴⁾).

🔀 Редактирование настроек клиентов	_ = ×
 Общие настройки Имя и описание Хартбит IP-адреса сервера Номер лицензии SysWatch Контроль активности Управление инцидентами Защита паролем 	Реакция на угрозу Выбор действия автоматически Выбор действия по окончанию проверки Запрос действия Типы файлов Проверка составных файлов
 Сканирование Общие настройки Настройки расписания Обновление Настройки интерфейса Отчеты Оповещения Одноразовые пароли Политика контроля DLP SysCmd 	
	Применить Отмена

Рисунок 59. Общие настройки сканирования

В области **Реакция на угрозу** выберите один из вариантов действий при обнаружении угроз в процессе антивирусного сканирования:

Выбор действия автоматически:

Обезвредить инфицированный объект или удалить его, если лечение не удается.

Выбор действия по окончанию проверки:

Запрос действия будет выведен локальному пользователю SoftControl SysWatch по всем обнаруженным угрозам по завершению проверки.

□ Запрос действия:

Запрос действия будет выведен локальному пользователю SoftControl SysWatch при обнаружении каждой угрозы.

В области **Типы файлов** выберите типы файлов, которые будут подвергнуты проверке:

Все файлы:

Сканирование всех типов файлов, за исключением составных типов, не отмеченных в области **Проверка составных файлов** (флажки **Почтовые базы** и **Архивы**).

П Только исполняемые файлы

Сканирование только файлов формата РЕ.

В области **Проверка съемных носителей** установите флажок **Автоматическая проверка съемных носителей**, если необходимо автоматически запускать антивирусное сканирование USB-носителей после их подключения к клиентскому хосту. Установите флажок **Спрашивать о проверке съемных носителей** для отображения диалогового окна с предложением проверки на клиентском хосте.

В области **Учетная запись для сканера** установите флажок **Использовать учетную запись** и введите учетные данные, если требуется указать учетную запись, под которой будет производиться проверка, отличную от системной на клиентском хосте.

В разделе Сканирование → Настройки расписания категории SysWatch можно установить расписание антивирусной проверки, для этого установите флажок Задать расписание и настройте параметры (рис. <u>Настройки</u> расписания <u>сканирования</u>⁽⁷⁵⁾).

🔀 Редактирование настроек клиентов	-			_ = ×
 Общие настройки SysWatch Контроль активности Управление инцидентами Защита паролем Сканирование Общие настройки Настройки расписания 	 Задать расписание Тип расписания: Частота дней: Время запуска: 		По дням	1
Настройки интерфейса Отчеты Оповещения Одноразовые пароли • Политика контроля • DLP • SysCmd	Сканирование памяти Сканирование загрузочных с Сканирование всех жестких д Сканирование всех съемных	Области ска екторов цисков носителей	анирования	Отмена

Рисунок 60. Настройки расписания сканирования

В счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

В разделе Области сканирования можно ограничить сканирование только выбранными областями.

Настройки обновления

В разделе **Обновление** → **Общие настройки** категории **SysWatch** настройте опции обновления (рис. Общие настройки обновления ⁷⁶).

SoftControl Service Center версия 6.0.98

Централизованное управление СИБ

🔀 Редактирование настроек клиентов	_ = ×
 Общие настройки 	(Comp eference)
SysWatch	Состав обновлении
Контроль активности	Программные модули
Эправление инцидентами	🗹 Антивирусные базы
Сканирование	
Сканирование	Соединение
Обнике изстройки	
Истолицие настройки	использовать параметры прокси-сервера
Настройки расписания	Адрес: Порт:
Настройки интерфейса	80
Отчаты	
Оповещения	Использовать авторизацию на прокси
Одноразовые пароли	Имя пользователя: Пароль:
 Политика контроля 	
► DLP	
 SysCmd 	
	Подтверждение от пользователя
	Запрашивать подтверждение перед обновлением
	Сбор профиля
	Выполнить обновление антивирусных баз перед сбором профиля
	Значения всех параметров корректны
	Применить Отмена

Рисунок 61. Общие настройки обновления

В области **Состав обновлений** выберите требуемые компоненты SoftControl SysWatch для обновления:

Программные модули;

□ Антивирусные базы.

В области **Соединение** установите флажок **Использовать параметры проксисервера** и укажите необходимые настройки, если для соединения с интернетсервером обновлений используется прокси-сервер.

В области **Подтверждение от пользователя** установите флажок **Запрашивать подтверждение перед обновлением**, если требуется отображать диалог с запросом подтверждения операции на клиентском хосте.

В области **Сбор профиля** установите флажок **Выполнить обновление** антивирусных баз перед сбором профиля, если требуется обновить базы перед сбором профиля на клиентском хосте.

В разделе **Обновление** \rightarrow **Источники обновлений** можно выбрать способ обновления:

 • Обновить через Сервисный Центр – обновление посредством внутрисетевого сервера обновлений; Обновить через интернет – обновление через сервер обновлений ООО «АРУДИТ СЕКЬЮРИТИ», доступный посредством сети Интернет. В области
 Источник обновлений указываются адреса, с которых производится
 обновление ядра проактивной защиты и баз антивирусных компонентов. Значения по умолчанию берутся из настроек обновления компонента SoftControl Service Center.

 Редактирование настроек клиентов Общие настройки SysWatch Контроль активности Управление инцидентами) ()) () 1ст	бновить чере Юновить чере очник обновл	ез Сервисный Центр ез интернет лений:		_ 🗆 ×
Защита паролем						
 Сканирование 		Þ	SNS	http://192.168.115.50/updates/		
• Обновление			AVN	http://updates.safensoft.com/AV5/		
Общие настройки						
Источники обновлений						
Настройки расписания						
Настройки интерфейса						
Отчеты						
Оповещения						
Одноразовые пароли		_				
 Политика контроля 						
► DLP	Зна	че	ния всех пара	метров корректны		
 SysCmd 						
					Применить	Отмена

Рисунок 62. Настройки источников обновления

В разделе **Обновление** → **Настройки расписания** категории **SysWatch** можно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. <u>Настройки расписания обновления</u>⁽⁷⁸⁾). В счетчике **Частота дней** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

Редактирование настроек клиентов		_ = ×
 Общие настройки 		
 SysWatch 	Задать расписание	
Контроль активности	Тип расписания	
Управление инцидентами	тип расписания.	Подням
Защита паролем	Userses and N	
 Сканирование 	частота днеи:	
 Обновление 		
Общие настройки	Время запуска:	00:00:00
Источники обновлений		
Настройки расписания		
Настройки интерфейса		
Отчеты		
Оповещения		
Одноразовые пароли		
 Политика контроля 		
► DLP		
 SysCmd 		
	Значения всех параметров корректны	
		Применить Отмена

Рисунок 63. Настройки расписания обновления

Настройки интерфейса

В разделе **Настройки интерфейса** категории **SysWatch** выберите необходимые опции интерфейса SoftControl SysWatch на клиентских хостах (рис. <u>Настройки</u> интерфейса⁷⁹):

SoftControl Service Center версия 6.0.98

Централизованное управление СИБ

🚩 Редактирование настроек клиентов	-	
 Редактирование настроек клиентов Общие настройки SysWatch Контроль активности Управление инцидентами Защита паролем Сканирование Обновление Настройки интерфейса Отчеты Оповещения Одноразовые пароли Политика контроля DLP SysCmd 	 Показывать значок программы в области уведомлений Включить звуковое сопровождение 	<u> </u>
	Значения всех параметров корректны Применить Отмена	

Рисунок 64. Настройки интерфейса

Показывать значок программы в области уведомлений:

отображение значка SoftControl SysWatch в области уведомлений.

Включить звуковое сопровождение:

сопровождать уведомления программы звуками.

🗢 Отчеты

В разделе **Отчеты** категории **SysWatch** настройте параметры SoftControl SysWatch по протоколированию в текстовые отчеты и регистрации событий в WMI (рис. <u>Настройки отчетов</u>⁸⁰).

В области **Отчеты** установите флажок **Формировать отчеты**, чтобы включить функцию ведения текстовых отчетов, и выберите виды событий для протоколирования:

- Обновление;
- Проверка;

Системный:

- 🛛 Угрозы;
- □ Службы и неподозрительные приложения.

Редактирование настроек клиентов	_ = ×
 Редактирование настроек клиентов Общие настройки SysWatch Контроль активности Управление инцидентами Защита паролем Сканирование Обновление Настройки интерфейса Отчеты Оповещения Одноразовые пароли Политика контроля DLP SysCmd 	Отчеты Формировать отчеты Обновление Проверка Системный Угрозы Службы и неподозрительные приложения Формировать отчеты (в днях): 30 Ротация отчетов Ротация отчетов Ограничение по времени: 0 Сек Ограничение по времени: 0 Количить ротацию Ограничение по времени: 0 МІВ Количить ротации ОТРАНИЧЕНИЕ С
	Регистрация событий в WMI Включить регистрацию событий в WMI Размер истории WMI: 10 Значения всех параметров корректны Применить Отмена

Рисунок 65. Настройки отчётов

Выставите галочку Службы и неподозрительные приложения, чтобы включить запись событий запуска/остановки служб. Службы, которые были запущены до системной службы safensec.exe, будут помечаться в отчетах как была запущена ранее.

В счетчике **Формировать отчеты (в днях)** установите количество дней, за которые сохраняется история событий.

В области **Ротация отчетов** при необходимости установите флажок **Включить ротацию** и укажите параметры ротации (один или несколько), ограничивающие количественные характеристики текстовых отчетов:

• Ограничение по времени:

введите в данном поле временной лимит одного файла отчета и выберите единицы величины в выпадающем списке (секунды, минуты, часы, дни).

• Ограничение по размеру:

введите в данном поле лимит по размеру одного файла отчета и выберите единицы величины в выпадающем списке (Б, КиБ, МиБ).

• Количество хранимых логов:

введите в данном поле максимальное число хранимых частей файлов отчетов.

В области **Регистрация событий в WMI** установите флажок **Включить регистрацию событий в WMI** для включения соответствующей функции и укажите **Размер истории WMI** в одноименном поле.

Для предотвращения проблем с повышенным потреблением системных ресурсов не рекомендуется задавать размер истории равным более 100 событий, оптимальная величина – от 10 до 50 событий.

▽ Оповещения

В разделе Оповещения категории SysWatch установите флажок Показывать оповещения для отображения локальных оповещений SoftControl SysWatch на клиентских хостах и выберите необходимые типы сообщений (рис. <u>Настройка</u> локальных оповещений⁽⁸²⁾):

- Статус защиты;
- Обновление программы;
- Проверка компьютера;
- Отчеты;
- Плицензия;
- **Установка (удаление)** программ;
- Блокирование модулей программы;
- Ограничение приложений.

🚩 Редактирование настроек клиентов	_ = ×
 Общие настройки SysWatch Контроль активности 	✓ Показывать оповещения
Управление инцидентами Защита паролем Сказироварино	🗌 Статус защиты
 Обновление Аастройки интерфейса 	Обновление программы
Отчеты Оповещения Одноразовые пароли	🗌 Проверка компьютера
 Политика контроля DLP SysCmd 	🗌 Отчеты
	Плицензия
	🗌 Установка (удаление) программ
	Блокирование модулей программы
	Ограничение приложений
	Значения всех параметров корректны
	Применить Отмена

Рисунок 66. Настройка локальных оповещений

Одноразовые пароли

В разделе **Одноразовые пароли** категории **SysWatch** установите флажок **Включить одноразовые пароли** и нажмите на кнопку **Сгенерировать ключ**) для выработки 256-битного ключа, на основе которого будут вычисляться одноразовые пароли (рис. <u>Настройки одноразовых паролей</u>⁽⁸³⁾).

Смена ключа делает недействительными все предыдущие пароли.

Редактирование настроек клиентов	_ = ×
 Редактирование настроек клиентов Общие настройки SysWatch Контроль активности Управление инцидентами Защита паролем Сканирование Обновление Настройки интерфейса Отчеты Оповещения Одноразовые пароли Политика контроля DLP SysCmd 	 Включить одноразовые пароли Ключ для генерации паролей (смена ключа делает недействительными все предыдущие пароли): О7UIFv5gtwGfpsPjwRP8plqUTuBFQxlavADkeyCjWJk=
	Значения всех параметров корректны Применить Отмена

Рисунок 67. Настройки одноразовых паролей

Для блокировки клавиатуры на клиентском хосте выставите галочку **Блокировать** клавиатуру. После того как SoftControl SysWatch получит настройки, клавиатура на клиентском хосте будет заблокирована. Для снятия блокировки необходимо ввести пароль. SoftControl SysWatch проверяет все введенные пользователем последовательности символов, и как только распознает пароль, блокировка клавиатуры снимается. Кроме того, блокировка снимается при отключении и перезапуске системной службы *safensec.exe*.

Если клавиатура не используется в течение 15 минут, она снова блокируется.

Непосредственная генерация одноразовых паролей осуществляется на вкладке Подразделения⁵⁷.

Политика контроля: Устройства

В разделе **Политика контроля** → **Устройства** категории **SysWatch** настройте правила использования следующих внешних устройств и портов системы на клиентских хостах (рис. <u>Политика контроля устройств</u>⁸⁵):

- СОМ-порты;
- LPT-порты;
- CD/DVD-устройства;

• USB-устройства.

Чтобы определить права доступа к USB-устройствам, задайте их соответствующими флажками в столбцах **Чтение**, **Запись** и **Удаление** для типа **USB-устройства**.

Дополнительно можно задать исключения – белый список USB-устройств, для которых назначенное правило действовать не будет. Для этого нажмите на ссылку **Дополнительно** и в появившемся окне нажмите на кнопку **+** (**Добавить**) (рис. Исключения для USB-устройств⁽⁸⁵⁾).

общие настройки		Устройство	- Чтение	- Запись	• Улаление •	
 SysWatch 		остройство	ПСПИС	Saluce	- удаление -	
Контроль активности	'	сом-порты				
Управление инцидентами		сругругра				
Защита паролем		СD/DVD-устроиства				
 Сканирование 		ОЅВ-устроиства	\checkmark	\checkmark	\checkmark	
 Обновление 						
Настройки интерфейса						
Отчеты						
Оповещения						
Одноразовые пароли						
 Политика контроля 						
Устройства						
Модули						
Доверенный список автозагру	3					
Файловая система						
Системный реестр						
Системный реестр Сеть] Запретить автозапуск ,	для всех устро	йств		
Системный реестр Сеть Хэш-суммы файлов		Запретить автозапуск ,	для всех устро	ЙСТВ		
Системный реестр Сеть Хэш-суммы файлов Профили безопасности) Запретить автозапуск ,	для всех устро	йств		
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов] Запретить автозапуск ,	для всех устро	ЙСТВ		
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов		Запретить автозапуск,	для всех устро	йств		
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов Сертификаты) Запретить автозапуск ,	для всех устро	йств		
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов Сертификаты Запрещенные службы		Запретить автозапуск ,	для всех устро [йств Іользователи и І	интервалы	Дополнительн
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов Сертификаты Запрещенные службы		Запретить автозапуск ,	для всех устро [йств Іользователи и І	интервалы	Дополнительн
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов Сертификаты Запрещенные службы > DLP > SysCmd	Зна) Запретить автозапуск , зчения всех параметров	для всех устро [в корректны	йств Іользователи и і	интервалы	Дополнительны
Системный реестр Сеть Хэш-суммы файлов Профили безопасности Привилегии процессов Взаимодействие процессов Сертификаты Запрещенные службы • DLP • SysCmd	Зна) Запретить автозапуск , ачения всех параметров	для всех устро [в корректны	иств	интервалы	Дополнительн

Рисунок 68. Политика контроля устройств

🚩 Белый спі	исок USB устройст	В					-	
Активно	ID поставщика	ID продукта	Ревизия	Серийный №	Чтение 🔻	Запись	Удаление	-
I	0930	6545	Kingston DT_101_G2 PMAP	001CC0C61220EA9044200183	\checkmark	\checkmark	\checkmark	A
								v
						Примени	ть Отмен	a
					5			

Рисунок 69. Исключения для USB-устройств

Введите параметры USB-устройства в соответствующих полях. Получить данные параметры USB-устройства можно следующим образом:

- 1) Вставьте носитель в USB-порт компьютера.
- 2) Откройте оснастку **Диспетчер устройств** (Device Manager) Панели управления Windows.
- 3) Разверните категорию **Дисковые устройства** (Disk drives) и дважды нажмите левой кнопкой мыши на имени искомого USB-носителя.
- 4) В появившемся окне перейдите на вкладку Сведения (Details).
- 5) В выпадающем меню выберите свойство **Родитель** (Parent). В поле **Значение** (Value) отобразится строка вида:

USB\VID_<ID поставщика>&PID_<ID продукта>\<Серийный №>,

где указаны соответствующие числовые значения параметров ID поставщика,

- ID продукта и Серийный № (показаны в угловых скобках).
- 6) В выпадающем меню выберите свойство ИД оборудования (Hardware Ids). В поле Значение (Value) отобразится список аппаратных идентификаторов, первый из которых необходимо использовать в качестве параметра Ревизия.

После ввода параметров выберите права доступа для данного устройства в соответствующих столбцах **Чтение**, **Запись** и **Удаление**. Чтобы включить устройство в белый список, установите флажок в столбце **Активно**.

Чтобы удалить устройство из списка, нажмите на кнопку 🧧 (Удалить).

Правила сохраняются после нажатия на кнопку Применить.

Для USB-устройств можно также задать временные интервалы и пользователей (или группы пользователей), для которых будут действовать выбранные права доступа. Для этого нажмите на ссылку Пользователи и интервалы. В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи SoftControl в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку Применить.

🚩 Пользователи и интерв	алы		-	
Пользователи Windows	Пользователи S	oftControl	Временные интервалы	
Выберите временные ин правило.	нтервалы, в течен	ие которых	будет действовать данно	e
Начало)		Конец	
12:39:53		17:05:53		
4		Доб	авить Удалить	
			рименить Отмен	a

Рисунок 70. Добавление временных интервалов и пользователей для правила

Чтобы заблокировать доступ к CD/DVD-устройствам, COM-портам или LPT-портам, сбросьте любой из флажков в столбцах **Чтение**, **Запись** или **Удаление** для соответствующих типов устройств (при этом будут сброшены все флажки для данного типа).

Для изменения прав доступа к портам (COM, LPT) дополнительно необходима перезагрузка системы на клиентских хостах.

Отметьте опцию Запретить автозапуск для всех устройств, если требуется блокировать автозагрузку всех USB- и CD/DVD-устройств.

🗢 Политика контроля: Модули

В разделе **Политика контроля** → **Модули** категории **SysWatch** вы можете задать правила для отдельных приложений, установленных на клиентских хостах (рис. <u>Политика контроля модулей</u>^{®7}). По умолчанию данная возможность отключена; для включения выставите флажок **Использовать частные настройки для модулей**.

При выставленном флажке Использовать частные настройки для модулей после применения настроек на клиентских хостах все локальные настройки будут удалены без возможности восстановления.

SoftControl Service Center версия 6.0.98

Централизованное управление СИБ

Редактирование настроек клиентов	-	_	_	_ [
Общие настроики	\checkmark	Использовать част	ные настройки для модулей	
Syswatch		L 🔉 🖮		
Контроль активности		- 🧶 🏠		
		14	V	2
		РМЯ	комментарии	зона выполнения
Сканирование	•	wuauclt.exe	Windows Upadate	Доверенные приложения
Истористичность с то ста		alg.exe	Application Layer Gateway Service	Доверенные приложения
Пастроики интерфеиса		smss.exe	Session Manager Windows NT	Доверенные приложения
Отчеты		csrss.exe	Client Server Runtime Process	Доверенные приложения
Оповещения		winlogon.exe	Windows NT Logon application	Доверенные приложения
Одноразовые пароли		services.exe	Services Control Manager	Доверенные приложения
• Политика контроля		svchost.exe	Generic Host Process for Win32 Services	Доверенные приложения
Устроиства		lsass.exe	LSA Shell	Доверенные приложения
Ловорони ий стисок оргозории		trustedinstaller.exe	Windows Modules Installer	Доверенные приложения
Доверенный список автозагруз		mscorsvw.exe	.NET Runtime Optimization Service	Доверенные приложения
Файловая система		wupdmar.exe	Windows Update Manager for NT	Доверенные приложения
Системный реестр		wuapp.exe	Windows Update Application Launcher	Ловеренные приложения
Хаш-одины файдов		drvinst.exe	Driver Installation Module	Ловеренные приложения
Профили безопасности		dinotify eve	Windows Device Installation	Ловеренные приложения
	E	ComEvec.eve	CCM agent service	Доверенные приложения
Вазимолействие процессов	E	TSManager eve	CCM TSMapager	Доверенные приложения
Сертификаты		adhinst ove	Application Compatibility Database Installer	Доверенные приложения
Запрешенные службы		sabinstexe	Application Compatibility Database Installer	доверенные приложения
П Р		wininit.exe	windows start-Up Application	доверенные приложения
SysCmd	Знач	ения всех параметр	оов корректны	
			При	менить Отмена

Рисунок 71. Политика контроля модулей

По умолчанию окно содержит ряд модулей ОС Windows. Чтобы добавить в список новый модуль, нажмите на кнопку **+** (**Добавить**). Появившееся окно (рис. <u>Создание правил для модуля</u>⁸⁸) содержит ряд вкладок для добавления информации о модуле и задания правил для него.

>			-	
Правила для реестра	Правил	а для сети	Привилегии процесса	
Общие настройки		Правила для файло	вой системы	
Идентификационные данные	модуля			
Имя модуля	Ko	мментарий		
Пути файлов				*
		Полобио		Ŧ
Harrison and the second second		Подробно		
Пазвание организации:	<u> </u>			- 1
Описание:				- 1
Авторские права:				- 1
Версия:				
<u>Добавить данные из файла</u>			ОК Отме	на

Рисунок 72. Создание правил для модуля

На вкладке Идентификационные данные модуля укажите общую информацию по модулю:

- Имя модуля обязательный параметр;
- Пути файлов множество возможных путей к файлу; поле может быть пустым;
- Комментарий краткое описание модуля.

В поле **Пути файлов** могут использоваться маски – инструмент задания правил для добавляемых объектов. Например, с помощью масок можно задать часть пути к файлу. Ниже приведен синтаксис масок:

- #*# заменяет любое количество символов, кроме символа '\';
- #**# заменяет любое количество символов;
- #?# заменяет ровно 1 любой символ.

Также вы можете выбрать модуль, щелкнув по ссылке **Добавить данные из** файла (рис. <u>Создание правил для модуля</u>⁽⁸⁸⁾) и указав в появившемся окне требуемый файл. Данные на вкладке **Идентификационные данные модуля** в этом случае будут заполнены автоматически.

При применении настроек на клиентском хосте исполняемые модули сопоставляются с заданными идентификационными данными следующим образом. Исполняемый модуль считается совпадающим с описанием, если все заданные в идентификационных данных поля соответствуют данному модулю. При этом:

- если для модуля задано несколько путей, достаточно совпадения любого из них;
- если информация о версии модуля представлена в ресурсах на разных языках, то достаточно <u>полного</u> совпадения описания версии на любом языке.

>		_ = ×
Правила для реестра	Правила для сети	Привилегии процесса
Идентификационные данные модуля	а Общие настройки	Правила для файловой системы
Зона выполне Включить режим обновления ПО Сохранять историю запуска Изолированный пользователь (Полированный пользователь (Полированный пользователь (Полированный пользователь Полированный пользователь Полирования Полированный пользователь Полированный	ния Ограниченные приложения Назначение учетной записи V.I.P.O. четной записи си зарте системы взовательской сессии	
Добавить данные из файла		ОК Отмена

Рисунок 73. Создание правил для модуля: Общие настройки

На вкладке Общие настройки укажите условия выполнения модуля.

В области Зона выполнения выберите зону, в которой должен запускаться модуль:

- Ограниченные приложения;
- Заблокированные приложения;
- Доверенные приложения.

Выставите галочки **Включить режим обновления ПО**, если модуль должен запускаться в данном режиме (только для Доверенных приложений), и **Сохранять историю запуска** для записи истории активности модуля.

В группе Назначение учетной записи выберите, под какой учетной записью запускать данное приложение (только для Ограниченных приложений):

- Изолированный пользователь V.I.P.O.;
- Не использовать назначение учетной записи.

Выставите галочку **В доверенном списке автозагрузки**, если данный модуль необходимо включить в доверенный список автозагрузки (подробнее про доверенный список автозагрузки написано в разделе <u>Политика контроля</u> → <u>Доверенный список автозагрузки</u>⁽⁹¹).

Выставите галочку Должен быть запущенным при старте системы, если

необходимо проверить, находится ли этот модуль среди запущенных модулей после старта системы (подробнее в разделе <u>Контроль активности</u>⁷⁰).

Выставите галочку **Должен быть запущенным в пользовательской сессии**, если необходимо проверить, находится ли этот модуль среди запущенных модулей после входа пользователя в систему (подробнее в разделе <u>Контроль активности</u>⁷⁰).

На вкладке **Правила для файловой системы** задаются правила для доступа приложения к объектам файловой системе (аналогично настройкам в разделе Политика контроля: Файловая система⁹²).

На вкладке **Правила для реестра** задаются правила для доступа приложения к объектам системного реестра (аналогично настройкам в разделе <u>Политика</u> контроля: Системный реестр⁹⁶).

На вкладке **Правила для сети** задаются правила контроля сетевой активности для приложения (аналогично настройкам в разделе Политика контроля: Сеть¹⁰⁰).

На вкладке **Привилегии процесса** задаются ограничения на использование процессом привилегий Windows на клиентских хостах (аналогично настройкам в разделе <u>Политика контроля: Привилегии процессов</u>¹⁰⁹).

Чтобы изменить данные модуля, нажмите на кнопку *(Изменить)* или дважды щелкните по нему и настройте параметры аналогично действиям при добавлении модуля.

Чтобы удалить модуль из списка, нажмите на кнопку 🛽 (Удалить).

Правила сохраняются после нажатия на кнопку Применить.

Политика контроля: Доверенный список автозагрузки

Доверенный список автозагрузки нужен для того, чтобы отслеживать запуск приложений, не включенных в этот список. Включать в доверенный список автозагрузки следует модули, при запуске которых нет необходимости создавать событие безопасности.

В разделе **Политика контроля** → **Доверенный список автозагрузки** категории **SysWatch** отображается список модулей, включенных в список автозагрузки (рис. <u>Доверенный список автозагрузки</u>⁹²). Добавить модули в список можно в

разделе Политика контроля → Модули (см. выше⁽⁹⁰⁾).

Если параметр **Использовать доверенный список автозагрузки** включен, при логировании процесса отмечается, входит запускаемый модуль в доверенный список или нет.

🔀 Редактирование настроек клиентов				-	
 Общие настройки 					
 SysWatch 		Использова	ть доверенный список автозаг	рузки.	
Контроль активности	E	Вы можете до	бавить модули в список на вк	ладке Модули.	
Управление инцидентами					
Защита паролем		Имя	Комментарий		
 Сканирование 	•	csrss.exe	Client Server Runtime Process		
 Обновление 		lsass.exe	LSA Shell		
Настройки интерфейса		drvinst.exe	Driver Installation Module		
Отчеты					
Оповещения					
Одноразовые пароли					
 Политика контроля 					
Устройства					
Модули					
Доверенный список автозагруз					
Файловая система					
Системный реестр					
Сеть					
Хэш-суммы файлов					
Профили безопасности					
Привилегии процессов					
Взаимодействие процессов					
Сертификаты					
Запрещенные службы					v
► DLP					
 SysCmd 	Зна	чения всех п	араметров корректны		
				Применить Отмен	a
▲ ►					

Рисунок 74. Доверенный список автозагрузки

Политика контроля: Файловая система

В разделе **Политика контроля** → **Файловая система** категории **SysWatch** определите правила доступа приложений к объектам файловой системы на клиентских хостах (рис. <u>Политика контроля файловой системы</u>⁹²):

- Чтение файла или каталога;
- Запись в файл или каталог (создание/изменение файла или каталога);
- Удаление файла или каталога.

Редактирование настроек клиентов						
Общие настроики	п	равила д	ля зоны			
Koutpost artisteroctie						
Управление инцилентами		Эграниче	нные приложения			
Защита пародем			🔊 🕅 🛛 🛧 💻 🔜			
Сканирование						
 Обновление 		ID	Ресурс	Чтение	Запись	Уда
Настройки интерфейса		100	#SYSTEM32#DRIVERS\ETC\hosts	Разрешить	Запретить	3anr
Отчеты		101	#SYSTEM32##**#.#MODEXT#	Разрешить	Запретить	Запр
Оповещения		102	#WINDIR##**#	Разрешить	Запретить	3an;
Одноразовые пароли		103	#WINDIR##**#.#MODEXT#	Разрешить	Запретить	3anp
 Политика контроля 		104	#WINDIR#WIN.INI	Разрешить	Запретить	Запр
Устройства		105	#WINDIR#SYSTEM.INI	Разрешить	Запретить	Запр
Модули		106	#WINDIR#CONTROL.INI	Разрешить	Запретить	Запр
Доверенный список автозагруз		107	#WINDIR#TASKS\AT#*#.JOB	Разрешить	Запретить	Запр
Файловая система		108	#C:\#BOOT.INI	Разрешить	Запретить	Запр
Системный реестр		109	#C:\#AUTOEXEC.BAT	Разрешить	Запретить	Запр
Сеть		110	#C:\#MSDOS.SYS	Разрешить	Запретить	Запр
Хэш-суммы файлов		111	#PERSONAL##**#	Разрешить	Запретить	Запр
Профили безопасности		112	#ANVSTARTUP##**#	Разрешить	Запретить	Запс
Привилегии процессов		114	#**# #MODEXT#	Разрешить	Запретить	3anr
Взаимодействие процессов		502	#\$N\$DIR##**#	Разрешить	Запретить	Запс
Сертификаты		502	#SVSTEM32#DRIVERS\SNISCORE BLK	Разрешить	Запретить	3anr
Запрещенные службы						•
	2					
syscma	Shav	спия все	х параметров корректны			
				Применит		мена

Рисунок 75. Политика контроля файловой системы

Правила разделены по спискам для приложений из следующих зон выполнения:

• Доверенные приложения;

• Ограниченные приложения.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- Все создать правило для обеих зон выполнения, если правило находится только в одном списке;
- Ограниченные переместить правило в список правил для ограниченных приложений;
- Доверенные переместить правило в список правил для доверенных приложений.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Чтение**, **Запись** и **Удаление**. Флажок в столбце **Активно** указывает, действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет

выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок **1** (**Вверх**) и **4** (**Вниз**).

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов файловой системы. Например, с помощью масок можно создать правило для каталога и всех объектов внутри него или правило для определенных типов (расширений) файлов.

Ниже приведен синтаксис масок:

- #*# заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на файлы корневой директории);
- #**# заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);
- #?# заменяет ровно 1 любой символ.

Чтобы создать правило, нажмите на кнопку + (Добавить).

В появившемся окне введите полный путь до объекта файловой системы или маску в поле **Файл или каталог** (рис. <u>Создание правила для объекта файловой</u> системы⁽⁹⁴⁾).

Вы можете указывать как папки на локальном жестком диске, так и сетевые папки. При создании правила для сетевых папок путь указывается в виде \ *\<имя_сервера>\<имя_папки>*. Вместо символа '\\' можно использовать маску #**#; в этом случае будут проверяться и сетевые, и локальные папки. Кроме того, можно указывать IP-адрес компьютера с сетевой папкой.

Если в правиле указан IP-адрес компьютера, то правило будет действовать, только если пользователь при доступе к папке указывает IP-адрес, а не сетевой путь. Поэтому если необходимо контролировать доступ и по IP-адресу, и по сетевому пути, создайте два отдельных правила.

