USK Suite

Программный комплекс наблюдения, анализа и предотвращения исполнения процессов (программ).

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

info@softdev.online

ОГЛАВЛЕНИЕ

info@softdev.online

Общая схема работы

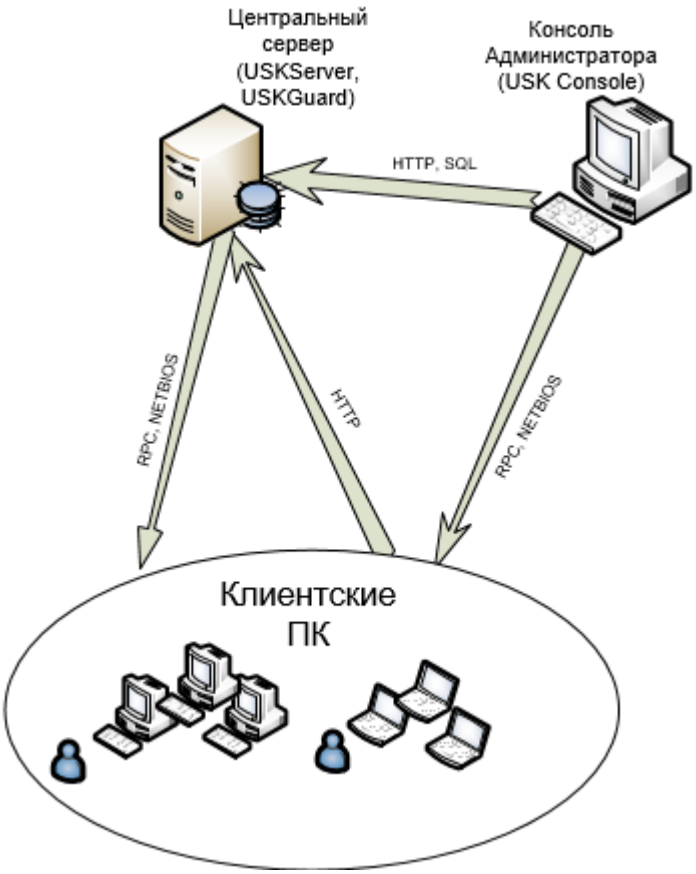


Рис.1

info@softdev.online

Функциональные возможности

1.1 Отслеживание создаваемых процессов
1.2 «*Жесткое*» или «*Мягкое*» предотвращение запуска нежелательных процессов
1.3 Опциональное удаление нежелательных файлов с носителей откуда они были запущены
1.4 Опциональное уведомление пользователя о допущенном нарушении
1.5 *Branding*-ресурсы для клиента (позволяют использовать произвольные логотипы) в уведомлениях
1.6 Гибкая система правил для оценки характеристик процессов (EXE) хранящаяся в зашифрованном виде
1.7 *Белые списки* (исключения) для *доменных* (Active Directory) и *локальных* групп, *аккаунтов*, имен *компьютеров* в каждом правиле. Возможна *инверсия* («черный список»)
1.8 Самозащита, контроль и восстановление работы клиентского агента в случае обнаружения неработоспособности
1.9 Кэширование всех событий на клиенте в случае невозможности отсылки их на сервер*
1.10 Шифрованный канал общения клиента с сервером обеспечивающий безопасность от «случайных взглядов 3х лиц»
1.11 Клиент и сервер поддерживают UNICODE во всех текстовых строках

2. *Выявление*:
2.1 Одинаковых исполняемых файлов
2.2 Новых (не встречавшихся ранее) исполняемых файлов
2.3 Файлов с фальшивой подписью кода (tampered)
2.4 Новых параметров запуска файлов
2.5 Изменения каждого запускаемого файла и ведение истории изменений

3. *Поиск*:
3.1 Файлов по различным критериям (хэш файла, хэш сертификата подписи, поля тэга VS_VERSIONINFO, размер, имя, путь)
3.2 По многочисленным типам событий, генерируемых сервером и клиентом

4. Группировка клиентских систем (одна конфигурация на группу)
4.1 Технология анализа файлов по специальному хэшу (magichash)
4.2 Гибкие возможности серверной фильтрации событий для предотвращения «замусоривания» ненужной информацией базы данных
4.3 Механизм автоматической маскировки командной строки и пути процесса для обезличивания *чувствительных* данных (например пароли)
4.4 Настраиваемые почтовые уведомления на различные события
4.5 Серверные части могут быть распределены (несколько серверов на одну БД)

*- В случае перезагрузки ОС или долгого отсутствия сетевого подключения, недоставленная информация до сервера будет сразу-же доставлена после появления соединения. Например это удобно в случаях мобильных клиентов (ноутбуков).

info@softdev.online

Системные требования

***Для сервера**:*

1. Windows Server 2008R2/2012/2012R2/2016/2019. Net Framework 4.5., 4Гб ОЗУ. 2 ЦПУ не ниже P4-2.4Ghz.
2. СУБД (может использоваться на основном сервере) MS SQL Server 2012/2014/2017/2019. Обязательна включенная поддержка CRL-процедур.
3. Для консоли управления: Windows 7/8/8.1/10/11 (32 и 64 бита) с установленным Net Framework 4.5. 1024 Мб ОЗУ.

***Для клиентского агента**:*

1. Windows Vista/7/8/8.1/10/11 (32 и 64бита). 256 Мб ОЗУ, 1 ЦПУ P3-500 Mhz. (ВНИМАНИЕ: Windows 2000 и XP не поддерживается вообще!). Работающие службы:
2. Windows Management Instrumentation (WMI)
3. Remote Registry *****.
4. Протокол File and Printer Sharing for MS Networks (RPC, NETBIOS ADMIN$/C$/IPC$ shares) *.
5. Remote Procedure Call (RPC).
6. Server (Lanman Server) *.

* - требуется только в случае удаленного подключения для восстановления клиента и\или обращения с консоли администрирования на клиентский компьютер.

Сервер имеет достаточную масштабируемость. Количество обрабатываемых в секунду событий и общее число клиентов определяется аппаратной конфигурацией сервера (серверов).

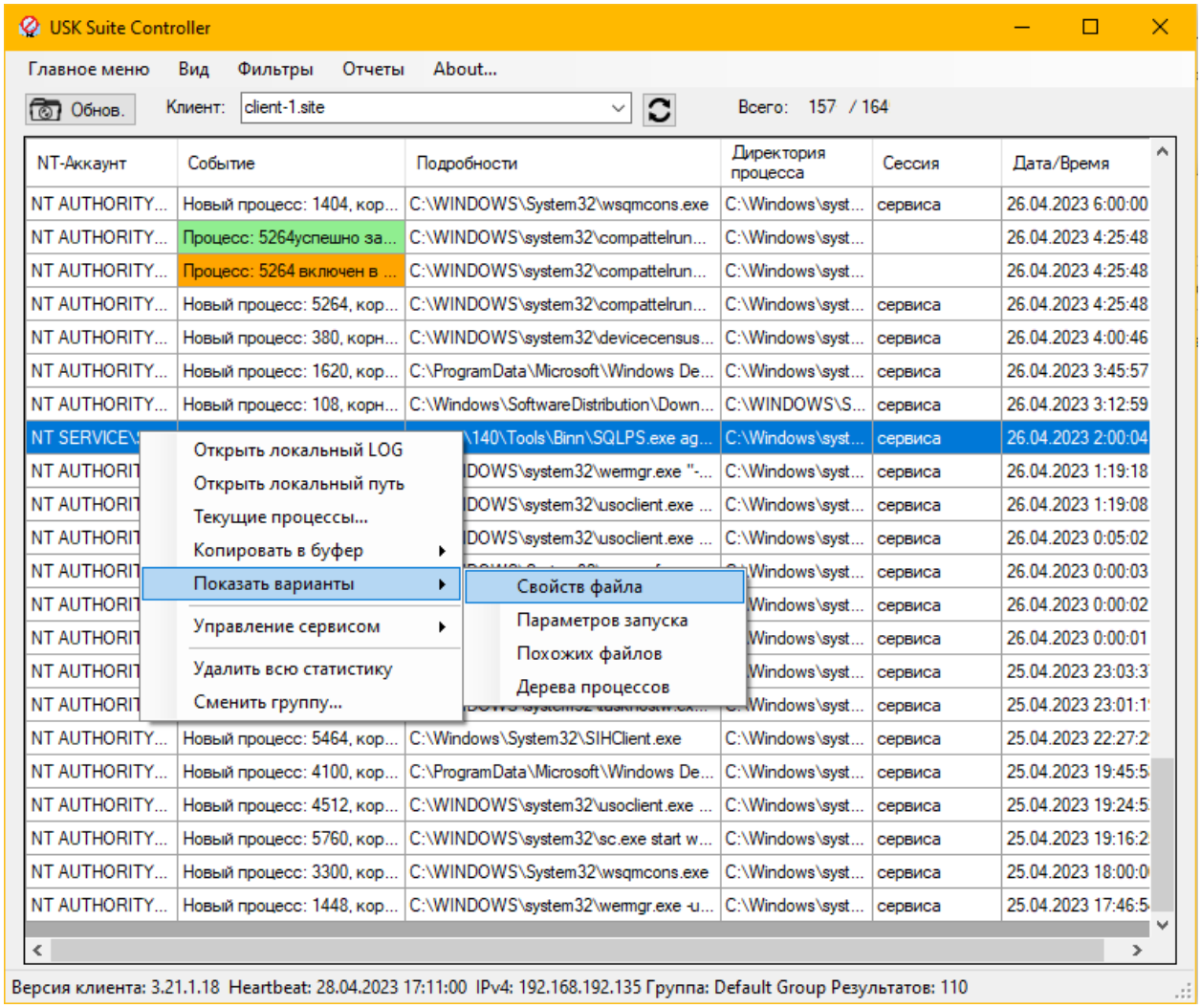
Проведенные эксперименты показывают высокую производительность сервера на базе *6 Core* CPU, *24 Гб* оперативной памяти, RAID-10 шпиндельные диски для БД обьемом *100 Гб* для 2000 обслуживаемых клиентских агентов в online. При «глубине» хранения данных статистики равной 4 месяцам.
Сторожевая компонента сервера - USGuard выполняет проверку работоспособности всех агентов за 1.5-3 минуты в этой конфигурации.

Помимо «больших» инсталяций, система может работать и с «маленькими» ресурсами. Сервер на базе 2 ядерного процессора Desktop-класса (с hyper threading), 4 Гб ОЗУ и одним жестким диском легко справляется с 130 клиентами в online.

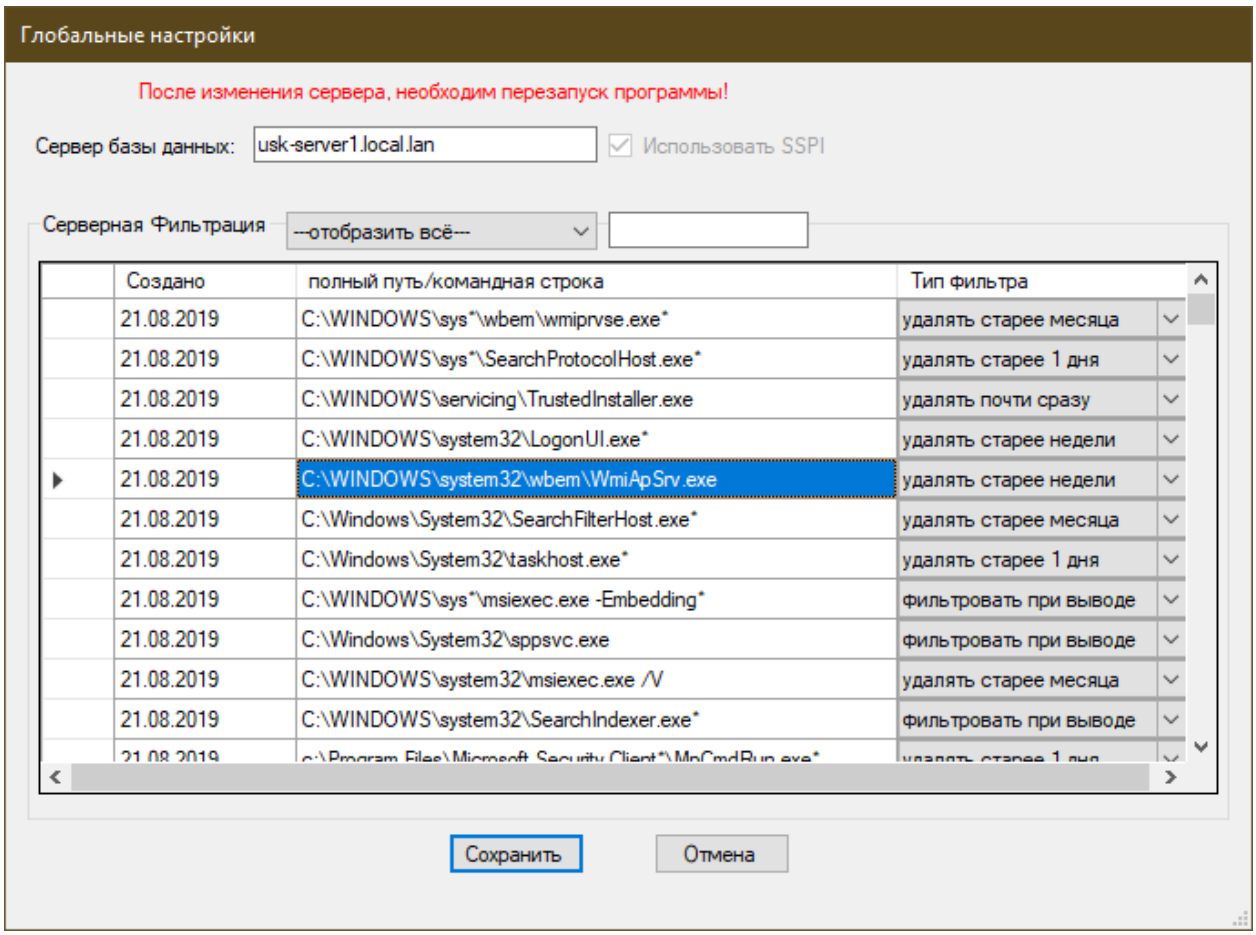
Клиентский агент не требует вычислительных ресурсов и не загружает систему лишним.

