Avira AntiVir

Security Management Center

Содержание

1 Об этом руководстве

1.1 Введение

В этом руководстве мы собрали всю необходимую информацию о AntiVir Security Management Center (SMC).

Дополнительную информацию и помощь предложат Вам наш сайт и тех. поддержка.

Ваша команда Avira

1.2 Структура данного руководства

Это руководство состоит из нескольких глав по следующим тематикам:

Глава	**Содержание**
1 О данном руководстве	Структура руководства, знаки и символы
2 Информация о продукте	Обзор основных возможностей
3 Установка	Важная информация по установке
4 Avira SMC Frontend	Обзор Avira SMC
5 Настройка	Настройка Avira SMC
6 Управление	Работа с Avira SMC
7 Обновление продуктов	Методы обновления продуктов Avira в SMC
8 Решение проблем	Методы решения и устранеия проблем Avira SMC
9 Продукты поддерживаемые Avira SMC	Продукты поддерживаемые Avira SMC
10 Сервис	Тех. поддержка Avira

1.3 Знаки и символы

В этом руководстве используются следующие знаки и символы:

Символ	Расшифровка
✓	... стоит перед условием, которое должно быть выполнено перед выполнением определенного действия
►	... стоит перед действием, которое Вы выполняете
↳	... стоит перед результатом произведенного действия
	... стоит пред предупреждением об опасности критической потери данных или повреждения аппаратной части
	... стоит перед советом с особо важной информацией, например, о дольнейших действиях
	...стоит перед советом, который облегчает понимание и использование консоли управления

Для лучшей читаемости и однозначного обозначения в тексте используются следующие выделения:

Выделения в тексте	Расшифровка
C:\AntiVirData	Имя файла и путь
Выбрать компоненты Отметить всё	Элементы программной оболочки, такие как пункты меню, заголовки окон, рабочие поверхности в диалоговых окнах
http://www.avirus.ru	URLs
Знаки и символы – стр…	Перекрестные ссылки в документе
Setup.exe /remove	Команды и редактируемые тексты в файлах