M		×
Файл или каталог (полный пут	ъ или маска)	
E:\#*#LOG#?#.TXT		
Профиль безопасности:	(profile_1
Чтение	Запись	Удаление
Запретить 💽	Запретить	Запретить
🗸 Активно	[ОК Отмена
Рисунок 76. Созда	ание правила дл	ія объекта файловой

системы

Выберите <u>профиль безопасности для правила</u>¹⁰⁵ в соответствующем выпадающем списке.

<u>Замечание</u>. Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** \rightarrow **Профили безопасности**.

В областях **Чтение**, **Запись** и **Удаление** выберите в выпадающих списках соответствующие права доступа к объекту:

- Разрешить позволить приложению выполнять операцию над объектом;
- Запретить заблокировать выполнение приложением операции над объектом.

Обратите внимание, что если запрещено чтение, автоматически запрещены также запись и удаление.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **ОК**.

Чтобы изменить правило, нажмите на кнопку \angle (Изменить) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия пользователей (или правила И группы 203 пользователей), К которым оно применяется, нажмите на кнопку (Дополнительно). В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи **SoftControl** в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку **Применить**..

🔀 Пользователи и интерв	алы		_ 🗆 X
Пользователи Windows	Пользователи S	oftControl	Временные интервалы
Выберите временные ин правило.	нтервалы, в течен	ие которых	будет действовать данное
Начало	b		Конец
12:39:53		17:05:53	
		Доб	авить Удалить
			рименить Отмена

Рисунок 77. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку 📴 (Удалить).

В наборе политик контроля SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на системные каталоги и объекты расположения компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы клиентского хоста.

Политика контроля: Системный реестр

В разделе **Политика контроля** → **Системный реестр** категории **SysWatch** определите правила доступа приложений к объектам системного реестра на клиентских хостах (рис. <u>Политика контроля системного реестра</u>⁹⁶):

- Запись в ключ или параметр реестра (создание/изменение ключа или параметра);
- Удаление ключа или параметра реестра.

Общие настройки SysWatch	п	равила д	ля зоны			
Контроль активности	6	Ограниче	нные приложения			
Управление инцидентами Защита паролем Сканирование			2 🙆 🛧 🎩 💀			
• Обновление		ID	Ресурс	Запись	Удаление	Актие
Настройки интерфейса		10	\REGISTRY\MACHINE\SOFTWARE\CLASSES\	Разрешить	Разрешить	
Отчеты		11	\REGISTRY\MACHINE\SOFTWARE\CLASSES\	Запретить	Разрешить	
Оповещения		12	\REGISTRY\MACHINE\SOFTWARE\CLASSES\	Запретить	Разрешить	
Одноразовые пароли		13	\REGISTRY\MACHINE\SOFTWARE\CLASSES\	Запретить	Разрешить	\checkmark
 Политика контроля 		14	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Разрешить	
Устройства		15	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Запрос	
Модули		16	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Запрос	
Доверенный список автозагруз		17	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Запрос	
Файловая система		18	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Разрешить	
Системный реестр		19	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Разрешить	
Сеть		20	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Разрешить	
Хэш-суммы файлов		21	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запретить	Разрешить	
Профили безопасности		22		Запретить	Разрешить	
Привилегии процессов		23	\REGISTRY\MACHINE\SOFTWARE\MICROS	Запрос	Разрешить	
Взаимодействие процессов		24	VREGISTRY MACHINE SOFTWARE MICROS	Запрос	Разрешить	
Сертификаты		24		Запрос	Разрешить	
Запрещенные службы						•
DLP . SysCmd	Знач	ения все	х параметров корректны			

Рисунок 78. Политика контроля системного реестра

Правила разделены по спискам для приложений из следующих зон выполнения:

• Доверенные приложения;

• Ограниченные приложения.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- Все создать правило для обеих зон выполнения, если правило находится только в одном списке;
- Ограниченные переместить правило в список правил для ограниченных приложений;
- Доверенные переместить правило в список правил для доверенных приложений.

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор **ID**. Объекты применения указываются в столбце **Ресурс**, права доступа к ним – в столбцах **Запись** и **Удаление**. Флажок в столбце **Активно** указывает, действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет

выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок **1** (**Вверх**) и **4** (**Вниз**).

Строка в столбце **Ресурс** представляет собой путь до объекта или объектов применения правила. В данной строке могут использоваться маски – инструмент задания правил для группы объектов системного реестра. Например, с помощью масок можно создать правило для раздела реестра и всех объектов внутри него. Ниже приведен синтаксис масок:

- #*# заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на параметры раздела);
- #**# заменяет любое количество символов (в случае размещения в конце строки распространяется на параметры раздела, подразделы и параметры подразделов);
- #?# заменяет ровно 1 любой символ.

Чтобы создать правило, нажмите на кнопку + (Добавить).

В появившемся окне введите полный путь до объекта системного реестра или маску в поле **Ключ или параметр реестра**, (рис. <u>Создание правила для объекта</u> <u>системного реестра</u>⁽⁹⁸⁾), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- \REGISTRY\MACHINE\SOFTWARE\CLASSES\-раздел HKEY_CLASSES_ROOT;
- \REGISTRY\MACHINE\ раздел HKEY_LOCAL_MACHINE;
- *REGISTRY\USER*\<*SID*>\ раздел HKEY_CURRENT_USER для пользователя с указанным идентификатором безопасности (<*SID*>);
- \REGISTRY\USER\ раздел HKEY_USERS.

\REGISTRY\MACHINE\TESTKE	(путь или маска) :Y\#**#
Профиль безопасности:	profile_1
Запись	Удаление
Запретить	Запретить 💽

Рисунок 79. Создание правила для объекта системного реестра

Выберите <u>профиль безопасности для правила</u>¹⁰⁵ в соответствующем выпадающем списке.

<u>Замечание</u>. Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** \rightarrow

Профили безопасности

В областях Запись и Удаление выберите в выпадающих списках соответствующие права доступа к объекту:

- Разрешить позволить приложению выполнять операцию над объектом;
- Запретить заблокировать выполнение приложением операции над объектом.

Обратите внимание, что если запрещено чтение, автоматически запрещены также запись и удаление.

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **ОК**.

Чтобы изменить правило, нажмите на кнопку \angle (Изменить) или дважды нажмите на него и настройте параметры правила аналогично действиям при его создании.

Чтобы задать время действия правила И пользователей (или группы 203 пользователей), К которым оно применяется, нажмите на кнопку (Дополнительно). В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи SoftControl в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку Применить.

🚩 Пользователи и интерв	алы		_	= ×
Пользователи Windows	Пользователи S	oftControl	Временные интервалы	
Выберите временные ин правило.	тервалы, в течен	ие которых	будет действовать данное	2
Начало)		Конец	
12:39:53		17:05:53		
۹(
		Доб	авить Удалить	
			рименить Отмена	

Рисунок 80. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку 🖾 (Удалить).

В наборе политик контроля SoftControl SysWatch содержатся предустановленные правила, распространяющиеся на ключи и параметры реестра, влияющие на работу системы и компонентов продукта. Изменение или удаление предустановленных правил может повлечь за собой нарушение защиты целостности системы клиентского хоста.

🗢 Политика контроля: Сеть

В разделе **Политика контроля** → **Сеть** категории **SysWatch** определите правила контроля сетевой активности приложений на клиентских хостах (рис. <u>Политика</u> контроля сетевой активности⁽¹⁰¹⁾):

- Прием данных;
- Передача данных.

Правила разделены по спискам для приложений из следующих зон выполнения:

- Доверенные приложения;
- Ограниченные приложения.

Для переключения между списками выберите соответствующую категорию в выпадающем списке **Правила для зоны**. Если требуется переместить правило в список для приложений из другой зоны выполнения, вызовите контекстное меню правила и выберите один из вариантов:

- Все создать правило для обеих зон выполнения, если правило находится только в одном списке;
- Ограниченные переместить правило в список правил для ограниченных приложений;
- Доверенные переместить правило в список правил для доверенных приложений.

🔀 Редактирование настроек клиентов							_ 🗆 ×
 Общие настройки SysWatch 	П	Іравила д	ля зоны		_		
Контроль активности		Ограниче	нные приложен	ия			
Управление инцидентами			×				
Защита паролем							
 Сканирование 	Ē		-			-	
 Обновление 		ID	Ресурс	Название	Направление	Проток	Разре.
Настройки интерфейса		300		Any-network-activity	Входящее/Исходящее	TCP/UDP	
Отчеты							
Оповещения							
Одноразовые пароли							
 Политика контроля 							
Устройства							
Модули							
Доверенный список автозагруз							
Файловая система							
Системный реестр							
Сеть							
Хэш-суммы файлов							
Профили безопасности							
Привилегии процессов							
Взаимодействие процессов							
Сертификаты							-
Запрещенные службы	•)			
► DLP							
 SysCmd 	Знач	чения все	х параметров к	орректны			
					применить		мена

Рисунок 81. Политика контроля сетевой активности

Каждое правило представляет собой запись в линейном списке и имеет свой уникальный идентификатор ID. Параметры правила указаны в столбцах Название, Направление и Протокол. Разрешение или запрет сетевого соединения указывается флажком в столбце Разрешение; необходимость обработки события, в случае его наступления, локальным пользователем – в столбце Подтверждение. Флажок в столбце Активно указывает, действует ли данное правило.

Если несколько правил имеют пересекающиеся области действия, то приоритет выполнения в таком случае имеет правило, расположенное в списке наиболее низко. Положение правила в списке изменяется с помощью кнопок **1** (**Вверх**) и **4** (**Вниз**).

Чтобы создать правило, нажмите на кнопку + (Добавить).

В появившемся окне задайте параметры правила (рис. Создание правила контроля

сетевой активности 102):

- Название наименование правила.
- Направление направление сетевой активности, определяющее инициатора соединения:
 - Входящее сетевое соединение, инициируемое удаленным хостом;
 - Исходящее сетевое соединение, инициируемое клиентским хостом;
 - Входящее/Исходящее любое из направлений.
- Протокол тип протокола передачи данных по сети:
 - TCP;
 - UDP;
 - TCP/UDP любой из протоколов.

На вкладках **Локальный адрес** и **Удаленный адрес** задаются конечные точки, между которыми осуществляется передача данных, на клиентском и удаленном хостах соответственно. В обеих вкладках выберите, на какие сетевые адреса и порты распространяется действие правила, и введите значения в соответствующие поля при необходимости:

- Адрес IP-адрес узла сети:
 - Любой адрес;
 - Определенный адрес;
 - Диапазон адресов.
- Порт сетевой порт:
 - Любой порт;
 - Определенный порт;
 - Диапазон портов.

2	×					
Название	HTTP Incoming Connection					
Направление	Входящее					
Протокол	ТСР					
 Разрешение Подтвержде Активно 	ние					
Профиль безопасности: profile_1						
Локальный адрес Удаленный адрес						
Адрес	Любой адрес					
Порт	Любой порт Image: Contract of the second seco					
	ОК Отмена					

Рисунок 82. Создание правила контроля сетевой активности

Для разрешения сетевого соединения с указанными параметрами установите флажок **Разрешение**, для запрещения – сбросьте его. Если предполагается обработка событий сетевой активности приложений локальным пользователем на клиентском хосте, установите флажок **Подтверждение** (при этом должна быть отключена <u>автоматическая обработка инцидентов</u>⁽⁷¹⁾).

Чтобы включить созданное правило в список и сделать его действующим, установите флажок **Активно** и нажмите на кнопку **ОК**.

Выберите <u>профиль безопасности для правила</u>¹⁰⁵ в соответствующем выпадающем списке.

<u>Замечание</u>. Установить или снять флажок **Активно** можно только в случае выбора профиля по умолчанию (**No group**). При выборе любого другого профиля, созданного пользователем, данное поле становится неактивным, и его значение совпадает со значением соответствующего поля в разделе **Политика контроля** \rightarrow **Профили безопасности**.

Чтобы изменить правило, нажмите на кнопку 🖄 (Изменить) или дважды нажмите

на него и настройте параметры правила аналогично действиям при его создании. Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на кнопку (Дополнительно). В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи SoftControl в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку Применить.

🔀 Пользователи и интерв	алы		_ 0	×		
Пользователи Windows	Пользователи So	oftControl	Временные интервалы			
Выберите временные интервалы, в течение которых будет действовать данное правило.						
Начало	b		Конец			
12:39:53		17:05:53				
4		Доб	авить Удалить			
			рименить Отмена			

Рисунок 83. Добавление временных интервалов и пользователей для правила

Чтобы удалить правило, нажмите на кнопку 🖾 (Удалить).

Политика контроля: Хэш-суммы файлов

В разделе **Политика контроля** → **Хэш-суммы файлов** вы можете создать список хэш-сумм, которые нужно включить в профиль, а также список хэш-сумм, которые из профиля нужно исключить. Эти хэш-суммы однократно применяются к профилю, но в дальнейшем настройки могут изменяться, например при запуске инсталлятора.

Хэш-суммы файлов можно добавлять в списки двумя способами: через кнопку **Добавить** или через кнопку **Импорт** (загружается файл XML).

Контрольные суммы файлов можно копировать из вкладок <u>Данные профиля⁽⁴⁹⁾</u> и Сравнение профилей¹⁸³.

 Общие настройки 								
 SysWatch 	Тип хэш-суммы							
Контроль активности	Хэш-суммы, которые нужно включить в профиль							
Управление инцидентами								
Защита паролем								
 Сканирование 								
 Обновление 	Имя файла Хэш-сумма Профиль безопасности							
Настройки интерфейса	CALC.EXE C899DA13EC520E514010CBA571838E061E No profile							
Отчеты								
Оповещения								
Одноразовые пароли								
 Политика контроля 								
Устройства								
Модули								
Доверенный список автозагруз								
Файловая система								
Системный реестр								
Сеть								
Хэш-суммы файлов								
Профили безопасности								
Привилегии процессов								
Взаимодействие процессов								
Сертификаты								
Запрещенные службы		v						
► DLP								
 SysCmd 	Значения всех параметров корректны							
	Применить От	мена						

Рисунок 84. Хэш-суммы файлов

Политика контроля: Профили безопасности

В разделе **Политика контроля** → **Профили безопасности** категории **SysWatch** вы можете загрузить из базы данных SoftControl Service Center профили безопасности, объединяющие различные правила контроля активности в логические группы (рис. <u>Профили безопасности</u>¹⁰⁵). Создать профили можно на вкладке Профили безопасности¹²⁵.

Редактирование настроек клиентов		
 Общие настройки 		
 SysWatch 		
Контроль активности		
Управление инцидентами	Имя Активно	
Защита паролем	No profile	•
 Сканирование 	Group_1	
 Обновление 	profile_1	
Настройки интерфейса		
Отчеты		
Оповещения		
Одноразовые пароли		
 Политика контроля 		
Устройства		
Модули		
Доверенный список автозагруз		
Файловая система		
Системный реестр		
Сеть		
Хэш-суммы файлов		
Профили безопасности		
Привилегии процессов		
Взаимодействие процессов		
Сертификаты		
Запрещенные службы		T
► DLP		
 SysCmd 	Значения всех параметров корректны	
	Применить Отмен	ia

Рисунок 85. Профили безопасности

По умолчанию окно содержит неизменяемый профиль (**No group**), в который включены все правила для файловой системы, системного реестра, сети и модулей, имеющиеся в соответствующих разделах окна настроек (см. рисунки <u>Политика контроля файловой системы</u>⁽⁹²⁾, <u>Политика контроля системного реестра</u>⁽⁹⁶⁾, <u>Политика контроля сетевой активности</u>⁽¹⁰¹⁾ и <u>Политика контроля модулей</u>⁽⁸⁷⁾). Правила этого профиля не подлежат редактированию и удалению. Для просмотра информации по профилю дважды нажмите на него или нажмите на кнопку **•** (**Просмотр**).

авила для файловой системы Правила для реестра		Правила для сети Модул		Модули	Хэш-суммы файлов					
Іравила д Ограниче	ля зоны нные приложения									
ID	Ресурс		Чтение	3a	пись	Удаление	Профиль	безопасности	Активно	
100	#SYSTEM32#DRIVERS\ETC\hosts		Разрешить	Запретить		Запретить	No	o group	\checkmark	
101	#SYSTEM32##**#.#N	#SYSTEM32##**#.#MODEXT#		Запретить		Запретить	No	o group	\checkmark	
102	#WINDIR##**#		Разрешить	азрешить Запретить		Запретить	No	o group	\checkmark	
103	#WINDIR##**#.#MO	DEXT#	Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
104	#WINDIR#WIN.INI	#WINDIR#WIN.INI		Зап	оетить	Запретить	No	o group	\checkmark	
105	#WINDIR#SYSTEM.INI		Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
106	#WINDIR#CONTROL	WINDIR#CONTROL.INI		азрешить Зап		Запретить	No	o group	\checkmark	
107	#WINDIR#TASKS\AT	#*#JOB	Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
108	#C:\#BOOT.INI		Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
109	#C:\#AUTOEXEC.BAT		Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
110	#C:\#MSDOS.SYS		Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	
111	#PERSONAL##**#		Разрешить	Зап	оетить	Запретить	No	o group	\checkmark	

Рисунок 86. Профиль безопасности по умолчанию

Чтобы загрузить профиль из базы данных, нажмите на кнопку **+** (**Загрузить**). В появившемся окне выберите требуемый профиль (рис. <u>Загрузка профиля</u> <u>безопасности</u>¹⁰⁷).



Рисунок 87. Загрузка профиля безопасности

Если профиль с выбранным именем уже имеется в текущих настройках, выдается сообщение об ошибке, и процесс прерывается.

Чтобы добавить правило определенной категории в профиль, выполните следующие действия:

- 1. Перейдите в соответствующий раздел настроек SoftControl SysWatch.
- 2. Создайте новое правило или откройте на редактирование существующее.
- 3. В окне создания правила выберите требуемый профиль в выпадающем списке (см. рисунки <u>Создание правила для объекта файловой системы⁹⁴</u>, <u>Создание правила для объекта системного реестра⁹⁸</u>, <u>Создание правила контроля сетевой активности¹⁰²</u>).

4. Нажмите на кнопку ОК.

Чтобы удалить из профиля правило определенной категории, перейдите в соответствующий раздел настроек SoftControl SysWatch и выполните стандартную операцию удаления в этом разделе.

Чтобы переименовать профиль, нажмите на кнопку *2* (**Переименовать**) и в появившемся окне задайте новое имя профиля.

Для просмотра информации по выбранному профилю нажмите на кнопку (**Просмотр**). В появившемся окне указана подробная информация по профилю, разделенная по категориям правил (см. рис. <u>Профиль безопасности по умолчанию</u> ⁽¹⁰⁶).

Чтобы удалить профиль безопасности, нажмите на кнопку (Удалить). Если входящие в профиль правила необходимо сохранить, в появившемся окне выберите профиль, в который они будут перенесены, и нажмите на кнопку Да (рис. Удаление профиля⁽¹⁰⁸⁾); в противном случае нажмите на кнопку Нет – тогда все правила будут удалены.

🔀 Удаление профиля	×
Перенести данные в другой профиль? При выборе варианта 'Нет' данные профиля удалятся.	
Профиль безопасности: Group_1	
Да Нет Отмена	

Рисунок 88. Удаление профиля

Политика контроля: Привилегии процессов

В разделе **Политика контроля** → **Привилегии процессов** категории **SysWatch** настройте ограничения на использование процессами следующих привилегий Windows на клиентских хостах (рис. <u>Политика контроля привилегий процессов</u>⁽¹⁰⁹⁾):

- Архивация файлов и каталогов;
- Обход перекрестной проверки;
- Создание глобальных объектов;
- Создание файла подкачки;
- Отладка программ;
- Имитация клиента после проверки пользователя;
- Увеличение приоритета выполнения;
- Настройка квот памяти для процесса;
- Загрузка и выгрузка драйверов устройств;
- Выполнение задач по обслуживанию томов;
- Профилирование одного процесса;
- Принудительное удаленное завершение работы;
- Восстановление файлов и каталогов;
- Управление аудитом и журналом безопасности;
- Завершение работы системы;
- Изменение параметров среды изготовителя;
- Профилирование производительности системы;
- Изменение системного времени;
- Смена владельцев файлов и других объектов;
- Отключение компьютера от стыковочного узла.



Рисунок 89. Политика контроля привилегий процессов

<u>Условие</u>: правила распространяются на все приложения из ограниченной зоны выполнения.

По умолчанию приложения (процессы) обладают всеми вышеуказанными привилегиями, но при этом могут быть ограничены ОС. Чтобы ограничить

привилегии вручную, сбросьте флажки у требуемых привилегий.

Описание привилегий и области их применения представлено в разделе <u>Дополнительная информация</u>²³⁷.

Чтобы действия задать время правила и пользователей (или группы 203 пользователей), которым применяется, кнопку К оно нажмите на (Дополнительно). В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи SoftControl в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку Применить.

🔀 Пользователи и интервалы 📃 🗖 🗙					
Пользователи Windows	Пользователи S	oftControl	Временные интервалы		
Выберите временные и правило.	нтервалы, в течен	ие которых	будет действовать данное		
Начало	þ		Конец		
12:39:53		17:05:53			
4					
		Доб	авить Удалить		
			рименить Отмена		

Рисунок 90. Добавление временных интервалов и пользователей для правила

Политика контроля: Взаимодействие процессов

В разделе Политика контроля → Взаимодействие процессов категории SysWatch настройте разрешения для взаимодействия процессов (рис. <u>Политика</u> контроля взаимодействия процессов⁽¹¹⁰⁾):

- Доступ приложения к буферу обмена;
- Установка приложением глобальных перехватчиков;
- Доступ к процессу и его потокам извне.

SoftControl Service Center версия 6.0.98

Централизованное управление СИБ

Редактирование настроек клиентов	
 Общие настройки Солистов 	Ограничения для процессов запускаемых в изодированной среде: взаимодействие
Syswatch	процессов с системой, межпроцессное взаимодействие.
контроль активности	
Управление инцидентами	✓ Доступ приложения к буферу обмена
защита паролем	✓ Установка приложением плооальных перехватчиков ✓ Лоступ к процессу и его потокам извне
Сканирование	
• Обновление	
Настройки интерфейса	Выбранные общие ограничения и разрешения работают только для ограниченных
Отчеты	приложении
Оповещения	
Одноразовые пароли	
 Политика контроля 	
Устройства	
Модули	
Доверенный список автозагруз	
Файловая система	
Системный реестр	
Сеть	
Хэш-суммы файлов	
Профили безопасности	
Привилегии процессов	
Взаимодействие процессов	
Сертификаты	
Запрещенные службы	Дополнительно
► DLP	
 SysCmd 	Значения всех параметров корректны
	Применить Отмена

Рисунок 91. Политика контроля взаимодействия процессов

Условие: правила распространяются на все приложения из ограниченной зоны выполнения, запущенные под учетной записью пользователя «V.I.P.O.». Чтобы задать время действия правила и пользователей (или группы пользователей), к которым оно применяется, нажмите на ссылку Дополнительно. В появившемся окне укажите временные интервалы на вкладке Временные интервалы и добавьте пользователей на вкладке Пользователи Windows с помощью кнопки Добавить (функциональность вкладки Пользователи SoftControl в текущей версии не реализована). Чтобы изменения вступили в силу, нажмите на кнопку Применить.

🔀 Пользователи и интере	алы		_ = ×
Пользователи Windows	Пользователи S	oftControl	Временные интервалы
Выберите временные ин правило.	нтервалы, в течен	ие которых	будет действовать данное
Начало	þ		Конец
12:39:53		17:05:53	
۹(▶
		Доб	авить Удалить
			рименить Отмена

Рисунок 92. Добавление временных интервалов и пользователей для правила

Политика контроля: Сертификаты

В разделе **Политика контроля** → **Сертификаты** категории **SysWatch** определите белый список сертификатов ЭЦП для дополнительного контроля активности процессов на клиентских хостах (рис. <u>Белый список сертификатов</u>⁽¹¹²⁾).

При запуске приложения SoftControl SysWatch эвристически определяет, является ли оно инсталлятором или скриптом. По умолчанию инсталлятор запускается в режиме обновления ПО, если имеет действительную ЭЦП. Помимо этого, возможна дополнительная проверка сертификата ЭЦП на наличие в белом списке сертификатов. Для этого установите флажок **Использовать белый список сертификатов** и сформируйте список.

Редактирование настроек клиентов		-
 Общие настройки 		
SysWatch	Использовать белый список сертификатов	
Контроль активности	Название	▼ Серийный номер md5
Управление инцидентами	VeriSign Class 3 Public Primary Certification Authorit	ty - C0e965295a89486d009b8185c16edff2
Защита паролем	VeriSign Class 3 Code Signing 2010 CA	55457f9620861e149c22b14416ab4e
 Сканирование 	PROTEKSHEN TEKHNOLODZHI, OOO	37f05e46c0d4523bd6fd128c3f3bfbe
 Обновление 	Protection Technology, Ltd.	a6f061c3e13986475def457f064ef0c8
Настройки интерфейса	Protection Technology, Ltd.	32549657ea535f09c8c705767bf0c78
Отчеты	Protection Technology, Ltd.	2e24f15473dd7fd28faab8bec05772a
Оповещения	Microsoft Root Authority	8eb4e1485b47be8616d5f8347c29ce
Одноразовые пароли	COMODO Time Stamping Signer	2112329c61f5cd01f63ea5752433402
 Политика контроля 	Class 3 Public Primary Certification Authority	160a6b895f88ad99abda036aa6d050
Устройства	outrie that a second se	100000000000000000000000000000000000000
Модули		
Доверенный список автозагруз		
Файловая система		
Системный реестр		
Сеть		
Хэш-суммы файлов		
Профили безопасности		
Привилегии процессов		
Взаимодействие процессов		
Сертификаты		
Запрещенные службы	Добавить Удалить	
DLP		
SvsCmd	Значения всех параметров корректны	
, ,		
		Применить Отмена

Рисунок 93. Белый список сертификатов

Изначально SoftControl SysWatch содержит базовый список сертификатов доверенных производителей, в том числе сертификаты Protection Technology, Ltd. Чтобы добавить новый сертификат, нажмите на ссылку **Добавить** и укажите приложение, инсталлятор или сценарий, подписанный ЭЦП, сертификат которого требуется включить в перечень, после чего нажмите на кнопку **Открыть**. В появившемся окне со списком сертификатов ЭЦП выбранного файла установите флажки в столбце **Добавить** для требуемых сертификатов и нажмите на кнопку **ОК** (рис. <u>Выбор сертификатов для добавления</u>⁽¹¹³⁾). Установите флажок в столбце **Добавлен**ых сертификатов (рис. <u>Белый список сертификатов</u>⁽¹¹²⁾).

Выберите сертификаты для добавления 🛛 🗖 🗙					
Перетяните сюда мышкой заголовок колонки для группировки данных по ней					
	Название	Добавить	Дата окончания		
	Microsoft Time-Stamp PCA		4/3/2021		
	Microsoft Code Signing PCA		9/1/2020		
۲	Microsoft Corporation	\checkmark	8/11/2018		
	Microsoft Time-Stamp Service		9/7/2018		
				V	
		(OK Ca	ncel	

Рисунок 94. Выбор сертификатов для добавления

Если необходимо исключить сертификат из перечня доверенных без его удаления, сбросьте флажок в столбце **Доверять**. Для полного удаления сертификата из списка выберите его и нажмите на ссылку **Удалить** (рис. <u>Белый список</u> <u>сертификатов</u>¹¹²).

Политика контроля: Запрещенные службы

В разделе Политика контроля → Запрещенные службы категории SysWatch задается список служб, выполнение которых на клиентских хостах требуется заблокировать.

По умолчанию запрещены следующие службы: *RemoteRegistry*, *TermService*, *SSDPSRV*, *RDSessMgr*, *Seclogon* (рис. <u>Запрещенные службы</u>⁽¹¹⁴⁾). Чтобы дополнить список, выставите галочку **Запретить выполнение следующих служб**, введите название службы в появившейся ячейке и нажмите Enter.

После применения настроек на клиентских хостах перечисленные службы переходят в состояние *Отключена*. Если какая-либо служба была запущена на момент применения настроек, она продолжит работу.

 Общие настройки SurMatab 	Запретить выполнение следующих служб:
Sysvatch	
Контроль активности	RemoteRegistry
Управление инцидентами	TermService
Защита паролем	SSDPSRV
• Сканирование	RDSessMgr
• Обновление	Seclogon
Настройки интерфейса	
Отчеты	
Оповещения	
Одноразовые пароли	
 Политика контроля 	
Устройства	
Модули	
Доверенный список автозагруз	
Файловая система	
Системный реестр	
Сеть	
Хэш-суммы файлов	
Профили безопасности	
Привилегии процессов	
Взаимодействие процессов	
Сертификаты	
Запрещенные службы	
DLP	
 SysCmd 	Значения всех параметров корректны
	Применить Отмен
Ри	сунок 95. Запрешенные службы

Снова включить выполнение служб, внесенных в список, можно только вручную.

4.6.3 Настройки SoftControl DLP Client

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl DLP Client.

🗢 Сбор данных

В разделе **Сбор данных** категории **DLP** установите флажок **Собирать данные** и отметьте необходимые области собираемой информации (рис. <u>Настройки сбора</u> <u>данных</u>¹¹⁶):

Время работы с приложением;

- Использование USB-устройств;
- Печать документов;
- Ввод текста с клавиатуры.

Наблюдение за файловой системой⁽¹¹⁷⁾, системным реестром⁽¹¹⁹⁾ и сетевым <u>трафиком⁽¹²¹⁾</u> активно при выставленной опции Собирать данные и заданном правиле (правилах) в соответствующих пунктах раздела Наблюдение.

Редактирование настроек клиентов	_ = ×
 Общие настройки SysWatch DLP Сбор данных Оптимизация Наблюдение Обновление SysCmd 	 Собирать данные Время работы с приложением Использование USB-устройств Печать документов Ввод текста с клавиатуры Значения всех параметров корректны
	Применить Отмена

Рисунок 96. Настройки сбора данных

▽ Оптимизация

В разделе **Оптимизация** категории **DLP** задаются временные параметры регистрации событий (рис. <u>Настройки оптимизации</u>¹¹⁶).

🔀 Редактирование настроек клиентов	
 Общие настройки SysWatch DLP Сбор данных Оптимизация Наблюдение Обновление SysCmd 	Время регистрации простоя по истечении (мс.): 30000 Не регистрировать однотипные события, если период времени меньше, чем (мс.): 10000
	Значения всех параметров корректны
	Применить Отмена

Рисунок 97. Настройки оптимизации

В соответствующих полях задайте временные интервалы Время регистрации простоя по истечении (мс.) и Не регистрировать однотипные события, если период времени меньше, чем (мс.) в миллисекундах.

<u>Примечание</u>: опция **Не регистрировать однотипные события, если промежуток** времени меньше, чем (мс.) применяется только при наблюдении за ресурсами файловой системы. Опция **Время регистрации простоя по истечении (мс)** работает при включенной опции **Время работы с приложением** (см. рис. <u>Настройки сбора данных</u>⁽¹¹⁶⁾) и учитывает время простоя активного приложения, когда пользователь не нажимает на кнопки и не двигает мышью в течение указанного времени.

Наблюдение: Файловая система

В разделе **Наблюдение** → **Файловая система** категории **DLP** осуществляется выбор объектов файловой системы для наблюдения (рис. <u>Настройки наблюдения</u> <u>за файловой системой</u>⁽¹¹⁸⁾).

Чтобы добавить объект для наблюдения, нажмите на кнопку + (**Добавить**) и введите полный путь до него в появившемся окне (рис. <u>Объект наблюдения</u>⁽¹¹⁸⁾).