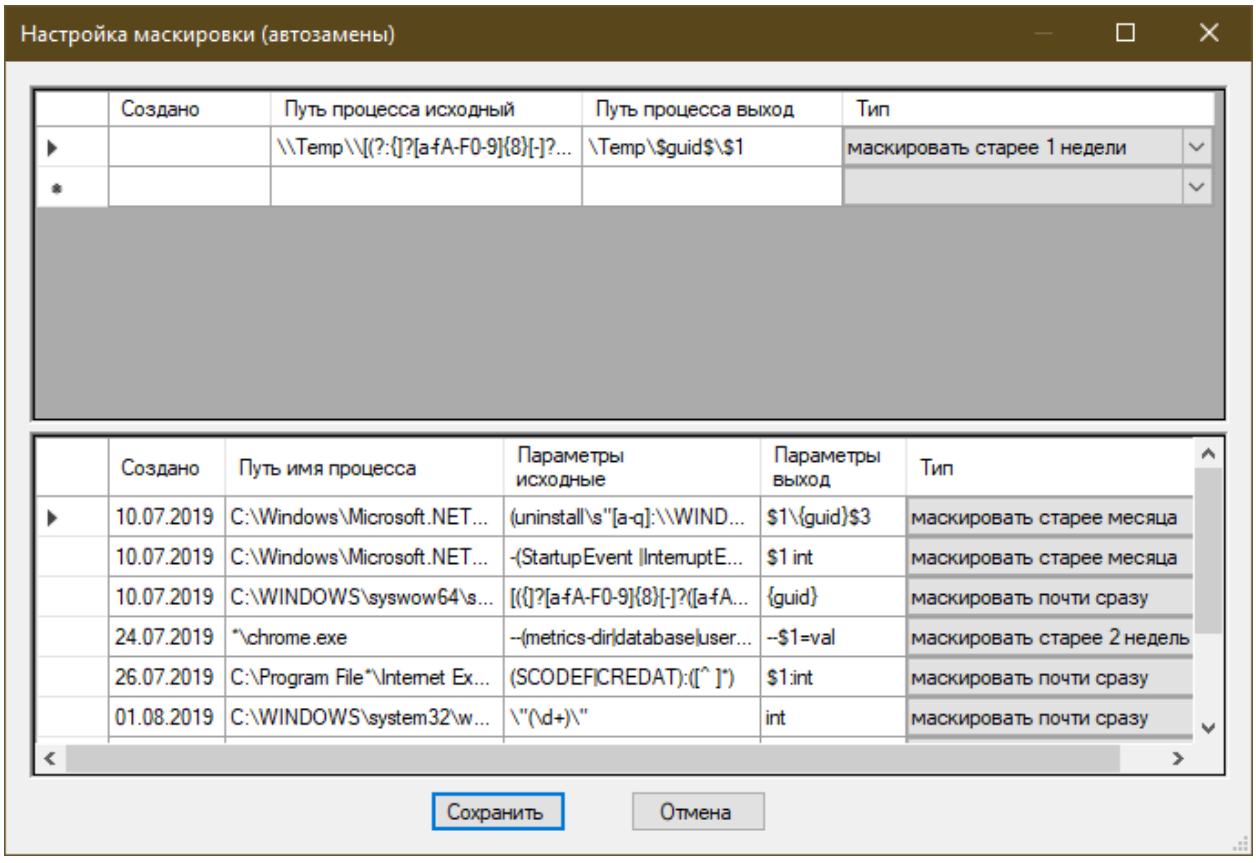
info@softdev.online

Общий вид интерфейса консоли управления

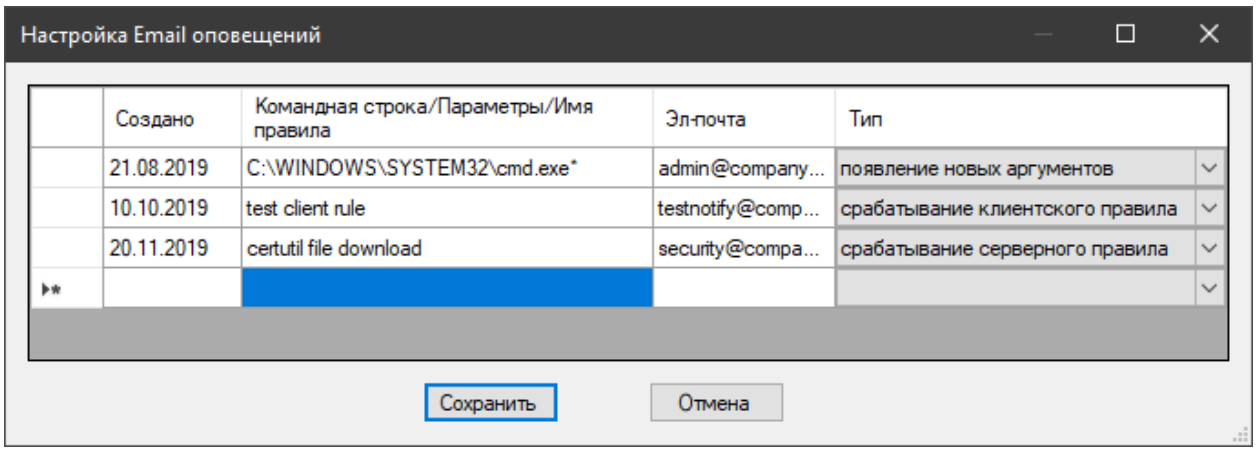


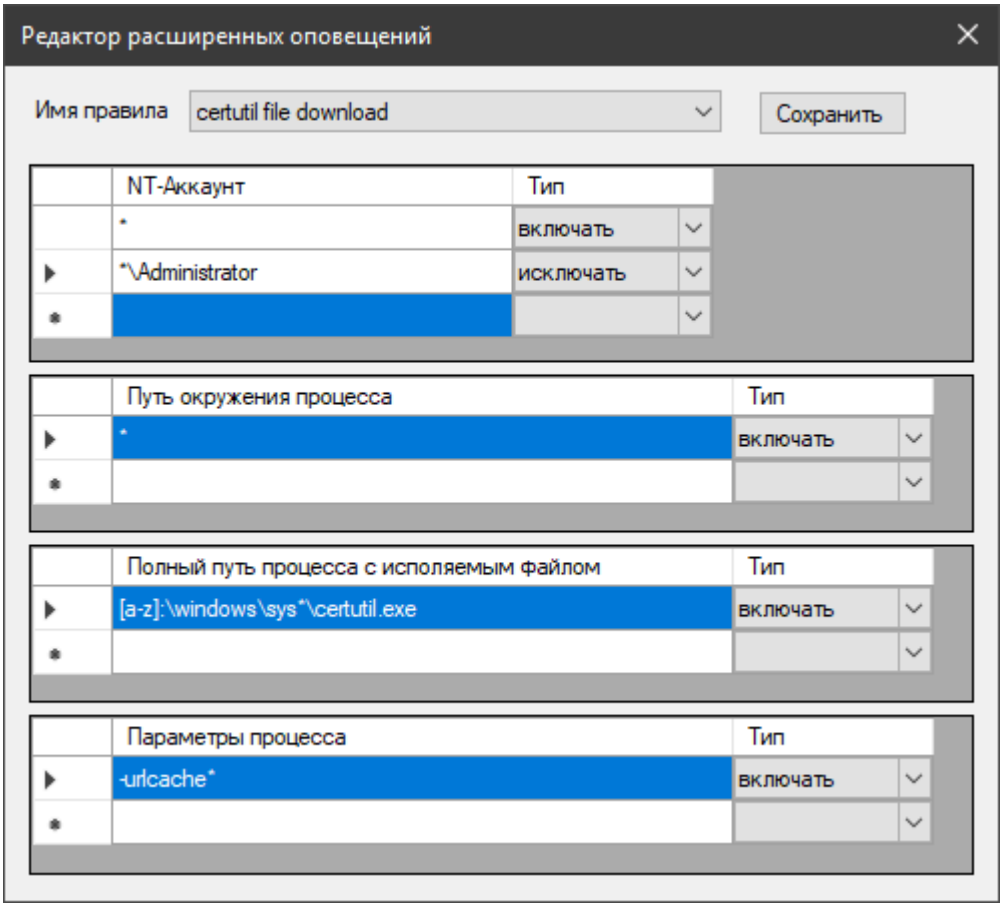
info@softdev.online



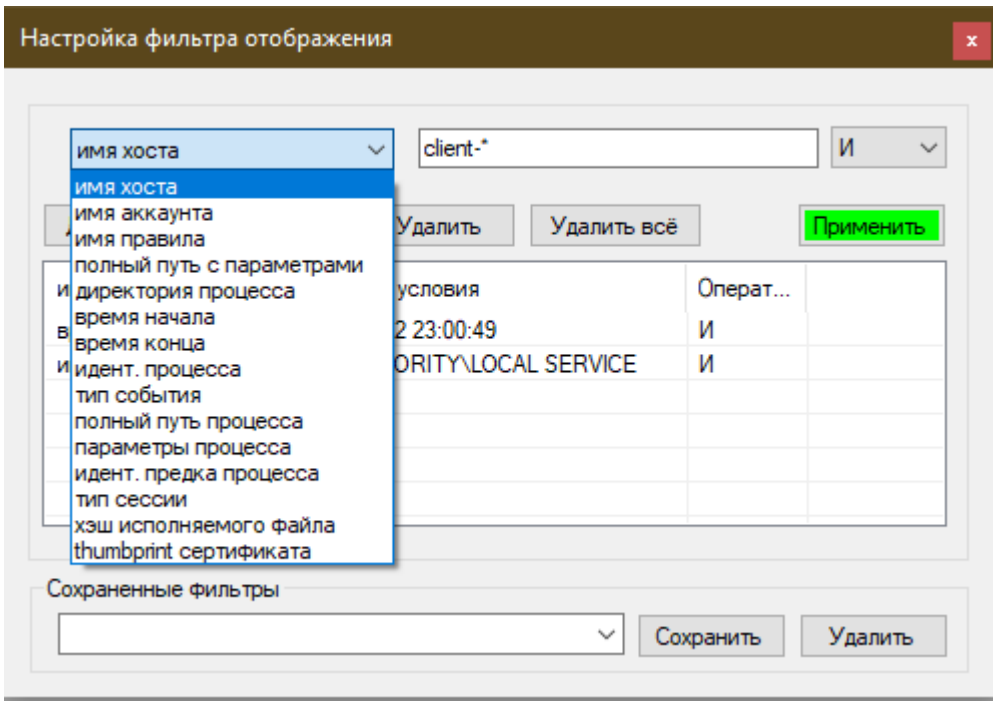


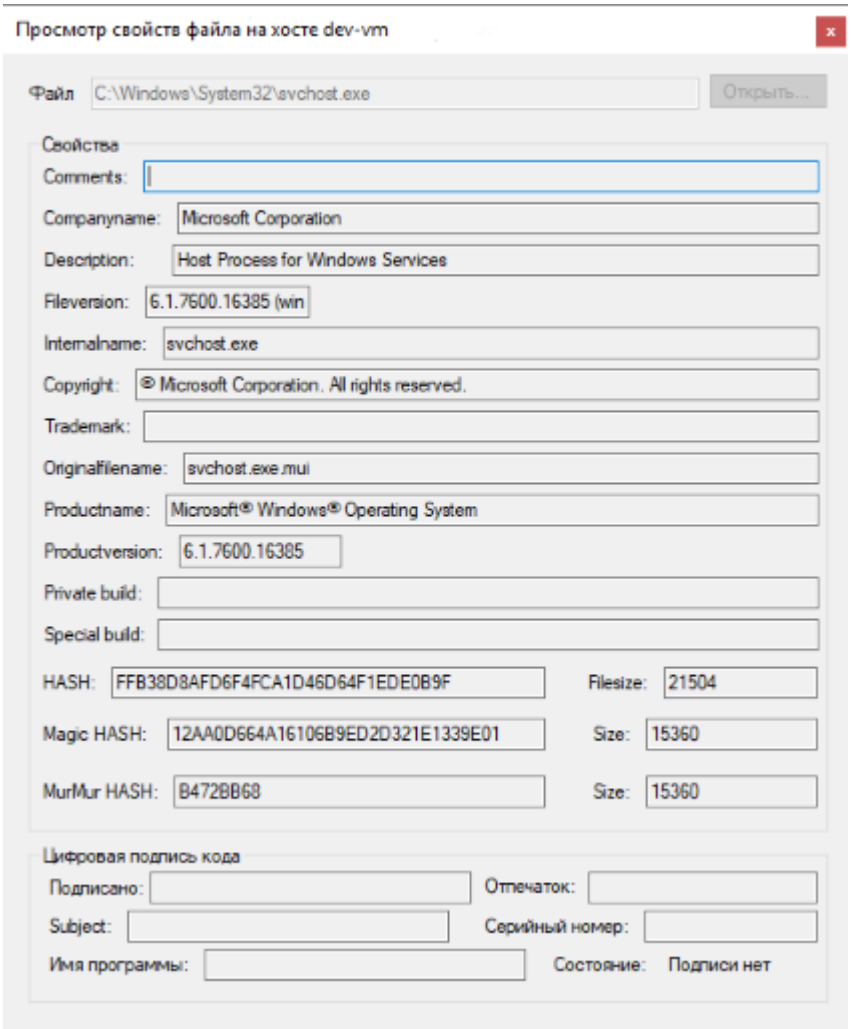
info@softdev.online

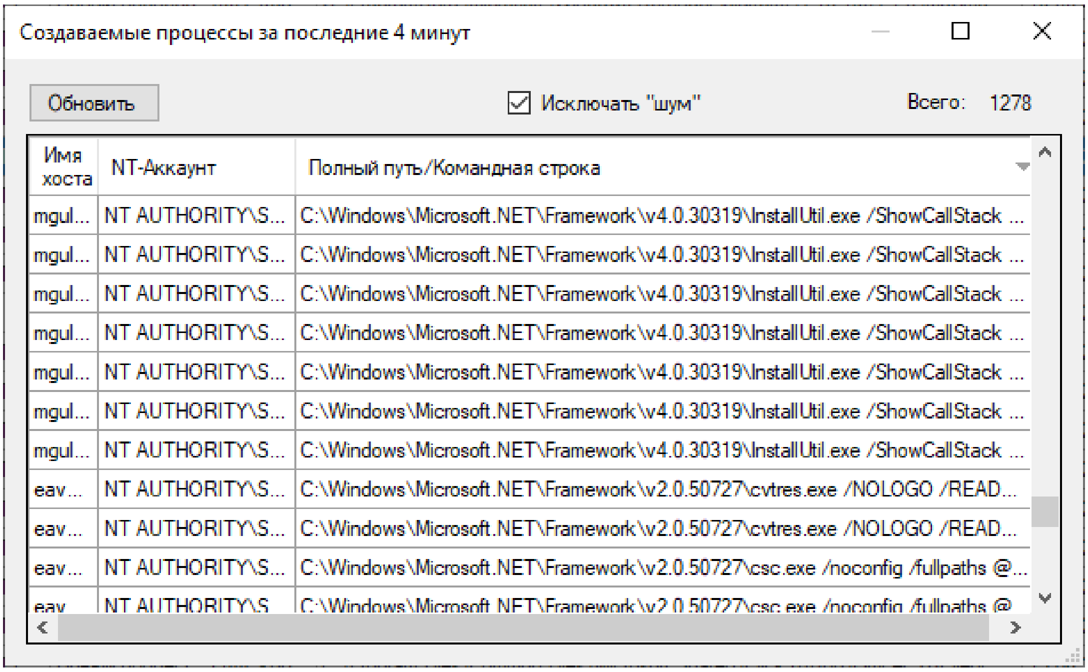


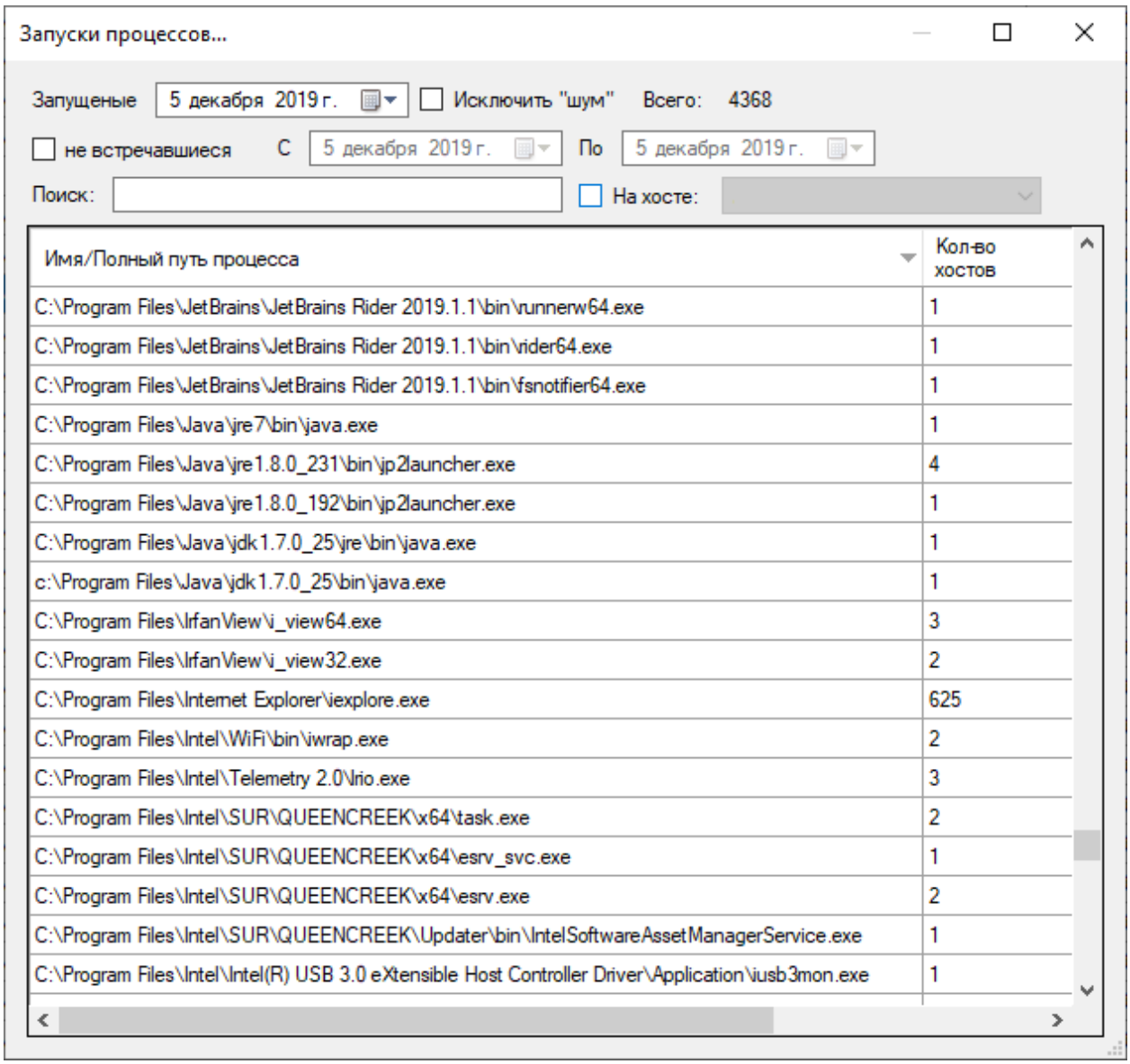


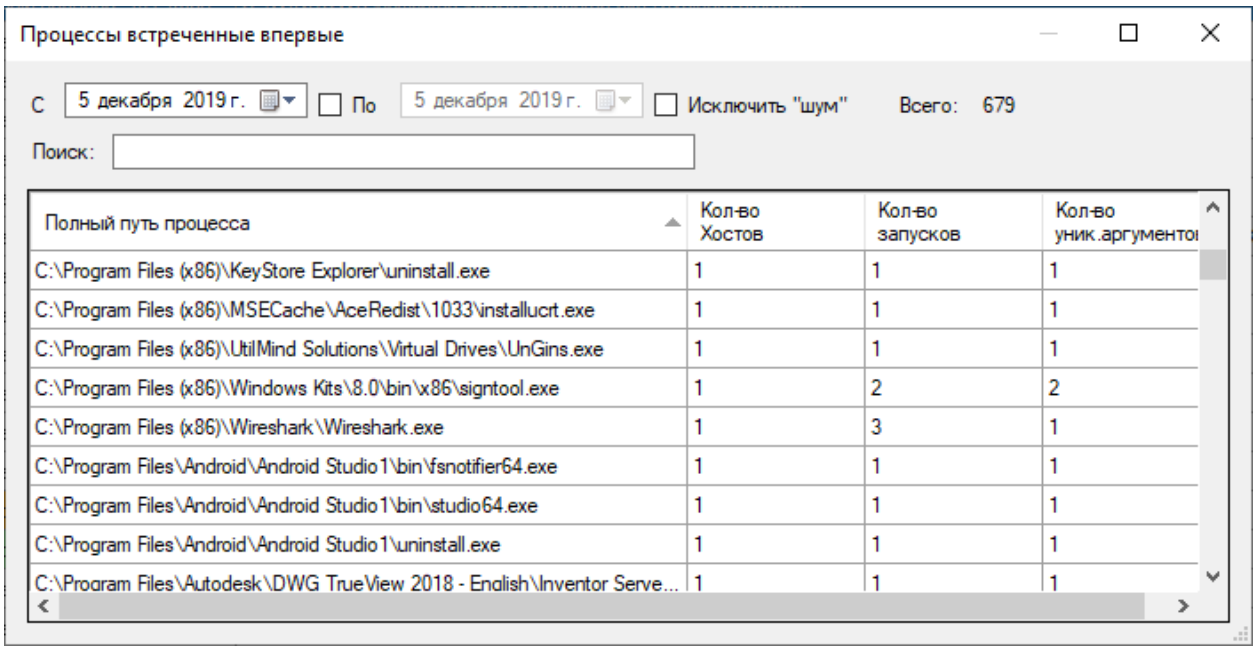
info@softdev.online

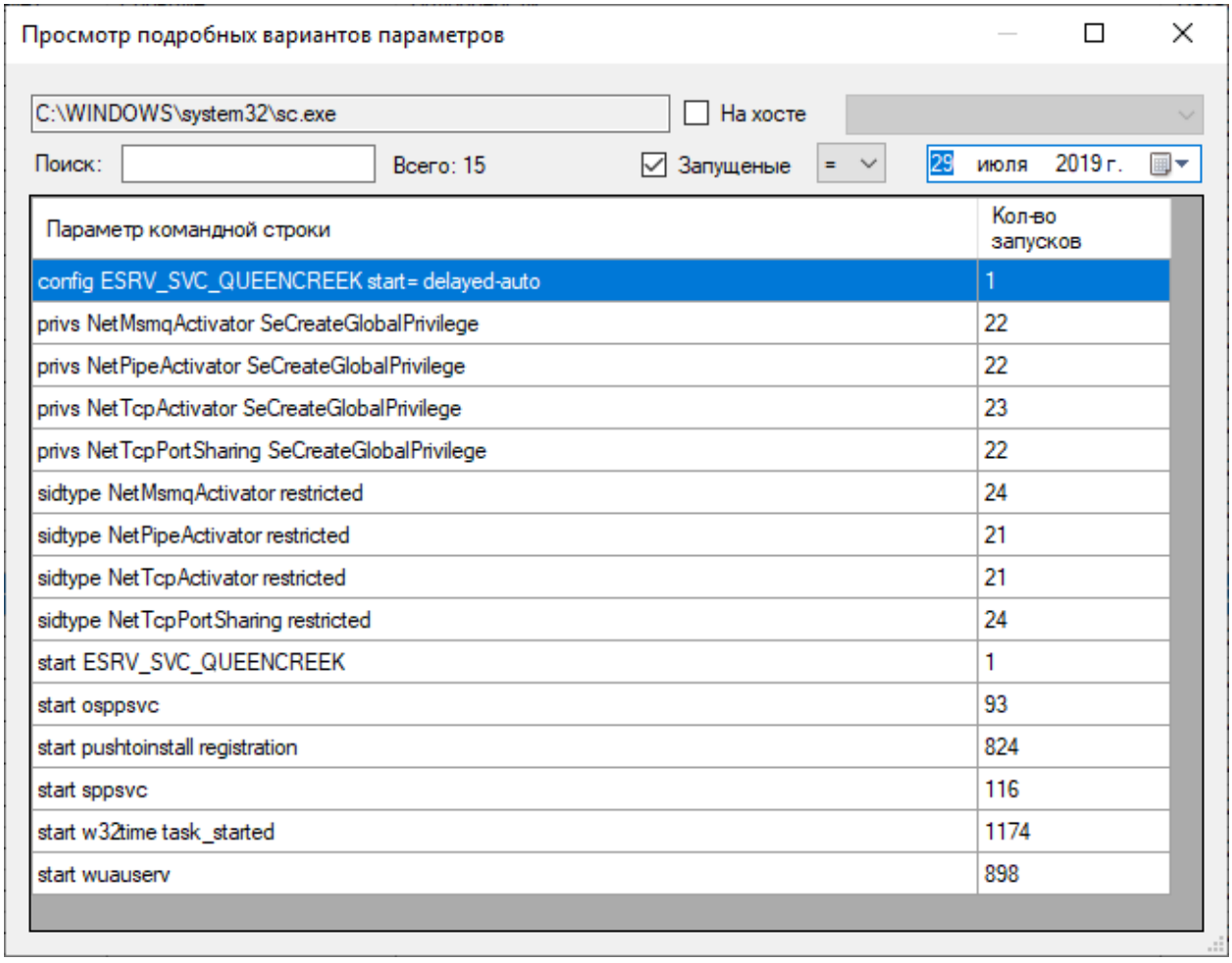




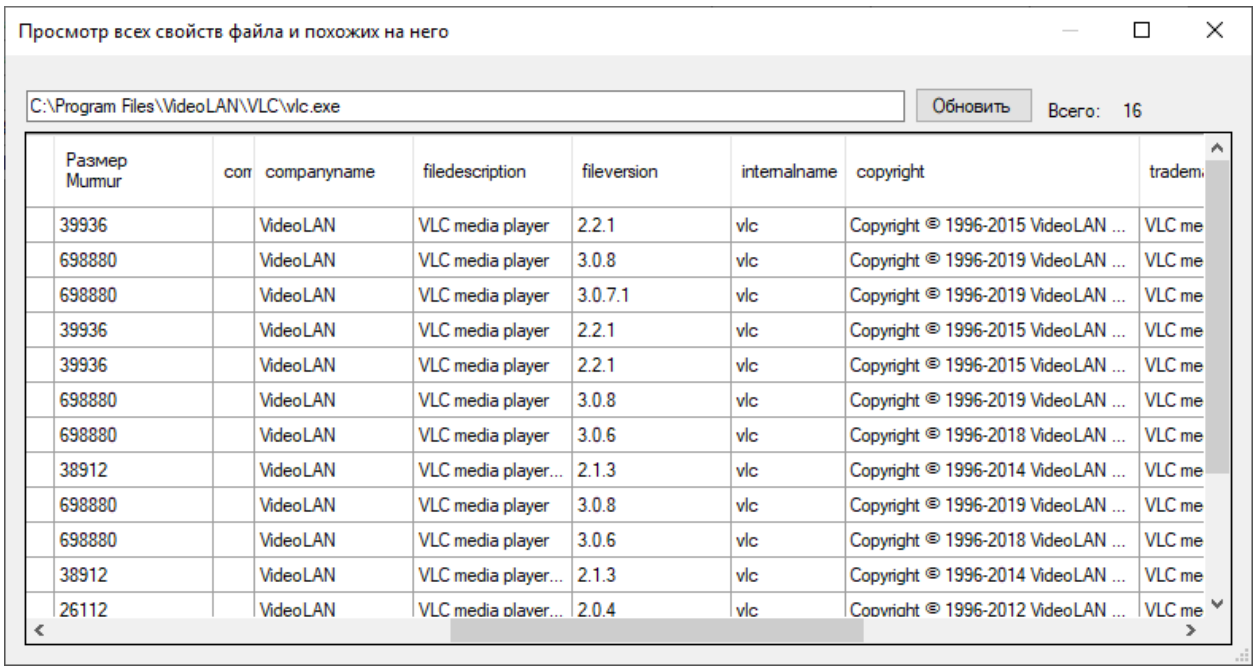


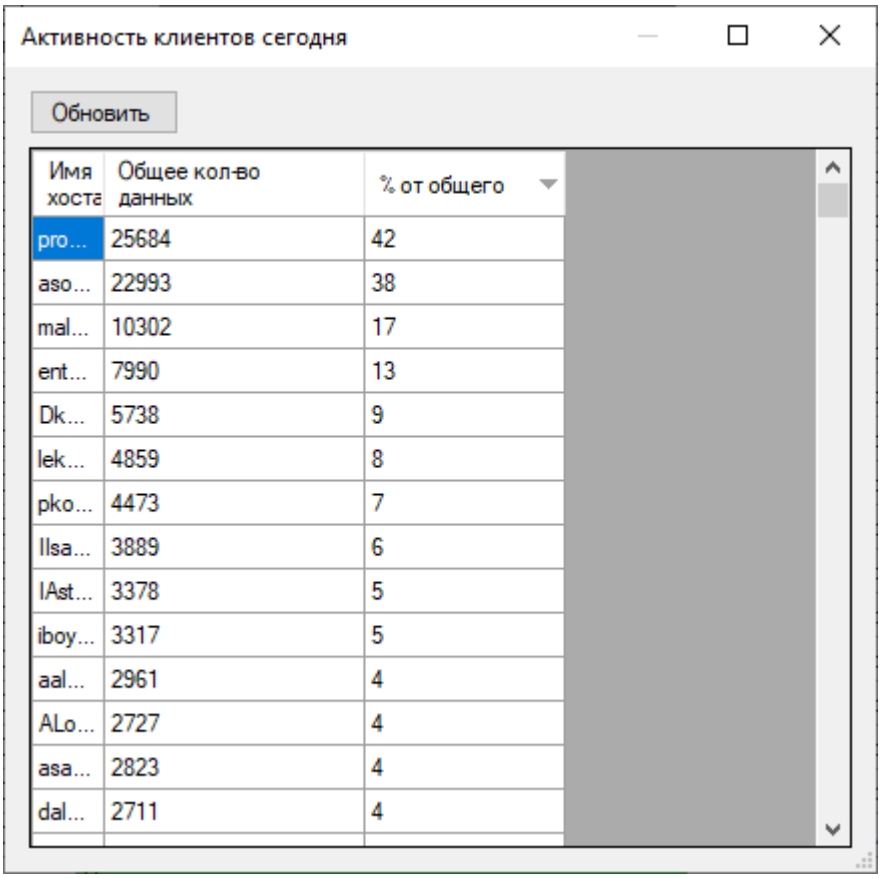


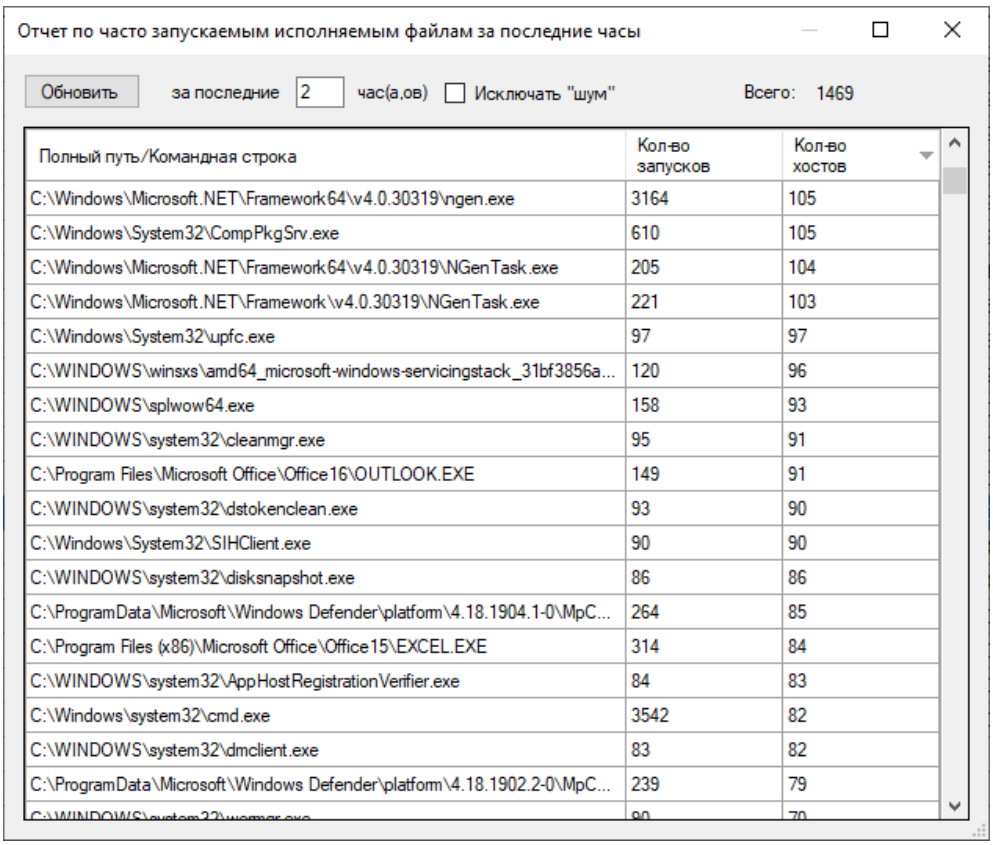




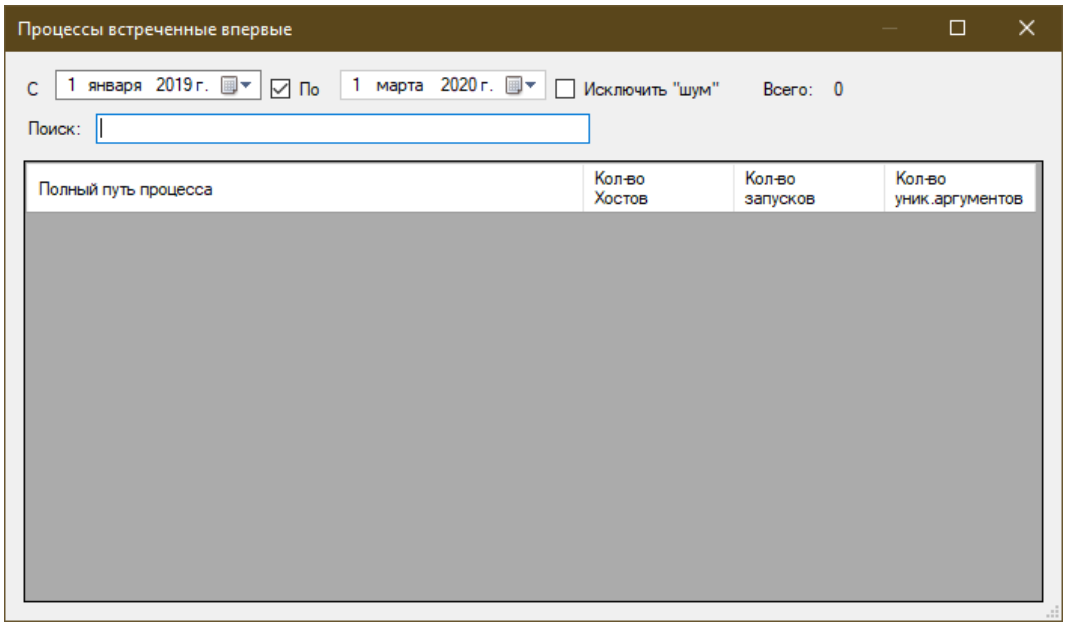
info@softdev.online



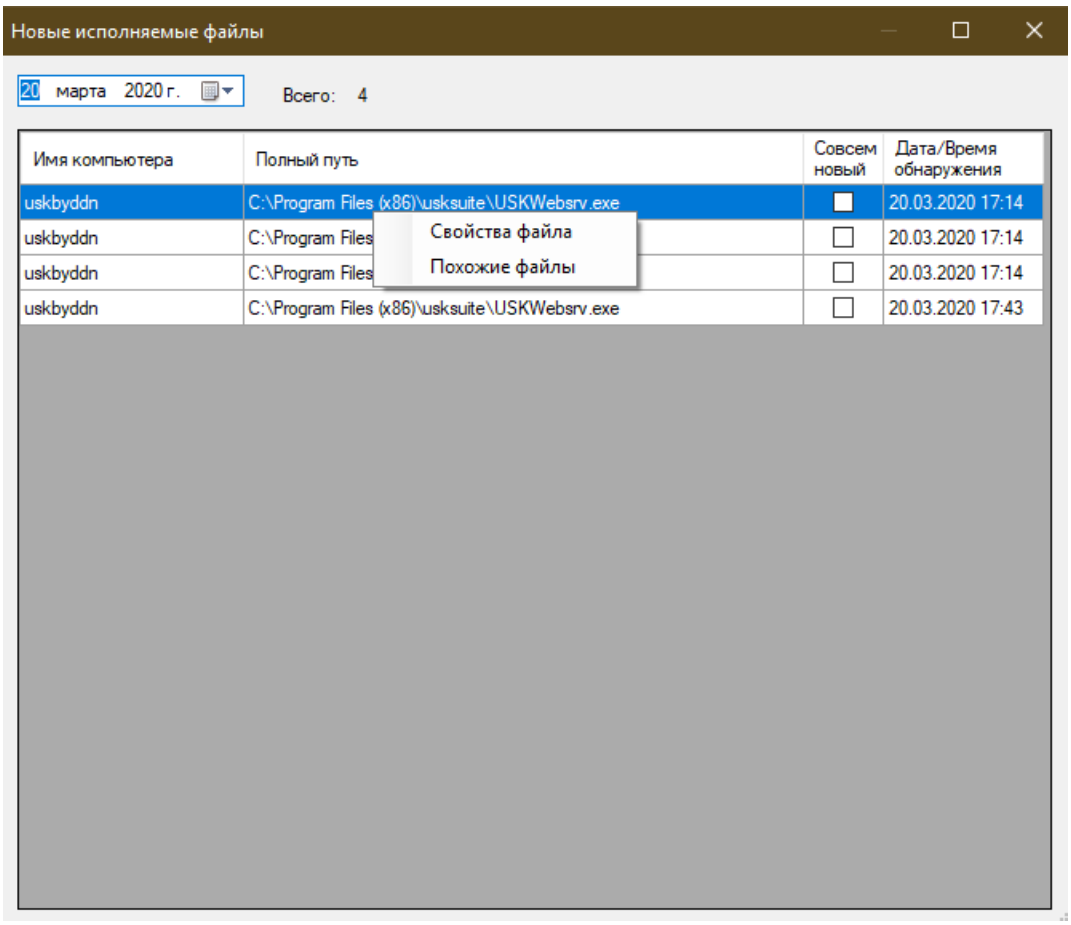


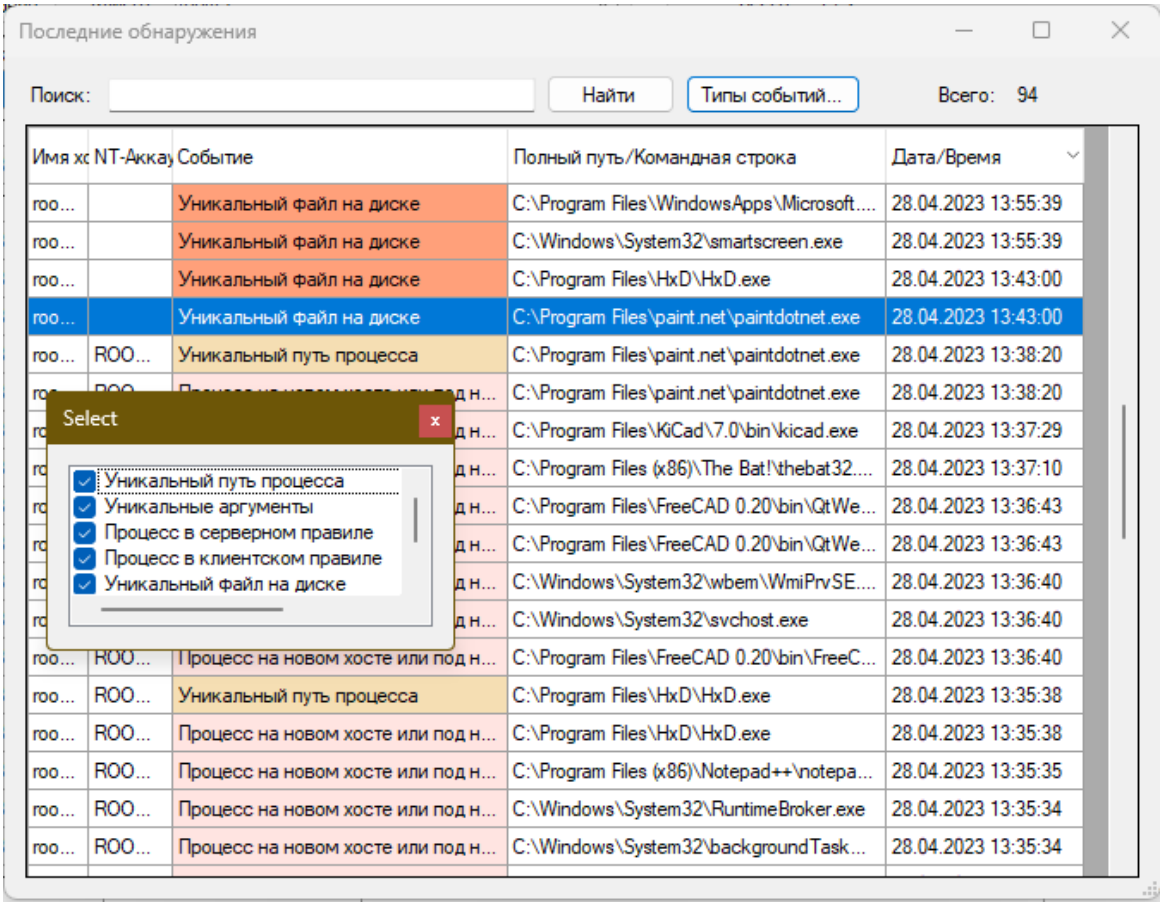


Полный путь/Командная строка	Кол-во запусков	Кол-во хостов
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe	3164	105
C:\Windows\System32\CompPkgSrv.exe	610	105
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\NGenTask.exe	205	104
C:\Windows\Microsoft.NET\Framework\v4.0.30319\NGenTask.exe	221	103
C:\Windows\System32\upfc.exe	97	97
C:\WINDOWS\winsxs\amd64_microsoft-windows-servicingstack_31bf3856a...	120	96
C:\WINDOWS\splwow64.exe	158	93
C:\WINDOWS\system32\cleanmgr.exe	95	91
C:\Program Files\Microsoft Office\Office16\OUTLOOK.EXE	149	91
C:\WINDOWS\system32\dstokenclean.exe	93	90
C:\Windows\System32\SIHClient.exe	90	90
C:\WINDOWS\system32\disksnapshot.exe	86	86
C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1904.1-0\MpC...	264	85
C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	314	84
C:\WINDOWS\system32\AppHostRegistrationVerifier.exe	84	83
C:\Windows\system32\cmd.exe	3542	82
C:\WINDOWS\system32\dmclient.exe	83	82
C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1902.2-0\MpC...	239	79
C:\WINDOWS\system32\wermgr.exe	90	70

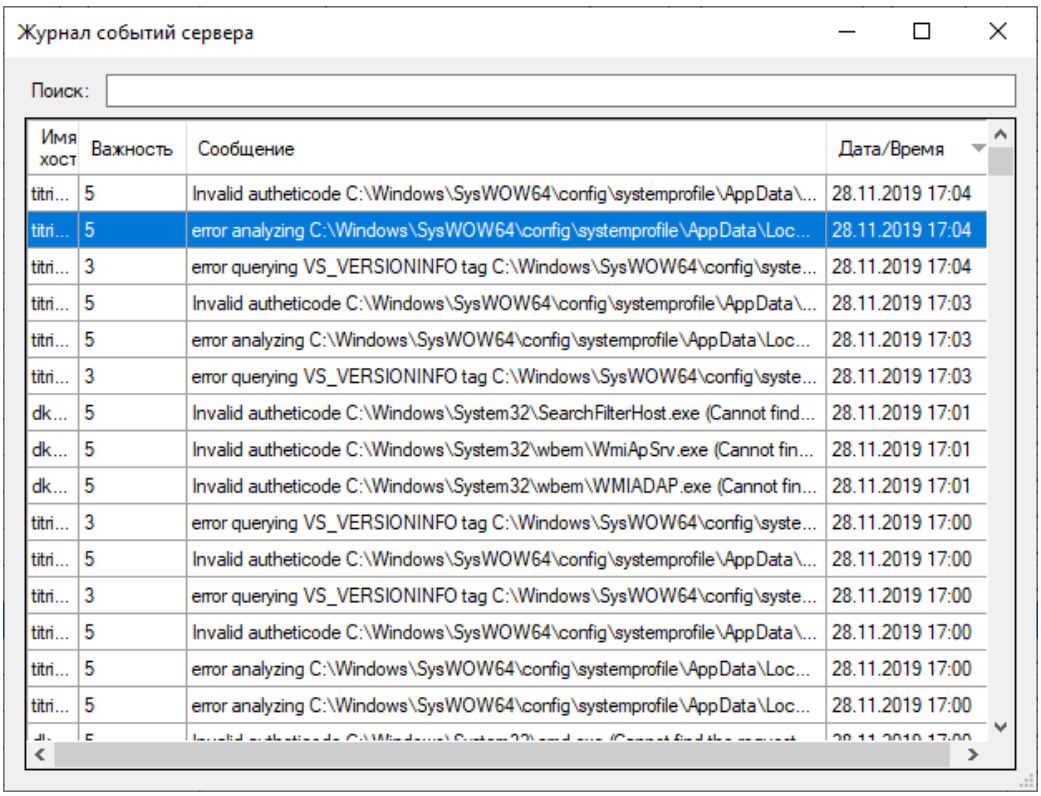


info@softdev.online





info@softdev.online



info@softdev.online

Установка и настройка сервера

Перед началом процедуры следует произвести настройки в используемом сетевом железе исходя из картинки коммуникаций на Рисунке 1.

Коммуникации

- Клиентские агенты, установленные на компьютерах, самостоятельно инициируют HTTP-соединение с сервером по порту указанными в настройках для группы. «Внутри» этого протокола используется свой собственный криптографический канал связи. Поэтому передача чувствительной информации от посторонних глаз безопасна.