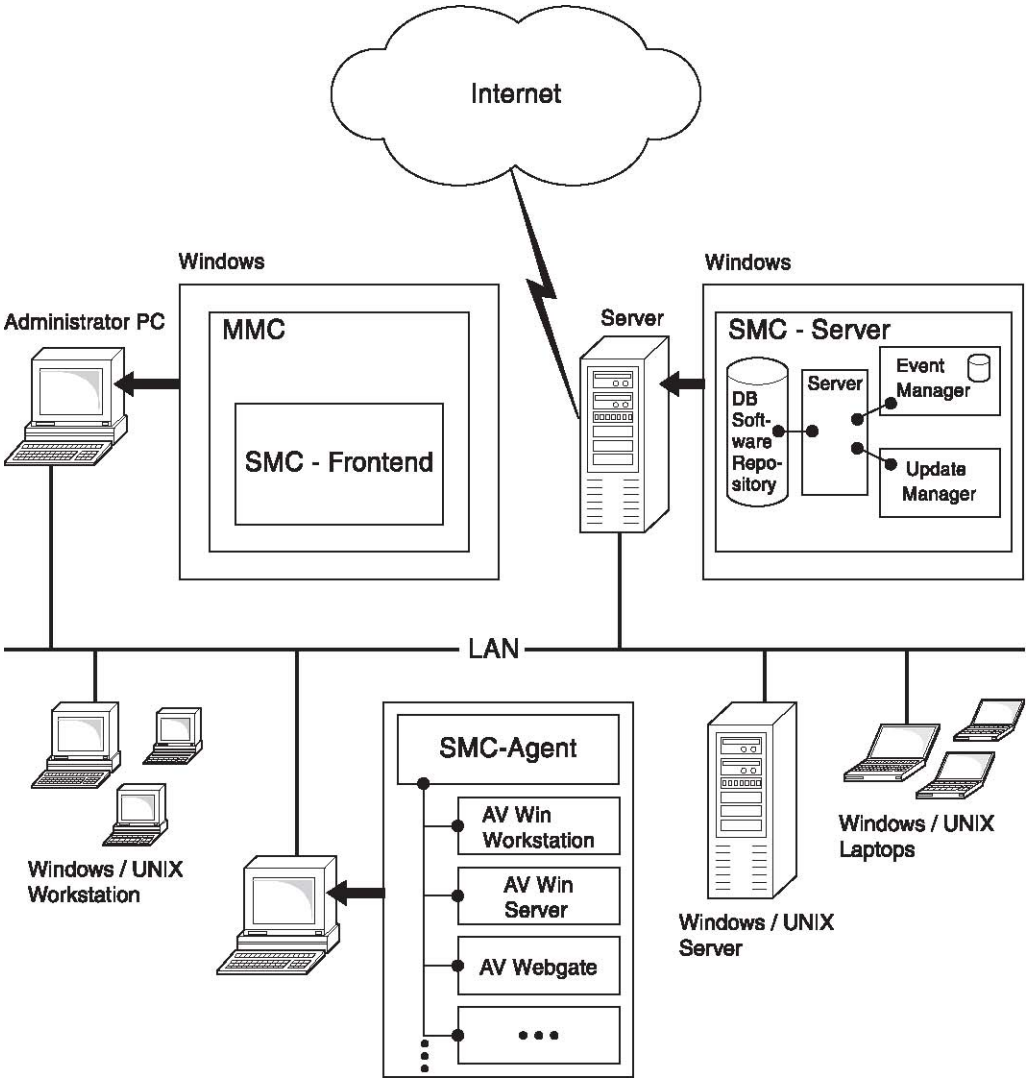
1.4 Сокращения

В данном руководстве используются следующие сокращения:

Сокращение	Значение
DHCP	Dynamic Host Configuration Protocol (протокол для динамического распределения IP-адресов хосту)
GUI	Graphical User Interface (графический пользовательский интерфейс)
MMC	Microsoft Management Console (консоль управления Microsoft)
TCP/IP	Transmission Control Protocol/Internet Protocol (протокол коммуникации между ПК)
SFX	Self Extractable program (самораспаковывающаяся программа)
SMC	AntiVir Security Management Center
SMTP	Simple Mail Transfer Protocol (TCP/IP-протокол для передачи сообщений)
SSL	Secure Socket Layer (алгоритм шифрования)
IUM	Avira Internet Update Manager
MMC	Microsoft Manegement Console

2. Информация о продукте

AntiVir Security Management Center (AntiVir SMC) служит для удаленной установки и управления продуктами AntiVir в сети.



Компоненты и службы

AntiVir SMC состоит из 3 компонентов:

- SMC-Server (3 службы), который работает на центральном сервере в сети:

– Server
– Event Manager (менеджер событий)
– Update Manager (менеджер обновлений)
– и две интегрированные базы данных для хранения продуктов AntiVir и управления событиями

- Службы SMC-Agent, которая работает на ПК в сети и обеспечивает связь между SMC-Server и продуктами AntiVir на ПК
- Графического пользовательского интерфейса SMC-Frontend, который установлен на ПК администратора и управляет службами и компонентами AntiVir SMC

2.1 Возможности

Avira SMC может управлять и контролировать все ПК в специальном окружении безопасности **Security Environment** сети компании (рабочие станции Windows и Linux и сервера). Компьютеры интегрируются в окружение безопасности **Security Environment** в виде настраиваемой древовидной структуры и иерархических групп.

Наиболее важные функции Avira SMC:

Настройка безопасного сетевого окружения:

• графический пользовательский интерфейс для настройки и управления Avira SMC (выполнено в виде snap-in для Microsoft Management Console);
• Скрытая установка SMC Agents по сети;
• Удаленная установка, настройка и удаление продуктов Avira на всех компьютерах сети;
• центральное хранилище продуктов Avira для сетевой установки;
• управление пользователями для добавления и контроля пользователей и их прав доступа;
• резервное копирование серверных файлов;
• использование протокола шифрования SSL;
• поддержка ПК с динамическими IP адресами (DHCP).

Управление продуктами Avira по сети:

• централизованное управление действиями характерными для каждого продукта (сканирование, обновление…) при помощи настраиваемых команд и задач;
• общий доступ к файлам / файлам лицензий и запуск удалённо программ из общей директории SMC Server;
• сохранение запланированных задач (установка, настройка, команды) для ПК временно недоступных в сети.