Вы можете использовать маски – инструмент задания правил для группы объектов файловой системы. Например, с помощью масок можно создать правило для каталога и всех объектов внутри него или правило для определенных типов (расширений) файлов. Ниже приведен синтаксис масок:

- #*# заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на файлы корневой директории);
- #**# заменяет любое количество символов (в случае размещения в конце строки распространяется на файлы корневой директории, поддиректории и файлы поддиректорий);
- #?# заменяет ровно 1 любой символ.

Например, чтобы установить наблюдение за каталогом и всеми вложенными объектами, добавьте символы *#**#* в конец строки. Нажмите на кнопку **ОК** для добавления указанного объекта в список.

Вы можете указывать как папки на локальном жестком диске, так и сетевые папки. При создании правила для сетевых папок путь указывается в виде \ *\<имя_сервера>\<имя_папки>*. Вместо символа '\\' можно использовать маску #**#; в этом случае будут проверяться и сетевые, и локальные папки. Кроме того, можно указывать IP-адрес компьютера с сетевой папкой.

Если в правиле указан IP-адрес компьютера, то правило будет действовать, только если пользователь при доступе к папке указывает IP-адрес, а не

сетевой путь. Поэтому если необходимо контролировать доступ и по IPадресу, и по сетевому пути, создайте два отдельных правила.

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку *∠* (Изменить). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку кнопку (Удалить).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчетах:

□ Чтение;

🛛 Запись;

Удаление;

Переименование;

• Изменение.

В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.



Рисунок 98. Настройки наблюдения за файловой системой

🔀 Укажите объект наблюдения	×
C:\Windows\System32\#**#	ר
ОК Отмена	1
	2

Рисунок 99. Объект наблюдения

Операция Запись регистрируется при открытии на запись файла, который еще не существует. Если файл уже существовал, то при открытии его на запись

регистрируется операция Изменение.

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции <u>теневого копирования</u>¹²² и выставленной галочке в полях **Удаление** или **Изменение**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с <u>заданными</u> параметрами¹²² в момент возникновения наблюдаемого события.

Наблюдение: Системный реестр

В разделе **Наблюдение** → **Системный реестр** категории **DLP** осуществляется выбор объектов системного реестра для наблюдения (рис. <u>Настройки наблюдения</u> за системным реестром⁽¹¹⁹⁾).

Редактирование настроек клиентов					_ 0
 Общие настройки 					
 SysWatch 					
▼ DLP			-		
Сбор данных	Объект наблюдения	Чтение	Запись	Удаление	Переиме
Оптимизация	\REGISTRY\MACHINE\SOFTWARE#**#	\checkmark	\checkmark	\checkmark	
 Наблюдение 					
Файловая система					_
Системный реестр					_
нттр					_
Теневое копирование					_
Настройки записи видео					_
Обновление					
 SysCmd 					•
	Значения всех параметров корректны				
1					
1			Прим	енить	Отмена
4					

Рисунок 100. Настройки наблюдения за системным реестром

Чтобы добавить объект для наблюдения, нажмите на кнопку **+** (**Добавить**) и введите полный путь до него в появившемся окне (рис. <u>Объект наблюдения</u>⁽¹²⁰⁾), при этом корневые разделы реестра в задаваемом пути должны быть указаны следующим образом:

- *REGISTRY\MACHINE\SOFTWARE\CLASSES* раздел HKEY_CLASSES_ROOT;
- \REGISTRY\MACHINE\ раздел HKEY_LOCAL_MACHINE;
- *REGISTRY\USER*\<*SID*>\ раздел HKEY_CURRENT_USER для пользователя с указанным идентификатором безопасности (<*SID*>);
- \REGISTRY\USER\ раздел HKEY_USERS.

Вы можете использовать маски – инструмент задания правил для группы объектов

системного реестра. Например, с помощью масок можно создать правило для раздела реестра и всех объектов внутри него. Ниже приведен синтаксис масок:

- #*# заменяет любое количество символов, кроме символа '\' (в случае размещения в конце строки распространяется только на параметры раздела);
- #**# заменяет любое количество символов (в случае размещения в конце строки распространяется на параметры раздела, подразделы и параметры подразделов);
- #?# заменяет ровно 1 любой символ.

Например, чтобы установить наблюдение за ключом реестра и всеми вложенными объектами, добавьте символы *#**#* в конец строки. Нажмите на кнопку **ОК** для добавления указанного объекта в список.

×
,

Рисунок 101. Объект наблюдения

Чтобы изменить путь к объекту, выберите его в списке и нажмите на кнопку *≧* (Изменить). Для удаления объекта из под наблюдения выберите его и нажмите на кнопку [™] (Удалить).

Для каждого объекта возможен выбор следующих операций, которые должны быть зарегистрированы в отчетах:

- 🛛 Чтение;
- 🛛 Запись;
- Удаление;
- Переименование.

В случае переименования объекта на клиентском хосте дальнейшее наблюдение за ним не производится.

При установке опции **Теневая копия** будет осуществляться сохранение резервной копии наблюдаемого объекта перед его модификацией, в случае включенной глобальной опции <u>теневого копирования</u>¹²² и выставленной галочке в полях **Удаление** или **Запись**. При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с <u>заданными параметрами</u>¹²² в

момент возникновения наблюдаемого события.

Наблюдение: НТТР-трафик

В разделе **Наблюдение** → **НТТР** категории **DLP** осуществляется задание наблюдаемых данных в сетевом трафике (рис. <u>Настройки наблюдения за сетевым</u> трафиком⁽¹²¹).

🔀 Редактирование настроек клиентов		_ 0
 Общие настройки 	1 💷 🔉 📷	
 SysWatch 		
▼ DLP	Объект наблюдения	Запись видео
Соор данных		
Оптимизация	maiware	
 Наблюдение 	Iexplorer.exe	
Файловая система		
Системный реестр		
НТТР		
Теневое копирование		
Настройки записи видео		
Обновление		
 SysCmd 		
	Значения всех параметров корректны	
		Применить Отмена

Рисунок 102. Настройки наблюдения за сетевым трафиком

Чтобы добавить данные для наблюдения, нажмите на кнопку **+** (**Добавить**) и введите строку в появившемся окне (рис. <u>Объект наблюдения</u>¹²¹). Наличие указанного текста будет отслеживаться при передаче данных по протоколу HTTP. В том числе это могут быть запросы пользователя в поисковых системах через интернет-браузер или имя файла, передаваемого по сети. Нажмите на кнопку **OK** для добавления строки в список.

🔀 Укажите объект наблюдения	×
malware	
ОК Отмена	

Рисунок 103. Объект наблюдения

Чтобы изменить отслеживаемый текст, выберите строку в списке и нажмите на кнопку *2* (Изменить). Для удаления текста из под наблюдения выберите строку в списке и нажмите на кнопку [™] (Удалить).

При установке опции **Запись видео** будет производиться сохранение снимков экрана клиентского хоста с <u>заданными параметрами</u>¹²² в момент возникновения наблюдаемого события.

Наблюдение: Теневое копирование

В разделе **Наблюдение** → **Теневое копирование** категории **DLP** осуществляется настройка сохранения теневых копий наблюдаемых объектов (рис. <u>Настройки</u> теневого копирования⁽¹²²⁾).

🔀 Редактирование настроек клиентов	_ = ×
 Общие настройки SysWatch DLP Сбор данных Оптимизация Наблюдение Файловая система Системный реестр НТТР Теневое копирование Настройки записи видео Обновление SysCmd 	Включить теневое копирование Локальный путь сохранения копий файлов
	Значения всех параметров корректны Применить Отмена

Рисунок 104. Настройки теневого копирования

Установите флажок **Включить теневое копирование** для включения функции сохранения резервных копий наблюдаемых объектов <u>файловой системы</u>⁽¹¹⁷⁾ и <u>системного peectpa</u>⁽¹¹⁹⁾ в случае их изменения. Индивидуальная настройка по включению данной опции для отдельных объектов задается в свойствах наблюдения. Теневые копии объектов передаются на сервер и доступны через консоль управления. Они также сохраняются локально на клиентских хостах с установленным SoftControl DLP Client по пути, указанному в поле **Локальный путь** сохранения копий файлов или в следующий каталог по умолчанию, если путь не указан:

<каталог установки SoftControl DLP Client>\Backups

Наблюдение: Настройки записи видео

В разделе **Наблюдение** → **Настройки записи видео** категории **DLP** осуществляется настройка сохранения снимков экрана при возникновении наблюдаемых событий (рис. Настройки записи видео⁽¹²²).

Редактирование настроек клиентов				_ = ×
 Общие настройки 				
 SysWatch 	Продолжительность записи (сек.)	15		
▼ DLP		200		
Сбор данных	астота кадров (мел.			
Оптимизация	Ширина кадра (рх.):	800		
 Наблюдение 				
Файловая система	Задать расписание			
Системный реестр	Тип расписания		—	
HTTP	Тип расписания:		По дням	
Теневое копирование				1
Настройки записи видео	частота днеи:			
Обновление	Время запуска:		00.00.00	
 SysCmd 			00.00.00	
	2			
	эначения всех параметров корректны			
			Применить	Отмена
			primetivite	Child

Рисунок 105. Настройки записи видео

Задайте следующие параметры записи:

- Продолжительность записи длительность сохранения снимков экрана, начиная с момента возникновения события (диапазон значений: 5-60 с);
- Частота кадров временной интервал между сохранением снимков экрана (диапазон значений: 50-500 мс);
- Ширина кадра ширина снимка экрана в пикселах (диапазон значений: 0-1920).

Чтобы начать запись видео в режиме реального времени, щелкните правой кнопкой мыши по требуемому клиентскому приложению SoftControl DLP Client на вкладке <u>Клиенты⁴⁶</u> и в контекстном меню выберите команду **Начать запись видео**.

Вы можете включить запись видео по расписанию, выставив галочку **Задать расписание**. В этом случае задайте следующие параметры записи:

- Тип расписания по дням или по часам;
- Частота дней/Частота часов периодичность, с которой будет выполняться задача;
- Время запуска время начала выполнения задачи в формате чч:мм:сс.

Настройки обновления

В разделе Обновление категории DLP можно установить расписание обновления,

для этого установите флажок **Задать расписание** и настройте параметры (рис. <u>Настройки расписания обновления</u>⁽¹²⁴).

Выберите тип расписания – **По дням** или **По часам**, в счетчике **Частота дней**/ **Частота часов** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:сс*.

🔀 Редактирование настроек клиентов		_ = ×
Общие настройкиSysWatch	👽 Задать расписание	
 DLP Сбор данных 	Тип расписания:	По дням
Оптимизация Наблюдение	Частота дней:	1
Обновление > SysCmd	Время запуска:	00:00:00
	Значения всех параметров корректны	
		Применить Отмена

Рисунок 106. Настройки расписания обновления

4.6.4 Настройки SoftControl SysCmd

Данная категория настроек включает в себя конфигурацию клиентского компонента SoftControl SysCmd.

Настройки обновления

В разделе **Обновление** категории **SysCmd** можно установить расписание обновления, для этого установите флажок **Задать расписание** и настройте параметры (рис. Настройки расписания обновления¹²⁴).

Выберите тип расписания – **По дням** или **По часам**, в счетчике **Частота дней**/ **Частота часов** укажите периодичность, с которой будет выполняться задача, а в поле **Время запуска** – время начала выполнения задачи в формате *чч:мм:cc*.

Редактирование настроек клиентов		_ = ×
 Общие настройки SysWatch DLP SysCmd 	Задать расписание Тип расписания:	Подням
Обновление	Частота дней:	1
	Время запуска:	00:00:00
	Значения всех параметров корректны	
		Применить Отмена

Рисунок 107. Настройки расписания обновления

4.7 Профили безопасности

Вкладка **Профили безопасности** предназначена для работы с наборами параметров безопасности (профилями), включающих в себя правила для файловой системы, системного реестра, сети и модулей. Профили объединяют различные правила контроля активности в логические группы. Созданные профили сохраняются в базе данных SoftControl Service Center; впоследствии их можно использовать в <u>настройках клиентских</u> приложений ¹⁰⁵.



Рисунок 108. Вкладка «Профили безопасности»

Основные операции с профилями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 16.

Кнопка	Название	Описание
Добавить Создание нового профиля безопасности.		Создание нового профиля безопасности.
Изменить Редактирование выбранного профиля.		Редактирование выбранного профиля.
4	Удалить Удаление выбранного профиля.	
Переименовать Переименование выбранного профиля.		Переименование выбранного профиля.
Скопировать Сохранение выбранного профиля под другим именем.		Сохранение выбранного профиля под другим именем.
импорт Импортирование профиля из XML-файла.		Импортирование профиля из XML-файла.
Экспорт Экспортирование выбранного профиля в XML-файл.		Экспортирование выбранного профиля в XML-файл.

Таблица 16. Элементы управления раздела «Профили безопасности»

Основные действия, выполняемые на данной вкладке:

Создание профиля

Чтобы создать профиль безопасности, нажмите на кнопку **+** (Добавить) и укажите имя профиля. В появившемся окне Данные профиля безопасности: <имя_профиля> задайте правила для файловой системы, системного реестра, сети и модулей.

Подробную информацию о добавлении правил контроля активности см. в соответствующих пунктах раздела **Настройки SoftControl SysWatch** (<u>Политика контроля: Файловая система</u>⁽⁹²⁾, <u>Политика контроля: Системный реестр</u>⁽⁹⁶⁾, <u>Политика контроля: Сеть</u>⁽¹⁰⁰⁾, <u>Политика контроля: Модули</u>⁽⁸⁷⁾).

Редактирование профиля

Чтобы изменить профиль безопасности, выберите его и нажмите на кнопку ∠ (Изменить) (рис. <u>Вкладка «Профили безопасности»</u>¹²⁵). В появившемся окне **Данные профиля безопасности: <имя_профиля>** отредактируйте требуемые данные.

Удаление профиля

Для удаления профиля выберите его, нажмите на кнопку 🖾 (Удалить)

(рис. <u>Вкладка «Профили безопасности»</u>⁽¹²⁵) и подтвердите удаление в диалоговом окне.

Переименование профиля

Для переименования профиля выберите его, нажмите на кнопку (Переименовать) (рис. <u>Вкладка «Профили безопасности»</u>¹²⁵) и укажите новое название в появившемся окне.

Копирование профиля

Для создания копии профиля выберите его, нажмите на кнопку (Скопировать) (рис. <u>Вкладка «Профили безопасности»</u>¹²⁵) и укажите название нового профиля в появившемся окне.

Импортирование профиля

Чтобы загрузить профиль безопасности из XML-файла, нажмите на кнопку (Импорт) (рис. <u>Вкладка «Профили безопасности»</u>⁽¹²⁵⁾). В окне выбора файла укажите имя XML-файла и нажмите на кнопку **ОК**.

Экспортирование профиля

Чтобы сохранить профиль безопасности в XML-файл, нажмите на кнопку (Экспорт) (рис. Вкладка «Профили безопасности»¹²⁵), затем в стандартном окне выбора файла укажите имя и путь к XML-файлу.

4.8 Задачи

Вкладка **Задачи** позволяет создавать задачи для клиентских приложений и отслеживать детали их выполнения (рис. <u>Вкладка «Задачи»</u>¹²⁸).

На вкладке представлен список всех задач и их параметры.

Основные операции с задачами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 17.

Кнопка	Название	Описание
	Добавить	Создание задачи для клиентских компонентов.
\$	Подробная информация	Просмотр отчета о выполнении выбранной задачи.

Таблица 17. Элементы управления вкладки «Задачи»

Кнопка	Название	Описание
×	Отменить	Отмена задачи, находящейся в статусе ожидание .

5	🚩 SoftControl Admin Console 📃 🗖 🗙						
(Файл Вид Фильтры Инструменты Опрограмме						
	Kauguru			⊾ <u>~</u> ч ⊌			_
٢							
	Илонт	nuduur 📼	Tun	Созлана	Roome samicka	Cranic	
	Иден	7 C	26	04 12 2020 10/20-20	04 12 2020 10-20-20	2	
		6	Јоновление	02 12 2020 10:20:38	02 12 2020 10:20:38	Завершена	
		5 6	выполнение команд на клиенте Выполнение команд на клиенте	03.12.2020 18:11:33	03 12 2020 18:06:13	Завершена	
		4 E	Зыполнение команд на клиенте	03.12.2020 18:00:37	03.12.2020 18:00:37	Завершена	
		3 E	Выполнение команд на клиенте	03.12.2020 17:57:04	03.12.2020 17:57:04	Завершена	
		2 E		03.12.2020 17:52:31	03.12.2020 17:52:31	Завершена	
		1 E	Выполнение команд на клиенте	03.12.2020 17:37:38	03.12.2020 17:37:38	Завершена	
	Имя поль	зователя: te	est Роли: Системный админие	стратор, Администрато	оры Session ID: 05c17ef7-672	9-4571-8801-69d2095efb81	Смена пароля

Рисунок 109. Вкладка «Задачи»

Перечень полей вкладки приведен в табл. 18.

Таблица	18.	Поля	вкладки	«Задачи»
---------	-----	------	---------	----------

Поле	Описание
Идентификатор	Порядковый номер задачи.
	Тип задачи:
	• сканирование;
Тип задачи	• сбор профиля;
	• обновление;
	• выполнение команд на клиенте.
Создана	Дата и время создания задачи.
Время запуска	Дата и время запуска задачи.
	Статус завершения задачи:
	• ожидание – выполнение задачи не начал ни один клиентский компонент;
Статус	 отменена – задача была отменена до начала выполнения;
Charyo	• выполняется – выполнение задачи начато как минимум одним из
	клиентских компонентов;
	• завершена – задача выполнена всеми клиентскими компонентами.

Основные действия, выполняемые на данной вкладке:

Создание задачи

Чтобы добавить новую задачу, нажмите на кнопку **Создать** (рис. <u>Вкладка «Задачи»</u>⁽¹²⁸⁾). В окне **Новая задача** задайте параметры задачи в зависимости от ее типа (см. рисунки, начиная с <u>Шаг «Тип задачи»</u>⁽¹³¹⁾ и до <u>Шаг «Клиенты»</u>⁽¹³⁵⁾ в разделе <u>Обновление</u>⁽¹³⁴⁾):

- <u>сбор профиля</u>⁽¹³¹⁾;
- антивирусное сканирование (132);
- <u>обновление</u>¹³⁴;
- выполнение команд на клиенте 136.

Просмотр подробностей выполнения задачи

Чтобы просмотреть подробности выполнения задачи, выберите ее и выполните одно из следующих действий:

- нажмите на кнопку **Подробная информация** в группе кнопок вкладки (рис. <u>Вкладка «Задачи»</u>⁽¹²⁸);
- дважды нажмите левой кнопки мыши на задаче.

В появившейся дополнительной вкладке **Задача: подробно** приведена детальная информация по задаче и ход выполнения для каждого клиентского компонента в отдельности (рис. <u>Подробности выполнения задачи</u>¹²⁹).

SoftControl Admin Console	_ = ×
Файл Вид Фильтры Инструменты Опрограмме	
S S 🖏 📑 🧠 🎥 🛦 😒 👯 🐨 🕒 😂 🌐 Li a	5 📬 🝯 😰 🗓
Клиенты Задачи Задача: подробно Задача: подробно ×	•
Подробная информация по задаче:	^
Тип Обновление	
Создана 04.12.2020 10:20:38	
Время запуска 04.12.2020 10:20:38	
Статус Завершена	
Параметры задачи Программные модули Антивирусные базы Выполнить перезагрузку клиентов Статус задачи на клиентах:	
Подразделение Имя клиента Тип клиента Статус Время окончания	
 CLIENT7X32 SysCmd Завершена 04.12.2020 10:21:29 	A
	v
Имя пользователя: test Роли: Системный администратор, Администраторы Session ID: 562df6bc-8a42-4d5d-a058-51050	V077c11 Смена пароля

Рисунок 110. Подробности выполнения задачи

Помимо основной информации (табл. 18) и параметров задачи, на вкладке отображается дополнительная таблица **Статус задачи на клиентах**, описание полей которой дано в табл. 19.

Поле	Описание
Подразделение	Подразделение, к которому относится клиентский компонент.
Имя клиента	Имя клиентского хоста.
	Статус завершения задачи для данного клиентского компонента:
	• ожидание – выполнение задачи не начато;
	 запуск – клиентскому компоненту успешно отправлена команда на запуск задачи;
	 ошибка запуска – клиентский компонент не смог произвести запуск задачи;
Статус	• выполняется – задача находится в процессе выполнения клиентским компонентом;
	 ошибка выполнения – в процессе выполнения задачи возникла ошибка;
	• отменена – задача была отменена;
	 завершена – выполнение задачи завершено;
	• ошибка завершения – при завершении задачи возникла ошибка.
Время окончания	Время завершения задачи на данном клиентском хосте.

Таблица 19. Поля таблицы «Ста-	тус задачи на клиентах»
--------------------------------	-------------------------

Чтобы просмотреть отчеты непосредственно по выполненным операциям, перейдите на вкладку **Лог** и примените <u>фильтры</u>¹⁶⁰ для соответствующих типов операций.

Подробная информация для задачи **Выполнение команд на клиенте** так же включает в себя результаты ваполнения команд. Просмотр результатов выполнения описан в разделе <u>Результаты выполнения команд</u>¹⁴¹.

4.8.1 Сбор профиля

1) На шаге Тип задачи выберите Сбор профиля в выпадающем списке и нажмите на кнопку Вперед (рис. <u>Шаг «Тип задачи»</u>¹³¹).



Рисунок 111. Шаг «Тип задачи»

2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после ее добавления, либо выберите опцию Указать время и определите дату и время запуска (рис. Шаг_ «Время запуска»¹³¹). Нажмите на кнопку Вперед для продолжения.

Шаги	<u>.</u>
	Время запуска
Тип задачи 💉	Выберите дату и время запуска задачи
Время запуска	
Клиенты	
	🔘 Сейчас
	🔘 Указать время:
	Выбранные дата и время запуска задачи должны быть больше текущих
	20.05.2020 12:03

Рисунок 112. Шаг «Время запуска»

3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг «Клиенты»¹³²). При выборе типа клиента SysWatch задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку Готово, чтобы создать задачу, или на кнопку Назад, если требуется изменить параметры задачи.

🔀 Новая задача	×
Шаги	Клиенты
Тип задачи 🖌	Выберите клиентов, на которых вы хотите выполнить задачу
рремя запуска * Клиенты *	 SysWatch По умолчанию WIN-MG2LKINUP4L WIN-MG2LKINUP4L WIN-UEGS3NA7DPC У ProductionPass WIN-MG2LKINUP4L
	<Назад Готово Отмена

Рисунок 113. Шаг «Клиенты»

4.8.2 Антивирусное сканирование

- 1) На шаге **Тип задачи** выберите **Сканирование** в выпадающем списке и отметьте области клиентского хоста для антивирусной проверки (рис. <u>Шаг «Тип задачи»</u>¹³³):
 - Сканирование памяти;
 - Сканирование загрузочных секторов;

Сканирование всех жестких дисков;

Сканирование всех съемных носителей.

Нажмите на кнопку Вперед для продолжения.

🔀 Новая задача	×
Шаги	Тип задачи
Тип задачи < Время запуска	Выберите тип задачи и задайте параметры для выбранного типа
Клиенты	Сканирование
	Области сканирования Сканирование памяти Сканирование загрузочных секторов Сканирование всех жестких дисков Сканирование всех съемных носителей
	<Назад Вперед> Отмена

Рисунок 114. Шаг «Тип задачи»

2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после ее добавления, либо выберите опцию Указать время и определите дату и время запуска (рис. <u>Шаг «Время запуска»</u>¹³³). Нажмите на кнопку Вперед для продолжения.

) Н овая задача	×
Шаги	Время запуска
Тип задачи 🕜	Выберите дату и время запуска задачи
Время запуска	
Клиенты	
	🔘 Сейчас
	Указать время:
	Выбранные дата и время запуска задачи должны быть
	больше текущих
	20.05.2020 12:03
	<назад впёред> Отмена

Рисунок 115. Шаг «Время запуска»

3) На шаге **Клиенты** отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг «Клиенты»¹³³).



Рисунок 116. Шаг «Клиенты»

При выборе типа клиента **SysWatch** задача будет назначена всем клиентским компонентам, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку **Готово**, чтобы создать задачу, или на кнопку **Назад**, если требуется изменить параметры задачи.

4.8.3 Обновление

- 1) На шаге **Тип задачи** выберите **Обновление** в выпадающем списке и отметьте необходимые компоненты для обновления и параметры задачи (рис. <u>Шаг «Тип задачи»</u> ⁽¹³⁴):
 - □ Программные модули обновление программных модулей компонентов типа SysWatch, DLP и SysCmd.
 - □ Антивирусные базы обновление антивирусных баз компонентов типа SysWatch.
 - □ Выполнить перезагрузку клиентов перезагрузка клиентских хостов по окончании обновления. Если данная опция не выбрана, то для завершения обновления программных модулей перезагрузку необходимо выполнить локально вручную на клиентском хосте, что отображается в статусе компонента на вкладке Клиенты⁽⁴⁵⁾ и событиях обновления в <u>отчетах</u>⁽¹⁴³⁾. Модулю SysCmd не требуется перезагрузка компьютера после обновления, поэтому этот параметр игнорируется в процессе обновления SysCmd.



Рисунок 117. Шаг «Тип задачи»

Нажмите на кнопку Вперед для продолжения.

2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после ее добавления, либо выберите опцию Указать время и определите дату и время запуска (рис. Шаг «Время запуска»¹³⁵). Нажмите на кнопку Вперед для продолжения.

🚩 Новая задача	×
Шаги	Время запуска
Тип задачи 🕜	Выберите дату и время запуска задачи
Время запуска	
Клиенты	
	О Сейчас
	Указать время:
	Выбранные дата и время запуска задачи должны быть больше текущих
	20.05.2020 12:03
	<Назад Вперед > Отмена

Рисунок 118. Шаг «Время запуска»

3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу (рис. <u>Шаг_«Клиенты»</u>⁽¹³⁵⁾). При выборе типа клиента задача будет назначена всем клиентским компонентам данного типа, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку Готово, чтобы создать задачу, или на кнопку Назад, если требуется изменить параметры задачи.



Рисунок 119. Шаг «Клиенты»

4.8.4 Выполнение команд на клиенте и обмен файлами с клиентом

Задача типа **Выполнение команд на клиенте** может быть выполнена на удаленном компьютере, где установлен клиент SoftControl SysCmd. В рамках одной задачи могут быть выполнены следующие команды: передача файлов на удаленный компьютер, запуск процессов на удаленном компьютере, скачивание файлов с удаленного компьютера.



Рисунок 120. Шаг «Клиенты»

4.8.4.1 Создание задачи

1) На шаге **Тип задачи** выберите **Выполнение команд на клиенте** в выпадающем списке и отметьте те <u>команды</u>⁽¹³⁹⁾, которые необходимо выполнить (рис. <u>Шаг «Тип</u> задачи»⁽¹³⁶⁾):

🔀 Новая задача		×
Шаги	Тип задачи	
Тип задачи 🖌	Выберите тип задачи и задайте параметры для выбранного	
Время запуска	1/11/2	
Клиенты	Выполнение команд на клиенте	
	Выполнение команд на клиенте	
	Передать файл на клиента Обзор	
	D:\Folder\file_for_upload.ext	
	Поместить в папку :	
	у запустить процесс для команд OC: cmd.exe /С команда; для команд PowerShell: powershell.exe -command "команда"; для скриптов PowerShell: powershell.exe -file "скрипт.ps1"	
	cmd.exe /C dir *.log	
	Рабочая папка на клиенте:	
	C:\Reports	
	l юлное имя фаила на клиенте: C:\Folder\file for download.ext	
	«Назад Вперед» Отмена	

Рисунок 121. Шаг «Тип задачи»

- □ Передать файл на клиент скопировать файл с локального компьютера, где в данный момент запущена консоль управления SoftControl Admin Console, на удаленный компьютер, где работает модуль SoftControl SysCmd.
 - Параметры:

Выберите файл с помощью кнопки **Обзор** и введите в поле **Поместить в папку** полный путь на удаленном компьютере куда необходимо этот файл сохранить. Оба параметра являются обязательными.

Запустить процесс – запускает указанный в параметрах исполняемый файл.

Параметры:

Команда для запуска процесса (обязательный параметр).

Рабочая папка на клиенте (необязательный параметр).

В команде указывается исполняемый файл для запуска с необходимыми параметрами. Можно указать рабочую папку, которая будет установлена как текущая для процесса.

Скачать файл с клиента – скопировать файл с удаленного компьютера, где работает модуль SoftControl SysCmd, на сервер SoftControl Server. Затем этот файл

можно скачать на локальный компьютер с помощью консоли управления SoftControl Admin Console.

Параметры:

Имя скачиваемого файла с полным путем в файловой системе клиента (обязательный параметр).

После заполнения параметров команд нажмите на кнопку Вперед для продолжения.

2) На шаге Время запуска выберите опцию Сейчас для немедленного запуска задачи после ее добавления, либо выберите опцию Указать время и определите дату и время запуска (рис. <u>Шаг «Время запуска»</u>⁽¹³⁵⁾). Нажмите на кнопку Вперед для продолжения.

🔀 Новая задача	×
Шаги	Время запуска
Тип задачи 🕜	Выберите дату и время запуска задачи
Время запуска	
Клиенты	
	О Сейчас
	Указать время:
	Выбранные дата и время запуска задачи должны быть больше текущих
	20.05.2020 12:03
	<hазад вперед=""> Отмена</hазад>

Рисунок 122. Шаг «Время запуска»

3) На шаге Клиенты отметьте клиентские компоненты, для которых необходимо создать задачу (рис. Шаг_ «Клиенты»¹³⁵). При выборе типа клиента задача будет назначена всем клиентским компонентам данного типа, при выборе подразделения – всем клиентским компонентам подразделения. Нажмите на кнопку Готово, чтобы создать задачу, или на кнопку Назад, если требуется изменить параметры задачи.



Рисунок 123. Шаг «Клиенты»

4.8.4.2 Описание работы команд

В процессе выполнения задачи типа Выполнение команд на клиенте производятся следующие действия:

Подготовка задачи. Если задача содержит команду передачи файла на клиент, то сначала SoftControl Admin Console передает файл на сервер. Файл сохраняется на сервере в папке, указанной в параметре *CmdFileStoreDir* файла конфигурации сервера (C:\ProgramData\SafenSoft\Server.Config.xml), по умолчанию C:\ProgramData\SafenSoft \CmdFileStore. Если передача файла на сервер не прошла успешно, то выдается сообщение об ошибке и задача не создается. Максимальный размер файла, который можно передавать на клиент и скачивать с него, задается параметром *MaxFileSizeByte* в файле конфигурации сервера.

Запуск задач на клиенте. Во время очередного хартбита клиент связывается с сервером и получает список задач. Для каждой задачи создается новый поток, в котором будут выполнятся команды из данной задачи. Поэтому несколько разных задач по выполнению команд могут выполниться в произвольном порядке, а команды внутри одной задачи выполняются строго в том порядке, в каком они описаны внутри задачи.

Передача файла на клиент. Клиент скачивает файл с сервера и сохраняет его в соответствии с заданными параметрами команды (путь, имя, времена и атрибуты файла). Если такой файл уже существует, он будет перезаписан. Если указанного в

параметрах пути не существует, будет предпринята попытка создать этот путь вне зависимости от его глубины. Информация о результате передается на сервер. После выполнения команды файл с сервера удаляется вне зависимости от успешности выполнения команды. В случае прерывания передачи файла с сервера на клиент вследствие разрыва связи или перезапуска клиента закачка продолжится, когда связь возобновится и служба SysCmd будет работать.