- USKGuardPart установленный на сервере периодически инициирует соединения, на клиентские компьютеры, используя RPC (механизмы удаленного реестра, сервис-контроллера и WMI) и NETBIOS (для работы с удаленной файловой системой.
  Для этого используется учетная запись, под которой запускается USKGuardPart.
- Консоль управления инициирует соединения с центральным сервером по протоколу TDS (порт 1433). Т.е. ходит только к SQL-серверу. По запросу, может инициировать соединения, с выбранными клиентскими компьютерами используя аналогичные USKGuardPart механизмы.
  Для хождения к MS SQL Server используется указанная в настройках учетная запись (или SSPI – доверенная учетная запись)
  Для хождения к клиентским компьютерам используется учетная запись, под которой запущен UI-controller.

После этого подготовить MS SQL-Server. Возможно использовать уже имеющийся или поставить новый (отдельный). В случае если устанавливается новый, то ставим дефолтовый инстанс (MSSQLSERVER), можно именованный. Старт и работа SQL под любой учетной записью. Авторизация, поддерживаемая: Mixed-Mode. Collation – Cyrillic General (Accent – sensitive, Case – insensitive).
В настройках SQL Server surface area configuration включаем remote TCP connections.
ВНИМАНИЕ! В текущей версии для отсылки e-mail уведомлений серверная часть использует штатный функционал Database mail. Это требует минимум редакции Web. (Express НЕ поддерживает dbmail).
После подготовки SQL-сервера начинаем установку самой системы USKSuite.

1. Используя учетную запись с административными привелегиями запускаем *uskserversetup.exe* и следуем инструкциям на экране. Так же в процессе конфигурации СУБД потребуется, временно, учетная запись администратора SQL.
2. Создаем профиль и учетную запись для отсылки информационных сообщений от системы на почту. Use msdb
3. Grant EXEC on sp_send_dbmail to user
4. EXEC sp_addrolemember N'DatabaseMailUserRole', N'user'
5. EXECUTE msdb.dbo.sysmail_add_principalprofile_sp
6. @profile_name = 'USKSuite',
7. @principal_name = 'user',

8. @is_default = 0 ;

Вы можете параллелить нагрузку на один сервер устанавливая несколько серверов с USKWebSrv и при этом разведя клиентов по разным серверам с помощью DNS-записи RoundRobin (на одну запись несколько IP), либо создав несколько групп клиентских с указанием в конфигурации разных серверов.