Обновление продуктов Avira software по сети:

• централизованное автоматическое обновление поддерживаемых программных пакетов и компонентов Avira SMC, используя Internet Update Manager;
• мониторинг статуса продуктов;
• централизованная команда обновления для установленных продуктов Avira, при помощи Internet Update Manager или планировщика;
• тестовый режим обновления до использования обновлений в сети.

Контроль активности продуктов Avira в сети:

• **Alert manager** используется для рассылки предупреждений по сети и электронной почте;
• настраиваемые отчеты сетевых продуктов Avira;
• централизованный обзор всех событий и отчётов, создаваемых продуктами Avira в сети.

2.2 Принцип действия

Главное приложение SMC-Server включает три службы с различными функциями, которые соединяются при помощи шифрованных SSL TCP/IP-соединений.

Служба Server управляет информацией:

- О компьютерах, которые включены в окружение безопасности AntiVir SMC
- О продуктах AntiVir установленных и
- О программных пакетах, хранящихся в AntiVir SMC.

Программа установки продуктов AntiVir на ПК в сети через AntiVir SMC обращается к внутренней базе данных, в которой продукты AntiVir хранятся в виде программных пакетов. Продукт AntiVir на ПК в группе безопасного окружения принимает при установке настройки, которые уже были определены для даной группы в SMC.

Служба **Event Manager** (менеджер событий) получает от SMC-Agent события (например, сообщение о вирусе), сохраняет их в базе данных и предоставляет их для отображения и создания отчета в SMC-Frontend.

Служба **Internet Update Manager** проводит обновления программных пакетов и компонентов AntiVir SMC.

SMC-Agent, который установлен на ПК в окружении безопасности, направляет команды, задания и настройки главного приложения SMC-Server к продуктам AntiVir на ПК. SMC-Agent может передавать события и сообщения продуктов AntiVir на SMC-Server, который отображает их в SMC-Frontend.

SMC-Frontend – этот модуль реализован в виде Snap-In для Microsoft Management Console (MMC), интегрирует компоненты, службы и функции в графический интерфейс и наглядно представляет всю информацию.

Кроме того, в окружении безопасности через SMC-Agents на отдельных ПК и группах могут раздаваться и запускаться любые файлы (при необходимости с параметрами запуска и командами), например, специальные вирусные дефиниции, специальные утилиты удаления вирусов, файлы лицензий и т.д.

2.3 Лицензирование

Лицензирование включает два шага: приобретение лицензии и лицензирование AntiVir SMC после инсталяции. Обычно при покупке продуктов AntiVir и AntiVir SMC Вы получаете файл лицензии на CD-ROM или по Email.

При установке SMC-Agent на ПК в сети, лицензия постоянно проверяется: в случае приобретения лицензии AntiVir SMC на 500 ПК, то Вы можете объединить в окружение безопасности максимум 500 ПК, на которых установлены SMC-Agent.

Лицензирование Вы проводите после установки AntiVir SMC.

Пробный режим
Если не провести лицензирование, при каждом запуске
SMC-Frontend будет появляться сообщение, что программа будет работать 30 дней в пробном режиме. В пробном режиме можно управлять максимум 100 ПК в окружении безопасности.

2.4 Системные требования

SMC Server:
• Операционная система: Windows 2000 Server, Windows 2003 Server (x32 или x64)
• RAM: 128MB
• Дисковое пространство: 512MB (включая все продукты и файлы обновлений)

SMC Frontend:
• Операционная система: Windows 2000 (Workstation или Server), Windows XP (x32 или x64), Windows Vista (x32 или x64), Windows 2003 Server (x32 или x64)
• RAM: 32MB
• Дисковое пространство: 16MB

SMC Agent:
• Операционная система: Windows 2000 (Workstation или Server), Windows XP (x32 или x64), Windows Vista (x32 или x64), Windows 2003 Server (x32 или x64), Linux (glibc22)
• RAM: 32MB
• Дисковое пространство: 16MB