Запуск процесса. Клиент создает процесс в соответствии с параметрами команды и подключается к его потокам stdout и errout. По окончании чтения данных из выходного потока процесса клиент отправляет его содержимое и сопутствующую информацию на сервер. Размер буфера в символах для приема выходного потока процесса задается параметром *MaxCmdOutputChars* в файле конфигурации сервера. В случае запуска процесса перезагрузки или выключения компьютера не следует заказывать немедленное действие, чтобы дать время на сохранение результата команды и отправку хартбита на сервер. Например, для команды shutdown следует использовать ключ /t. Поскольку процесс запускается в сессии, в которой работают службы и ГИП⁽⁷⁾ не доступен, не следует запускать процессы, требующие участия пользователя как для работы, так и для своего завершения.

Скачивание файла с клиента. Клиент отправляет файл на сервер, и сервер сохраняет файл в папке, указанной в параметре *CmdFileStoreDir* в Server.Config.xml. Также клиент отправляет на сервер имя, время и атрибуты файла. В случае прерывания передачи файла с клиента на сервер вследствие разрыва связи или перезапуска клиента закачка продолжится, когда связь возобновится и служба SysCmd будет работать.

Завершение задачи. После завершения выполнения всех команд задаче устанавливается соответствующий статус, который будет передан на сервер только при очередном хартбите. Т.е. результаты выполнения отдельных команд на сервере могут быть доступны до обновления статуса всей задачи.

Время выполнения всего набора команд в задаче можно ограничить параметром *MaxCmdExecTimeSec* в файле конфигурации сервера. При превышении этого времени команда будет прервана и ее (и всем следующим за ней командам) будет установлен статус «Превышено время ожидания». Если после перезапуска службы SysCmd или перезагрузки клиента продолжается выполнение команд в задаче, то отсчет времени начинается заново.

При выполнении команд могут возникнуть ошибки. В случае критических ошибок (отсутствие запрашиваемого или запускаемого файла, невозможность создания пути или файла) выполнение команды прекращается. В случае не критических ошибок (сетевые ошибки передачи файлов) производится повторная попытка выполнения команды до тех пор, пока она не выполнится успешно, не произойдет критическая ошибка или не будет превышено время *MaxCmdExecTimeSec*. До успешного завершения команды перехода к следующей команде не произойдет. Между выполнением команд набора выдерживается пауза 5 сек.

Перед и после выполнения каждой команды передачи файлов ее состояние сохраняется на клиенте для возобновления выполнения незавершенных команд после перезапуска службы.

4.8.4.3 Результаты выполнения команд

Информация о результатах выполнения команд доступна на вкладке <u>Задача: подробно</u>¹²⁹ в таблице **Статус задачи на клиентах**. Если результаты доступны, в первом столбце появится значок •, который позволяет открыть подробную информацию о результатах (рисунки <u>Просмотр результатов работы команд передачи файла на клиент и запуска</u> <u>процесса</u>¹⁴² и <u>Просмотр результатов работы команды скачивания файла с клиента</u>¹⁴³).

Вид Фильтры Инструменты Бид Фильтры Инструменты Бид Фильтры Инструменты Вадачи Задача: подробно тус задачи на клиентах:	О программе	😫 👦 🞑	🤜 🥴 🎬 🗋 .	5 🗈 🟮 🧐	≩ ∐
Подразделение Имя клиен	та Тип клиента	Статус	Время окончания		
Действие: Время начала выполнения Время окончания выполнения Статус Код возврата Код ошибки Сообщение Имя файла: #1 Действие: Время окончания выполнения Время окончания выполнения Статус Код возврата Код ошибки Сообщение Кодовая страница [866, Кир Том в устройстве С не и Серийный номер тома: 8E Содержимое папки C:\tes 14.12.2020 19:02 <01 14.12.2020 11:07 14.12.2020 12:20 10.12.2019 13:06 14.12.2020 12:21 14.12.2020 12:20 2 папок	Передать файл на клиен 12/14/2020 7:02:57 РМ 12/14/2020 7:02:58 РМ Выполнено успешно 0 file_for_transfer.ext Запустить процесс 12/14/2020 7:03:04 РМ 12/14/2020 7:03:04 РМ 12/14/2020 7:03:04 РМ 12/14/2020 7:03:04 РМ 0 0 иллица (DOS)] меет метки. 0E-3EFA t 10 196 ClientSett 12 660 7:36 DLP_Client 474 571 file_for_t 9:35 488 SysCmd.ms; 19 406 336 SysWatchAV 242 087 327 6a¥r 54 89 88 256 ба¥r	ings.xmlc .msi ransfer.ext /5.msi юбодно			

Рисунок 124. Просмотр результатов работы команд передачи файла на клиент и запуска процесса

Статус выполнения команды может принимать следующие значения:

- Выполнено успешно.
- Произошла ошибка.
- Превышено время ожидания.

Код возврата содержит код, возвращенный процессом в команде Запуск процесса.

Если в ходе выполнения команды произошла ошибка при вызове функций API Windows или запросе к веб-серверу, то номер ошибки будет указан в поле **Код ошибки**, и в поле **Сообщение** краткое описание случившегося.

Для команды Запуск процесса можно выбрать Кодовую страницу, в которой будет представлен вывод процесса.

Если команда **Скачать файл** с клиента выполнена успешно и файл сохранен на сервере, то воспользовавшись кнопкой **Скачать** можно получить файл с сервера, а с помощью кнопки **Удалить** с сервера удалить его.

▶ SoftControl Admin Console	_ = ×
Файл Вид Фильтры Инструменты О программе	
S S 👫 🕂 💀 🏩 🛦 😒 🐹 😁 🔛 🤜 27 🎬 🔓 🌽 関 28 🦉	
Клиенты Задачи Задача: подробно ×	-
Кодовая страница [866, Кириллица (DOS)]	A
Том в устройстве С не имеет метки. Серийный номер тома: 8E0E-3EFA	
Содержимое папки C:\test	
14.12.2020 19:02 <dir> .</dir>	
14.12.2020 19:02 <dtr> 11.12.2020 11:07 10 196 ClientSettings.xmlc</dtr>	
14.12.2020 12:20 12 660 736 DLP_Client.msi 474 571 5106 474 571 5105	
14,12,2020,12,21, 9,535,488,5ysCmd.msi	
1+.12.2020 12.28 алов 24.2 406 336 Зузмастстичу.пьт 5 файлов 24.2 087 327 байт	
2 папок >> 489 888 2>ъ ваит своюдно	
#2	
Действие: Скачать файл с клиента Во про император и по склиента	
время начала выполнения 12/14/2020 г/03:10 PM	
Код возврата 0	
Код ошибки 0	
Сообщение	
Имя файла: C:\test\file_for_transfer.ext	
Atprøytis davaa: Archive	
время создания фаила: 12/8/2020 10:50:39 АМ	
время изменения файла: 12/10/2019 100:34 FM	
Pasmeo baña: 463 45 KB	
Скачать Удалить с сервера	
Имя пользователя: test Роли: Системный администратор, Администраторы Session ID: 1af7829e-b955-4b8e-9511-2c9274811ddf	Смена пароля

Рисунок 125. Просмотр результатов работы команды скачивания файла с клиента

4.9 Просмотр отчетов

Для просмотра отчетов клиентских приложений в агрегированном виде через консоль управления SoftControl Admin Console предназначена вкладка **Лог событий**. Она позволяет в реальном времени отслеживать события на нескольких клиентских хостах одновременно и производить выборку необходимых данных с помощью гибкого <u>механизма фильтрации</u>¹⁵⁹. На вкладке администратор получает доступ к следующим данным в удобной форме:

- <u>Отчеты SoftControl SysWatch</u>⁽¹⁴⁴⁾;
- Отчеты SoftControl DLP Client⁽⁵⁾;
- Отчеты SoftControl SysCmd¹⁵⁵.

Полученные отчеты могут быть выведены на печать или экспортированы в электронный формат¹⁶⁷.

Кроме того, поддерживается резервное копирование отчетов 168.

4.9.1 Отчеты SoftControl SysWatch

Вкладка **Лог событий** предоставляет возможности по детальному мониторингу событий безопасности, регистрируемых SoftControl SysWatch на клиентских хостах (рис. <u>Вкладка</u> «Лог событий» для компонента SoftControl SysWatch¹⁴⁴). Чтобы просмотреть все события, поступившие с клиентов SysWatch, выделите нужные клиенты и следуйте инструкции, приведенной в разделе <u>Клиенты</u>⁴⁹.

🔀 SoftControl Admin C	onsole						_ 🗆 ×
Файл Вид Фильтры	и Инструменты	О программе					
≶ 🗞 🍕	1) 🖄 🔬 🚉	💦 🗰 [1) 🎬 🗋	🌙 💼 😝 🕸 📗	
Клиенты Лог событи	ий ×						-
	🧧 · 🔏 ·	🤹 🔒 🔒					
[ClientID] In (1)							
		Перет	яните сюда мышкой за	головок колонки д	ля группировки дан	ных по ней	
Идентификато І	Имя клиента	Тип события	Время	Важность	Тип клиента		
► 15 (DESKTOP-LELO	Нарушение политики к	20.02.2021 12:13:31	Критическая	SysWatch		
14 [DESKTOP-LELO	Нарушение политики к	20.02.2021 12:13:30	Критическая	SysWatch		
13 [DESKTOP-LELO	Изменение настроек	20.02.2021 12:07:47	Обычная	SysWatch		
12 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:07:24	Высокая			
11 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:07:24	Обычная			
10 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:07:24	Обычная			
9 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:07:24	Обычная			
8 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:06:52	Обычная			
7 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:06:52	Высокая			
6 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:06:52	Обычная			
5 [DESKTOP-LELO	Обновление клиента	20.02.2021 11:06:50	Обычная			
4 [DESKTOP-LELO	Изменение настроек	20.02.2021 11:06:46	Высокая	SysWatch		
3 [DESKTOP-LELO	Изменение настроек	20.02.2021 11:06:46	Высокая	SysWatch		
2 [DESKTOP-LELO	Нарушение политики к	20.02.2021 10:54:06	Критическая	SysWatch		
1 [DESKTOP-LELO	Нарушение политики к	20.02.2021 10:54:05	Критическая	SysWatch		
							v
Первая страница	Первая страница Предыдущая страница Следующая страница Страница №1 (последняя) Прошло времени: 00:00:01						1: 00:00:01
Имя пользователя: add	min Роли: Сис	темный администратор, Ад	цминистраторы			Смена па	роля

Рисунок 126. Вкладка «Лог событий» для компонента SoftControl SysWatch

Полный перечень полей вкладки **Лог событий** для компонента SoftControl SysWatch приведен в табл. 20.

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <u>отчет серверного компонента в журнале Windows</u> ¹⁹⁹ вносится соответствующее предупреждение. Исключением являются события типа Статус , для которых данный параметр принимает значения <i>-1</i> или <i>-2</i> .
Поле	Описание
--------------------------	---
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl SysWatch к серверу SoftControl Server
Тип события	Тип события безопасности (инцидента): • нарушение политики контроля; • контроль активности; • обновление клиента; • запуск процесса; • антивирус; • изменение настроек; • статус; • вход пользователя; • выход пользователя; • события DeCrypt.
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: • обычная; • высокая; • критическая. Каждому уровню приоритета соответствует свой цвет ячейки.
Действие	Действие в случае события типа нарушение политики контроля: • чтение файла; • изменение файла; • переименование файла; • удаление файла; • открытие каталога; • открытие каталога; • открытие ключа реестра; • создание ключа реестра; • создание ключа реестра; • удаление значения реестра; • удаление значения реестра; • удаление значения реестра; • удаление значения реестра; • загрузка DLL-модуля; введен неверный пароль. Действие в случае события типа запуск процесса (данные выводятся в одну строку): • Инсталлятор: да/нет; • В профиль: да/нет; • В профиль: да/нет; • В профиль: да/нет; • Имеет действительную ЭЦП: да/нет (только для инсталляторов); • Белый список сертификатов включен: да/нет (только для инсталляторов); • Сертификат в белом списке: да/нет (только для инсталляторов, и если включен белый список); • Глобальный режим обновления ПО включен: да/нет (только для инсталляторов);

Поле	Описание
	• Был ли отслеживаемым: да/нет;
	 Запуск в режиме обновления ПО: да/нет.
	Действие в случае события типа антивирус :
	• запуск сканера;
	 запуск сбора профиля;
	• завершение сканирования;
	• профиль собран;
	• сканирование объекта.
	Действие в случае события типа обновление :
	• запуск обновлений;
	• обновление завершено.
	Действие в случае события типа изменение настроек :
	 настройки изменены локально;
	 настройки изменены сервером.
	Действие в случае события типа события DeCrypt :
	 NOTIFY-DEV0;Загрузка, все устройства найдены;
	 NOTIFY-PRETEST;Загрузка с незашифрованным контейнером;
	 NOTIFY-ERROR;Ошибка при загрузке;
	• NOTIFY-PW;Загрузка с паролем;
	 NOTIFY-DEV1;Загрузка, одно из устройств не найдено;
	• NOTIFY-DEV2;Загрузка, два устройства не найдены (КРИТИЧНО);
	• NOTIFY-ACTION: DEV-GET;Запрос списка найденных устройств;
	• NOTIFY-ACTION: DEV-CHANGE;Обновить список устройств;
	• NOTIFY-ACTION: PW-CHANGE;Изменить пароль;
	• NOTIFY-ACTION: DISK-ENC STARTED;Шифрование диска начато;
	• NOTIFY-ACTION: DISK-ENC FINISHED;Шифрование диска завершено;
	• NOTIFY-ACTION: DISK-DEC STARTED;Дешифрование диска начато;
	• NOTIFY-ACTION: DISK-DEC FINISHED;Дешифрование диска завершено;
	• NOTIFY-ACTION: BOOT-PREPARE;Установить системный загрузчик;
	• NOTIFY-ACTION: BOOT-CLEAR;Удалить системный загрузчик.
	Статус действия в случае события типа антивирус:
	• сканер запущен;
	 ошибка при запуске сканера;
	• сканер был остановлен;
	• успешно;
	• неудачно.
	Статус действия в случае события типа обновление:
	 процесс обновления запущен;
Статус действия	• ошибка запуска;
	 новых обновлений не найдено;
	 обновление прервано пользователем;
	 обновления успешно установлены;
	 нужна перезагрузка системы;
	• обновление завершено с ошибками.
	Статус действия в случае события типа события DeCrypt:
	• SUCCESS;
	• FAIL.

Поле	Описание
	Статус зарегистрированного клиентского компонента:
	• активен;
Статус клиента	• остановлен;
	 работа службы была прервана;
	 ошибка статуса. неверный статус.
14	Приложение или инсталлятор, вызвавшая события типов нарушение политики
исполняемыи фаил	контроля или запуск процесса.
	– Команда, вызвавшая событие типа запуск процесса .
	– Имя объекта файловой системы/реестра, в отношении которого произошло
Командная строка	событие типа нарушение политики контроля , или имя DLL-модуля,
процесса	загружаемого процессом, вызвавшим событие нарушение политики
	контроля.
	– Неверно введенный пароль.
	Учетная запись, под которой произошли события типов запуск процесса или
ПОЛЬЗОВАТЕЛЬ	изменение настроек.
	Зона выполнения приложения:
0	• доверенные (разрешенные);
Зона	• по умолчанию (ограниченные);
	• блокированные (запрещенные).
	Уникальный порядковый идентификатор процесса (PID) в ОС для события типа
Идентификатор процесса	запуск процесса.
Идентификатор	Уникальный порядковый идентификатор родительского процесса (PPID) в ОС
родительского процесса	для события типа запуск процесса .
Родительский процесс	Наименование родительского процесса для события типа запуск процесса.
	Решение по запуску приложения:
Remente	• разрешен;
Решение	• запрещен.
	Каждому решению соответствует свой цвет ячейки.
Проверено объектов	Количество объектов, проверенных в процессе антивирусного сканирования.
Угроз найдено	Количество найденных угроз в процессе антивирусного сканирования.
Угроз обезврежено	Количество обезвреженных угроз в процессе антивирусного сканирования.
	Количество встроенных сертификатов, обнаруженных в процессе
встроенные сертификаты	автоматической настройки (сбора профиля).
	Количество сертификатов каталогов, обнаруженных в процессе автоматической
Сертификаты каталогов	настройки (сбора профиля).
	Статус контроля активности приложений:
Приложения	• активно;
	• неактивно.
Файловая система	Статус контроля файловой системы:
	• активно;
	• неактивно.
Системный реестр	Статус контроля системного реестра:
	• активно,
	• неактивно.
	Статус контроля сетевой активности:
Сеть	• активно;
	• неактивно.

Поле	Описание
Имя вошедшего пользователя	Учетная запись, под которой произошел вход в ОС клиентского хоста.
Имя вышедшего пользователя	Учетная запись, под которой произошел выход из ОС клиентского хоста.
Ошибка	Код ошибки в базе данных на сервере.
Тип клиента	Тип клиента, для которого отображается отчет. Для общих событий (SysWatch и DLP) поле имеет пустое значение.
Детали	Идентификатор (UID) правила, в отношении которого произошло нарушение политики контроля.
Имя службы	Системное имя службы, которая была запущена/остановлена.
Отображаемое имя	Название службы в оснастке Службы ОС Windows.
Событие службы	Статус службы: • ServiceStarted; • ServiceFoundRunning; • ServiceStopped.

Следующие события содержат в себе расширенную информацию об инциденте:

▽ Событие антивирусного сканера

Событие антивирусного сканера позволяет просматривать подробный отчет о результатах проведения антивирусного сканирования¹³² клиентских хостов.

Откройте список событий на вкладке **Лог событий** для компонента SoftControl SysWatch и выберите событие типа **Антивирус** с действием **Завершение сканирования**. Чтобы вызвать отчет с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду Показать дополнительную информацию события антивируса.
- Отчет с дополнительной информацией будет открыт только в том случае, если в результате антивирусного сканирования найдены угрозы (ненулевой счетчик в поле **Угроз найдено**) или в случае наличия необезвреженных угроз при предыдущей проверке.

В появившейся дополнительной вкладке **Сканер** представлены все объекты, содержащие обнаруженные угрозы по результатам проверки (рис. <u>Вкладка</u> «<u>Сканер</u>»¹⁴⁸).

SoftControl Admin Console					-
йл Вид Фильтры Инструменты Опро	грамме				
🏚 🛃 🙀 🕴 🕵	🚣 🕄 👪 💼 ڬ 剩	3 🎁 🔓 4	3 🗈 🛢	₽ 🛛	
лиенты Лог событий Сканер ×					
Путь 🔺					
Событие	Файл	Вирус	Результат	Действие	
🗐 Путь: С:				·····	
	pagefile.sys		Ошибка	Пропущен	
	swapfile.sys		Ошибка	Пропущен	
🗐 Путь: C:\Boot					
	BCD		Ошибка	Пропущен	
	BCD.LOG		Ошибка	Пропущен	
Путь: C:\Program Files (x86)\SoftControl\	SysWatch\Data				
	Storage.dbs		Ошибка	Пропущен	
Путь: C:\ProgramData\Microsoft\Search\	Data\Applications\Windows				
	edb.log		Ошибка	Пропущен	
	Windows.edb		Ошибка	Пропущен	
Путь: C:\System Volume Information					
	{3808876b-c176-4e48-b7ae-0404		Ошибка	Пропущен	
	{b736e582-9444-11ea-beed-000c		Ошибка	Пропущен	
Путь: C:\Users\admin					

Рисунок 127. Вкладка «Сканер»

Полный перечень полей вкладки приведен в табл. 21.

Таблица 21. Поля вкладки «Сканер»

Поле	Описание
Событие	Дата и время окончания антивирусного сканирования.
Путь	Каталог расположения объекта в файловой системе клиентского хоста.
Файл	Имя объекта.
Вирус	Наименование вредоносного кода, которым заражен объект.
Результат	Результат антивирусного сканирования: • Чист; • Заражен; • Подозрителен; • Ошибка; • Ошибка лечения; • Ошибка перемещения; • Ошибка удаления.
Действие	Действие, выполненное для данного объекта по результатам антивирусного сканирования: • Излечен; • Перемещен; • Пропущен; • Удален; • Нет действия.

▽ Событие изменения настроек

Событие изменения настроек позволяет просматривать полный список изменений в конфигурации SoftControl SysWatch. Настройки SoftControl SysWatch могут быть

изменены следующими способами:

- <u>администратором через SoftControl Admin Console</u>⁽⁶⁶⁾;
- локальным пользователем с помощью:
 - ГИП программы;
 - применения конфигурационного файла.

Откройте список событий на вкладке **Лог событий** для компонента SoftControl SysWatch и выберите событие типа **Изменение настроек**. Чтобы вызвать отчет с дополнительной информацией, выполните одно из следующих действий для выбранного события:

- дважды нажмите левой кнопки мыши на событии;
- вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите команду Показать дополнительную информацию события изменения настроек.

🔀 SoftControl Admin Console		-
Файл Вид Фильтры Инструменты Опрограмме		
🖻 🎭 🎇 🚅 👵 🖕 🖄 😒 👪 🎃 🕍 🤊	🛃 🎯 🎬 🖪 🌽 📬 🛢	
Клиенты Лог событий Измененные настройки ×		
l leper	гяните сюда мышкои заголовок колонки для группировки да	иных по неи
Имя настройки	Значение настройки	
 Контроль активности/Файловая система 	Включено	
Контроль активности/Сеть	Включено	
Контроль активности/Приложения	Включено	
Контроль активности/Реестр	Включено	
Контроль активности/Включить	Включено	
AfterLoginDelay	5	
AfterSystemStartDelay	5	
Инциденты/Включить автоматическую обработку	Включено	
Alert/DIILoadResult	Запретить	
Alert/PeModificationResult	Запретить	
Alert/ScriptEngineResult	Запретить	
Инциденты/Включить таймаут алерта запуска приложения не в профиле	Выключено	
Инциденты/Запуск приложения не в профиле	Заблокировать (по умолчанию)	
Инциденты/Длительность алерта запуска приложения не в профиле	1	
Инциденты/Включить таймаут алерта запуска неподписанного инсталлятора	Выключено	
Инциденты/Запуск неподписанного инсталлятора	Заблокировать (по умолчанию)	
Инциденты/Длительность алерта запуска неподписанной программы установки	1	
Инциденты/Включить таймаут алерта нарушения политики контроля	Выключено	
Инциденты/Нарушение политики контроля	Запретить	
Инциденты/Длительность алерта нарушения политики контроля	1	
Защита паролем/Изменение свойств программы	Выключено	
Защита паролем/Удаление программы	Включено	
DeCryptLicense	7MLXQT63-APYCVB29	

Рисунок 128. Вкладка «Измененные настройки»

В появившейся дополнительной вкладке **Измененные настройки** представлен перечень настроек SoftControl SysWatch с указанием их нового состояния (рис. <u>Вкладка «Измененные настройки»</u>¹⁵⁰).

Полный перечень полей вкладки приведен в табл. 22.

Таблица 22. Поля вклад	ки «Измененные настройки»
Поле	Описание
Имя настройки	Название настройки.
Значение настройки	Значение настройки, на которое оно было изменено в результате события.

4.9.2 Отчеты SoftControl DLP Client

Вкладка **Лог событий** предоставляет возможность просмотра отчетов по данным, собираемым SoftControl DLP Client на клиентских хостах (рис. <u>Вкладка «Лог событий» для</u> компонента SoftControl DLP Client¹⁵¹). Чтобы просмотреть все события, поступившие с клиентов DLP, выделите нужные клиенты и следуйте инструкции, приведенной в разделе Клиенты⁴⁹.

SoftControl Admin Console					_ D ×
Файл Вид Фильтры Инструмент	ы Опрограмме				
🖻 🎭 🍇 🚅 🛛	5 🏂 🛦 😒	🛛 👪 👼 🕻	i 📢 🔏) 🏥 🔓	🎜 📬 📦 🥸 🚺
Клиенты Лог событий ×					•
	🤬 🔐 🏭				
[ClientID] In (1)					
		1	Перетяните сюда мы	ышкой заголовок ко	юнки для группировки данных по ней
Идентификато Имя клиента	Тип события	Время	Важность	Тип клиента	
-2 DESKTOP-63K	Статус	02.02.2021 8:19:45	Высокая		A
-1 DESKTOP-63K	Статус	02.02.2021 7:42:09	Высокая		
-2 DESKTOP-63K	Статус	02.02.2021 2:34:36	Высокая		
-1 DESKTOP-63K	Статус	02.02.2021 2:28:50	Высокая		
-2 DESKTOP-63K	Статус	01.02.2021 9:26:26	Высокая		
-1 DESKTOP-63K	Статус	01.02.2021 9:25:26	Высокая		
-2 DESKTOP-63K	Статус	29.01.2021 11:50:27	Высокая		
-1 DESKTOP-63K	Статус	29.01.2021 11:45:39	Высокая		
-2 DESKTOP-63K	Статус	28.01.2021 12:00:39	Высокая		
-1 DESKTOP-63K	Статус	28.01.2021 8:41:12	Высокая		
Первая страница Предыдущая с	траница Следующая стр	раница Страница №	21 (последняя)		ту Прошло времени: 00:00:01
Имя пользователя: admin Роли: С	истемный администратор, А	Администраторы			Смена пароля

Рисунок 129. Вкладка «Лог событий» для компонента SoftControl DLP Client

Полный перечень полей вкладки **Лог событий** для компонента SoftControl DLP Client приведен в табл. 23.

The stand of the second of the	Таблица 23.	Поля вкладки	«Лог СОБЫ	тий» для S	SoftControl DLP	Client
--	-------------	--------------	-----------	------------	-----------------	--------

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <u>отчет серверного компонента в журнале Windows</u> ¹⁹⁹

Поле	Описание
	вносится соответствующее предупреждение. Исключением являются события
	типа Статус, для которых данный параметр принимает значения -1 или -2.
Уникальный ID	Уникальный идентификатор клиентского хоста, который автоматически
устройства	присваивается ему при первом обращении клиентского приложения SoftControl
	тип события собра данных. • побавлено устройство:
	• файл.
	• HTTP;
Тип события	• монитор клавиатуры;
	• принтер;
	• реестр;
	 устройство отсоединено;
	• время работы.
Время	Дата и время регистрации события.
	Важность (приоритет) события с точки зрения угрозы информационной
	оезопасности клиентского хоста:
Важность	
	Каждому уровню приоритета соответствует свой цвет ячейки.
	Статус зарегистрированного клиентского компонента:
	• активен;
Статус клиента	• остановлен;
	 работа службы была прервана;
	• ошибка статуса. неверный статус.
Путь к процессу	Путь к процессу, вызвавшему событие типов файл, реестр, НТТР, монитор
	клавиатуры, время работы, принтер.
Описание процесса	Описание процесса, вызвавшего событие типов файл, реестр, НТТР, монитор
	клавиатуры, время расоты, принтер.
Пользователь	событие типов файл реестр НТТР монитор клавиатуры время работы
	принтер.
IP	IP-адрес назначения HTTP-запроса для события типа HTTP .
Url	URL назначения HTTP-запроса для события типа HTTP .
Заголовок	Заголовок НТТР для события типа НТТР.
Маска доступа	Тип операции над наблюдаемым объектом для событий типов файл и реестр:
	• чтение;
	• запись;
	• удаление;
	• переименование;
	• изменение.
Резервная копия	локальный путь к теневой копии наблюдаемого объекта с именем вида <Полное
	копии. лля событий типов файл и реестр
Путь к файлу	Путь к наблюдаемому каталогу или файлу лля события типа файл
тип диска	тип носителя, на котором располагается наолюдаемый каталог или файл для

Поле	Описание
	события типа файл :
	• локальный носитель;
	• съемный носитель.
Ветка реестра	Путь к наблюдаемому разделу реестра или параметру раздела реестра для
	события типа реестр .
Время записи события	Дата записи ввода с клавиатуры для события типа монитор клавиатуры .
	Текст, введенный пользователем с клавиатуры, для события типа монитор
Саписанные данные	клавиатуры.
Детали	Описание источника печати для события типа принтер .
	ID периферийного устройства для событий типов добавлено устройство и
по устройства	устройство отсоединено.
Класс устройства	Класс периферийного устройства для событий типов добавлено устройство и
Пасс устроиства	устройство отсоединено.
Описание устройства	Описание периферийного устройства для событий типов добавлено устройство
Описание устроиства	и устройство отсоединено.
Время старта	Время начала работы с приложением для события типа время работы .
Время окончания	Время окончания работы с приложением для события типа время работы.
Продолжительность	Продолжительность работы с приложением для события типа время работы.
Индекс файла	Индекс файла для событии типа HTTP .
Тип клиента	Тип клиента, для которого отображается отчет. Для общих событий (SysWatch и
	DLP) поле имеет пустое значение.
Имя принтера	Логическое имя принтера, на который отправлено задание на печать.

События типов **файл**, **реестр** и **НТТР** выделяются в отчетах цветом, если содержат в себе дополнительные данные (видеозаписи, теневые копии) (рис. <u>Контекстное меню</u> <u>события с дополнительными данными</u>¹⁵³).



дополнительными данными

Просмотр видеозаписей

SoftControl DLP Client сохраняет последовательность снимков экрана клиентского хоста, которая может быть воспроизведена как видеозапись в консоли управления. Для событий типов файл, реестр и HTTP доступен просмотр видеозаписей, если в настройках наблюдаемых объектов выставлена опция **Запись видео**. Вызовите контекстное меню нажатием правой кнопки мыши на событии и выберите пункт **Видео DLP**, чтобы открыть видеозапись (рис. <u>Контекстное меню события с</u>дополнительными данными¹⁵³). В появившемся окне проигрывателя нажмите на кнопку **Загрузить** и управляйте воспроизведением с помощью кнопок (рис. <u>Проигрыватель</u> <u>видеозаписей</u> <u>SoftControl DLP Client</u>¹⁵⁴), предназначение которых приведено в табл. 24.



Client

Таблица 24. Элементы	уΠ	равления виде	опроиг	рывателя
•				

Кнопка	Название	Описание
0	Воспроизвести	Воспроизведение записи.
0	Пауза	Пауза воспроизведения.
0	Стоп	Остановка воспроизведения.

Для корректной обработки записей серверным компонентом SoftControl Server в OC Microsoft® Windows® Server 2008 R2 и Microsoft® Windows® Server 2012 / 2012 R2 необходимо предварительно установить дополнительный системный компонент *Возможности рабочего стола* (*Desktop Experience*). Указания по установке даны в <u>приложении</u>²²⁵.

Просмотр теневых копий

Для событий типов файл и реестр доступен просмотр теневых копий объектов, если в настройках наблюдения для данных объектов выставлена опция **Теневая** копия. Вызовите контекстное меню нажатием правой кнопки мыши на событии, выберите пункт **Теневая копия DLP** (рис. <u>Контекстное меню события с</u> дополнительными данными¹⁵³) и в появившемся окне **Просмотр теневой копии DLP** нажмите на кнопку **Открыть**, чтобы просмотреть сохраненную копию указанного объекта наблюдения (рис. <u>Теневая копия объекта наблюдения</u>¹⁵⁵).



Рисунок 132. Теневая копия объекта наблюдения

4.9.3 Отчеты SoftControl SysCmd

Вкладка **Лог событий** предоставляет возможность просмотра отчетов по данным, собираемым SoftControl SysCmd на клиентских хостах (рис. <u>Вкладка «Лог событий» для компонента SoftControl SysCmd</u>¹⁵⁵). Чтобы просмотреть все события, поступившие с клиентов, выделите нужные клиенты и следуйте инструкции, приведенной в разделе Клиенты⁽⁴⁹⁾.