Для ускорения работы с SQL-Server'ом опционально можно установить на машине с серверными компонентами SQL Server Native Client. После того как вы это сделаете следует открыть текстовым редактором (Блокнот) конфигурационные файлы и заменить Driver={SQL Server} на Driver={SQL Server Native Client **11.0**} . Версия зависит от установленного пакета. Для Sql server 2012 это 11.0

Первым делом, после установки серверных компонентов, следует зайти в консоль администрирования и настроить изначальную конфигурационную политику для «*Default Group*» на правильный сервер и порт. Пункт «главное меню» -> «редактор правил».

Серверный компонент uskserver требует от аккаунта (отличного от SYSTEM) иметь права на создание обработчиков HTTP NAMESPACES.
Если вы будете запускать сервис под отличной от SYSTEM учетной записью, то выдайте ей права на сервере путем выполнения данного действия:

netsh http add urlacl url=http://*uskbyddn*:*8880*/Default.aspx user=*SERVER\ACCOUNT*

info@softdev.online

Конфигурация серверной части (USKServer)

Файл конфигурации **uskweb.xml** конфигурирует серверную компоненту.
Атрибут sqldsn. Указывает строку подключения к базе данных SQL.
Атрибут sumseconds. Указывает через сколько секунд будет производится суммаризация данных принятых от клиентов. Интервал 10-300. В этот момент сервер в ходе цикла проверяет появились ли новые процессы, не встречавшиеся ранее, а также производит отсылку трапов (если они настроены).
Атрибут workthreads. Позволяет переопределить (отключив динамический механизм) кол-во потоков, обрабатывающих данные поступающие от клиентов.
Атрибут clientactualver. Указывает актуальную версию клиентского агента и включает механизм автоматического апгрейда сервером старых версий клиентов.
Атрибут selfupdatefile. Перекрывает имя по-умолчанию файла пакета обновления клиентской части.
Атрибут autoanaluf. Включает механизм автоматического запроса у клиента анализа файлов которые сервер определил, как новые (не встречавшиеся ранее). Запрос на анализ будет помещен в очередь и при следующей коммуникации клиента с сервером будет обработан.
Атрибут lastdetectiondays. Принимает значения от 1 до 30. Удаляет все события старее указанного кол-ва дней из списка «последних событий».