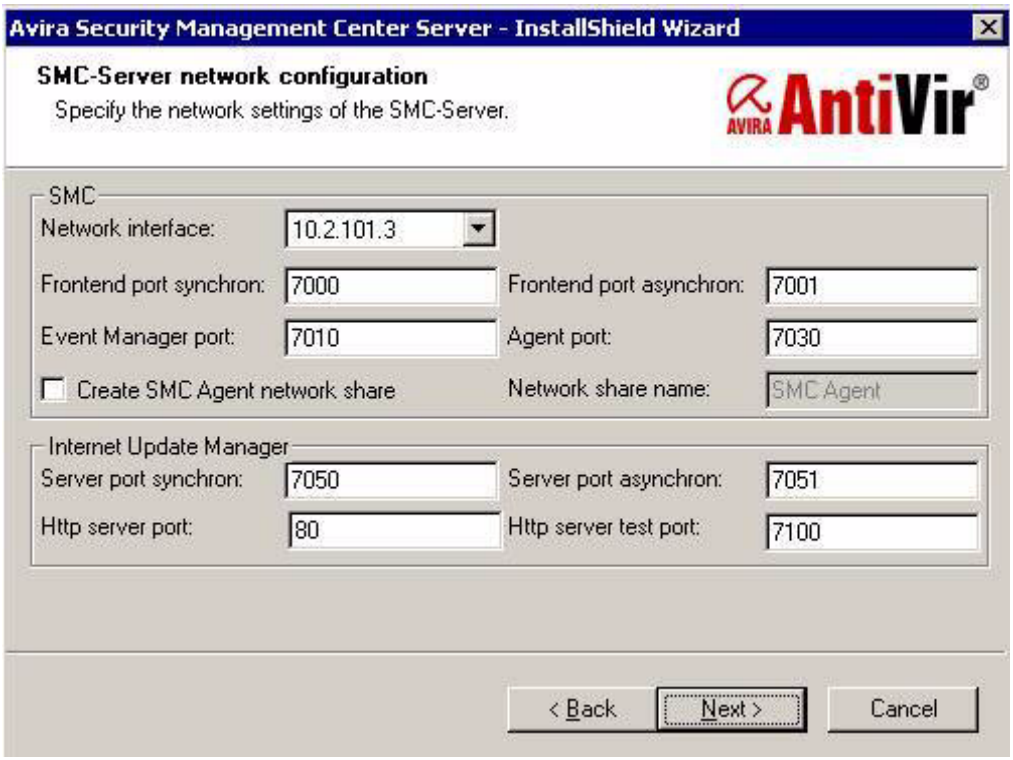
3 Установка

3.1 Что необходимо знать перед установкой

Перед установкой

Обычно AntiVir SMC со службами устанавливается на центральном сервере сети, а пользовательский графический интерфейс SMC-Frontend на одном из ПК в сети, который используется администратором. Оба компанента могут быть установлены на один ПК.

Так как службы и компоненты программы AntiVir SMC для связи используют IP-адреса и определенные открытые порты, то при инсталляции они прочитываются и отображаются в диалоговом окне.



Если Вы устанавливаете SMC-Frontend на ПК вне сети, то в FireWall, если таковой имеется, должны быть открыты следующие порты для связи с SMC-Server:

- 7000
- 7001

Если в Вашей сети IP-адреса выделяются динамически (DHCP), мы рекомендуем при установкевместо актуального IP-адреса указывать имя хоста сервера.

Шаги по установке:

- установка SMC-Server
- установка SMC-Frontend

3.2 Выполнение установки

3.2.1 Установка SMC-Server

- ✓ на сервере имеются права администратора
- ✓ Должны быть открыты порты SMC Server и они не должны использоваться другими программами: 7000, 7001, 7020, 7021, 7030, 7050, 7051, 7100.

➢ Вставьет AntiVir-CD-ROM в CD-привод на символ CD-ROM-привода

– или –

Загрузите актуальную версию AntiVir SMC с сайта AntiVir (http://www.avira.com) и распакуйте ZIP-файл в локальную папку.

➢ Дважды кликните на AntiVir-CD-ROM или в локальной папке, где распакован ZIP-архив самораспаковывающийся файл AntiVir_Security_Management_Center_Server_en.exe.

↳ Появится диалоговое окно распаковки установочных файлов и запуска установки.

➢ Кликните «Принять».

↳ Установочные файлы будут распакованы. Появится диалоговое окно InstallShield Wizard.

➢ Подтвердите **Далее**.

↳ Появится окно лицензионного соглашения.