SoftControl Admin Console						
		Перегините сюда мышкой заголов	зок колонки для группировки	данных по неи		
Идентификатор события	Имя клиента	Идентификатор клиента	Тип события	Время	Важность	Действие
-1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Статус	02.12.2020 11:58:56	Высокая	A
-2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Статус	02.12.2020 11:59:56	Высокая	
-1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Статус	03.12.2020 9:47:34	Высокая	
-2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Статус	03.12.2020 14:36:47	Высокая	
1	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Обновление клиента	04.12.2020 10:20:15	Обычная	Запуск обновлений
• 2	CLIENT7X32	5d12505d-4c34-4e3a-b617-0689df0eeffd	Обновление клиента	04.12.2020 10:20:33	Высокая	Обновление завершено
Первая страница (Предь) ідущая страница)	Следующая страница Страница №1 (по	кледняя)			▶ Прошло времени: 00:00:(
1мя пользователя: test Pc	ли: Системный ад	министратор, Администраторы				Смена пароля

Рисунок 133. Вкладка «Лог событий» для компонента SoftControl SysCmd

Полный перечень полей вкладки **Лог событий** для компонента SoftControl SysCmd приведен в табл. 25.

Поле	Описание
Имя	Имя клиентского хоста.
Идентификатор события	Уникальный идентификатор события. Если происходит прием события с дублированным идентификатором, дублируемая строка помечается красным цветом. В случае нарушения целостности порядка идентификаторов (разрывы в последовательности), в <u>отчет серверного компонента в журнале Windows</u> ¹⁹⁹ вносится соответствующее предупреждение. Исключением являются события типа Статус , для которых данный параметр принимает значения <i>-1</i> или <i>-</i> 2.
Уникальный ID устройства	Уникальный идентификатор клиентского хоста, который автоматически присваивается ему при первом обращении клиентского приложения SoftControl SysCmd к серверу SoftControl Server.
Тип события	Тип события сбора данных: • обновление клиента; • статус.
Время	Дата и время регистрации события.
Важность	Важность (приоритет) события с точки зрения угрозы информационной безопасности клиентского хоста: • <mark>обычная</mark> ; • <mark>высокая</mark> ;

Таблица 25. Поля вкладки «Лог СОбытий» для SoftControl SysCm	۱d
--	----

Поле	Описание
	• критическая.
	Каждому уровню приоритета соответствует свой цвет ячейки.
	Статус зарегистрированного клиентского компонента:
	• активен;
Статус клиента	• остановлен;
	 работа службы была прервана;
	 ошибка статуса. неверный статус.
	Действие в случае события типа обновление :
Действие	• запуск обновлений;
	• обновление завершено.
	Статус действия в случае события типа обновление :
	 процесс обновления запущен;
	• ошибка запуска;
	 новых обновлений не найдено;
статус деиствия	 обновление прервано пользователем;
	 обновления успешно установлены;
	 нужна перезагрузка системы;
	 обновление завершено с ошибками.

4.9.4 Интегрированный лог событий

Вкладка **Интегрированный лог событий** предоставляет возможность просмотра всех логов событий в общем списке (рис. <u>Вкладка «Интегрированный лог событий»</u>⁽¹⁵⁷⁾), а именно:

- события, регистрируемые SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd на клиентских хостах;
- события из журналов Windows с клиентских хостов, на которых работает SoftControl SysWatch;
- события безопасности SoftControl Service Center.

🚩 Sof	tControl Admin Consc	ble							_ = 2
Файл	Вид Фильтры И	1нструменты Ог	программе						
Į	ا 😒 😒 🛃 🚽 🕹 😓 😓 😹 🐨 ڬ 📢 🖉 🛱 🗅 🎜 🖫 🕼								
Кли	енты Интегрирован		×						
		1	1	Перетяните сюда мышкой з	аголовок колонки ,	для группировки д	цанных по ней		
	Время (UTC+0)	Идентификато	Имя клиента	Тип события	Важность	Тип клиента	Пользователь	Детали	Журнал
•	19.04.2021 8:38:43			Начало сессии			admin		A
	19.04.2021 8:35:36			Начало сессии			admin		
	19.04.2021 8:35:32			Неавторизованный зап			admin		
	19.04.2021 8:35:26			Неавторизованный зап			admin		
	19.04.2021 8:12:56			Конец сессии			non-admin		
	19.04.2021 8:11:22			Начало сессии			admin		
	19.04.2021 8:10:28			Начало сессии			non-admin		
Пер	Первая страница Предыдущая страница Следующая страница №1 Прошло времени: 00:00:02								
Имя	Имя пользователя: admin Роли: Системный администратор, Администраторы Смена пароля								

Рисунок 134. Вкладка «Интегрированный лог событий»

Обратите внимание, что за один хартбит (интервал между обращениями SoftControl SysWatch к SoftControl Server, по умолчанию 60 секунд) клиентское приложение передает не более 1000 событий из журналов Windows. Если в течение длительного времени в среднем за хартбит в журналах Windows появляется больше событий, то события не будут успевать приходить на сервер и могут теряться.

Описание полей вкладки **Интегрированный лог событий**, относящихся к событиям клиентам и SoftControl Service Center можно найти в соответствующих разделах данного документа:

- Отчеты SoftControl SysWatch¹⁴⁴;
- Отчеты SoftControl DLP Client¹⁵¹.
- <u>Отчеты SoftControl SysCmd</u>⁽⁵⁾.
- События безопасности⁽⁴²⁾;

Поля, относящиеся к событиям из журнала Windows и не описанные в указанных выше разделах, приведены в таблице 26.

Таблица 26. Поля вкладки «Интегрированный лог событи	ИЙ», относящиеся к событиям из
журнала Windows	

Поле	Описание
<Без названия>	Для событий, содержащих подробную информацию, присутствует
	значок 💿, позволяющий просмотреть ее.
Идентификатор события	Идентификатор события в журнале Windows.

Поле	Описание
Тип события	Поле всегда имеет значение Событие журнала Windows.
Важность	Значение соответствует полю Уровень в журнале Windows.
	Название журнала, где зарегистрировано событие:
	Application;
	• System;
Журнал	Security;
	SafenSoft.
	События из журнала SafenSoft регистрируются SoftControl Server и могут
	присутствовать в данном логе, если на сервере работает SoftControl SysWatch.
Источник	Источник (провайдер) события
Кол операции	Код операции. Значение, определенное провайдером для логической
Код операции	группировки событий.
ID задачи	Идентификатор задачи. Значение, определенное провайдером для логической
	группировки событий.

4.9.5 Фильтрация событий

▽ Страничное отображение

Информация на вкладке **Лог событий** отображается в постраничном режиме. Ограничение максимального количества событий на странице задается в <u>настройках интерфейса SoftControl Admin Console⁽³²⁾</u> (по умолчанию – 10 000 событий).

Не рекомендуется выставлять значение параметра **Размер страницы событий** большим 100 000 событий, так как это может снизить производительность.

Записи расположены в обратном хронологическом порядке, т.е. на первой странице находятся записи о последних событиях. Для навигации по страницам используйте соответствующие кнопки в нижней части вкладки (рис. <u>Навигация по страницам</u>¹⁵⁹). Переход осуществляется только на соседние страницы.



Рисунок 135. Навигация по страницам

Группировка данных

Информация на вкладке **Лог событий** может группироваться по всем полям (категориям) для удобства отображения. На дополнительной вкладке **Сканер** можно группировать по следующим полям (категориям): **Путь** (по умолчанию), **Вирус**, **Результат** и **Действие**. Для группировки по категориям перетащите заголовок колонки на панель, расположенную между заголовком таблицы и группой кнопок вкладки. Если группировка производится по нескольким категориям, то приоритет (вложенность категорий) уменьшается слева направо в зависимости от расположения на панели.

Фильтрация с использованием предустановленных фильтров

В SoftControl Admin Console предусмотрены встроенные фильтры для выборки событий.

Чтобы применить предустановленные в программе общие фильтры, откройте меню Фильтры и выберите один из вариантов:

- По умолчанию отображение всех типов событий по полям, несущим основную информацию (применяется по умолчанию при открытии вкладки).
- Полный вид отображение всех типов событий по всем возможным полям.
- Статус отображение событий по изменению статуса клиентских приложений.
- Обновление клиента отображение событий по обновлению клиентских приложений.

Чтобы применить предустановленные фильтры, соответствующие типам событий клиентского компонента SoftControl SysWatch, откройте меню **Фильтры** → **Фильтры событий SysWatch** и выберите один из вариантов:

- Bce;
- Нарушение политики контроля;
- Контроль активности;
- Запуск процесса;
- Антивирус;
- Изменение настроек;
- Вход пользователя;
- Выход пользователя;
- Событие службы.

Чтобы применить предустановленные фильтры, соответствующие типам событий клиентского компонента SoftControl DLP Client, откройте меню **Фильтры** → **Фильтры событий DLP** и выберите один из вариантов:

- Bce;
- Добавлено устройство;

- Файл;
- HTTP;
- Монитор клавиатуры;
- Принтер;
- Реестр;
- Устройство отсоединено;
- Время работы.

Фильтрация применяется только к записям текущей страницы.

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

Фильтрация с использованием пользовательских фильтров

Возможно самостоятельно настроить параметры выборки и сохранить их в качестве нестандартного фильтра, который вызывается из меню **Фильтры** → **Пользовательские фильтры**.

Чтобы добавить новое поле в таблицу текущей вкладки нажмите кнопку Выбрать колонки и перетащите требуемое поле из окна Выбор колонок (рис. Выбор колонок (¹⁶¹) в необходимое место заголовка таблицы. Для удаления существующего поля перетащите его в окно Выбор колонок, либо за пределы заголовка таблицы.



Рисунок 136. Выбор колонок

Для того чтобы отфильтровать выборку по значениям полей, переместите курсор мыши на название поля и нажмите левой кнопкой мыши на появившемся значке ключа, после чего укажите критерий выборки в выпадающем списке (рис. <u>Фильтр</u> по полю⁽¹⁶²).

Фильтрацию выборки можно производить по нескольким полям одновременно. В заголовках полей, по которым производится фильтрация, значок ключа отображается постоянно.



Рисунок 137. Фильтр по полю

Когда вы отфильтруете записи, внизу окна появится строка, описывающая настроенный фильтр. Его можно удалить или изменить с помощью соответствующих иконок справа от строки.

🔀 SoftControl Admin	SoftControl Admin Console						
Файл Вид Фильтр	Файл Вид Фильтры Инструменты О программе						
≶ 🙈 🍕	8 Sa 🐕 🚅 5 🏩 🛦 😒 🕌 🕢 😒 🗮 😂 🎬 🔒 4 🎬 🔓 🔛						
Клиенты Лог собы	тий ×					· · · · · · · · · · · · · · · · · · ·	
8	a · a	🍇 🗿 🕘					
				Перетяните сюда м	иышкой заголовок ко	лонки для группировки данных по ней	
Идентификато	Имя клиента	Тип события [™]	Время	Важность	Тип клиента 🍸		
28	DESKTOP-63K	Антивирус	02.02.2021 8:21:23	Высокая	SysWatch	· · · · · · · · · · · · · · · · · · ·	
26	DESKTOP-63K	Антивирус	02.02.2021 8:20:01	Высокая	SysWatch		
25	DESKTOP-63K	Антивирус	02.02.2021 8:19:46	Высокая	SysWatch		
6	DESKTOP-63K	Антивирус	02.02.2021 7:17:16	Обычная	SysWatch		
5	DESKTOP-63K	Антивирус	01.02.2021 15:00:49	Обычная	SysWatch		
[Тип клиента] = 'S	iysWatch' И [Тип с	события] = 'Антивирус' •				08	
Первая страница	Предыдущая ст	граница 🛛 Следующая стр	аница Страница N	≌1 (последняя)		Прошло времени: 00:00:01	
Имя пользователя: а	dmin Роли: Си	стемный администратор, А	дминистраторы			Смена пароля	

Рисунок 138. Настроенный фильтр

Нажмите на значок карандаша в правой части строки фильтра, чтобы открыть средство **Редактор фильтра**.

Ŷ Редактор фильтра
ИФ
Тип события Равен VirusScanEvent 😳
Тип клиента Равен SysWatch 😳
ОК Отмена Применить

Рисунок 139. Редактор фильтра

В первой строке редактора красным цветом указан логический оператор, по которому объединяются параметры фильтра. Чтобы изменить логический оператор, нажмите на него левой кнопкой мыши. При этом в выпадающем меню вы увидите следующие варианты:

- •И;
- ИЛИ;
- Не И;
- Не ИЛИ.

Чтобы добавить новый параметр фильтра, нажмите на значок плюса около логического оператора. Чтобы удалить условие из фильтра, нажмите на крестик Синтаксис строки параметра фильтра выглядит следующим образом: *<поле, по которому производится фильтрация> <оператор сравнения> <значение>.* Каждый элемент строки параметра можно изменить, нажав на него. Варианты автоматически определяются исходя из типа поля.

На вкладке **Интегрированный лог событий** редактор фильтра состоит из трех разделов, позволяющих отдельно редактировать фильтры для логов клиентов, событий безопасности сервера и журнала событий Windows.

5	Редактировать запрос		_ = ×
ſ	🗹 Журнал событий клиентов	🗹 Журнал событий безопасности	Журнал событий Windows
	Укажите запрос:	Укажите запрос:	Укажите запрос:
	ИО	ИФ	ио
			Отмена

Рисунок 140. Редактор фильтра интегрированного лога событий

Для упорядочивания данных в таблицах вкладок по определенным полям нажмите левой кнопкой мыши на требуемом поле и одиночным нажатием задайте направление сортировки, которое обозначается стрелкой правее названия поля.

Чтобы сохранить полученную с параметрами пользователя выборку для дальнейшего использования, нажмите на кнопку **Сохранить настройки вида**, введите имя фильтра в появившемся окне и нажмите **ОК** (рис. <u>Сохранение</u> фильтра¹⁶⁴).

🔀 Сохранить настройки те	кущего вида	×
Введите имя фильтра:	Пользовательский фильтр 1	
	Отмена ОК	

Рисунок 141. Сохранение фильтра

Фильтрация применяется только к записям текущей страницы.

При наличии большого количества событий во время работы фильтра отображается индикатор выполнения. При необходимости процесс можно остановить.

4.9.6 Запросы к базе данных

Если вам часто приходится искать записи о событиях, отвечающих определенным условиям, вы можете создать запрос с этими условиями и сохранить его. Тогда в следующий раз можно будет загрузить созданный ранее запрос и получить по нему соответствующие записи из базы данных.

Работать с запросами к базе данных позволяют иконки, расположенные на дополнительной панели.

🖌 SoftControl Admin Console 📃 🗖 🗶						
Файл Вид Фильтры Инструменты О программе						
ا 😒 😒 💱 ا 🛃 😓 😒 🛛 😂 💭 😒 🕬 🖉 🕮 🖓 👘 🖓 🖉						
Клиенты Лог событий ×					•	
		г	Іеретяните сюда м	ышкой заголовок ко	юнки для группировки данных по ней	
Идентификато Имя клиента Т	Гип события	Время	Важность	Тип клиента		
28 DESKTOP-63K A	Антивирус	02.02.2021 8:21:23	Высокая	SysWatch		
26 DESKTOP-63K A	Антивирус	02.02.2021 8:20:01	Высокая	SysWatch		
25 DESKTOP-63K A	Антивирус	02.02.2021 8:19:46	Высокая	SysWatch		
24 DESKTOP-63K C	Обновление клиента	02.02.2021 8:19:42	Высокая			
23 DESKTOP-63K C	Обновление клиента	02.02.2021 8:19:42	Обычная			
22 DESKTOP-63K C	Обновление клиента	02.02.2021 8:19:41	Обычная			
27 DESKTOP-63K V	Изменение настроек	02.02.2021 8:20:34	Обычная	SysWatch		
-2 DESKTOP-63K C	Статус	02.02.2021 8:19:45	Высокая			
21 DESKTOP-63K 3	Запуск процесса	02.02.2021 8:18:15	Высокая	SysWatch		
20 DESKTOP-63K 3	Запуск процесса	02.02.2021 8:18:15	Высокая	SysWatch		
19 DESKTOP-63K C	Обновление клиента	02.02.2021 8:17:41	Высокая			
18 DESKTOP-63K C	Обновление клиента	02.02.2021 8:17:41	Высокая			
17 DESKTOP-63K C	Обновление клиента	02.02.2021 8:17:39	Обычная			
16 DESKTOP-63K B	Зход пользователя	02.02.2021 8:16:28	Обычная			
15 DESKTOP-63K B	Зыход пользователя	02.02.2021 8:16:05	Обычная			
					T T	
Первая страница 🗌 Предыдущая стра	Первая страница Предыдущая страница Следующая страница №1 (последняя) Прошло времени: 00:00:01					
Имя пользователя: admin Роли: Системный администратор, Администраторы Смена пароля						

Рисунок 142. Кнопки для работы с запросами

Чтобы создать запрос, нажмите на кнопку

🙋 (**Редактировать запрос**). Откроется окно

редактора запроса.

Редактировать запрос
Укажите запрос:
И 🕞 Тип события Равен Нарушение политики контроля 🕄 Время Между 10.12.2019 и 17.12.2019 💽 😒
Отмена

Рисунок 143. Редактирование запроса

В первой строке редактора красным цветом указан логический оператор, по которому объединяются параметры фильтра. Чтобы изменить логический оператор, нажмите на него левой кнопкой мыши. При этом в выпадающем меню вы увидите следующие варианты:

- •И;
- ИЛИ;
- Не И;
- Не ИЛИ.

Чтобы добавить новый параметр фильтра, нажмите на значок плюса около логического оператора. Чтобы удалить условие из фильтра, нажмите на крестик

Синтаксис строки параметра фильтра выглядит следующим образом: *<поле, по которому производится фильтрация> <оператор сравнения> <значение>.* Каждый элемент строки параметра можно изменить, нажав на него. Варианты автоматически определяются исходя из типа поля.

Все кнопки для работы с запросами перечислены в таблице ниже.

Кнопка	Название			Описание)		
	Редактировать запрос	Открывает параметры і	редактор и желаемые	запроса. е значения	Здесь	МОЖНО	выбрать
	Очистить запрос	Сбрасывает	введенные	е критерии	запроса		

Таблица 27. Запросы к базе данных

Кнопка	Название	Описание
e .	Выбрать запрос	Предлагает выбрать запрос из списка сохраненных запросов. Запросы хранятся в файле C:\ProgramData \SafenSoft\UserFilters\QueryCriteria.xml
	Сохранить запрос	Сохраняет текущий запрос в файле C:\ProgramData \SafenSoft\UserFilters\QueryCriteria.xml
	Удаление запросов	Открывает окно со списком сохраненных запросов, откуда вы можете их удалить
	Импорт запроса	Позволяет выбрать файл XML и импортировать из него запрос
	Экспорт запроса	Экспортирует текущий запрос в файл XML

4.9.7 Печать и экспорт в файлы отчётов

В SoftControl Admin Console существует несколько возможностей экспорта накопленной информации в отчетах клиентских приложений.

Для вывода отчета на печать произведите выборку с помощью необходимых <u>фильтров</u>¹⁵⁹ и нажмите на кнопку **Печать**. В открывшемся окне предварительного просмотра можно задать **Настройки страницы** и **Масштаб** с помощью соответствующих кнопок (рис. <u>Предварительный просмотр печати</u>¹⁶⁷).

Тип события	Время	Важность
Имя: VM-AS-W51ENX86		
Запуск процесса	16.07.2012 15:14:21	Обычная
Запуск процесса	16.07.2012 15:14:20	Обычная
Запуск процесса	16.07.2012 15:14:20	Высокая
Запуск процесса	16.07.2012 15:14:16	Обычная
Запуск процесса	16.07.2012 15:13:43	Высокая
Запуск процесса	16.07.2012 15:12:52	Обычная
Контроль активности	16.07.2012 15:11:08	Критическая
Контроль активности	16.07.2012 15:11:06	Критическая
Запуск процесса	16.07.2012 14:51:31	Обычная
Запуск процесса	16.07.2012 14:51:29	Обычная
Запуск процесса	16.07.2012 14:15:29	Обычная
Запуск процесса	16.07.2012 14:15:13	Обычная
Запуск процесса	16.07.2012 14:15:12	Обычная
Запуск процесса	16.07.2012 14:15:11	Обычная
Запуск процесса	16.07.2012 14:15:09	Обычная

Рисунок 144. Предварительный просмотр печати

Нажмите на кнопку Печать для вывода стандартного окна настроек принтера, либо на

кнопку Быстрая печать для мгновенной отправки на печать с установками принтера по умолчанию.

Для сохранения отчета в таблицу Excel произведите выборку с помощью необходимых фильтров¹⁵⁹ и нажмите на кнопку **Экспорт в Excel**. В диалоговом окне сохранения укажите место для сохранения отчета и его имя, после чего нажмите на кнопку **Сохранить** (Save).

4.9.8 Резервное копирование отчетов

В SoftControl Admin Console существует возможность резервного копирования таблиц с логом событий и с событиями безопасности. Для настройки копирования выберите команду Настройки сервера в меню Файл SoftControl Admin Console. В появившемся окне (рис. <u>Резервное копирование событий</u> ⁽¹⁶⁸⁾) перейдите на вкладку Таблица Событий или Таблица Событий безопасности, в зависимости от того, какие события необходимо сохранить. На каждой из вкладок установите переключатель в положение Осуществлять резервное копирование и укажите Путь на сервере для сохранения таблиц, Период сохранения (в днях) и Время создания резервных копий.

🔀 Настройки сервера	×					
Настройки резервного копирования						
Таблица Событий Таблица Событий безопасности						
Установка режима резервного копирования Я сам настрою резервное копирование Осуществлять резервное копирование						
Путь						
Период (дней) 5 🕄						
Время 00:00:00						
Syslog Включить логирование в Syslog для событий Включить логирование в Syslog для событий безопасности Включить логирование в Syslog для событий EventLogs Сервер Порт 514						
Применить Отмена	9					

Рисунок 145. Резервное копирование событий

Вы также можете настроить резервное копирование с помощью сторонних средств, без использования инструментов SoftControl Service Center. В этом случае в окне **Настройки сервера** (см. <u>выше</u>⁽¹⁶⁸⁾) выберите пункт **Я сам настрою резервное копирование**.

4.9.9 Отправка событий по протоколу Syslog

Вы можете отправлять события на сторонний сервер по протоколу Syslog. Для этого выберите команду **Настройки сервера** в меню **Файл** SoftControl Admin Console. В области **Syslog** отметьте флажками необходимые варианты:

- Включить логирование в Syslog для событий все события клиентских устройств (Event),
- Включить логирование в Syslog для событий безопасности все события по управлению системой SoftControl (**SecurityEvent**),
- Включить логирование в Syslog для событий EventLogs все события из отслеживаемых журналов событий Windows на устройствах (**EventLog**).

Затем введите имя сервера, номер порта и выберите тип протокола.

🔀 Настройки сервера	×			
Настро	йки резервного копирования			
Таблица Событий	Таблица Событий безопасности			
Установка режима резервного копирования				
Включить логиров Включить логиров Включить логиров	Syslog ание в Syslog для событий ание в Syslog для событий безопасности ание в Syslog для событий EventLogs			
Сервер				
Порт 514	UDP			
	Применить Отмена			
D	40 II			

Рисунок 146. Настройки для Syslog

Сообщения для отправки на сторонний сервер с использованием протокола Syslog соответствуют стандарту RFC 5424. Основные сведения о событии находятся внутри

элемента Syslog-сообщения STRUCTURED-DATA. Дополнительную информацию вы можете найти в статьях:

- <u>http://kb.safensoft.com/index.php/Sending_events_with_Syslog_protocol</u> элементы Syslogсообщений;
- <u>http://kb.safensoft.com/index.php/Information_about_SoftControl_events</u> события SoftControl.

4.10 Оповещения о событиях

Оповещения (нотификации) о событиях, регистрируемых в Сервисном Центре, позволяют администратору оперативно реагировать на возникающие угрозы, даже в случае отсутствия за штатной рабочей станцией с установленной консолью управления SoftControl Admin Console.

Первоначально необходимо задать контактные данные ¹⁷⁰ получателей оповещений, после чего настроить параметры отправки ¹⁷¹.

4.10.1 Контакты

На вкладке **Контакты** производится задание адресатов – получателей нотификаций (рис. <u>Вкладка «Контакты»</u>¹⁷⁰).



Рисунок 147. Вкладка «Контакты»

Основные операции с контактами осуществляются с помощью графических кнопок

вкладки, предназначение которых приведено в табл. 28.

Кнопка	Название	Описание				
	Добавить	Создание нового контакта.				
	Редактировать	Редактирование свойств выбранного контакта.				
0	Удалить	Удаление выбранных контактов.				
	Переместить	Перемещение выбранного контакта в другое подразделение.				

Таблица 28. Элементы управления вкладки «Контакты»

Перечень полей вкладки приведен в табл. 29.

Таблица 29. Поля вкладки «Контакты»

Поле	Описание
Подразделение	Подразделение, к которому принадлежит данный контакт.
Имя	Имя получателя.
Почта	Адрес электронного почтового ящика получателя.

Чтобы добавить нового получателя, нажмите на кнопку **Создать** (рис. <u>Вкладка «Контакты»</u> ⁽¹⁷⁰). В появившемся окне укажите данные получателя в полях **Имя** и **Электронная почта** и нажмите на кнопку **Применить** (рис. <u>Добавление контакта</u>⁽¹⁷¹).

🔀 Контакт	×
Имя:	security_officer
Электронная почта:	example2@example.com
	Применить Отмена

Рисунок 148. Добавление контакта

Для правки и удаления контактов воспользуйтесь соответствующими кнопками.

4.10.2 Нотификации

Вкладка **Управление нотификациями** предназначена для настройки параметров отправки оповещений о событиях посредством электронной почты (рис. <u>Вкладка</u> <u>«Управление нотификациями»</u>¹⁷¹).

	SoftControl Admir	Console							_ = ×
0	айл Вид Фильт	ры Инс	струменты	О программе					
	🕏 😼 🦻			h 🏂 🚣 🕙	📸 💼 📔 📢	3 🏥 🔓 🌙			
	Клиенты Контакт	ы Упран	вление но	гификациями ×					
	🛨 🖉 🛯								
	Подразделение	Имя 🔫	Активна	Всплывающее сообщение	Интервал между отправками	Время последней нотификации	Правило	Контакты	
	По умолчанию	Notif	\checkmark		Сутки	02.02.2021 11:43:31	Срок действия лицензии зака	Показать	A
	По умолчанию	Notif	\checkmark		Нет	02.02.2021 11:41:43	При сканировании обнаруже	Показать	
I									
L									
V	імя пользователя:	admin	Роли: Си	стемный администратор, Ад	аминистраторы				Смена пароля

Рисунок 149. Вкладка «Управление нотификациями»

Основные операции с нотификациями осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 30.

Кнопка	Название	Описание
	Создать	Создание новой нотификации.
<u>/</u>	Редактировать	Редактирование выбранной нотификации.
0	Удалить	Удаление выбранных нотификаций.
-R	SMTP	Настройка SMTP-сервера.

Таблица 30. Элементы управления вкладки «Управление нотификациями»

Перечень полей вкладки приведен в табл. 31.

Таблица 31. Поля вкладки «Управление нотификациями»

Поле	Описание		
Подразделение	Подразделение, к которому относится данная нотификация. Перемещение нотификаций между подразделениями не поддерживается. Каждой нотификации назначается то подразделение, к которому принадлежит создавший ее пользователь.		
Имя	Наименование нотификации.		
Активна	Флажок состояния нотификации.		
Всплывающее сообщение	Флажок, указывающий, отображается ли всплывающее уведомление при отправке нотификации.		
Интервал между	Минимальный временной интервал после отправки предыдущей нотификации,		
отправками	по истечении которого возможна отправка следующей.		

Поле	Описание	
Время последней нотификации	Время отправки последней нотификации.	
Правило	Условия отправки нотификации.	
Контакты	Список адресатов электронного письма с нотификацией.	

Основные действия, выполняемые на данной вкладке:

Настройка SMTP-сервера

Для работы нотификаций необходимо предварительно настроить параметры сервера исходящей почты по протоколу SMTP, для этого нажмите на кнопку **SMTP** (рис. Вкладка «Управление нотификациями»⁽⁷¹⁾).

В окне **Настройка почтового сервера** введите в поле **Почтовый сервер** адрес почтового сервера, с электронного ящика которого предполагается отправка нотификаций, а также **Номер порта** для отправки (рис. <u>Настройка почтового</u> <u>сервера</u>¹⁷³). В полях **Логин**, **Пароль** и **Почтовый ящик** введите данные учетной записи и адрес почтового ящика, с которого предполагается отправка нотификаций. Установите флажок **Использовать SSL** для криптографической защиты при передаче данных.

Чтобы проверить работоспособность введенных настроек, нажмите на кнопку Отправить тестовое письмо.

🔀 Настройка почтовог	о сервера 🛛 🗙
Почтовый сервер:	smtp.mail.ru
Номер порта:	587
Логин:	notify_server
Пароль:	•••••
Почтовый ящик:	notify_server@mail.ru
🗸 Использовать SSL	
	Отправить тестовое письмо
	Отмена ОК
Рисунок 150	Настройка почтового

Рисунок 150. Настройка почтового сервера

Нажмите на кнопку ОК для применения настроек.

Создание нотификации

Чтобы добавить новую нотификацию, нажмите на кнопку **Создать** (рис. <u>Вкладка</u> «Управление нотификациями»¹⁷¹).

В появившемся окне на вкладке **Общие** укажите **Имя** нотификации, выберите минимальный **Интервал между отправками** в выпадающем списке, введите **Тему** письма и установите флажок **Активировать** (рис. <u>Общие параметры нотификации</u> ⁽¹⁷⁴).

🖉 Настро	йка нотифик	ации	×
Общие	Правила	Контакты	
Имя: Интері	вал между о	Нар тправками:	рушение политики контроля Один час
Тема:		Авто	оматическое оповещение Service Center
✓ Akt √ Πο	ивировать сазывать всп	лывающее о	сообщение
			Отмена ОК
P	исуно	к 151.	Общие параметры

нотификации

Чтобы **Показывать всплывающее сообщение** при отправке нотификации, установите соответствующий флажок. В этом случае после отправки нотификации будет отображаться всплывающее уведомление с заголовком оповещения.



На вкладке **Правила** выберите условие, при наступлении которого будет производиться отправка нотификации (рис. <u>Условия срабатывания отправки</u> <u>нотификации</u>¹⁷⁴):



Рисунок 153. Условия срабатывания отправки нотификации

о Изменение контроля активности:

Изменение статусов контроля активности компонента SoftControl SysWatch по любой из областей.

о Запуск процесса запрещен:

Регистрация события типа **Запуск процесса** компонентом SoftControl SysWatch с решением «запрещено».

о При сканировании обнаружены угрозы:

Обнаружение вредоносного кода в процессе антивирусной проверки компонентом SoftControl SysWatch.

• Нарушение политики контроля:

Регистрация компонентом SoftControl SysWatch одного или нескольких событий типа **Нарушение политики контроля**, выбираемых по ссылке **<Выбор>** (рис. Выбор типов политик контроля для отправки нотификации¹⁷⁵).



Рисунок 154. Выбор типов политик контроля для отправки нотификации

о Срок действия лицензии заканчивается:

До конца срока действия лицензионного ключа клиентского компонента остается меньше 10 дней.

Рекомендуется устанавливать значение параметра Интервал между отправками для данной нотификации не менее 4 часов.

Запуск процесса с именем:

Регистрация события типа **Запуск процесса** с именем, заданным по ссылке **Имя процесса**, компонентом SoftControl SysWatch.