Атрибут cleanupdays. Принимает значения от 0 до 360. Включает автоматическую очистку *всех* старых данных из системы старее указанного кол-ва дней. (фильтры тут не используются). При этом из системы будут удалены данные:

- *о запусках приложений,*
- *данные уникальных запущенных приложений, неиспользуемые в течении указанного кол-ва дней,*
- *данные по параметрам командной строки,*
- *аккаунтам,*
- *именам (путям) приложений,*
- *старым анализам файлов,*
- *журнал сообщений сервера.*

Атрибут unuseddays. Принимает значения от 0 до 360. Включает очистку данных, срок использования которых последний раз был выше указанного числа дней.
Помимо этого, через консоль управления можно настроить неограниченное число фильтров процессов для исключения «замусоривания» журнала событий («фильтровать при выводе»).
Очистка происходит по нескольким, заранее заданным, временным критериям:

- *Сразу при поступлении* *. Происходит не сразу, а в очередной цикл суммаризации данных принятых с клиентов. Это необходимо для обеспечения минимальной вычислительной нагрузки на сервер БД.
- *Через 1 день*
- *Через 1 неделю*
- *Через 1 месяц*

- *Фильтрация при выводе*. Это специальный тип. Он не удаляет из лога ничего, а только используется при выводе информации консолью и расчетам новых процессов, и аргументов.

Поскольку некоторые процессы создаются системой и программами достаточно часто и имеют некоторые сильно вариативные параметры в аргументах процессов то дополнительно существует система «автозамены» параметров процессов действующая на основе регулярных выражений. Её настройки можно открыть через консоль управления выбрав в главном меню пункт «маскировка параметров».
Аналогичный механизм есть для автозамены путей запуска процессов. Например, для замены имени аккаунта профиля в пути на единый символ для исключения замусоривания БД.
Помимо этой цели, механизм может использоваться для маскирования чувствительных аргументов таких как пароли и т.п. информация, относящаяся к секретной. Её историческое складирование в системе таким образом будет «обезличено».
Правила регулярных выражений соответствуют Microsoft .NET Framework. Для подробностей стоит ознакомиться с руководством https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference

Для исключения замусоривания не актуальными версиями анализа файлов они удаляются из базы если с даты последнего анализа прошло больше недели и число вариантов больше 10ти.