➢ Отметьте опцию **Я согласен** и подтвердите **Далее**.

↳ Появится диалоговое окно **Каталог установки**.

➢ При необходимости выберите другой каталог установки и подтвердите **Далее**.

↳ Откроется диалоговое окно для настройки IP-адреса и портов сервера.

➢ Отметьте при необходимости опцию **Network interface** (сетевой интерфейс) и подтвердите кнопкой **Далее**

↳ Появится диалоговое окно для ввода пользовательских данных.

➢ Введите имя пользователя локальной учетной записи администратора или администратора домена и пароль для входа на этом ПК и подтвердите **Далее**.

↳ Программа готова для установки.

➢ Кликните Install.

↳ Главное приложение SMC Server, службы и база данных будут установлены. Появится диалоговое окно завершения установки.

➢ Кликните **Finish** (завершить).

↳ SMC Server установлен. Службы Server, Event Manager и Internet Update Manager запускаются на сервере.

3.2.2 Установка SMC-Frontend

- ✓ Необходимы права администратора
- ✓ Должны быть открыты порты SMC Server и они не должны использоваться другими программами: 7000, 7001, 7020, 7021, 7030, 7050, 7051, 7100
  - ➢ Дважды кликните на самораспаковывающийся файл, который расположен на AntiVir-CD-ROM или в локальной папке, куда был распакован ZIP-архив: AntiVir_Security_Management_Center_Server_en.exe.
  - ↳ Появится диалоговое окно распаковки установочных файлов и запуска установки
  - ➢ Кликните **Принять**
  - ↳ Установочные файлы будут распакованы. Появится диалоговое окно InstallShield Wizard.
  - ➢ Подтвердите **Далее**.
  - ↳ Откроется окно лицензионного соглашения
  - ➢ Отметьте опцию **Я согласен** и подтвердите **Далее**
  - ↳ Откроется диалоговое окно с указанием пути установки
  - ➢ Если необходимо, выберите другой путь установки и подтвердите **Далее**
  - ↳ Откроется диалоговое окно завершения установки
  - ➢ Подтвердите **Готово**
  - ↳ SMC-Frontend установлен. В меню ПУСК Windows созданна программная группа Antivir Security Management Center

4 Программная оболочка AntiVir SMC

Службы и компоненты AntiVir SMC управляются при помощи графической оболочки SMC-Frontend, которая сделана в виде Snap-In для MMC.

Вид, строение и структура меню MMC могут различаться в зависимости от операционной системы. Следующие данные основаны на MMC 1.2, версии 5.0 для ОС MS Windows 2000 Professional.

При наведении указателем мыши на поля ввода SMC, Вы увидите подсказку желтого цвета.

В этой главе описываются только собственные элементы SMC-Frontend.

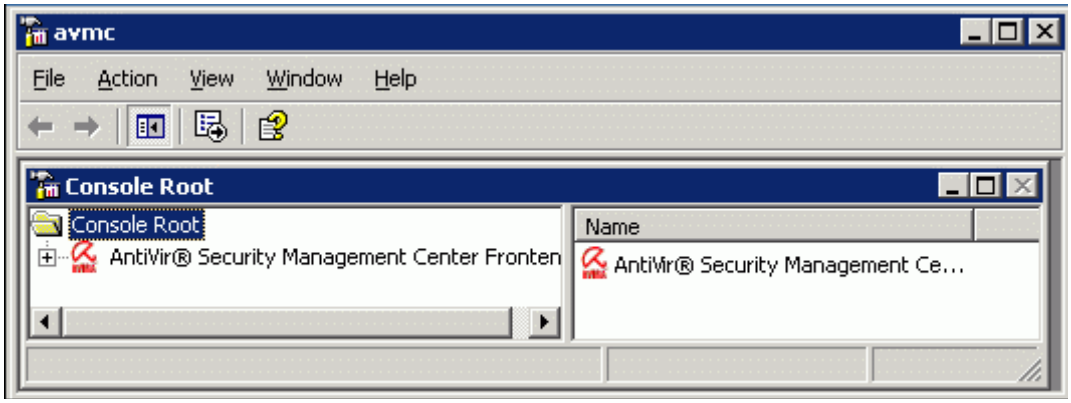
- Дополнительную информацию о MMC и ручном подключении Snap-In Вы найдете в руководстве к Вашей ОС или в Online-помощи.