Произошло одно из событий безопасности:

Обнаружение компонентом SoftControl SysWatch одного или нескольких событий безопасности, выбираемых по ссылке **<Выбор>** (рис. <u>Выбор_событий</u> <u>безопасности для отправки нотификации</u>¹⁷⁶).



Рисунок 155. Выбор событий безопасности для отправки нотификации

На вкладке **Контакты** отметьте адресатов отправки нотификации (рис. <u>Выбор</u> получателей нотификации ⁽¹⁷⁷).

🚩 Настрой	іка нотифик	ации	*			
Общие	Правила	Контакты]			
Выбер	оите контакт	ы:				
	Администра	тор				
	Офицер без	опасности ф	филиала Южный			
	Администра	тор ЛВС Сев	веро-Восточного филиала			
	Отдел по бо	рьбе с кибе	ерпреступностью			
	Администра	тор ЛВС фил	ілиала Северный			
	Отмена ОК					
P	Рисунок 156. Выбор получателей нотификации					

Нажмите на кнопку ОК, чтобы подтвердить создание нотификации.

Изменение свойств нотификации

Чтобы изменить свойства нотификации, выберите ее и выполните одно из следующих действий:

• нажмите на кнопку Редактировать в группе кнопок вкладки (рис. Вкладка

«Управление нотификациями»⁽¹⁷¹);

• дважды нажмите левой кнопки мыши на нотификации.

В появившемся окне измените необходимые параметры аналогично работе с новой нотификацией (рис. <u>Общие параметры нотификации</u>⁽¹⁷⁴⁾, <u>Условия срабатывания отправки нотификации</u>⁽¹⁷⁴⁾, <u>Выбор получателей нотификации</u>⁽¹⁷⁷⁾). Нажмите на кнопку **ОК**, чтобы подтвердить изменения.

✓ Отключение и удаление нотификации

Если необходимо отключить получение нотификации без ее удаления из списка, вызовите окно редактирования свойств, сбросьте флажок **Активировать** на вкладке **Общие** и нажмите на кнопку **ОК** (рис. <u>Общие параметры нотификации</u>¹⁷⁴). Для удаления нотификации выберите ее, нажмите на кнопку **Удалить** (рис. <u>Вкладка «Управление нотификациями»</u>¹⁷¹) и подтвердите удаление в диалоговом окне.

4.11 Снимки конфигурации

Вкладка Снимки конфигурации предназначена для создания снимков конфигурации любого подключенного клиентского хоста. Снимок конфигурации – это профиль компьютера с установленным клиентским приложением SoftControl SysWatch. SoftControl Admin Console также позволяет сравнить снимок с текущим состоянием выбранных клиентских хостов.

NoftControl Admin Console	2						_ = >
Файл Вид Фильтры Ин	струменты Опрограм	ime K 😒 👪	👼 🔟 📢	3) <i>4</i> •) ()	Q	
Клиенты Снимки конфигу	рации ×						
Снимки:							
🕂 🖸 🛉							
Имя Комм	ентарий	Готов					
Snapshot 1 на DE	SKTOP-63KNC18 в \$CRE4	ATIO					<u>^</u>
Задачи снимков:							v
Все Закрепленные							
Тип	Имя снимка	Имя клиента	Состояние	Время начала	Время окончания		
Создание сними	ca Snapshot 1	DESKTOP-63KNC18	Started	02.02.2021 11:48:31			×
Имя пользователя: admin	Роли: Системный адмі	инистратор, Админист	раторы				Смена пароля

Рисунок 157. Вкладка «Снимки конфигурации»

Кнопка Снимки конфигурации доступна только для пользователей, у которых есть все перечисленные ниже разрешения: Просматривать клиентов, подключенных к серверу, Создавать новые задачи для клиентов, Просматривать существующие подразделения.

Вкладка состоит из двух разделов:

- СНИМКИ¹⁷⁹;
- задачи снимков¹⁸².

4.11.1 Снимки

Основные операции со снимками в разделе **Снимки** осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 32.

Кнопка	Название	Описание
	Добавить	Создание нового снимка конфигурации.
0	Удалить	Удаление выбранного снимка.
	Сравнить	Сравнение созданного снимка с профилем клиентского хоста.

Таблица 32. Элементы управления раздела «Снимки»

Перечень полей раздела приведен в табл. 33.

Таблица 🕄	33. Поля	раздела	«Снимки»
-----------	----------	---------	----------

Поле	Описание
Имя	Наименование задачи.
Комментарий	Текстовый комментарий. По умолчанию указывается имя клиентского хоста и время создания снимка.
Готов	Индикатор завершения задачи. В данном поле выставляется галочка для снимков после получения ответа от клиентского хоста.

Основные действия, выполняемые на данной вкладке:

Создание снимка

Чтобы создать снимок конфигурации, нажмите на кнопку **(Добавить**) (рис. <u>Вкладка «Снимки конфигурации»</u>⁽¹⁷⁸⁾). В появившемся окне укажите имя снимка и комментарий, выберите клиентский хост, с которого требуется сделать снимок, и нажмите на кнопку **Создать** (рис. <u>Создание снимка</u>⁽¹⁸⁰⁾). После этого генерируется задача по созданию снимка, и в <u>таблице</u>⁽¹⁸²⁾ в разделе **Задачи снимков** появляется соответствующая запись.

🔀 Создание снимка 📃 🗖 🗙
Имя снимка:
Снимок_1
Комментарий:
на \$CLIENT_NAME в \$CREATION_TIME
Выберите клиента
▼ SysWatch
 По умолчанию
WIN-MG2LK1NUP4L
WIN-MG2LK1NUP4L
WIN-UEG53NA7DPC
ProductionPass
Добавить Отмена

Рисунок 158. Создание снимка

В комментарии по умолчанию используются следующие макросы: \$CLIENT_NAME и \$CREATION_TIME. При создании задачи они автоматически заменяются на имя клиентского хоста и время создания задачи соответственно.

До того как будет получен ответ от клиентского хоста, статус задачи в таблице в разделе **Задачи снимков** (см. <u>ниже</u>)¹⁸² помечается как **Started**. После получения
ответа снимок помечается как **Готов** (в соответствующем столбце <u>таблицы</u>¹⁸⁰ выставляется галочка), а задача по получению снимка становится завершенной (в таблице статус задачи сменяется на **Finished**).

Сравнение снимков конфигурации

Чтобы сравнить снимок конфигурации с текущим состоянием выбранного клиентского хоста, выберите снимок и нажмите на кнопку **(Сравнить)** (рис. <u>Вкладка «Снимки конфигурации»</u>¹⁷⁸). В появившемся окне выберите клиентский хост (или несколько хостов) и нажмите на кнопку **Создать** (рис. <u>Выбор</u> <u>клиентских хостов для сравнения</u>¹⁸¹). Если для сравнения выбрано несколько клиентских хостов, для каждого из них создается отдельная задача сравнения.



Рисунок 159. Выбор клиентских хостов для сравнения

Для сравнения можно использовать только снимки со статусом Готов.

🗢 Удаление снимка

Для удаления снимка выберите его, нажмите на кнопку (Удалить) (рис. <u>Вкладка</u> «Снимки конфигурации»¹⁷⁸) и подтвердите удаление в диалоговом окне.

Удалить можно только те снимки, с которыми не связана ни одна задача. Если для данного снимка имеются связанные с ним задачи, то для его удаления необходимо сначала удалить эти задачи.

4.11.2 Задачи снимков

Раздел **Задачи снимков** содержит список задач, выполняемых на вкладке **Снимки** конфигурации (создание снимков и их сравнение), и состоит из двух вкладок: **Все** и **Закрепленные**.

Основные операции с задачами осуществляются с помощью графических кнопок вкладки, предназначение которых приведено в табл. 34.

Таблица 34. Элементы управления раздела «Задачи снимков», вкладка «Все»

Кнопка	Название	Описание			
0	Удалить	Удаление выбранного снимка.			
۲	Показать результаты	Просмотреть результаты сравнения снимка конфигурации и профиля клиентского хоста.			

Перечень полей вкладки приведен в табл. 35.

Поле	Описание
Тип	Тип задачи: Создание снимка или Сравнение снимков.
Имя снимка	Наименование задачи, заданное в разделе Снимки.
Имя клиента	Наименование клиентского хоста.
Состояние	Состояние задачи: Started, Finished
Время начала	Время начала задачи
Время окончания	Время окончания задачи

Таблица 35. Поля раздела «Задачи снимков», вкладка «Все»

Для закрепления требуемой задачи выберите ее в таблице и щелкните левой кнопкой мыши по левой (пустой) ячейке таблицы. После этого в данной ячейке появляется иконка *****, задача становится **Закрепленной** и появляется в таблице на вкладке **Закрепленные** (рис. <u>Закрепленные задачи</u>¹⁸²). Задачи, которые не были закреплены, удаляются через 180 дней после их завершения.

Централизованное управление СИБ

🔀 SoftControl Admin Console							_ = >
Файл Вид Фильтры Инстру	ументы Опрограм	ме					
5 5 5 5	- 🗟 🏂 🛛	1 😒 👪	👼 🙋 🤜	3		😰 📙	
Клиенты Снимки конфигурац	Клиенты Снимки конфигурации ×						
Снимки:							
- 14 🔤 🚽							
Имя Коммента	арий	Готов					
Snapshot 1 на DESKTO на DESKTO	OP-63KNC18 в 2/2/20	21 🔽					A
Snapshot 2 на DESKTO	DP-63KNC18 в 2/2/20	21 🔽					
l							▼
Задачи снимков:							
Все Закрепленные							
0							
Тип	Имя снимка	Имя клиента	Состояние	Время начала	Время окончания		
Создание снимка 🖇	Snapshot 1	DESKTOP-63KNC18	Finished	02.02.2021 11:48:31	02.02.2021 11:48:58		A
👷 Создание снимка 🤉	Snapshot 2	DESKTOP-63KNC18	Finished	02.02.2021 11:51:35	02.02.2021 11:52:01		
имя пользователя: admin Po	оли: Системный адми	нистратор, Админист	раторы				Смена пароля

Рисунок 160. Закрепленные задачи

Чтобы просмотреть результаты сравнения снимка с текущей конфигурацией клиентского хоста, выберите требуемую задачу сравнения и нажмите на кнопку • (Показать результаты). Открывшаяся вкладка Результаты сравнения содержит два поля: Пропавшие записи и Появившиеся записи (рис. <u>Результаты сравнения снимков</u>⁽¹⁸³⁾).

При необходимости хэш-суммы можно копировать, вызывая контекстное меню нажатием правой кнопки мыши.

🔀 SoftControl Admin Console				_ 0		
Файл Вид Фильтры Инструменты Опрог	рамме					
🖻 🛸 🍢 🚅 💀 🐲 🛆 😒 🚵 💼 ڬ 🤜 23 🎬 🗅 45 🖺 🛢 😰 🗓						
Клиенты Снимки конфигурации WIN-UEG531	NA7DPC vs Снимок SW 🗙					
Пропавшие записи Нет элементов для отображения	Экс	портировать выбо	орку в файл			
О Появившиеся записи						
		•	Оильтр			
Показывать записи за период:	20.05.2020, 15:47:58 - 20.	05.2020, 15:48:52				
Имя файла содержит:						
Путь к файлу солержит:			_			
Хэш-сумма файла	Имя файла	Размер файла	Время добавления	Путь к файлу		
▶ 1240D0C0662890E21B2FF33D407	MSI7269.TMP	116144	20.05.2020 15:47:58	\DEVICE\HARDDISKVOLUME1\USERS\ADMIN\APPDATA\LOCAL\TEMP 🔺		
1C4C663A190E98579AFA56316F6	MSI3403.TMP	750256	20.05.2020 15:48:48	\DEVICE\HARDDISKVOLUME1\WINDOWS\INSTALLER		
07B83FB61280589D4263A08DC9	EVENTSVC.DLL	8049808	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\DLP		
2FC65C5E486C7E69319AD87C803	HTTPFILTER64.DLL	1239128	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\DLP		
ACD5C8D5B39E715E9A7E1CCC9F	HTTPFILTER32.DLL	1039640	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\DLP		
E807539CCDB6AA81ECBB49073B	INSTLSP64.EXE	182480	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\DLP		
1E480E37466E69BB2FF60F4733CE	INSTLSP32.EXE	161128	20.05.2020 15:48:51	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES (X86)\SAFENSOFT\DLP		
Имя пользователя: console_admin Роли: Сист	емный администратор, Администра	торы		Смена пароля		

Рисунок 161. Результаты сравнения снимков

Для просмотра изменений за определенный период времени выберите требуемые даты в поле **Фильтр**. Вы также можете указать в фильтре часть имени файла и пути к нему. Внизу каждого из разделов есть гиперссылка **Экспортировать выборку в файл**. Нажмите на нее, чтобы создать файл XML с выбранными записями.

5. Обновление компонентов СИБ

SoftControl Service Center предоставляет возможность централизованного обновления всех компонентов системы с сервера обновлений. Это может быть либо сервер SoftControl, либо сервер, развернутый на предприятии. Вкладка **Обновления** позволяет произвести настройку и просмотреть историю обновлений (рис. <u>Вкладка «Обновления»</u> для программных модулей ⁽¹⁸⁵⁾, Вкладка «Обновления» для антивирусных баз⁽¹⁸⁹⁾).

В верхней части вкладки представлено две категории настроек для обновления соответствующих компонентов:

- Программные модули⁽¹⁸⁵⁾;
- Антивирусные базы¹⁸⁹.

В нижней части вкладки представлена история обновлений, содержащая список выполняемых операций. Перечень полей списка приведен в табл. 36.

Поле	Описание
Последняя проверка	Дата и время последней проверки наличия обновлений.
Последнее обновление	Дата и время последней установки обновлений.
Компонент	Название обновляемого компонента.
Статус обновления	Состояние обновления: • Обновление не требуется; • Доступно обновление; • Обновление загружено; • Обновление установлено; • Ошибка обновления.
Размер обновления	Размер обновления в байтах.
Актуальная версия	Текущая версия установленного компонента.
Новая версия	Версия компонента, доступная к обновлению.
Детали	Дополнительная информация.

Таблица 36. Поля списка истории обновлений

5.1 Настройка обновления программных модулей

Данная категория настроек позволяет настраивать и управлять обновлением программных модулей компонентов SoftControl Service Center, а также скачиванием обновлений программных модулей клиентских компонентов SoftControl SysWatch, SoftControl DLP Client и SoftControl SysCmd с внешних (Интернет) серверов.

 SoftControl Admin Console Файл Вид Фильтры Инструменты О прогр Вид Фильтры Инструменты О прогр Клиенты Обновления × Программные модули АУ4 	amme 🚠 😒 👪 🥌 🕍 🥩 🧭	9 🎬 🔓 🥵 👫 📔 😰 🚺	
Режим обновления Выключено Только проверка Автоматическое обновление Интервал проверки обновлений (мин.): 720	Пути обновлений URL обновления: http://updates.safensoft.com/SoftControl/AV4/RU Папка для сохранения обновлений: Updates\Modules\	Статус обновления Последняя проверка: 01.02.2021 16:43:59 Результат последнего обновления: Обновление не требуется Детали: Последнее успешное обновление: 28.01.2021 12:24:11 Актуальная версия сервера: 6.0.58.0 Актуальная версия консоли: 6.0.58.0	Доступные обновления Версия обновления: Обновление не требуется Размер обновления: Обновление не требуется Проверить обновления Установить обновления
Сохранить История обновлений	Перетяните сюда мышкой	заголовок колонки для группировки данных по ней	

Рисунок 162. Вкладка «Обновления» для программных модулей

Настройка режима обновления

В секции Режим обновления возможен выбор трех режимов работы:

Выключено:

Обновление в автоматическом режиме отключено.

о Только проверка:

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике Интервал проверки обновлений (мин.), но не загружает и не устанавливает их.

о Автоматическое обновление:

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике Интервал проверки обновлений (мин.) и в случае нахождения более новых версий, чем установленные, происходит скачивание пакетов обновлений на сервер. Если найдена новая версия SoftControl Service Center, по окончании загрузки установочных пакетов происходит автоматическое обновление компонентов SoftControl Server и SoftControl Admin Console в фоновом режиме на сервере.

При отсутствии доступа в Интернет или в случае возникновения проблем в процессе автоматического обновления, возможно <u>обновление_SoftControl</u> <u>Service_Center в ручном режиме¹⁹¹</u> при наличии установочного пакета требуемой версии.

<u>Обновление клиентских компонентов</u>⁽¹⁹⁴⁾ осуществляется с созданного локального «зеркала».

Настройка путей обновления и параметров прокси-сервера

В секции Пути обновления задаются следующие параметры:

URL обновления:

Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений. В пути необходимо указать номер текущей лицензии: http://updates.safensoft.com/<номер_лицензии>/SoftControl/av/ru <u>Примечание</u>. Номер лицензии необходимо указать вручную.

Папка для сохранения обновлений:

Путь сохранения пакетов обновления с внешних серверов относительно директории C:\ProgramData\SoftControl. Укажите следующую папку: Updates\Modules\

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

• Адрес:

IP-адрес или имя хоста прокси-сервера.

Порт:

Номер порта для связи с прокси-сервером (если не указан – используется порт 80 по умолчанию).

• Имя пользователя:

Имя пользователя для аутентификации на прокси-сервере.

Пароль:

Пароль для аутентификации на прокси-сервере.

Поддерживается базовый (Basic) тип авторизации. Если аутентификация на прокси-сервере не требуется, то поля **Имя пользователя** и **Пароль** следует оставлять пустыми.

Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с помощью следующих кнопок:

• Проверить обновления:

Проверка наличия обновлений программных модулей. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).

• Установить обновления (для случая, когда SoftControl Server и SoftControl Admin Console установлены на одном компьютере):

Проверка и, в случае обнаружения, скачивание пакетов обновлений с внешних серверов, установка обновлений SoftControl Server и SoftControl Admin Console.

• Обновить сервер (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

Проверка и, в случае обнаружения, скачивание пакетов обновлений с внешних серверов, установка обновлений серверного компонента (SoftControl Server).

• Обновить консоль (для случая, когда SoftControl Server и SoftControl Admin Console установлены на разных компьютерах):

Проверка и, в случае обнаружения, установка обновлений консоли управления (SoftControl Admin Console).

После обновления программных модулей настройки SoftControl Server и SoftControl Admin Console, а также пользовательские фильтры SoftControl Admin Console сохраняются. Накопленные события в SoftControl Admin Console хранятся в БД, поэтому при обновлении не затрагиваются.

В секции Статус обновления доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения измененных установок нажмите на кнопку Сохранить.

5.2 Настройка обновления антивирусных баз

Данная категория настроек позволяет настраивать и управлять скачиванием антивирусных баз клиентского компонента SoftControl SysWatch с внешних (Интернет) серверов (рис. Вкладка «Обновления» для антивирусных баз¹⁸⁹).

SoftControl Admin Console			_ = ×
Файл Вид Фильтры Инструменты Опрогр	амме		
Клиенты Обновления ×	🚣 🕙 👪 🖶 🐚 📢 🥹	🎬 G 🍜 🔁 📳 🕸 👖	•
Программные модули АV4			îl
Режим обновления Выключено Только проверка Автоматическое обновление Интервал проверки обновлений (мин.): 60	Пути обновлений URL обновления: http://updates.safensoft.com/AV4/ Папка для сохранения обновлений: Updates/AV4 Использовать прокси-сервер Адрес: Порт: 0 Имя пользователя: Пароль:	Статус обновления Последняя проверка: 02.02.2021 11:20:37 Результат последнего обновления: Обновление установлено Детали: Последнее успешное обновление: 02.02.2021 11:20:37 Актуальная версия антивирусных баз: Нет информации	Доступные обновления Версия обновления: Нет информации Размер обновления: Нет информации Проверить обновления Установить обновления
Сохранить			
	Перетяните сюда мышкой за	оловок колонки для группировки данных по ней	
Послелная проверка. Послелнее обновлен	ие Компонент Статус обновления Разм	еп обновления Актуальная версия. Новая версия. Летали	
Имя пользователя: admin Роли: Системный ад	министратор, Администраторы		Смена пароля

Рисунок 163. Вкладка «Обновления» для антивирусных баз

Настройка режима обновления

В секции Режим обновления возможен выбор трех режимов работы:

о Выключено:

Обновление в автоматическом режиме отключено.

о Только проверка:

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике Интервал проверки обновлений (мин.), но не загружает их.

о Автоматическое обновление:

SoftControl Service Center автоматически проверяет наличие обновлений на внешних серверах с периодичностью, указанной в счетчике Интервал проверки обновлений (мин.) и в случае нахождения более новых версий, чем установленные, происходит скачивание обновлений баз на сервер. Обновление антивирусных баз осуществляется в рамках обновления

клиентского компонента SoftControl SysWatch¹⁹⁴ с созданного локального «зеркала».

Настройка путей обновления и параметров прокси-сервера

В секции Пути обновления задаются следующие параметры:

• URL обновления:

Ссылка на внешний сервер, по которой SoftControl Service Center проверяет наличие обновлений. Ссылки для разных антивирусных баз описаны в таблице 37.

Таблица 37. Адреса обновлений антивирусных баз

Название	Адрес	Папка для сохранения
Антивирусные базы AV4 http://updates.safensoft.com/ <номер_лицензии>/av4/		Updates\AV4
Антивирусные базы AV5	http://updates.safensoft.com/ <номер_лицензии>/av5/	Updates\AV5

Примечание. Номер лицензии необходимо указать вручную.

Папка для сохранения обновлений:

Путь сохранения пакетов обновления с внешних серверов относительно директории C:\ProgramData\SoftControl. Папки для разных антивирусных баз описаны в табл. 37.

Установите флажок **Использовать прокси-сервер**, если соединение с внешними серверами требуется осуществлять через прокси-сервер. В этом случае задайте его параметры:

• Адрес:

IP-адрес или имя хоста прокси-сервера.

Порт:

Номер порта для связи с прокси-сервером (если не указан – используется порт 80 по умолчанию).

Имя пользователя:

Имя пользователя для аутентификации на прокси-сервере.

Пароль:

Пароль для аутентификации на прокси-сервере.

Поддерживается базовый (Basic) тип авторизации. Если аутентификация на

прокси-сервере не требуется, то поля Имя пользователя и Пароль следует оставлять пустыми.

Проверка и обновление по запросу

В секции **Доступные обновления** возможно выполнение операций по запросу с помощью следующих кнопок:

Проверить обновления:

Проверка наличия обновлений антивирусных баз. В случае обнаружения обновлений отображается **Версия обновления** и **Размер обновления** (в байтах).

• Установить обновления:

Проверка и, в случае обнаружения, скачивание антивирусных баз с внешних серверов.

В секции Статус обновления доступна информация по текущей версии и последним проведенным операциям проверки и установки обновлений.

Для применения измененных установок нажмите на кнопку Сохранить.

5.3 Обновление SoftControl Server и SoftControl Admin Console в ручном режиме

- 1) Запустите установочный пакет Service. Center. msi версии, на которую необходимо произвести обновление.
- 2) В окне Установка SoftControl Service Center нажмите на кнопку Далее (рис. <u>Запуск</u> программы обновления⁽¹⁹¹).



Рисунок 164. Запуск программы обновления

3) В случае вашего согласия, отметьте опцию **Я принимаю условия лицензионного** соглашения и нажмите на кнопку **Далее** (рис. <u>Лицензионное соглашение</u>¹⁹²).

😸 Установка SoftControl Service Center 📃 🖃 💌
Лицензионное соглашение Внимательно прочитайте следующее лицензионное соглашение SoftControl
1. Предмет соглашения
Настоящее лицензионное соглашение (далее Соглашение) является юридическим документом, заключаемым между SAFE 'N SEC Corporation (далее - Правообладатель) и Вами, физическим или юридическим лицом (далее - Пользователь), правомерно владеющим экземпляром программного продукта группы "SoftControl" (далее - Программный продукт). Устанавливая, копируя, загружая или иным образом используя т
Я принимаю условия лицензионного соглашения
<u>П</u> ечать <u>Н</u> азад <u>Да</u> лее Отмена
Рисунок 165. Лицензионное соглашение

4) Нажмите на кнопку Обновить (рис. Готовность к обновлению [192]).



Рисунок 166. Готовность к обновлению

5) Дождитесь окончания процесса обновления (рис. <u>Процесс обновления (193</u>).

становка SoftControl Service	Center		
Идет обновление SoftControl Service Center		SoftContro	
юдождите, пока мастер устан	овки обновляет SoftControl S	ervice Center.	
Состояние:			

Рисунок 167. Процесс обновления

6) После появления сообщения Установка SoftControl Service Center завершена нажмите на кнопку Готово (рис. <u>Завершение обновления</u>¹⁹³).



Рисунок 168. Завершение обновления

5.4 Обновление клиентских компонентов

После скачивания обновлений с внешних серверов клиентские компоненты могут быть обновлены с SoftControl Service Center следующими способами:

- □ После подключения к Сервисному Центру SoftControl SysWatch и SoftControl DLP Client автоматически переключаются в режим обновлений с него. Обновление компонентов производится по запросу посредством создания соответствующей <u>задачи</u>¹³⁴ или по расписанию, если оно настроено для <u>SoftControl SysWatch</u>⁷⁶ / <u>SoftControl DLP Client</u>¹²³.
- Находясь в автономном режиме работы, SoftControl SysWatch также может быть обновлен с Сервисного Центра. Для этого в настройках источников обновления SoftControl SysWatch через интернет замените предустановленные адреса на соответствующие табл. 38 локальные адреса для необходимых компонентов. Порт связи с сервером по умолчанию – 8088. После применения указанных настроек обновление можно произвести по запросу через ГИП.

Компонент	Описание	Адрес
Core	Программные модули	http:// <ip-адрес сервера="">:<порт связи с сервером>/api/ updates/SNS</ip-адрес>
AV-AV4	Антивирусные базы AV4	http:// <ip-адрес сервера="">:<порт связи с сервером>/api/ updates/AV4</ip-адрес>
AV-AV5	Антивирусные базы AV5	http:// <ip-адрес сервера="">:<порт связи с сервером>/api/ updates/AV5</ip-адрес>

Таблица 38. Адреса обновлений с SoftControl Service Center

6. Удаление компонентов SoftControl Service Center

<u>Удаление SoftControl Server и SoftControl Admin Console</u>: в Панели управления Windows в разделе **Программы** (Programs) → **Программы и компоненты** (Programs and Features) выберите *SoftControl Service Center* и нажмите на кнопку **Удалить** (Uninstall). Удаление одного из компонентов:

- В Панели управления Windows в разделе Программы (Programs) → Программы и компоненты (Programs and Features) выберите SoftControl Service Center и нажмите на кнопку Изменить (Change).
- 2) В окне Установка SoftControl Service Center нажмите на кнопку Далее (рис. <u>Запуск</u> программы удаления¹⁹⁵).



Рисунок 169. Запуск программы удаления

- 3) Выберите операцию Изменить (рис. <u>Типы операций (195</u>).
- 4) Выберите компонент для удаления (рис. <u>Выбор компонентов для удаления</u>¹⁹⁶): нажмите на пиктограмму компонента и в выпадающем меню выберите опцию Компонент будет полностью недоступен (рис. <u>Опции установки компонента</u>¹⁹⁶). После того как все установки завершены, нажмите на кнопку Далее.

Удаление компонентов SoftControl Service Center

😸 Установка SoftControl Service Center 📃 📼 💌
Изменение, восстановление или удаление установки Выберите операцию, которую следует выполнить.
Изменить Позволяет изменить параметры установки компонентов.
Восстановить Исправление ошибок в последней установке путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра.
Удалить Удаление SoftControl Service Center с компьютера.
<u>Н</u> азад Д <u>а</u> лее Отмена

Рисунок 170. Типы операций

😸 Установка SoftControl Service Center	
Выборочная установка Укажите конфигурацию установки компоненто	5. SoftControl
Для изменения параметров установки какого-л соответствующий значок в расположенном ниж	ибо компонента щелкните се дереве.
SoftControl Server Microsoft SQL Server 20 SoftControl Admin Console	SoftControl Admin Console
	Компонент освободит 96МБ на жестком диске.
С <u>б</u> рос Использование <u>ди</u> ска	Назад Далее Отмена

Рисунок 171. Выбор компонентов для удаления

	Будет установлен на локальный жесткий диск
	Компонент будет полностью установлен на локальный жесткий диск
P	Компонент будет установлен при необходимости
×	Компонент будет полностью недоступен
F	Рисунок 172. Опции установки компонента

5) Нажмите на кнопку Изменить (рис. Готовность к удалению 196).

Удаление компонентов SoftControl Service Center



Рисунок 173. Готовность к удалению

6) Дождитесь окончания процесса удаления (рис. <u>Процесс удаления (197</u>).

😸 Установка SoftControl Service Center	
Изменение SoftControl Service Center	SoftControl
Подождите, пока мастер установки изменяет SoftControl S	ervice Center.
Состояние:	
<u>Н</u> азад	<u>Да</u> лее Отмена
Рисунок 174. Процесс уд	аления

7) После появления сообщения *Установка SoftControl Service Center завершена* нажмите на кнопку **Готово** (рис. <u>Завершение удаления</u>¹⁹⁷).

Удаление компонентов SoftControl Service Center



Рисунок 175. Завершение удаления

В случае, если SoftControl Server был установлен со встроенной СУБД (например, была выбрана <u>полная установка</u>⁽¹⁴⁾), удаление Microsoft® SQL Server® 2014 Express SP1 необходимо произвести вручную. Для этого выполните удаление следующих элементов СУБД стандартными средствами Windows:

- Microsoft SQL Server 2014;
- Microsoft SQL Server 2012 Native Client;
- Microsoft SQL Server 2014 Setup (English);
- Microsoft SQL Server 2008 Setup Support Files;
- Microsoft SQL Server 2014 Transact-SQL ScriptDom.