Начиная с версии сервера 4.14 доступен механизм автоматической синхронизации учетных записей компьютеров со внешними службами каталогов Active Directory (LDAP). В текущей реализации механизм служит для автоматической пометки компьютерной записи в системе USK если была удалена учетная запись компьютера из LDAP. Система автоматически удалит все данные и учетную запись из USK при по прошествии cleanupdays интервала с момента обнаружения отсутствия записи в каталоге LDAP. Настройка синхронизации выполняется в свойствах выбранной вами группы. Можно настроить для разных групп из разных доменов. В дальнейшем появится функционал автоматического создания записей для появляющихся в каталоге LDAP компьютеров.

Компьютерные записи, которые были помечены как отсутствующие в LDAP-каталоге будут исключены автоматически из проверок на живость клиентского агента.

Периодичность синхронизации – Ежесуточно. При поиске учитывается наличие у машин суффикса имени домена. Если имя записи компьютера comp1.site.local и включена синхронизация с LDAP-каталогом, то будет проверяться именно эта запись. Запись без суффикса comp1 проверке подвергнута не будет.

Конфигурация сторожа (USKGuard)

Для правильной работы функции контроля за работоспособностью, требуется учетная запись пользователя имеющего права администратора на машинах подконтрольных. Под этой учетной записью с центрального сервера происходит опрос и экзаменация «живости» клиентской части. В случае отрицательных выводов под ней-же происходит удаленное восстановление клиентской части.

Клиентская часть тоже обладает встроенным механизмом обеспечения работоспособности. Для него не требуется специальной учетной записи. В случае обнаружения проблем, подконтрольная машина самостоятельно полностью разрушается (метод мгновенного синего экрана смерти BSOD) предотвращая нежелательные действия пользователя.

После запуска USKGuard проверяет на «живость» всех клиентов, которые давно не выходили на связь с сервером. Для каждого клиента используется интервал heartbeat указанный в конфигурации группы в которую он входит.

Файл конфигурации **uskguard.xml** может содержать специальные параметры у узла uskguard.

Атрибут loglevel. Принимает значения от 1 до 10. Позволяет настроить уловень логирования сообщений в usk.log. По-умолчанию уровень логирования 6.

Атрибут cleanupdays. Принимает значения от 0 до 360. Позволяет включить автоматическую очистку всех старых событий запуска приложений из базы данных старее указанного кол-ва дней (устарело и функционал будет удален).

Атрибут serviceflsize32 и serviceflsize64. Размер в байтах клиентского агента uskclientsvc.exe для 32х битной и 64х битной версий. Включает механизм верификации, автовосстановления и поддержания версионности агента.

Атрибут reinstallalways=”true”. Форсирует авто-переустановку клиента всегда в случае отсутствия отклика от клиента, не делая никаких дополнительных проверок. Делать это рекомендуется только в *крайних* случаях!

Атрибут timeout. (опциональный) Изменяет умолчательное время ожидания окончания всех проверок для всех хостов.

Атрибут fqdnfilter. (опциональный) Включает режим проверки только хостов, у которых имя удовлетворяет указанной маске. Это позволяет иметь для каждого отдельного домена свой инстанс сервиса и запускать его через штатный планировщик заданий ОС. (упрощает управление жизненным циклом используемой учетной записи ОС).

Установка клиентского агента

Клиентскую часть (*usksetup.exe*) можно любыми доступными способами устанавливать на машины.

- Используя решения по автоматизации обслуживания компьютеров – MS SCCM, Symantec Altiris, IBM LanDesk).
- Используя встроенный механизм развертывания через USKGuard. Через консоль администратора (Главное меню –> Добавить клиента).
- Можно инициировать установку запустив от учетной записи имеющей административные права файл *usksetup.exe* .

Поддерживаются ключи командной строки:

- Для «тихой» установки следует запускать с ключом /S. Никаких диалоговых окон клиент в этом случае не показывает и устанавливается в silent-режиме.
- Ключи /h *имясервера* /p *портсервера*. Позволяет указать изначальный сервер, который будет обслуживать данного клиента. Если не указывать этих параметров, то в Silent-режиме будут использованы параметры по-умолчанию uskbyddn DNS-имя и порт 8880. А инсталляция в режиме диалога – сделает запрос настроек.

В случае успеха errorlevel-код будет установлен в значение 0, в случае отсутствия VC Runtime - 1068, в случае отсутствия необходимого минимального уровня ОС -1.

Клиентский агент уведомлений запускаемый в контексте каждого залогинившегося пользователя может показывать во всплывающих уведомлениях изображение (иконку) вашей компании. Для этой функции необходимо в конце вашей процедуры развертывания клиента «подкладывать» в каталог с файлом uskcliui.exe два ресурса: *branding.png* и *branding.ico* . Первый файл используется на ОС Windows 8.1 и выше, а второй в более старых ОС.

Обновление клиентской части

Модуль серверной защиты (USKGuardPart) умеет обновлять клиентский агент в ходе цикла проверок его работоспособности. Для этого ему требуется указать размер правильный файлов uskclientsvc.exe для 32х и 64х разрядных версий клиента. (См. настройки uskguard).

Начиная с версии клиента 3.7 он может самостоятельно по команде сервера обновлять себя сам.

Конфигурация клиента (USKClient)

Клиентский агент, можно конфигурировать изменяя его системные настройки поведения. Изменения будут применены после очередного сеанса связи с сервером.

heartbeat – указывает в секундах время через которое клиент будет считаться «неактивным» и попадать под проверку живости (если стоит соответствующая галка в свойствах клиента). Интервал значений *10…1800* секунд (другими словами от 10ти секунд до 30минут). Не следует указывать интервал слишком коротким т.к. во время перезагрузки клиентского компьютера система может ошибочно посчитать что клиент – недоступен.
Максимальное время, через которое клиент синхронизирует с сервером изменившуюся конфигурацию равен времени *heartbeat*.
Для предотвращения перегрузки сервера множеством клиентов, интервал у каждого клиента будет выбран псевдослучайно, но не больше указанного.

Метод отслеживания. Позволяет выбрать каким именно образом клиент будет следить за созданием и завершением процессов.

1. WMI (безопасно). Будет использоваться безопасный асинхронный метод получения событий.
2. WMI. Будет использован полу синхронный режим.
3. Через Ядро ОС. Самый быстрый способ получения информации, но требующий больше ресурса CPU.

BSoD если убит –Включать систему самозащиты клиента. При попытке умышленно завершить процесс, компьютер мгновенно ловит «синий экран» с ошибкой.

Тип ограничения. Позволяет задать каким образом будет организовано блокирование нежелательных приложений:

- Soft. Блокировка процесса наступит асинхронно по мере его оценки. Важно отметить что процесс не будет «заморожен» и все манипуляции будут происходить в фоне. Это обеспечит отсутствие любых задержек запуска процессов.
- Hard (FS). Переводит клиента в режим жесткого предотвращения попыток исполнения запрещенных приложений. В этом режиме загружается специальный драйвер, через который проходят анализ _все_ запускаемые на системе приложения со всех носителей. В отличие от обычного режима – процесс с запрещенным приложением даже не сможет стартовать. Но при этом стоит учитывать, что нагрузка на систему будет больше (это аналогично работе антивирусных программ). *Данный способ игнорирует условия execparams, proccurdir, sessiontype*.

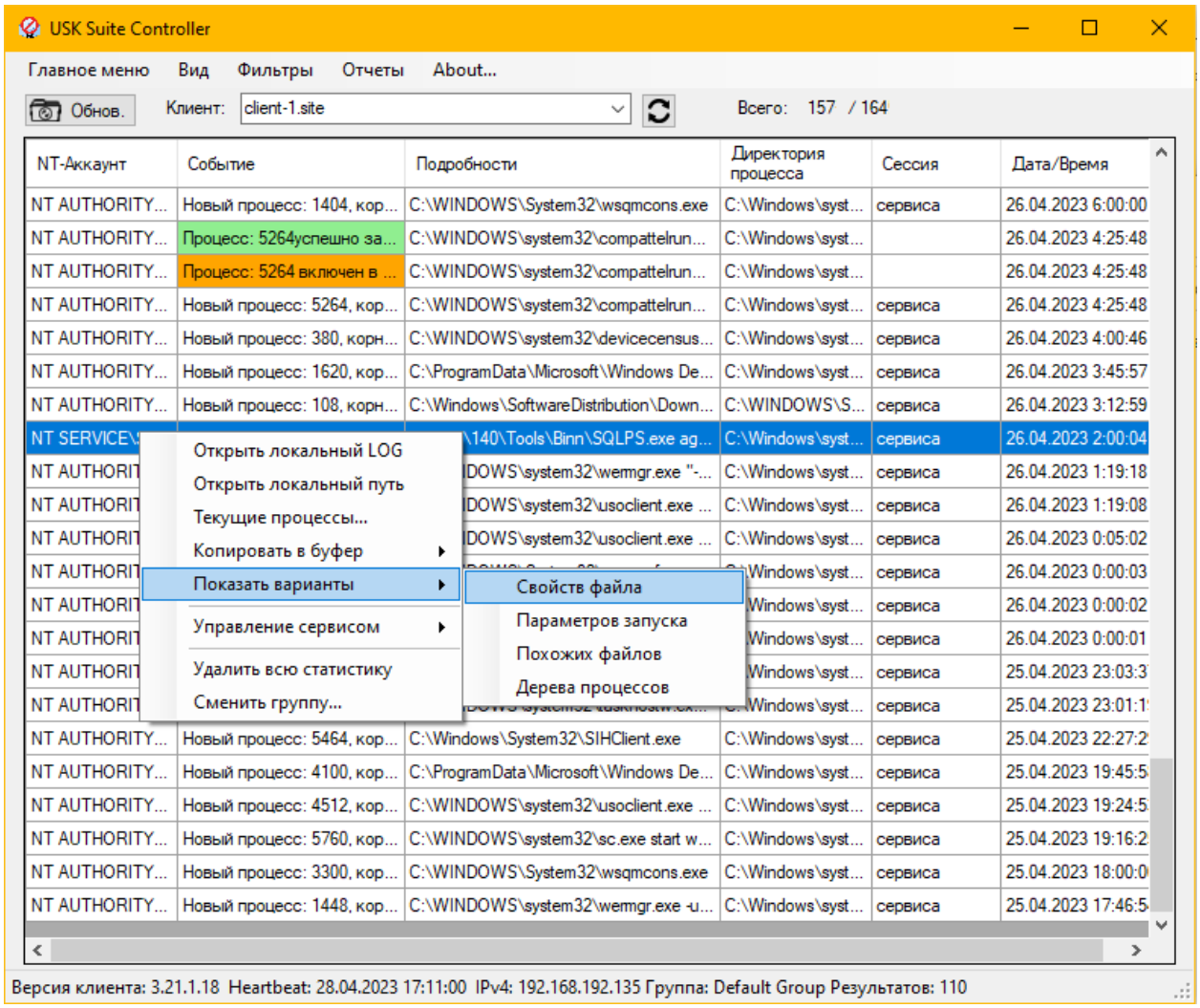
Авто-анализ новых процессов. Включает в агенте возможность автоматического анализа запускаемых в первый раз файлов синхронно с их исполнением. Это сокращает конечное время получения сведений подробных о процессе. Если файл уже был проанализирован клиентом ранее и не изменялся на диске, то повторно он не будет анализироваться. Это экономит ресурсы как клиента, так и сервера.

Ограничить доступ. Включает возможность менять настройки сервиса только для указанных учетных записей или групп.

info@softdev.online

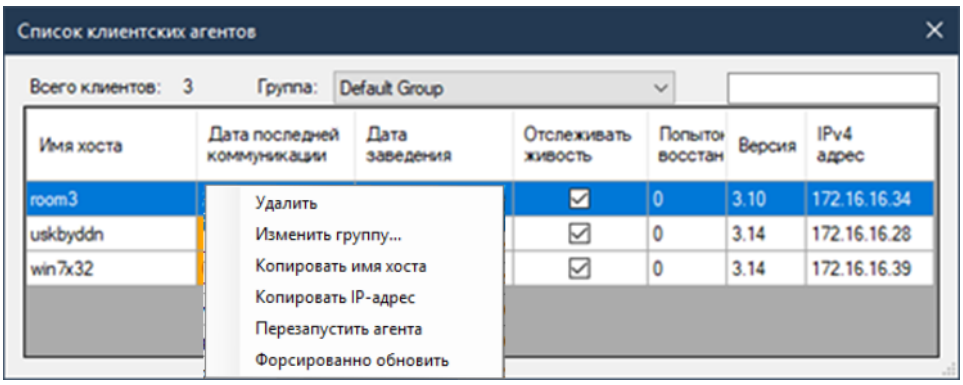
Работа с консолью администрирования

При запуске консоли появится окно авторизации на SQL сервере и в случае успешного логина на экране появится центральное окно:



В центральном месте окна будет основной список содержащий информацию, поступающую от клиентского агента выбранного. Сверху окна можно выбрать клиентский агент. Контекстное меню открываемое по щелчку мышки позволяет быстро выполнить базовые операции.

Выбрав в главном меню сверху окна пункт «Клиенты...» можно вызвать окно отображающее список всех клиентских агентов в выбранной группе. Окно отображает не только их имена, но еще и версию, статус наличия в LDAP-каталоге (если для данной группы была активирована синхронизация), IP-адрес и даты коммуникации последней с агентом, а также заведения записи.