4.1 Запуск SMC-Frontend и регистрация на SMC-Server

Запуск SMC-Frontend

- Выберите в меню Windows-пуск Пуск/Все программы/AntiVir Security Management Center/Management Center.

↳ Появится MMC с AntiVir SMC. Вы видите вобласти навигации сетевые узлы дерева консоли и встроенный SMC-Frontend (AntiVir Security Management Center Frontend).

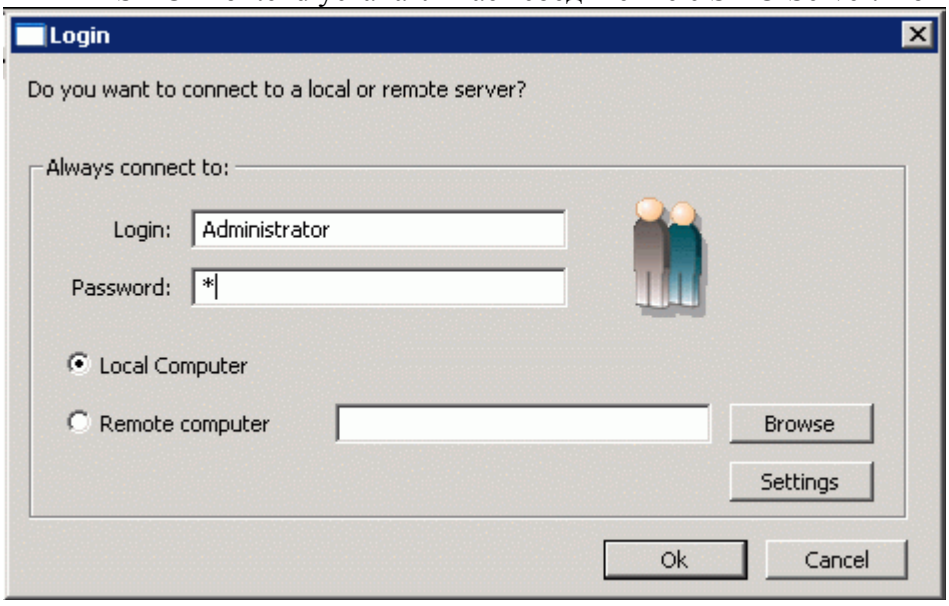


Подключение к SMC-Server

Мы рекомендуем изменить паоль после входа на SMC-Server после первой установки (см. Настройка регистрации в сети и на SMC-Server).

- Кликните на закладку **AntiVir Security Management Center Frontend**.

↳ SMC-Frontend устанавливает соединение с SMC-Server. Появится диалоговое окно входа.