7. Диагностика проблем

В случае возникновения проблем при развертывании и функционировании SoftControl Service Center в первую очередь обратитесь к отчету **SafenSoft** в журнале событий Windows. Для этого откройте Панель управления Windows, выберите раздел **Система и безопасность** (System and Security) → **Администрирование** (Administrative Tools), в нем откройте средство **Просмотр событий** (Event Viewer). В открывшемся окне в панели слева разверните категорию **Журналы приложений и служб** (Applications and Services Logs) и в ней выберите журнал **SafenSoft**. При анализе ошибок, предупреждений и уведомлений в данном отчете может быть найдена причина, вызвавшая сбой при установке, запуске и установлении соединения между компонентами. Если определить причину самостоятельно невозможно, приложите файлы текстовых отчетов компонентов к запросу в <u>техническую</u> <u>поддержку</u> <u>ООО «АРУДИТ СЕКЬЮРИТИ»</u> . Сп²⁰²сок

Название	Имя файла	Путь	Краткое	Авторотация по	Управление
			описание	умолчанию	авторотацией
	-	Логи Serv	ice Center		
Лог Service Center	ServerDetaile dLog.txt	C:\Program Files (x86) \SafenSoft\Service Center\Server\logs\	Лог Service Center	При превышении размера 209715200 создается новый файл	Черезфайл SafenSoft.Ente rprise.Server. exe.nlog
Журнал обновлений	checks.log	C:\Program Files\(x86) \Safensoft\Service Center\Server\Tools \Updates\Reports\	Лог проверок наличия обновлений	-	_
Журнал обновлений	sns.log	C:\Program Files\(x86) \Safensoft\Service Center\Server\Tools \Updates\Reports\	Журнал обновления модулей	-	_
Журнал обновлений	[av_name].log	C:\Program Files\(x86) \Safensoft\Service Center\Server\Tools \Updates\Reports\	Лог обновления антивируса, вместо av_name имя антивируса (av4, av5)	_	_
Журнал обновлений	root.log	C:\Program Files\(x86) \Safensoft\Service Center\Server\Tools \Updates\Reports\	Сборный лог, в который дублируются записи sns.log и [av_name].log	_	_
		Логи Adm	in Console		
Лог Admin Console	ConsoleDetail edLog.txt	C:\ProgramData \SafenSoft\	Лог Admin Console	-	-

Таблица 39. Текстовые отчеты компонентов SoftControl Service Center

Название	Имя файла	Путь	Краткое Авторотация по описание умолчанию		Управление авторотацией
	4	Локальные логи н	лиента SysWatch		
Отчеты о событиях безопасности	system_[date] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Отчеты о событиях безопасности	30 дней	Через настройки
Отчеты о сборе профиля	profile_[date]_[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Лог сбора профиля, список проверенных объектов и результаты сбора профиля	ог сбора рофиля, список роверенных бъектов и езультаты бора профиля	
Отчеты об антивирусной проверке	scan_[date] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Лог антивирусной проверки	30 дней	Через настройки
Отчеты об обновлениях	update_[date] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Отчеты об обновлениях	30 дней	Через настройки
Перечень зараженных файлов	threats.xml	C:\ProgramData \S.N.Safe&Software \Safe'n'Sec	Перечень зараженных файлов	-	_
Общие логи SysWatch	safensec_[dat e]_[time] _[foobar].txt	C:\ProgramData \S.N.Safe&Software \Safe'n'Sec\Common Logs \	Вывод сообщений и ошибок процессов службы safensec.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	_
Общие логи SysWatch	snsmcon_[date]_[time] _[foobar].txt	C:\ProgramData \S.N.Safe&Software \Safe'n'Sec\Common Logs \	Вывод сообщений и ошибок графического интерфейса snsmcon.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	-
Общие логи SysWatch	snsods_[date] _[time] _[foobar].txt	C:\ProgramData \S.N.Safe&Software \Safe'n'Sec\Common Logs \	Вывод сообщений и ошибок антивирусного сканера snsods.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	-

Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
Журнал соединения с Service Center	sw_notify_[da te] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	_	-
	=	Локальные ло	оги DLP Client	=	
Журнал соединения с Service Center	dlp_notify_[d ate] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	_	-
Журнал обновления DLP Client	update_log.tx t	C:\Program Files \SafenSoft\DLP Client	Вывод сообщений и ошибок при запуске обновления	_	-
Журнал обновления DLP Client	checks.log	C:\Program Files \SafenSoft\DLP Client \Updater\Reports	Лог проверок наличия обновлений	-	-
Журнал обновления DLP Client	sns.log	C:\Program Files \SafenSoft\DLP Client \Updater\Reports	Журнал обновления модуля	-	-
Журнал обновления DLP Client	root.log	C:\Program Files \SafenSoft\DLP Client \Updater\Reports	Сборный лог, в который дублируются записи sns.log	-	_
		Локальные л	юги SysCmd	-	
Общие логи SysCmd	SysCmd_[date] _[time] _[foobar].txt	C:\ProgramData \S.N.Safe&Software \Safe'n'Sec\Common Logs \	Вывод сообщений и ошибок процессов службы SysCmd.exe	При превышении числа записей (может не совпадать с числом строк) в один файл больше 50000 создается новый файл	-
Журнал соединения с Service Center	scmd_notify_[date] _[time].txt	C:\Documents and Settings\All Users \Application Data\ (Windows XP) или C: \ProgramData \S.N.Safe&Software \Safe'n'Sec\Reports\ (Windows 7 и новее)	Вывод ошибок при подключении к Service Center	_	_
Журнал обновления SysCmd	update_log.tx t	C:\Program Files \SoftControl\SysCmd	Вывод сообщений и ошибок при запуске обновления	_	_
Журнал	checks.log	C:∖Program Files	Лог проверок	-	-

Диагностика проблем

Название	Имя файла	Путь	Краткое описание	Авторотация по умолчанию	Управление авторотацией
обновления SysCmd		\SoftControl\SysCmd \Updater\Reports	наличия обновлений		
Журнал обновления SysCmd	sns.log	C:\Program Files \SoftControl\SysCmd \Updater\Reports	:\Program Files Журнал SoftControl\SysCmd обновления Updater\Reports модуля		-
Журнал обновления SysCmd	root.log	C:\Program Files \SoftControl\SysCmd \Updater\Reports	Сборный лог, в который дублируются записи sns.log	-	_
		Локальные л	тоги DeCrypt		
Стандартный файл журнала	DecryptLog.lo g	C:\Windows\	Содержит список устройств и уведомления о событиях	При достижении 100 Мб создается DeCryptLog(rotated dd.mm.yyyy).log , где dd.mm.yyyy – дата ротации файла	_
Подробный файл журнала	DeCrypt.log	C:\ProgramData\DeCrypt\	Содержит события системы шифрования и причины неудачного завершения операций	При достижении 100 Мб создается DeCrypt.log_old1,DeC rypt.log_old2 и т.д.	-

<u>Примечание 1</u>. Для отчета по работе серверного компонента происходит ротация файлов, позволяющая контролировать размер файлов отчетов. Ротация позволяет формировать отчеты, автоматически разбиваемые на идентичные по своим параметрам части вида

Log.000, ..., Log.N,

при этом последний по времени отчет имеет максимальный индекс. Новый файл создается каждый раз, когда размер основного файла с отчетом (*ServerDetailedLog.txt*) превышает 200Мб.

<u>Примечание 2.</u> В таблице 39 приведены логи, включенные по умолчанию. Чтобы узнать о выключенных по умолчанию логах, прочитайте статью: <u>http://kb.safensoft.com/index.php/</u> <u>SoftControl_logs</u>.

Расшифровка сообщений из логов компонентов системы SoftControl описана в статье http://kb.safensoft.com/index.php/Understanding messages from SoftControl log files.

8. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl Service Center вы можете обращаться в техническую поддержку по электронной почте <u>support@sns-</u> <u>control.ru</u>.

9. Приложение

9.1 Установка и настройка PostgresQL 9.5

Программный продукт SoftControl Service Center поддерживает работу с разными версиями SQL-серверов. Ниже приведена инструкция по установке и настройке СУБД PostgreSQL на OC Windows для ее совместного применения с OC Windows.

- Установка PostgreSQL 9.5
- 1) Запустите установочный файл PostgreSQL 9.5 от администратора.
- 2) Нажмите Next.



Рисунок 176. Начало установки

3) Укажите путь для установки PostgreSQL и нажмите Next.



Рисунок 177. Выбор места для установки

4) Укажите путь для хранения данных и нажмите Next.

🐳 Setup			_	□ ×
Data Directo	ry			
Please select a	directory under which to store your data.			
Data Directory	ram Files (x86)\PostgreSQL\9.5\data	~		
vMware InstallBui	der	< Back	Next >	Cancel

Рисунок 178. Выбор места для хранения данных

5) Задайте пароль для администратора БД по имени postgres. Этот пароль позже потребуется для конфигурирования SoftControl Server для работы с СУБД PostgreSQI. Нажмте **Next**.

Setup				_	• ×
Password					
Please provide a passwo	ord for the database s	uperuser (postgr	es).		
Password					
Retype password					
Mware InstallBuilder					
Piware instalibulitier					

Рисунок 179. Ввод пароля

6) Задайте номер порта для работы сервера PostgreSQL. Этот номер порта позже потребуется для конфигурирования SoftControl Server для работы с СУБД PostgreSQL. Нажмите Next.

剩 Setup		_	×
Port			-
Please select the port number the server should listen Port 5432	on.		
VMware InstallBuilder	< Back	Next >	Cancel

Рисунок 180. Ввод номера порта

7) Выберите локаль (можно оставить значение по умолчанию) и нажмите Next.

🐳 Setup		_	□ ×
Advanced Options			-
Select the locale to be used by the new database cluster. Locale [[Default locale]			
VMware InstallBuilder	< Back	Next >	Cancel

8) Все готово к установке. Нажмите Next.

<table-of-contents> Setup</table-of-contents>			_	□ ×
Ready to Install				
Setup is now ready to begin installing Po	ostgreSQL on your co	mputer.		
VMware InstallBuilder		< Back	Next >	Cancel
Рисунок 18	2. Все гот	ово к уст	ановке	

9) Снимите флажок для установки инструмента Stack Builder и нажмите Finish.

Приложение



Рисунок 183. Установка завершена

10) Если SoftControl Server устанавливается на тот же компьютер, что и PostgreSQL, никаких дополнительных настроек не требуется. Чтобы установить SoftControl Server на другой компьютер, надо разрешить PostgreSQL принимать соединения с других IP адресов. Для этого необходимо модифицировать файл pg_hba.conf (по умолчанию располагается в папке C:\Program Files \PostgreSQL\9.5\data). В нем надо найти раздел # IPv4 local connections и модифицировать в этом разделе строчку

host all all 127.0.0.1/32 md5

Вместо 127.0.0.1/32 следует написать all (для разрешения соединений со всех IPадресов), либо указать конкретный IP-адрес, откуда будет подключаться SoftControl Server.

9.2 Установка и настройка Microsoft® SQL Server® 2008

Программный продукт SoftControl Service Center поддерживает работу с разными версиями SQL-серверов: SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, SQL Server 2016, SQL Server 2017. Ниже приведена инструкция по установке и настройке СУБД Microsoft® SQL Server® 2008 для ее совместного применения с SoftControl Service Center. Другие версии SQL-серверов устанавливаются аналогично.

✓ Подготовка к установке Microsoft® SQL Server® 2008

Перед установкой убедитесь, что система удовлетворяет минимальным

<u>требованиям к оборудованию и ПО для установки и запуска Microsoft® SQL</u> <u>Server® 2008</u> и, в случае наличия несоответствий заявленным требованиям, устраните их до начала установки.

Установка Microsoft® SQL Server® 2008

- 1) Запустите установочный файл Microsoft® SQL Server® 2008.
- 2) В окне Центра установки SQL Server (SQL Server Installation Server) откройте раздел Installation и выберите тип установки New SQL Server stand-alone installation or add features to an existing installation (рис. <u>Раздел Installation</u>²⁰⁹).

📸 SQL Server Installation Center		x
Planning Installation	New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2008 in a non-clustered environment or to add feature to an existing SQL Server 2008 instance.	5
Maintenance Tools Resources	New SQL Server failover cluster installation Launch a wizard to install a single-node SQL Server 2008 failover cluster.	
Advanced Options	 Launch a wizard to add a node to an existing SQL Server 2008 failover cluster. Upgrade from SQL Server 2000 or SQL Server 2005 Launch a wizard to upgrade SQL Server 2000 or SQL Server 2005 to SQL Server 2008. Before 	
	you upgrade, you should run the Upgrade Advisor to detect potential problems. Search for product updates Search Microsoft Update for SQL Server 2008 product updates.	
South Server 2008		

Рисунок 184. Раздел Installation

3) В разделе Setup Support Rules выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. <u>Проверка проблем при установке</u> <u>вспомогательных файлов</u>²⁰⁹). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **OK**.

👸 SQL Server 2008 Setup		
Setup Support Rules		
Setup Support Rules identify proble corrected before Setup can continu	ms that might occur when you install SQL Server Setup support file e.	s. Failures must be
Setup Support Rules	Operation completed. Passed: 6. Failed 0. Warning 0. Skipped 0	Re-run
	View detailed report	
	Kule	Status
	Cature administrator	Passed
	Setup administrator	Passed
	Windows Management Instrumentation (WMD service	Passed
	Consistency validation for SOL Server registry low	Passed
	Long nath namer to files on SOL Server installation media	Passed
	ОК	Cancel Help

Рисунок 185. Проверка проблем при установке вспомогательных файлов

4) В разделе Product Key выберите вариант Enter the product key, введите лицензионный ключ для Microsoft® SQL Server® 2008 и нажмите на кнопку Next (рис. <u>Раздел Product Key</u>²¹⁰).

💈 SQL Server 2008 Setup	
Product Key	
Specify the edition of SQL	Server 2008 to install.
Product Key License Terms Setup Support Files	Specify a free edition of SQL Server or provide a SQL Server product key to validate this instance of SQL Server 2008. Enter the 25-character key from the Microsoft certificate of authenticity or product packaging. If you specify Enterprise Evaluation, the instance will be activated with a 180-day expiration. To upgrade from one edition to another edition, run the Edition Upgrade Wizard. • Specify a free edition: Enterprise Evaluation • • • Enter the product key: • Enter the product key:

Рисунок 186. Раздел Product Key

5) Прочитайте условия лицензионного соглашения (License Terms) и, если Вы с ними согласны, то установите флажок I accept the license terms и нажмите на кнопку Next (рис. <u>Paздел License Terms</u>²¹¹).

🃸 SQL Server 2008 Setup	
License Terms To install SQL Server 2008, you n	nust accept the Microsoft Software License Terms.
Product Key License Terms Setup Support Files	MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SQL SERVER 2008 EVALUATION EDITION These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the evaluation software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft • updates, • supplements, • Internet-based services, and • support services
	< Back Next > Cancel

Рисунок 187. Раздел License Terms

6) В разделе **Setup Support Files** нажмите на кнопку **Install** (рис. <u>Раздел Setup</u> <u>Support Files</u>⁽²¹¹⁾).

📸 SQL Server 2008 Setup			
Setup Support Files Click Install to install Setup Support	ort files. To install or update SQL	Server 2008, these files are required.	
Product Key	The following components a	re required for SQL Server Setup:	
License Terms	Feature Name	Status	
Setup Support Files	Setup Support Files		
		< Back Install	Cancel

Рисунок 188. Раздел Setup Support Files

7) В разделе Setup Support Rules выполняется проверка на возможные проблемы, которые могут возникнуть при установке вспомогательных файлов установки Microsoft® SQL Server® 2008 (рис. <u>Раздел Setup Support Rules. Подробные</u> <u>данные</u>²¹²). Ошибки должны быть исправлены перед продолжением установки. Если проблем нет, то нажмите на кнопку **Next**.

🐮 SQL Server 2008 Setup		
Setup Support Rules		
Setup Support Rules identify corrected before Setup can co	problems that might occur when you install SQL Server Setup support fiontinue.	iles. Failures must be
Setup Support Rules	Operation completed. Passed: 10. Failed 0. Warning 1. Skippe	d 0.
Feature Selection		
Disk Space Requirements		
Error and Usage Reporting	Hide details <<	Re-run
Installation Rules	View detailed report	
Ready to Install		
Installation Progress	Rule	Status
Complete	Fusion Active Template Library (ATL)	Passed
	Unsupported SQL Server products	Passed
	Performance counter registry hive consistency	Passed
	Previous releases of SQL Server 2008 Business Intelligence De	evel Passed
	Previous CTP installation	Passed
	Consistency validation for SQL Server registry keys	Passed
	Computer domain controller	Passed
	Microsoft .NET Application Security	Passed
	Edition WOW64 platform	Passed
	< Back Next >	Cancel Help

Рисунок 189. Раздел Setup Support Rules. Подробные данные

8) В разделе Feature Selection выделите компонент Database Engine Services, укажите путь для установки в поле Shared feature directory и нажмите на кнопку Next (рис. <u>Paздел Feature Selection</u>²¹³).

Select the Standard features to i be clustered.	nstall. For clustered installations, only Database Engine Se	rvices and Analysis Services can
Feature Selection Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Instance Features Database Engine Services SQL Server Replication Full-Text Search Analysis Services Reporting Services Shared Features Business Intelligence Development Studio Client Tools Connectivity Integration Services Client Tools Backwards Compatibility Client Tools SDK SQL Server Books Online Management Tools - Basic Management Tools - Complete	Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.
	Select All Unselect All Shared feature directory: C:\Program Files\N	/icrosoft SQL Server\

Рисунок 190. Раздел Feature Selection

9) В разделе Instant Configuration выберите параметр Default Instance и нажмите

на кнопку Next (рис. <u>Раздел Instance Configuration</u>²¹⁴).

🚼 SQL Server 2008 Setup					x 5 -
Instance Configuration Specify the name and instance ID f	or the SQL Server instance.				
Setup Support Rules Feature Selection Instance Configuration	 Default instance Named instance: 	MSSO	QLSERVER		
Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install	Instance ID: Instance root directory: SQL Server directory: Analysis Services directory Benoting Services directory	C:\Pr C:\Pr r: C:\Pr	QLSERVER ogram Files\Microsof ogram Files\Microsof ogram Files\Microsof	ft SQL Server\ t SQL Server\MSSQL: t SQL Server\MSAS1(t SQL Server\MSAS1)	10.MSSQLSERVER D.MSSQLSERVER
Installation Progress Complete	Installed instances:	tures	Edition	Version	Instance ID
			< Back	Next > Ca	ancel Help

Рисунок 191. Раздел Instance Configuration

10) В разделе Disc Space Requirements нажмите на кнопку Next (рис. Раздел Disc Space Requirements²¹⁴).

🐮 SQL Server 2008 Setup	
Disk Space Requiremen	ts
Review the disk space summary f	or the SQL Server features you selected.
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Disk Usage Summary:
	- Cancel Help

Рисунок 192. Раздел Disc Space Requirements

 В разделе Server Configuration на вкладке Service Accounts нажмите на кнопку Use the same account for all SQL Server services (рис. <u>Вкладка Service</u> Accounts раздела Server Configuration²¹⁵).

В открывшемся окне выберите учетную запись **NETWORK SERVICE** и нажмите на кнопку **OK** (рис. <u>Учетная запись</u>²¹⁶).

На вкладке Collation для компонентов Database Engine и Analysis Services установите параметр Cyrillic_General_CI_AS (рис. <u>Вкладка Collation раздела</u> Server Configuration⁽²¹⁶⁾).

髋 SQL Server 2008 Setup					P XX
Server Configuration					
Setup Support Rules Feature Selection Instance Configuration	Service Accounts Collation	se a separate account for ea	ach SQL Server s	service.	•
Disk Space Requirements	Service	Account Name	Password	Startup Type	
Server Configuration	SQL Server Agent			Manual	T
Database Engine Configuration	SQL Server Database Engine			Automatic	Ť
Analysis Services Configuration	SQL Server Analysis Services			Automatic	Π
Reporting Services Configuration	Sql Server Reporting Services			Automatic	E
Error and Usage Reporting	SQL Server Integration Services 1	NT AUTHORITY\Netw		Automatic	Ι
Installation Rules Ready to Install Installation Progress Complete	These services will be configured a On some older Windows versions t more information, click Help.	Use the same sutomatically where possibl the user will need to specify III	e to use a low p r a low privilege	SQL Server service rivilege account. account. For	
		< Back Next	> Can	cel He	p

Рисунок 193. Вкладка Service Accounts раздела Server Configuration

Use the same accou	unt for all SQL Server 2008 services		
Specify a user na	me and password for all SQL Server service accounts.		
Account Name:	NT AUTHORITY\NETWORK SERVICE		Browse
Password:			
		ОК	Cancel

Рисунок 194. Учетная запись
📸 SQL Server 2008 Setup		
Server Configuration		
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Service Accounts Collation Database Engine:	Customize
	Warning: The Database Engine and Analysis Services collations are not the same.	Help

Рисунок 195. Вкладка Collation раздела Server Configuration

Для этого нажмите на кнопку Customize для компонента Database Engine, в открывшемся окне установите переключатель в положение Windows collation designator and sort order, в выпадающем списке Collation designator выберите параметр Cyrillic_General, установите флажок Accent-sensitive и нажмите на кнопку OK (рис. Установка параметров Collation для Database Engine²¹⁷).

Customize the SQL Server 2008 Database Engine Collation				
Select the collation you would like to use:				
Windows collation des	ignator and sort order			
Collation designator:	Cyrillic_General 🔹			
🔲 Binary	Binary-code point			
Case-sensitive	Kana-sensitive			
Accent-sensitive	Width-sensitive			
 SQL collation, used fo SQL_Hungarian_CP1250_ SQL_Hungarian_CP1250_ SQL_Icelandic_Pref_CP1_ SQL_Latin1_General_CP1_ SQL_Latin1_General_CP1_ 	r backwards compatibility CI_AS CS_AS CI_AS CI_AI			
Collation description:				
Latin1-General, case-inse Data, SQL Server Sort Orc	ensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode der 52 on Code Page 1252 for non-Unicode Data			
	OK Cancel			

Рисунок 196. Установка параметров Collation для Database Engine

Нажмите на кнопку Customize для компонента Analysis Services, в открывшемся окне в выпадающем списке Collation designator выберите параметр Cyrillic_General, установите флажок Accent-sensitive и нажмите на кнопку OK (рис. Установка параметров Collation для Analysis Services²¹⁸).

Customize the SOL Server 2008 Analysis Services Collation				
Customize the SQE Server 2000 Analysis Services Conduloff				
Select the collation you would like to use:				
Windows collation designator and sort order				
Collation designator:	Cyrillic_General		•	
Binary	Binary-code point			
Case-sensitive	Kana-sensitive			
Accent-sensitive	Width-sensitive			
			OK Canad	
			UK Cancel	

Рисунок 197. Установка параметров Collation для Analysis Services

В разделе Server Configuration нажмите на кнопку Next для продолжения установки.

12) В разделе Database Engine Configuration выберите параметр Mixed Mode и задайте пароль для учетной записи Built-in SQL Server system administrator account в поле Enter password и его подтверждение в поле Confirm password (рис. <u>Раздел Database Engine Configuration</u>²¹⁹). Нажмите на кнопку Add Current User и убедитесь, что в списке Specify SQL Server administrators отображается текущая системная учетная запись, после чего нажмите на кнопку Next.

髋 SQL Server 2008 Setup		
Database Engine Configu	uration	
Specify Database Engine authentic	cation security mode, administrators and data directories.	
Setup Support Rules	Account Provisioning Data Directories FILESTREAM	
Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Specify the authentication mode and administrators for the Database Engine. Authentication Mode Windows authentication mode Mixed Mode (SQL Server authentication and Windows authentication) Built-in SQL Server system administrator account Enter password: Confirm password: Specify SQL Server administrators SQL Server administrators Submin (admin) SQL Server administrators	tors have d access to
	Add Current User Add Remove	
	< Back Next > Cancel	Help

Рисунок 198. Раздел Database Engine Configuration

13) В разделе Analysis Services Configuration на вкладке Account Provisioning нажмите на кнопку Add Current User и убедитесь, что в списке Specify which users have administrative permissions for Analysis Services отображается текущая учетная запись, после чего нажмите на кнопку Next (рис. <u>Раздел</u> <u>Analysis Services Configuration</u>⁽²⁰⁾).

🐮 SQL Server 2008 Setup	
Analysis Services Configu	ration
Specify Analysis Services administrat	tors and data directories.
Setup Support Rules Feature Selection	Account Provisioning Data Directories Specify which users have administrative permissions for Analysis Services.
Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	admin (admin) Analysis Services administrators have unrestricted access to Analysis Services. Add Current User Add
	< Back Next > Cancel Help

Рисунок 199. Раздел Analysis Services Configuration

14) В разделе Reporting Services Configuration выберите параметр Install the native mode default configuration и нажмите на кнопку Next (рис. <u>Раздел</u> <u>Reporting Services Configuration</u>²²¹).

Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	 Install the native mode default configuration. Setup will install the report server and configure it in Native mode to use the default values. The report server is usable as soon as Setup is finished. Install the SharePoint integrated mode default configuration. Setup will create the report server database in SharePoint integrated mode and configure the report server to use the default values. However, integrated operations will not be supported until a minimal installation of a SharePoint product or technology is deployed on the report server computer and the Reporting Services Add-in for SharePoint Technologies is installed and configured on the instance of the SharePoint product or technology you are using. Install, but do not configure the report server. Setup will install, but will not configure, the report server software. After installation is finished, you can use the Reporting Services Configuration tool to set options that are required to run the report server.

221

15) В разделе Error and Usage Reporting нажмите на кнопку Next (рис. <u>Раздел</u> Error and Usage Reporting²²²).

📸 SQL Server 2008 Setup	
Error and Usage Report	ing
Help Microsoft improve SQL Serv	er features and services.
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration	Specify the information that you would like to automatically send to Microsoft to improve future releases of SQL Server. These settings are optional. Microsoft treats this information as confidential. Microsoft may provide updates though Microsoft Update to modify feature usage data. These updates might be downloaded and installed on your machine automatically, depending on your Automatic Update settings.
Database Engine Configuration Analysis Services Configuration Reporting Services Configuration	View the Microsoft policy for SQL Server privacy and data collection. Read more about Microsoft Update and Automatic Update.
Error and Usage Reporting Installation Rules Ready to Install	Send Windows and SQL Server Error Reports to Microsoft or your corporate report server. This setting only applies to services that run without user interaction.
Installation Progress Complete	Send feature usage data to Microsoft. Feature usage data includes information about your hardware configuration and how you use Microsoft software and services.
	< Back Next > Cancel Help

Рисунок 201. Раздел Error and Usage Reporting

16) В разделе Installation Rules выполняется проверка на возможные проблемы, которые могут возникнуть при установке Microsoft® SQL Server® 2008 (рис. <u>Раздел_Installation Rules</u>⁽²²²⁾). Если ошибок не найдено, то нажмите на кнопку Next.

🔓 SQL Server 2008 Setup						x
Installation Rules						
Setup is running rules to determi	ine if the i	installation process will be blocked. For more information	n, click Help			
Setup Support Rules	Oper	ation completed. Passed: 11. Failed 0. Warning 0. Skip	ped 0.			
Feature Selection						
Instance Configuration						
Disk Space Requirements	Hid	e details <<			Re-run	
Server Configuration	View	detailed report				_
Database Engine Configuration		· · · · ·				
Analysis Services Configuration		Rule	S	tatus		-
Reporting Services Configuration		Same architecture installation	Pa	assed		
Error and Usage Reporting		Cross language installation	Pa	assed		
Installation Rules		Existing clustered or cluster-prepared instance	Pa	assed		
Ready to Install		Reporting Services Catalog Database File Existence	Pa	assed		E
Installation Progress		Reporting Services Catalog Temporary Database File Exist	ence Pa	assed		
Complete		SQL Server 2005 Express tools	 	assed		
				acced		
				15500		
		FA132 File System	<u>Pa</u>	issed		
		SQL Server 2000 Analysis Services (64-bit) install action	Pa	assed		-
		-				
				Connect	Hala	
		< Back INE	xt >	Cancel	нер	

Рисунок 202. Раздел Installation Rules

17) В разделе **Ready to Install** проверьте состав устанавливаемых компонентов и нажмите на кнопку **Install** (рис. <u>Раздел Ready to Install</u>²²³).

🐮 SQL Server 2008 Setup	
Ready to Install Verify the SQL Server 2008 feature	s to be installed.
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Ready to install SQL Server 2008: Summary Edition: Standard Action: Install General Configuration Features Database Engine Services SQL Server Replication Full-Text Search Analysis Services Business Intelligence Development Studio Client Tools Connectivity Integration Services Client Tools SDK Configuration file path:
	C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20120925_150200\ConfigurationFile.ini < Back

Рисунок 203. Раздел Ready to Install

 В разделе Installation Progress отображается процесс установки компонентов Microsoft® SQL Server® 2008 (рис. <u>Раздел Installation Progress</u>²²⁴).

🐮 SQL Server 2008 Setup	
Installation Progress	
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Performing Windows Installer actions. Install_sql_common_core_Cpu32_Action : InstallInitialize.
	Next > Cancel Help

Рисунок 204. Раздел Installation Progress

После окончания установки нажмите на кнопку Next.

Для завершения установки в разделе **Complete** нажмите на кнопку **Close** (рис. <u>Раздел Complete</u>²²⁴).

Приложение

📸 SQL Server 2008 Setup		23
Complete Your SQL Server 2008 installation of	completed successfully.	
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Error and Usage Reporting Installation Rules	Summary log file has been saved to the following location: <u>C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\20120925 150200\Summary VM-AS-W61RUX86 20120925 150200.bt</u> Information about the Setup operation or possible next steps: Your SQL Server 2008 installation completed successfully.	
Ready to Install Installation Progress Complete	Supplemental Information: The following notes apply to this release of SQL Server only. Microsoft Update For information about how to use Microsoft Update to identify updates for SQL Server 2008, see the Microsoft Update Web site <http: ?linkid="108409" fwlink="" go.microsoft.com=""> at http://go.microsoft.com/fwlink/?LinkId=108409.</http:>	•
	Close Help	

Рисунок 205. Раздел Complete

9.3 Добавление компонента Desktop Experience

<u>Примечание</u>: продемонстрировано на примере OC Microsoft® Windows® Server 2008 R2.

 Откройте оснастку Server Manager из раздела Administrative Tools меню Start. Перейдите в раздел Features и в области Features Summary нажмите на кнопку Add Features (рис. Оснастка Server Manager²²⁵).

Server Manager		_ 8 ×
File Action View Help		
🗢 🔿 🖄 📅 🔽		
Server Manager (VM-AS-W61SENX64)	Features	
Roles Features Endingenetics Configuration Storage	View the status of features installed on this server and add or remove features.	
	 Features Summary 	Features Summary Help
	ⓒ Features: 0 of 41 installed	Add Features
	C Last Refresh: Today at 1:48 PM Configure refresh	
	,	

Рисунок 206. Оснастка Server Manager

2) В появившемся окне Add Features Wizard установите флажок у компонента Desktop Experience (рис. <u>Выбор компонентов для добавления</u>⁽²²⁸⁾) (в Microsoft® Windows® Server 2012/2012 R2: User Interfaces and Infrastructure → Desktop Experience).



Рисунок 207. Выбор компонентов для добавления

3) При появлении диалогового окна с информацией о необходимости добавления связанных компонентов выберите вариант Add Required Features (рис. <u>Запрос</u> <u>добавления связанных компонентов</u>²²⁶).



Рисунок 208. Запрос добавления связанных компонентов

4) Убедитесь, что компонент **Desktop Experience** выбран и нажмите на кнопку **Next** (рис. <u>Выбор компонентов для добавления</u>²²⁶).



Рисунок 209. Выбор компонентов для добавления

5) На шаге **Confirmation** нажмите на кнопку **Next** (рис. <u>Подтверждение добавления</u> компонентов⁽²²⁷⁾).

Add Featur	res Wizard		X
	Confirm Installa	tion Selections	
Features Confirmati Progress	on	To install the following roles, role services, or features, dick Install. (1) 1 informational message below	
Results		(i) This server must be restarted after the installation completes. Desktop Experience	
		Ink and Handwriting Services Ink Support Print, e-mail, or save this information	
		< Previous Next.> Install Cancel	

Рисунок 210. Подтверждение добавления компонентов

6) Дождитесь завершения установки (рис. <u>Процесс установки ⁽²²⁷⁾)</u>.

Add Features Wizard	
Installation Prog	ress
Features	The following roles, role services, or features are being installed:
Progress	Desktop Experience
Results	Ink and Handwriting Services
	Installing
	<previous next=""> Install Cancel</previous>

Рисунок 211. Процесс установки

- 7) На шаге **Results** нажмите на кнопку **Close** (рис. <u>Завершение добавления компонентов</u>
- 8) В диалоговом окне с предложением перезапуска системы выберите **Yes**, после чего система будет отправлена на перезагрузку для завершения установки (рис. <u>Запрос</u> перезагрузки²²⁹).
- 9) После перезапуска системы в появившемся окне **Resume Configuration Wizard** убедитесь, что все требуемые компоненты установлены успешно (**Installation succeeded**) и нажмите на кнопку **Close** (рис. <u>Результат добавления компонентов</u>²²⁹).