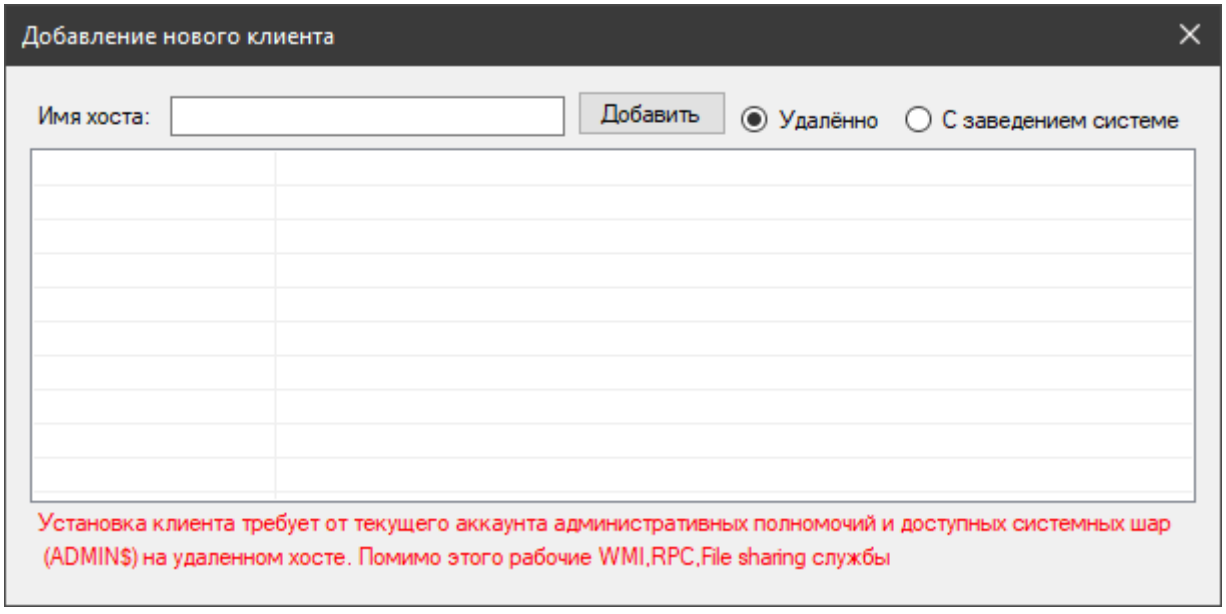


Сверху слева есть полоска ввода поискового фильтра результатов. Поиск поддерживает wildcard-символ *.

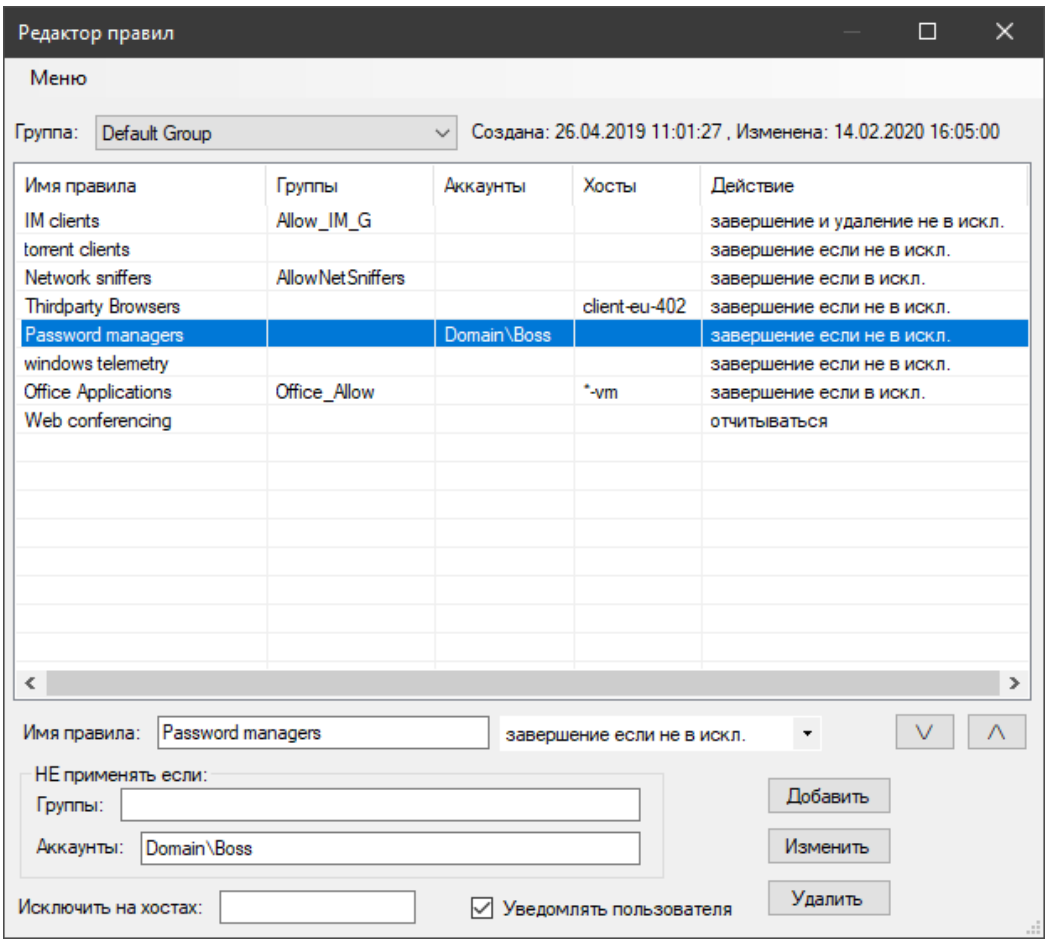
Используя контекстное меню, вызываемое мышкой, можно совершать операции:

1. перемещать в другую группу
2. удалять
3. форсировать переустановку агента
4. перезапускать агента
5. копировать имена хостов
6. Копировать IP-адреса хостов

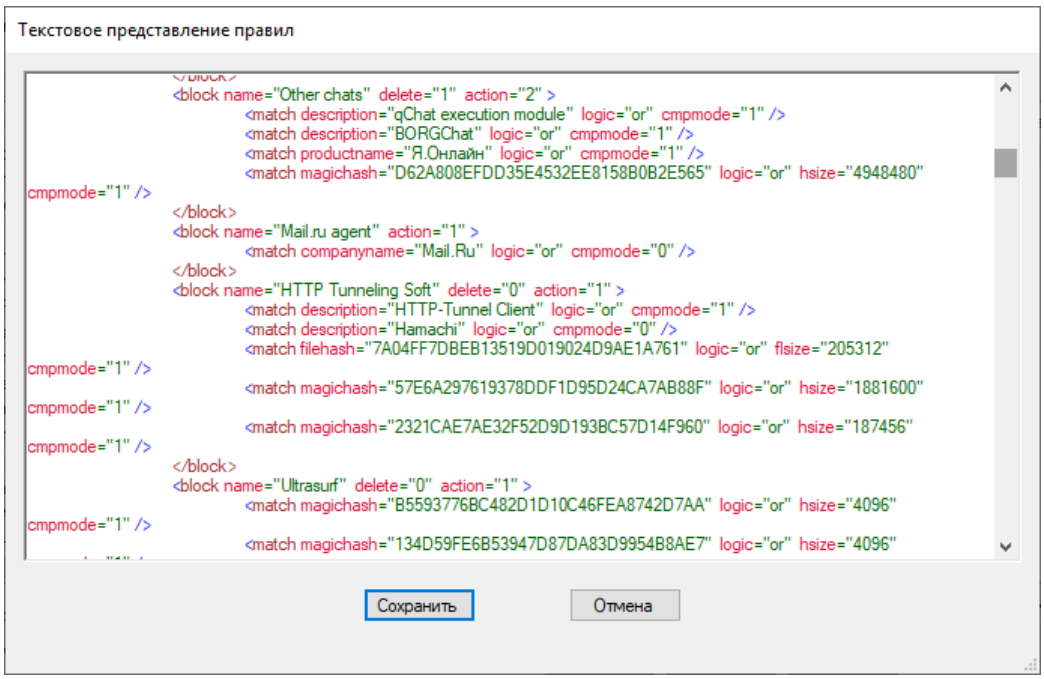
В главном меню так-же доступен пункт «Добавить клиента…» позволяющий установить клиентского-агента на выбранный компьютер указав его сетевое имя.



Щелкнув в верхней полоске главного меню на пункт «Редактор правил», мы запустим окно, позволяющее управлять правилами и политикой клиентских агентов.



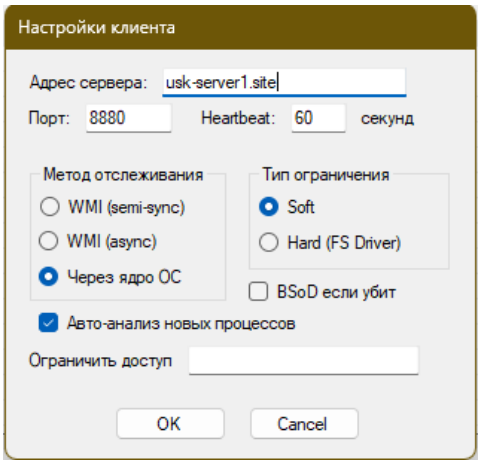
Выбрав в меню сверху пункт «В виде текста (advanced)» откроется окно с текстовым представлением всей политики и правил у выбранной группы.



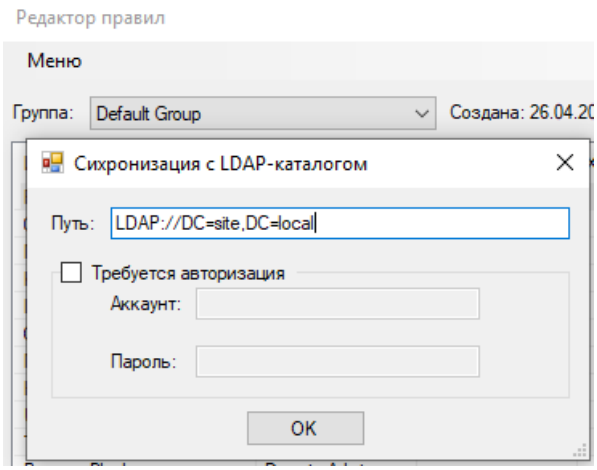
Это позволяет вручную скопировать, отредактировать интересующие правила или всю политику целиком.

Поскольку это прямое редактирование стоит быть особенно осторожным!

Выбрав в верхнем меню пункт «Дополнительные опции» можно сконфигурировать опции, относящиеся к клиентским агентам в выбранной группе. Подробно они рассмотрены в главе «Конфигурация клиента».

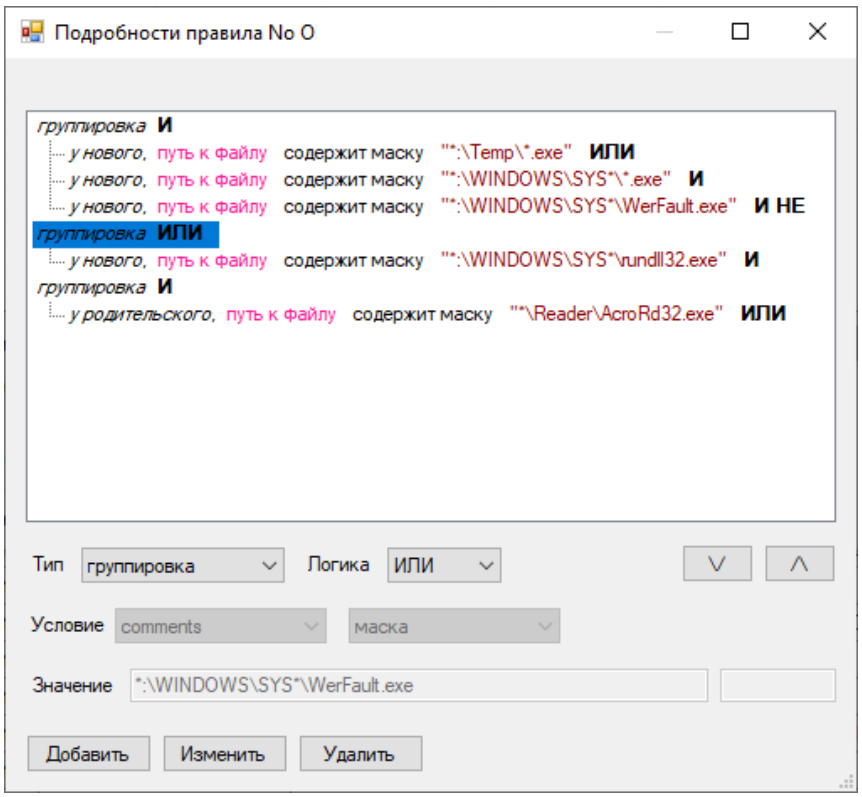


В главном меню также можно включить синхронизацию выбранной группы с LDAP-каталогом.