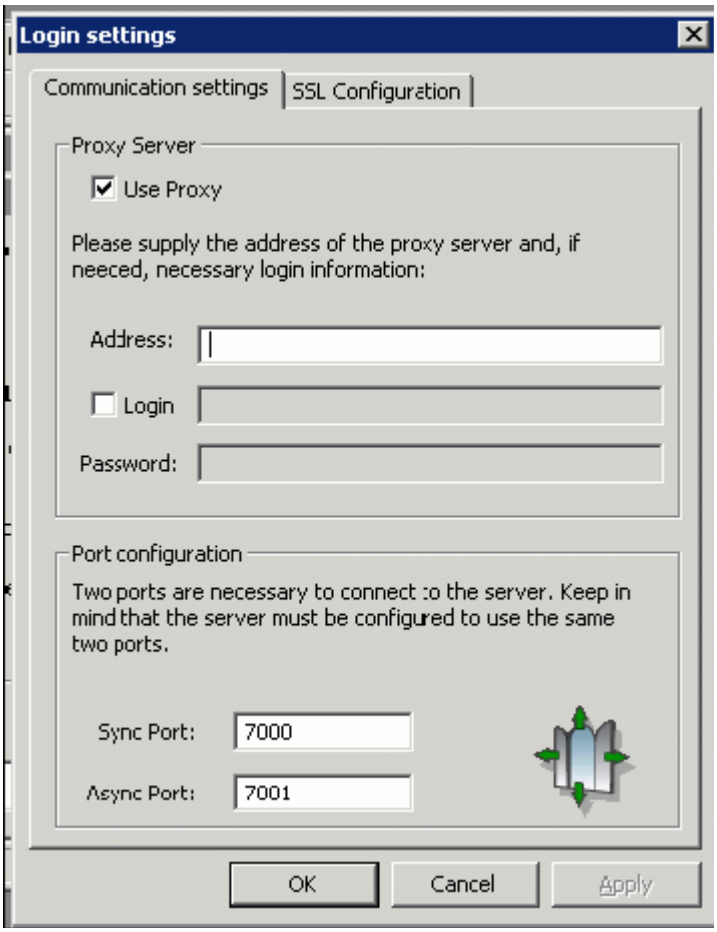


- Отметьте в зависимости от того, куда был установлен SMC-Server, локальный компьютер или компьютер в сети и выберите при необходимости при помощи **Browse (Обзор)** сервер.

Для первого входа, введите `Administrator` *для* ***username*** и `a` для поля ***password*** *подтвердите* OK.
Мы рекомендуем после установки сменить пароль для SMC

Если для Интернет-соединения сети Вы используете Proxy и при инсталляции изменили порты:

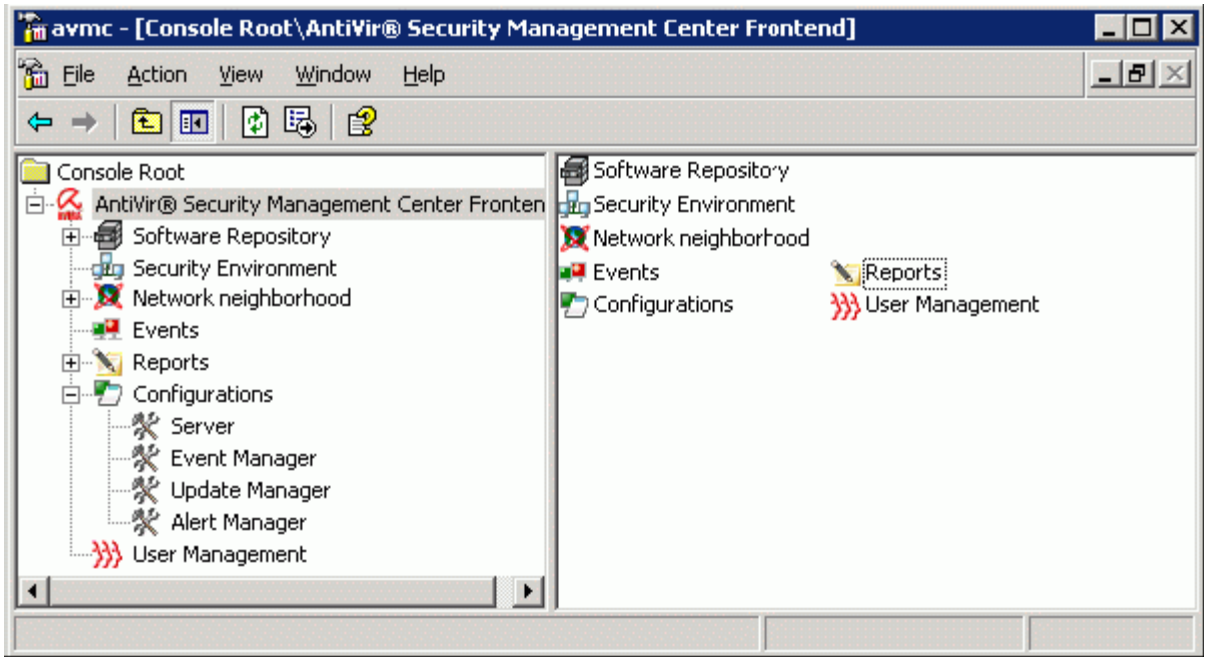
- Кликните **Settings (Настройки)**



- Выберите Use proxy и определите адрес и порты. Кликните **OK**

- При необходимости отметьте опцию использования Proxy, введите необходимые данные и подтвердите **OK**.
- При первой регистрации введите имя **Administrator** и пароль **a** и подтвердите **OK**.

↳ SMC-Frontend устанавливает соединение с SMC-Server.