Add Features Wizard			×
Installation Resu	llts		
Features Confirmation Progress	One or more of the following roles, role servic	es, or features require you to restart:	
Results	Desktop Experience	🚹 Restart Pending	
	A You must restart this server to finish t	he installation process.	
	Ink and Handwriting Services	🔔 Restart Pending	
	You must restart this server to finish t	he installation process.	
	_	Previous Next > Close Car	icel

Рисунок 212. Завершение добавления компонентов



Рисунок 213. Запрос перезагрузки

Resume Configuration Wizard			×
Installation Resul	ts		
Resuming Configuration Progress	The following roles, role services, or features	were installed successfully:	
Results	Desktop Experience	Installation succeeded	
	Ink and Handwriting Services	Installation succeeded	
	The following features were installed: Ink Support		
	Print, e-mail, or save the installation report		
	_	Previous Next > Close C	ancel

Рисунок 214. Результат добавления компонентов

10. Дополнительная информация

10.1 О сертификатах

В настоящем разделе рассматриваются некоторые важные аспекты криптографической защиты канала связи между Сервисным Центром и клиентскими приложениями (далее – «клиентами»).

Для взаимодействия между серверным компонентом SoftControl Server и клиентами в SoftControl Service Center используется протокол HTTPS. Все данные между сервером и конечной точкой передаются в зашифрованном виде по защищенному каналу, при этом для авторизации клиентов используются сертификаты стандарта X.509.

В процессе работы SoftControl Server генерирует следующие виды сертификатов:

- Сертификат УЦ самоподписанный корневой сертификат удостоверяющего центра (УЦ) в рамках СИБ SoftControl. В момент конфигурации сервер генерирует этот сертификат и помещает в хранилище Windows. Все остальные виды сертификатов продукта подписаны сертификатом УЦ, что является одним из критериев их достоверности.
- Серверный сертификат сертификат, подписанный сертификатом УЦ и используемый сервером для установки защищенного SSL/TLS-соединения с клиентами. Сервер генерирует этот сертификат в момент конфигурации и помещает в хранилище Windows на серверной машине.
- Общий клиентский сертификат сертификат, подписанный сертификатом УЦ и используемый клиентом для установки защищенного SSL/TLS-соединения с сервером в момент первичного подключения. Данный сертификат является общим для всех новых клиентов и предназначен только для подачи ими первого запроса на сервер. Сертификат встроен в зашифрованный <u>файл клиентских настроек</u>⁽²⁷⁾, применяемый к клиенту на конечной точке. Общий клиентский сертификат генерируется сервером в момент конфигурации и хранится на серверной машине по следующему пути:

C:\ProgramData\SafenSoft\Client.pem

 Индивидуальный клиентский сертификат – сертификат, подписанный сертификатом УЦ и используемый клиентом для установки защищенного SSL/TLSсоединения с сервером после подтверждения регистрации⁽⁵⁰⁾ администратором через консоль управления SoftControl Admin Console. Данный сертификат уникален для каждого клиента, что делает невозможным несанкционированный доступ к каналу связи при наличии у злоумышленников украденного индивидуального сертификата другого клиента или общего сертификата. В случае если доверие к индивидуальному сертификату по какой-либо причине утеряно или истек срок его действия, существует возможность выдачи другого сертификата (обновление⁽⁵¹⁾) или его отзыв (отклонение регистрации⁽⁶¹⁾).



Рисунок 215. Сертификаты в СИБ SoftControl

10.2 Управление сертификатами

Чтобы управлять сертификатами УЦ, нажмите на пункт Инструменты и выберите Управление сертификатами УЦ.

۶	🔀 SoftControl Admin Console 🛛 📃 🗖 🗙											
	райл	Вид Фильтры	Инструменты О п	рограмме								
	$\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{\mathbf{$	<u>s</u>	Управление с	ертификатами	уц 🕺 🙈 🔯 📢	⊥ ∰				U		
"	~		Очистка съём	ного накопит	еля Управление сертификатами УL	· [[™] [□]			- 46	<u></u>		
Ir	Клиенты × Генерация и выбор сертификатов УЦ											
ľ					Перетяните сюда мышкой заголовок к	олонки для группиро	вки данных по не	ай				
	ID	Подразделение	Имя	Тип клиента	Тип настроек	Версия продукта	Статус	Информация		Изменён		
	⊢ 1	Unit South	DESKTOP-63KNC18	SysCmd	Настройки подразделения	6.0.58.0	Активен	Наблюдение	Частично	09.02.2021 17:40:14		
								Профиль	Завершено			
	2	Cert New	DESKTOP-63KNC18	SysWatch	Настройки подразделения	6.0.58.0	Отклонен	Обновление	Не найдено	02.02.2021 12:33:13		
								Защита Сканирование	Включено Ошибка			
								Защита	Включено			
	3	Stop service	DESKTOP-63KNC18	SysWatch	Настройки подразделения	6.0.60.0	Остановлен	Сканирование	Завершено Развершено	06.02.2021 23:38:24		
								Обновление	завершено Установлено			
											-11	
	_										v	
l	< <u> </u>						_					
	Имя п	ользователя: adm	nin Роли: Системнь	ій администра	тор, Администраторы					Смена пароля		

Рисунок 216. Управление сертификатами УЦ

Поля **Текущий сертификат УЦ** и **Новый сертификат УЦ** содержат сведения о действующем сертификате УЦ и сертификате УЦ, который начнет использоваться по истечении действующего. Автоматически новый сертификат УЦ на смену текущему генерируется за три года до конца действия текущего сертификата УЦ. У вас может возникнуть необходимость начать использовать новый сертификат УЦ раньше, если вы обновляете программное обеспечение SoftControl на версию 6.0 или более позднюю (с версий до 6.0). Уже подключенные к серверу SoftControl Server клиенты продолжат работать без изменений, но для регистрации новых клиентов потребуется обновить сертификат УЦ.

Чтобы сгенерировать новый сертификат УЦ, нажмите Сгенерировать и подтвердите свое намерение нажатием кнопки ОК во всплывающем окне.

Нажмите Применить или ОК, чтобы активировать сертификат в поле Текущий

сертификат УЦ как действующий и сертификат в поле **Новый сертификат УЦ** как сертификат, приготовленный для смены действующего. Подробнее об обновлении сертификатов при переходе на версию 6.0 и более поздние читайте в статье <u>http://kb.safensoft.com/index.php/Updating SoftControl 5 to SoftControl 6</u>.

۶	Управление сертификатами УЦ 🛛 🗙
	Новый сертификат УЦ
	2021-02-09/2041-02-04 ЕКИ D30B2382F1C9481757D47648858656CB8B32BC84 [NewCA]
	Текущий сертификат УЦ
	2021-01-28/2041-01-23 EKU DE4D3A7CB6BC4CD9B940278865885633A9306960 [CA]
	Применить ОК Отмена

Рисунок 217. Окно управления сертификатами УЦ

Сведения о сертификатах УЦ представлены в следующем формате:

<дата_генерации_сертификата>/

<окончание_срока_действия_сертификата><флаг_ЕКU_при_наличии><имя_сертиф иката>.

10.3 Восстановление связи с сервером

В системе взаимодействия «клиент-сервер» (в рамках СИБ на основе Сервисного Центра) существует вероятность возникновения ситуаций, при которых IP-адрес сервера может быть изменен автоматически, например, при входе в сеть после перезагрузки. В этом случае клиентские приложения, в конфигурации которых прописаны только IP-адреса компьютера с установленным серверным компонентом SoftControl Server, а не его сетевое имя, теряют связь с ним. Чтобы не корректировать IP-адреса вручную локально в настройках каждого клиентского компонента, предусмотрен функционал резервного сервера восстановления. Для его активации выполните следующие шаги:

- 1) Откройте файл конфигурации сервера, расположенный по следующему пути: C:\ProgramData\SafenSoft\Server.Config.xml
- 2) В элементе RescueSettings замените значение флага Active на True.
- 3) Добавьте в элемент *RescueSettings* подэлементы следующего вида: <Address Uri="<новый IP-адрес или имя сервера>" Port="<порт связи>" />
- 4) Сохраните изменения в файле конфигурации.
- 5) Измените имя компьютера с установленным SoftControl Server на screstore.
- 6) Перезагрузите компьютер с установленным SoftControl Server для применения

новых настроек и изменения сетевого имени хоста.

- 7) После запуска системной службы SoftControl Server порт 8888 для резервного подключения будет автоматически добавлен в брандмауэр Windows.
- 8) По истечении 10 неудачных попыток подключения по списку адресов, заданных в настройках, клиентские компоненты будут предпринимать попытку подключения к резервному серверу с именем *screstore* на порт 8888 (по умолчанию). После успешного подключения по данному адресу, клиентам будет передан заданный в настройках новый список адресов сервера и произведена автоматическая замена старого списка адресов на обновленный в настройках. После того как соединение со всеми подключенными к Сервисному Центру клиентами будет восстановлено, сетевое имя сервера может быть изменено на изначальное.

10.4 Резервное копирование SoftControl Service Center

В некоторых случаях существует необходимость в <u>создании резервной копии</u>²³⁴ компонентов Сервисного Центра, с целью дальнейшего <u>восстановления</u>²³⁶ полностью работоспособной конфигурации без потери связи с клиентскими приложениями на удаленных хостах. Случаи, к которым применимы данные операции:

- необходимость переустановки ОС на компьютере с компонентами SoftControl Service Center;
- необходимость переноса SoftControl Service Center на другой компьютер.

10.4.1 Создание резервной копии

Резервная копия файлов SoftControl Service Center включает в себя необходимые для восстановления файлы конфигурации серверного компонента SoftControl Server и <u>сертификаты²³⁰</u>. Также могут быть сохранены <u>пользовательские фильтры¹⁶¹</u> SoftControl Admin Console (опционально). Чтобы создать резервную копию, выполните следующую последовательность действий:

- В основном меню SoftControl Admin Console выберите пункт Вид → Резервное копирование.
- 2) В появившемся окне установите **Режим копирования** в области **Файлы** сервера (рис. <u>Создание резервной копии</u>²³⁴).

Дополнительная информация

Резервное копирование								
Файлы сервера								
Путь к директории теневого копирования на сервере Сгенерировать подкаталог								
C:\SC backup\files\20140925121156848								
О Режим восстановления	Копировать							
Режим копирования								
repeariyerino espacipini koncono								
Файлы пользовательских фильтров								
Райлы пользовательских фильтров Локальный путь к директории теневого копи	рования	Сгене	рировать подкаталог					
Файлы пользовательских фильтров Локальный путь к директории теневого копи C:\SC backup\uf\20140925121417959	рования	Сгене	рировать подкаталог					
Файлы пользовательских фильтров Локальный путь к директории теневого копи С:\SC backup\uf\20140925121417959 О Режим восстановления	рования Копировать	Сгене	рировать подкаталог					
Файлы пользовательских фильтров Локальный путь к директории теневого копи C:\SC backup\uf\20140925121417959 ○ Режим восстановления @ Режим копирования	рования Копировать	Сгене	рировать подкаталог Восстановить					
Файлы пользовательских фильтров Локальный путь к директории теневого копи C:\SC backup\uf\20140925121417959 ○ Режим восстановления @ Режим копирования	рования Копировать	Сгене	рировать подкаталог					

Рисунок 218. Создание резервной копии

Введите путь до каталога, куда предполагается сохранить файлы резервной копии, в соответствующее поле. Если требуется сформировать подкаталог с уникальным идентификатором по введенному пути, нажмите на кнопку Сгенерировать подкаталог. Если нажать на указанную кнопку при пустом поле ввода, подкаталог будет по умолчанию располагаться в следующей директории: C:\Windows\System32

Нажмите на кнопку Копировать, чтобы создать резервную копию файлов по выбранному пути. В нижней части окна будет отображен статус операции.

 Для сохранения пользовательских фильтров в окне Резервное копирование (рис. <u>Создание резервной копии</u>²³⁴) повторите действия п. 2 для области Файлы пользовательских фильтров.

Если нажать на кнопку **Сгенерировать подкаталог** при пустом поле ввода, подкаталог будет по умолчанию располагаться в директории установки SoftControl Admin Console.

4) В случае, если БД Сервисного Центра располагается на внешнем сервере (отличном от компьютера с установленными компонентами SoftControl Service Center), сохранять ее копию не требуется. В обратном случае создайте резервную копию текущей БД средствами Microsoft® SQL Server®.

10.4.2 Восстановление из резервной копии

Для восстановления SoftControl Service Center из резервной копии выполните следующую последовательность действий:

- 1) Убедитесь, что на компьютере установлено правильное время.
- 2) <u>Установите</u>⁽¹¹⁾ SoftControl Service Center той же версии, что использовался на компьютере, с которого создавалась резервная копия.
- Выполните восстановление ранее сохраненной БД. Пропустите этот шаг, если БД находилась на другом компьютере и не удалялась.
- 4) Произведите первичную настройку сервера⁽²¹⁾. При настройке укажите новое Имя базы данных, отличное от имени старой БД, чтобы не повредить данные в ней. После восстановления из резервной копии сервер автоматически переключится на старую базу данных.
- 5) В основном меню SoftControl Admin Console выберите пункт Вид → Резервное копирование.
- 6) В появившемся окне установите Режим восстановления в области Файлы сервера (рис. <u>Восстановление из резервной копии</u>²³⁶). Введите путь до каталога с ранее сохраненными файлами резервной копии в соответствующее поле и нажмите на кнопку Восстановить. В нижней части окна будет отображен статус операции.

Г Резервное копирование		×
Файлы сервера		
Путь к директории теневого копирования на	сервере	Сгенерировать подкаталог
C:\SC backup\files\20140925121156848		
Режим восстановления		Восстановить
	Перезапуст	ить сервер и консоль
Файлы пользовательских фильтров Локальный путь к директории теневого копии	оования	
C:\SC backup\uf\20140925121417959		
 Режим восстановления Режим копирования 		Восстановить
		Закрыть

Рисунок 219. Восстановление из резервной копии

7) При необходимости восстановления пользовательских фильтров в окне **Резервное копирование** (рис. <u>Восстановление из резервной копии</u>²³⁶) повторите действия п. 6²³⁶ для области Файлы пользовательских фильтров.

 8) Нажмите на кнопку Перезапустить сервер и консоль для перезапуска системной службы SoftControl Server и применения восстановленной конфигурации.

<u>Примечание</u>: на некоторых системах может также понадобиться перезагрузка компьютера.

- 9) Удалите временную базу данных, созданную на шаге <u>4</u>²³⁶.
- 10) <u>Авторизуйтесь⁽²⁷⁾</u> в консоли управления SoftControl Admin Console. Проверьте работоспособность компонентов.

10.5 Привилегии процессов

В табл. 40 представлено описание привилегий Windows, используемых процессами (см. также <u>https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716(v=vs.85).aspx</u> и <u>https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4704</u>).

Привилегия	Описание
Управление аудитом и журналом безопасности	Добавление записей в журнал безопасности.
Архивация файлов и каталогов	Выполнение операций по резервному копированию. Эта привилегия заставляет систему выдать права на чтение любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Любой другой запрос на доступ, кроме чтения, по-прежнему оценивается с помощью ACL.
Восстановление файлов и каталогов	Выполнение операций восстановления. Эта привилегия заставляет систему выдать права на запись любого файла, независимо от того, что указано в списке управления доступом (ACL) для этого файла. Пользователь с данной привилегией может обходить разрешения файлов, папок, реестра и других постоянных объектов при восстановлении файлов и папок из резервных копий. Дополнительно данная привилегия позволяет назначить любого пользователя или группу с действующим идентификатором безопасности (SID) владельцем файла.
Изменение системного времени	Изменение системного времени. Пользователь с данной привилегией может изменять время и дату на внутренних часах компьютера. Пользователи с такими правами могут влиять на вид журналов событий. Если системное время изменено, события, которые были записаны, будут отображать это новое время, а не реальное время, в которое они произошли.
Завершение работы системы	Завершение работы локальной системы.
Принудительное удаленное завершение работы	Выключение системы с помощью запроса по сети.

Таблица 40. Описание привилегий процессов

Привилегия	Описание
Смена владельцев файлов и других объектов	Привилегия необходима, чтобы стать владельцем объекта без получения избирательного доступа. Пользователь с данной привилегией может стать владельцем любого защищаемого объекта в системе, включая объекты Active Directory, файлы и папки, принтеры, разделы реестра, процессы и потоки.
Отладка программ	Отладка и настройка памяти процесса, который принадлежит другой учетной записи. Пользователь с данной привилегией может присоединять отладчик к любому процессу или ядру. Разработчикам, отлаживающим свои собственные приложения, это пользовательское право не нужно. Разработчикам, отлаживающим новые компоненты системы, это право нужно. Данное право дает полный доступ к чувствительным и критичным компонентам операционной системы.
Изменение параметров	Изменение энергонезависимой памяти (RAM) систем, которые используют
среды изготовителя Профилирование производительности системы	данный тип памяти для хранения информации о конфигурации. Сбор профиля всей системы. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности системных процессов.
Профилирование одного процесса	Сбор профиля по одному процессу. Пользователь с данной привилегией может использовать средства наблюдения за производительностью для контроля производительности несистемных процессов.
Увеличение приоритета выполнения	Увеличение базового приоритета процесса. Пользователь с данной привилегией может использовать процесс с доступом к свойству «запись» другого процесса для увеличения приоритета выполнения, назначенного этому другому процессу. Такой пользователь может изменять запланированный приоритет процесса через пользовательский интерфейс Диспетчера задач.
Загрузка и выгрузка драйверов устройств	Загрузка и выгрузка драйверов устройств. Пользователь с данной привилегией может динамически загружать и выгружать драйвера устройств или другой код в режиме ядра. Это пользовательское право не применяется к драйверам устройств Plug and Play.
Создание файла подкачки	Создание файла подкачки. Пользователь с данной привилегией может создавать и изменять размер файла подкачки.
Настройка квот памяти для процесса	Увеличение квоты, назначенной процессу.
Обход перекрестной проверки	Получение уведомлений об изменениях в файлах и директориях. Привилегия также заставляет систему пропустить все перекрестные проверки на доступ. По умолчанию включена для всех пользователей.
Отключение компьютера от стыковочного узла	Отстыковка ноутбука. Пользователь с данной привилегией может отключить портативный компьютер от стыковочного узла, не выполняя вход в систему.
Выполнение задач по обслуживанию томов	Включение привилегий по обслуживанию томов. Необходима для проведения задач по обслуживанию на томе, например, удаленной дефрагментации.
Имитация клиента после проверки пользователя	Имитация клиента. Пользователь с данной привилегией может имитировать другие учетные записи.
Создание глобальных	Создание именованных объектов сопоставления файлов в глобальном

Привилегия	Описание
объектов	пространстве имен во время удаленных терминальных сессий. Привилегия по умолчанию включена для администраторов, сервисов и учетной записи LocalSystem.

10.6 Трафик SoftControl SysWatch

Есть три источника трафика SoftControl SysWatch:

- 1) Оверхеды HTTPS,
- 2) Логи с клиентского устройства,
- 3) Обновления (клиентского модуля и антивирусных баз).

Оверхеды HTTPS

Трафик оверхедов HTTPS составляет 3,7 КБ за хартбит. (Хартбит – это параметр клиентских компонентов, отвечающий за периодичность установки связи с серверным компонентом SoftControl Server.)

Трафик в месяц от оверхедов HTTPS можно оценить по следующей формуле: T1=3,7*30*24*3600/значение хартбита [секунды]. Результат будет выражен в килобайтах в месяц.

Логи с клиентского устройства

Объем трафика, который генерируется на одно событие, составляет около 500 байт. По количеству событий можно оценить для типового устройства объем трафика, который генерируют логи за сутки, а также заполняемость базы данных.

Чтобы выгрузить сведения о событиях на типовом устройстве за сутки, выполните следующие действия:

- 1. Откройте в SoftControl Admin Console лог событий для нужного устройства.
- 2. Выберите в верхней панели меню Фильтры –> Фильтры событий SysWatch –> Все.

SoftControl Adm	nin Console									_ = ×
Файл Вид Фильтры Инструменты О программе										
	Сохранить настро	йки вида F2 🧳	1 🥺 🦱 🚺	1 🛋 🛛	1	1 👬 🖪				
🦢 🌌	По умолчанию	Ctrl+1	2 📢 📟 関					🛎 🗎		
Клиенты /	Полный вид	Ctrl+2								▼
	Статус	Ctrl+3								
1 C 2 C	Обновление клие	нта	1							
[ClientID] In (Фильтры событий	SysWatch	Все							
	Фильтры событий	DLP +	Нарушение политики ко	онтроля						
	Пользовательские	фильтры	Контроль активности		мышкой	і заголовок колонк	и для группировки данных п	10 ней		
14	14	Turn and unun	Запуск процесса			T				
идентификато		Типсобытия	Антивирус			Тип клиента				
	30 DESKTOP-03K	Запуск процесс	Изменение настроек	45 	ая <mark>с</mark>	SysWatch				i
	28 DESKTOP-63K	Антивирис	Риза возграние		ая 5	SysWatch				
	26 DESKTOP-63K	Антивирус	вход пользователя		aa S	SysWatch				
	25 DESKTOP-63K	Антивирус	выход пользователя		aa S	SysWatch				
	24 DESKTOP-63K	Обновление кл	Не стартовавшие проце	ссы	ая					
	23 DESKTOP-63K	Обновление кл	Событие службы	-6	ая					
	22 DESKTOP-63K	Обновление кл	События DeCrypt	н	ая					U
	27 DESKTOP-63K	Изменение настроек	02.02.2021 8:20:34	Обычна	ая S	SysWatch				
	21 DESKTOP-63K	Запуск процесса	02.02.2021 8:18:15	Высока	ая S	SysWatch				
	20 DESKTOP-63K	Запуск процесса	02.02.2021 8:18:15	Высока	ая S	SysWatch				
	19 DESKTOP-63K	Обновление клиента	02.02.2021 8:17:41	Высока	ая					
	18 DESKTOP-63K	Обновление клиента	a 02.02.2021 8:17:41	Высока	ая					
	17 DESKTOP-63K	Обновление клиента	a 02.02.2021 8:17:39	Обычна	ая					
	16 DESKTOP-63K	Вход пользователя	02.02.2021 8:16:28	Обычна	ая					
										•
Первая страница			я страница Страница №	?1 (последня	яя)					Прошло времени: 00:00:00
Имя пользователя	a: admin Poge: Cu	истемный администрат	ор. Администраторы							Смена дарода
Plink nonesonaten	PONN. CV	истемпни одминистрат	ор, сдалитистраторы							Смена пароля

Рисунок 220. Настройка фильтра для лога событий

- 3. Нажмите на кнопку (Редактировать запрос). Подробнее см. разделы Фильтрация событий ¹⁵⁹ и Запросы к базе данных ¹⁶⁵.
- 4. Чтобы добавить фильтр по времени, нажмите на зеленый кружок со знаком «плюс», затем выберите **Время**, **Между** и задайте интервал в одни сутки.

SoftControl Admin Console											
Файл Вид Фильтры Инструменты О программе											
چ 🗟 🧟	ا ١٩ 🛱 ا 🛃 😓 😒 🕹 😁 😒 📢 😂 🎬 🔓 🍤 🔁										
Клиенты Лог с	Knuertei Jor co6urnix ×									-	
	- 🔒 - 😜 🤬					,					
[ClientID] In (2)		Редактировать запрос			- 4 ~						
		Укажите запрос:									
		O N				ах по н	ей				
		ClientID Один из 2 🙂 🕄									
Имя к Иде	ентификатор Идентификато	Время (UTC+0) Между 13.01.2	2021 и 14.01.2021	8		лие	Исполняемый файл	Тип клиента	Командная строк	Пользовате	3
DESKT	30 02af9f41-d2c8						C:\PROGRAM FILES	SysWatch	"C:\Program Files\	DESKTOP-63	Д_
DESKT	29 02af9f41-d2c8						C:\PROGRAM FILES	SysWatch	"C:\Program Files\	DESKTOP-63	Д
DESKT	28 02af9f41-d2c8					_		SysWatch			
DESKT	26 02af9f41-d2c8							SysWatch			
DESKT	25 02af9f41-d2c8							SysWatch			
DESKT	24 02af9f41-d2c8					-					
DESKT	23 02af9f41-d2c8					-					
DESKT	22 02af9f41-d2c8							C			-
DESKT	27 02af9f41-d2c8					-	C) 000 CD 414 5% 50	Syswatch	1010 51.0	DECKTOD CO	
DESKI	21 02af9f41-d2c8						C:\PROGRAM FILES	Syswatch	C:\Program Files\	DESKTOP-63	4
DESKI	20 02af9f41-02c8						C:\PROGRAM FILES	Syswatch	C:\Program Files\	DESKIOP-03	д
DESKT	19 02af9f41-d2c8			Отмена							
DESKT	17 02af9f41-d2c8	-419 Обновлени 02.02.2	Обычная	Запуск обновлений Про	цесс обно						
			5001 1101					-			
1											
Переза страница (Предидущая страница) (Следующая страница №1 (последняя) Прошло времени: 00:00:00											
										<u> </u>	5
Имя пользовател	Имя пользователя: admin Роли: Системный администратор, Администраторы Смена пароля Смена пароля										

Рисунок 221. Настройка запроса к базе данных. Задание времени

5. На экране появятся записи о событиях, произошедших за указанные сутки. Нажмите на иконку **Экспорт в Excel** и выберите директорию, в которую вы хотите сохранить лог с событиями.

	🖌 SoftControl Admin Console 📃 🗖 🛛										
Φa	Файл Вид Фильтры Инструменты Опрограмме 🕼 🕼 📲 🔜 🚈 🕂 🐖 🛛 🛠 🦛 🕼 🛋 🖉 🎬 🎽 🔽 🖷 🖢 🖉										
K	Клиенты Лог событий ×										
[C	lientID] In	(11) And [Occurrence	eTime] Between(#2020	-04-06#, #2020-	06-04#)						
-				Перетяните	юда мышк	ой заголовок колон	нки для группировки дан	ных по ней			
	Имя	Идентификатор	Уникальный ID уст	Тип события	Время	Важность	Действие	Статус действия	Статус клие	Исполняемый файл	Тип кл
•	WIN	-1	1e9c01a2-59ba-42	Статус	26.05.2	Высокая			Остановлен		A
	WIN	97	1e9c01a2-59ba-42	Обновлени	23.05.2	Высокая	Обновление заве	Обновление з			0
	WIN	96	1e9c01a2-59ba-42	Обновлени	23.05.2	Высокая	Информация обн	Проверка: Ош			
	WIN	95	1e9c01a2-59ba-42	Антивирус	23.05.2	Обычная	Завершение скан	Успешно			SysWat
	WIN	-2	1e9c01a2-59ba-42	Статус	22.05.2	Высокая			Активен		
	WIN	94	1e9c01a2-59ba-42	Антивирус	22.05.2	Обычная	Запуск сканера	Сканер запущен			SysWat
	WIN	93	1e9c01a2-59ba-42	Обновлени	22.05.2	Обычная	Запуск обновлений	Процесс обно			
	WIN	-1	1e9c01a2-59ba-42	Статус	22.05.2	Высокая			Остановлен		
∎											
ſ	Первая страница Предыдущая страница Следующая страница №1(последняя) Прошло времени: 00:00:01										
N	Имя пользователя: console_admin Роли: Системный администратор, Администраторы Смена пароля										

Рисунок 222. Экспорт выборки в файл XLSX

 В созданном файле посчитайте количество строк. Умножьте это число на 500 байт, и вы получите приблизительный объем трафика за сутки, который приходится на логи от устройства.

Обновления

Обновления клиентского модуля

Объем одного обновления составляет 30 МБ. Обновления выходят 3-4 раза в год.

Обновления антивирусных баз

Объем первого обновления после установки составит 60 МБ. Далее за каждый день объем обновлений может составлять от 400 до 1 300 КБ (по мере выпуска новых антивирусных баз).

10.7 Источники

Источники дополнительной информации приведены в табл. 41.

Таблица 41. Вспомогательная документация

Название	Описание	
Руководство пользователя SoftControl ATM Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl ATM Client	
Руководство пользователя SoftControl Endpoint Client	Руководство по установке, настройке и работе с клиентским компонентом SoftControl Endpoint Client	
Руководство пользователя SoftControl SClient	Руководство по установке, настройке и работе с клиентским компонентом SoftControl SClient	
Руководство по установке SoftControl DLP Client	Руководство по установке и настройке клиентского компонента SoftControl DLP Client	

10.8 Обновление клиентских компонентов и антивирусных баз на Windows XP

Windows XP в зависимости от версии Service Pack может либо вовсе не поддерживать новые сертификаты, либо поддерживать их частично. Это связано с тем, что при их генерации использовались более современные алгоритмы (SHA-256).

Чтобы обновления продуктов SoftControl баз работали корректно, необходимо правильно настроить параметры запуска модулей обновления.

<u>Примечание</u>. Если вы установили приложение SoftControl SysWatch версии 5.1.79 или позднее и при этом ранее это приложение у вас не было установлено, выполнять инструкции из этого раздела не нужно: обновление пройдет корректно. Для SoftControl DLP и SoftControl SysCmd выполнять инструкции из этого раздела не нужно, если у вас версия 6.0.95 или позднее.

1. Откройте в SoftControl Admin Console редактор клиентских настроек.

2. Перейдите в раздел Модули.

3. Нажмите на иконку 🗍

4. На вкладке Идентификационные данные модуля введите имя модуля (название исполняемого файла) и путь к нему согласно таблице:

Обновляемый компонент	Имя модуля	Путь			
SoftControl SysWatch	snsupd.exe	C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH\			

Таблица 42. Модули обновления

Обновляемый компонент	Имя модуля	Путь			
SoftControl SysCmd	upd.exe	C:\Program Files\SoftControl\SysCmd\Updater			
SoftControl DLP Client	upd.exe	C:\Program Files\SafenSoft\DLP Client\Updater			

бщие настройки Имя и описание Хартбит тр	Использовать частные настройки для модулей
ІР-адреса сервера	
Номер лицензии	- U ^
ysWatch	Правила для реестра Правила для сети Привилегии процесса
Контроль активности	Общие настройки Правила для файловой системы
Управление инцидентами	Илентификационные данные молуля
Защита паролем	пдетнификационные данные модуля
Сканирование	Имя модуля Комментарий
Общие настройки	snsupd.exe
Настройки расписания	Пути файлов
Обновление	C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH
Общие настройки	
Источники обновлений	
Настройки расписания	
Настройки интерфейса	• • • • • • • • • • • • • • • • • • •
Отчеты	Полробно
Оповещения	
Одноразовые пароли	Название организации:
Политика контроля	Внутреннее имя файла:
Устройства	Описание:
Модули	Авторские права:
Доверенный список автоза	версия:
Файловая система	
Системный реестр	
Сеть	Дооавить данные из фаила ОК Отмена
Хэш-суммы файлов	

Рисунок 223. Настройка модуля обновления на примере SoftControl SysWatch

5. На вкладке **Общие настройки** выберите зону выполнения **Доверенные приложения** и отметьте флажком **Включить режим обновления ПО**.

		_ = ×					
Правила для реестра	Правила для сети	Привилегии процесса					
Идентификационные данные модуля							
Общие настройки Правила для файловой системы							
Общие настройки Правила для файловой системы Зона выполнения Доверенные приложения Включить режим обновления ПО Сохранять историю запуска Назначение учетной записи Изолированный пользователь VIPO. ④ Не использовать назначение учетной записи В доверенном списке автозагрузки							
Добавить данные из файла		ОК Отмена					

Рисунок 224. Добавление модуля в доверенные приложения

6. Нажмите ОК.

7. Сохраните клиентские настройки под новым именем и примените их к подразделению, в котором находятся клиенты, которые необходимо обновить

Если вы настраиваете обновление для SoftControl SysWatch, далее вы можете создать задачу для обновления антивирусных баз или дождаться запуска обновления по расписанию.