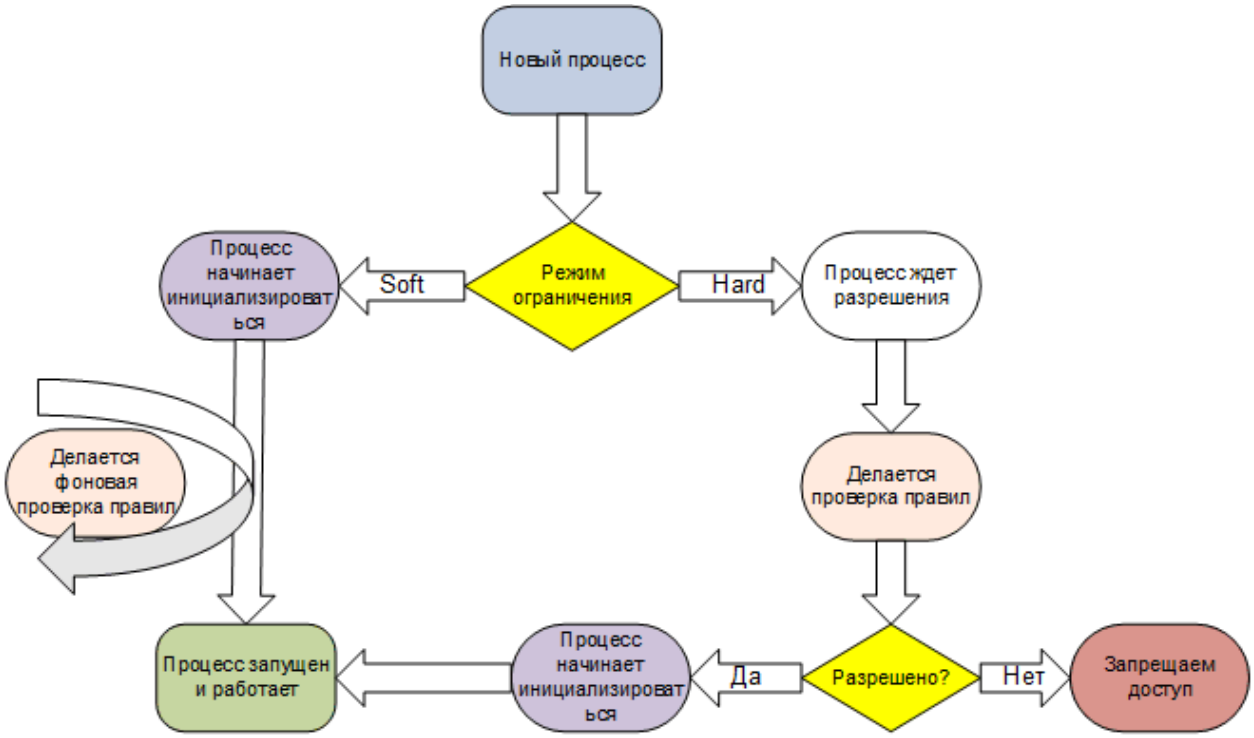
После включения синхронизации, раз в сутки будет производится проверка наличия или отсутствия указанных учетных записей компьютеров в указанном пути. В случае отсутствия – запись клиентского агента будет подсвечиваться в консоли красным и статус в списке всех клиентов изменится на «отсутствует в каталоге».

Двойной клик мышкой на каждом из названий правил открывает удобный редактор с подробностями всех условий правила. Отсюда можно добавить новое условие, удалить существующее, переместить вверх\вниз (поменяв таким образом логику обработки всего блока клиентом), отредактировать свойства.



Механизм правил

При создании каждого нового процесса, клиентский агент системы проводит проверки правил действуя двумя путями, конфигурируемыми на уровне группы где, числится клиент.
Общий вид процесса проверки правил представлен на диаграмме ниже.



Виды условий, применяемые в правилах:

1. Тэг VS_FILEINFO. Если он присутствует в файле, то становятся доступными для проверки условия: *comments*, *companyname*, *productname*, *description*, *internalname*, origfilename, copyright, trademark, *fileversion*, *productversion*
2. Условие *filehash* – хэш файла и его размер (для ускорения получения результата).
3. Условие *magichash* – «интеллектуальный» хэш и его размер. Уникальная технология. Позволяет более быстрым и эффективным способом блокировать нежелательные исполняемые файлы вне зависимости от попыток пользователя поменять содержимое этих файлов (например, тэг VS_FILEINFO или ресусы). Например, при размере EXE файла в 1 мегабайт, «анализу» будет подвергнуто примерно 100кб. Т.к. этот способ более экономный. Минусом, является требование создания правила на каждую новую версию запрещаемого приложения.
4. Условие *mmhash* – хэш критических частей файла и размер файла. Дальнейшее развитие «интеллектуального хеша». Позволяет еще более быстрым и эффективным способом блокировать\разрешать определенные исполняемые файлы. *Является приоритетным (и рекомендуемым для использования вместо MD5 и magichash*.
5. Условие *filepath*. Полный путь до исполняемого файла включая его имя.

6. Условие *execparams*. Параметры, передаваемые исполняемому файлу (командная строка). Следует использовать с аккуратностью и соединять его в блоке с другими условиями.
7. Условие *proccurdir*. Текущий путь процесса при его создании. Он аналогичен столбцу в консоли «Директория процесса».
8. Условие *sessiontype*. Тип сессии в которой был создан процесс. Всего 5 типов. Позволяет создавать правила, контролирующие запуск определенных процессов только в определенных сессиях (1. только сервиса, 2. только консольная, 3. активная консольная сессия, 4. Только удаленная сессия, 5. Активная удаленная сессия).
9. Условие *authcodepolicy*. Проверка наличия и доверия ОС к цифровой подписи файла (Autheticode). Всего 8 типов условий

9.1. Нет сигнатуры подписи вообще. Считаем это «нормальным»
9.2. Полностью прошла проверки. *Из проверок исключены: Таймстампинг (считается вечно валидным) и отзыв сертификата (требует много времени т.к. связан с сетью)
9.3. Хеши не совпадают (кто-то изменил намеренно или случайно файл)
9.4. Подпись явным образом была запрещена
9.5. У ОС нет доверия Subject'у
9.6. Истек сертификат
9.7. Нарушена цепочка доверия
9.8. Все остальные ошибки

10. Если цифровая подпись (Autheticode) присутствует у файла то добавляются еще 5 условий проверки сертификата подписи: *certthumbprint* , *certserialnumber* , *certsubjname* , *certprogname* , *certissuername*. Важно отметить что у файлов с двойной подписью проверяется только первая по счету подпись!

Каждое условие имеет различные типы сравнения с эталоном:

1. Если условие содержит тэг *fileversion* или *productversion* то:

1.1. Больше. Версия файла (формата x,y,z,w) должна быть больше указанной.
1.2. Меньше. Версия файла (формата x,y,z,w) должна быть меньше указанной.
1.3. Соответствует. Версия файла (формата x,y,z,w) должна быть равна указанной.
1.4. Маска. Версия файла, любого формата должна быть похожа на указанную (wildcards).

2. Если условие содержит *certthumbprint* , *certserialnumber* , *certsubjname* , *certprogname* , *certissuername* , *filehash* , *magichash* , *mmhash* то доступны только «Соответствует».
3. В остальных случаях доступны следующие типы сравнений:

3.1 Содержит. *Регистрозависимо*. Ищется подстрока в строке.
3.2 Соответствует. *Регистрозависимо.* Ищется полное соответствие строк.
3.3 Маска. *РегистроНЕзависимо*. Ищется соответствие по wildcards маске (символы * и ?)

Каждое условие содержит одну логическую операцию которая будет выполнена над результатом «оценки» условия (т.е. выполнится после обработки условия):

1. И. Логическое «И»
2. ИЛИ. Логическое «ИЛИ».
3. И НЕ. Логическое «И НЕ».

Каждый тип сканирования может включать неограниченное число блоков. Блок - это контейнер правил. Количество правил в блоке также не имеет ограничений. Если проверяемый файл "попадает" под правила блока - файл может остаться в живых если в блоке, присутствуют AD-исключения и пользователь запустивший процесс входит в указанный список групп или аккаунт пользователя входит в «белый список». Имена групп исключений, аккаунтов и хостов разделяются запятой или точкой с запятой (,;). Число таких групп - неограниченно.

В списках исключений из правила система «понимает» локальные группы и членство в них доменных или локальных учетных записей. Т.е. если локально на каком-то компьютере создать группу group1 и включить в неё учетную запись доменную или локальную – можно указать её в исключениях, и она будет применяться. При указании только имени группы (без домена или компьютера) поиск будет выполняться в очередности 1. Локальный компьютер 2. Домен Active Directory. Можно указывать имя компьютера или домена перед именем группы и тогда правило исключений будет срабатывать только на доменную группу или локальную группу определенной машины. Вместо человеческого именования группы можно указывать её SID (Пример: S-1-5-18). Это позволяет работать на мультиязычных ОС где языком по-умолчанию установлен не Английский язык.
Аналогичная ситуация с именем аккаунтов.

Правила проверяются в блоке последовательно: с самого первого (верхнего) до самого последнего (нижнего) используя логические условия операций (**И**, **ИЛИ**, **И НЕ**). Если встретилось соответствие какому-либо правилу – дальнейшие блоки после него уже не обрабатываются. Есть возможность группировок условий в пределах одного правила с глубиной вложенности не больше 1-го.

Используя типы проверок *fileversion* или *productversion* можно проконтролировать что используемое ПО имеет минимально необходимую нужную версию (не старее какой-то). Или наоборот.

Клиентский агент автоматически синхронизирует правила в момент очередной коммуникации с сервером (какое-либо событие, срабатывание правила, ошибка, создание процесса и т.п.), или если ничего не происходит, то через время, указанное в настройках группы клиента *heartbeat*.

Поддерживается 5 типов действий после срабатывания соответствующего правила блока:

- **Отчитаться** на сервер о найденном соответствии
- **Отчитаться и завершить форсировано процесс** если аккаунт запустившего не является членом групп либо не входит в список аккаунтов.
- **Отчитаться, завершить форсировано процесс и удалить** с носителя где он был расположен EXE-файл если аккаунт не является членом групп либо не входит в список аккаунтов.
- **Отчитаться и завершить форсировано процесс** если аккаунт является членом групп либо входит в список аккаунтов.
- **Отчитаться, завершить форсировано процесс и удалить** с носителя где он был расположен EXE-файл если аккаунт является членом групп либо входит в список аккаунтов.

Если в правиле указать хосты-исключения, то соответствующий блок НЕ будет обрабатываться на компьютерах, у которых DNS-имя (короткое!) соответствует указанному. В именах компьютеров могут применяться символы wildcards для соответствия по маске.

Клиентский агент может отображать пользователю предупреждение о недопустимости нарушений политик безопасности запуская запрещенные процессы. Для этого в редакторе правил у каждой группы можно поставить галку напротив «*Уведомлять пользователя*». В таком случае завершая процесс\удаляя файл, пользователю в его сессии будет выведено уведомление. Это поможет пользователю ориентироваться и понимать происходящее.
* - Для этого функционала у пользователя должен быть запущен в его сессии uskcliui.exe

Меняя очередность следования блоков правил и применяя разные типы действий можно добиться необходимого вам, гибкого, функционала.

События, создаваемые клиентским агентом, имеют цветовую раскраску в консоли для обеспечения лучшей визуализации важности событий.

- События **красных** оттенков свидетельствуют о наличии каких-либо ошибок в работе агента
- События **зеленых** оттенков говорят о статусе того или иного действия агента (например, старт и стоп агента)
- События **оранжевых** оттенков говорят о срабатывании правил

Tips and Tricks (советы по использованию)

Как правило, из практики, для большинства (98% клиентов) хватает опций по-умолчанию (т.е. все галочки сняты). Для остальных клиентов создается отдельная группа с правилами и дополнительными флагами конфигурации клиента.

Есть класс приложений, исполнение которых разделено на части, исполняющиеся под разными аккаунтами. К примеру, VirtualBox. Для его работы под пользовательским аккаунтом запускается одна часть П.О. и в результате действий пользователя при старте машин запускается сервис системного уровня (системный аккаунт). В этом случае исключение стоит делать либо на конкретные хосты, либо вариант с выносом таких клиентских машин в отдельную группу где нет самого правила «запрещающего».

При отображении в консоли полного пути и параметров процесса используется «склеивание» пути процесса и его параметров. При этом стоит учитывать, что клиентский агент «видит» этот весь путь - раздельно. Это важно при создании правил. Например, в консоли вы видите:
"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe" /WatchService
Это означает что путь к процессу C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe. А параметры процесса это /WatchService.

info@softdev.online

Утилита командной строки (pk-config.exe)

В комплекте консоли администрирования есть утилита командной строки **pk-config.exe** .
Если нужно быстро смоделировать ситуацию гипотетическую с запускаемыми (синтетически) процессами и обработкой политики правил или проведения анализа исполняемых файлов, то эта утилита станет вашим незаменимым помощником.
Синтаксис: pk-config.exe <действие> <child_executable_file> [<child_params> <parent_executable_file> <parent_params>]

Аргументы:
<действие> - либо *check* , либо *listprop*. Первый вариант производит проверку по списку правил из файла pk-conf.xml заданных аргументов. Второй вариант производит оценку свойств указанного в следующем аргументе исполняемого файла.
<child_executable_file> - Задает имя (если нужно то с полным путем) исполняемого файла для анализа свойств либо для проверки соответствия правилам.
<child_params> - Указывает синтетические параметры командной строки в ходе эмуляции запускаемого файла.
<parent_executable_file> - Задает имя «родительского» процесса по отношению к первому исполняемому файлу.
<parent_params> - Указывает синтетические параметры командной строки для эмуляции. Они относятся к «родительскому» процессу.

Для выполнения оценки свойств (*listprop*) должен быть указан только один аргумент – файл исполняемый, а для выполнения симуляции (*check*) должны быть заданны все параметры. Двойные "" кавычки указывают на его отсутствие.

info@softdev.online