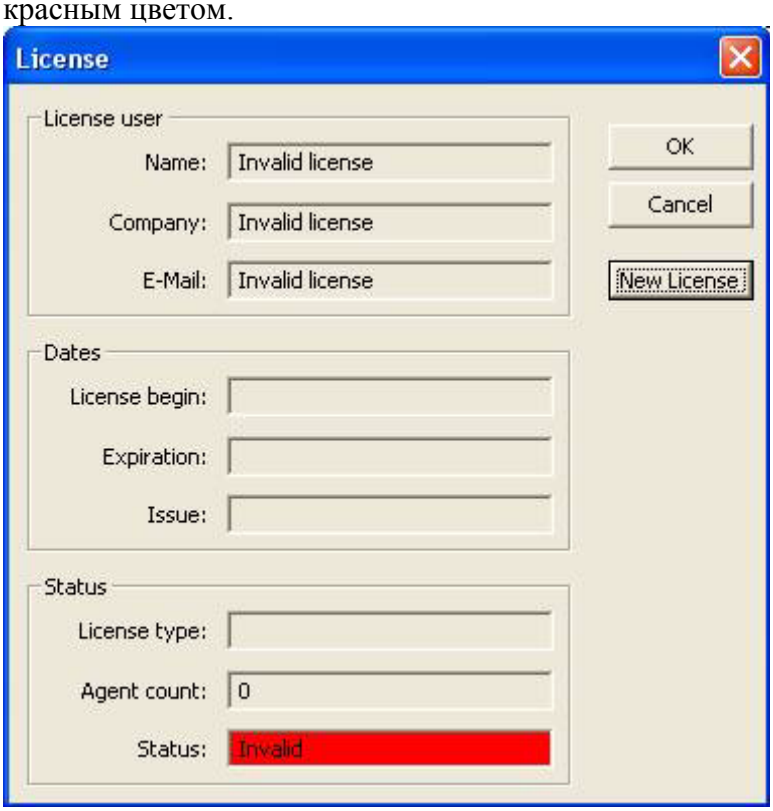
Ошибка? Нет лицензии?
Проведите лицензирование и войдите под правильным паролем.

4.2 Лицензирование AntiVir SMC

√ Установлено главное приложение SMC-Server и графическую оболочку SMC-Frontend (см. установка)
√ Имеется файл лицензии (сохранен локально)
√ Запустите SMC-Frontend войдите на SMC-Server (SMC-Frontend запуск и вход на SMC-Server).
Появится MMC с интегрированным AntiVir. Вы увидите узлы сети дерева консоли с узлами AntiVir Security Management Center.

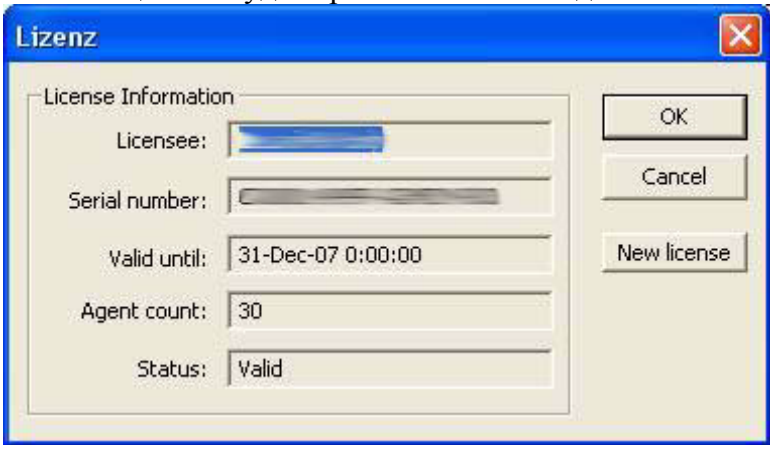
- Кликните правой кнопкой на AntiVir Security Management Center и выберите лицензия .

↳ Появится диалоговое окно лицензия, в котором поле статус будет выделено красным цветом.



- Кликните поле «Новая лицензия» New License и введите путь к файлу лицензии.
- Отметьте файл лицензии (например, hbedv_smc.key) и подтвердите OK.

Файл лицензии будет прочтен. Появится диалоговое окно с актуальными данными лицензии:



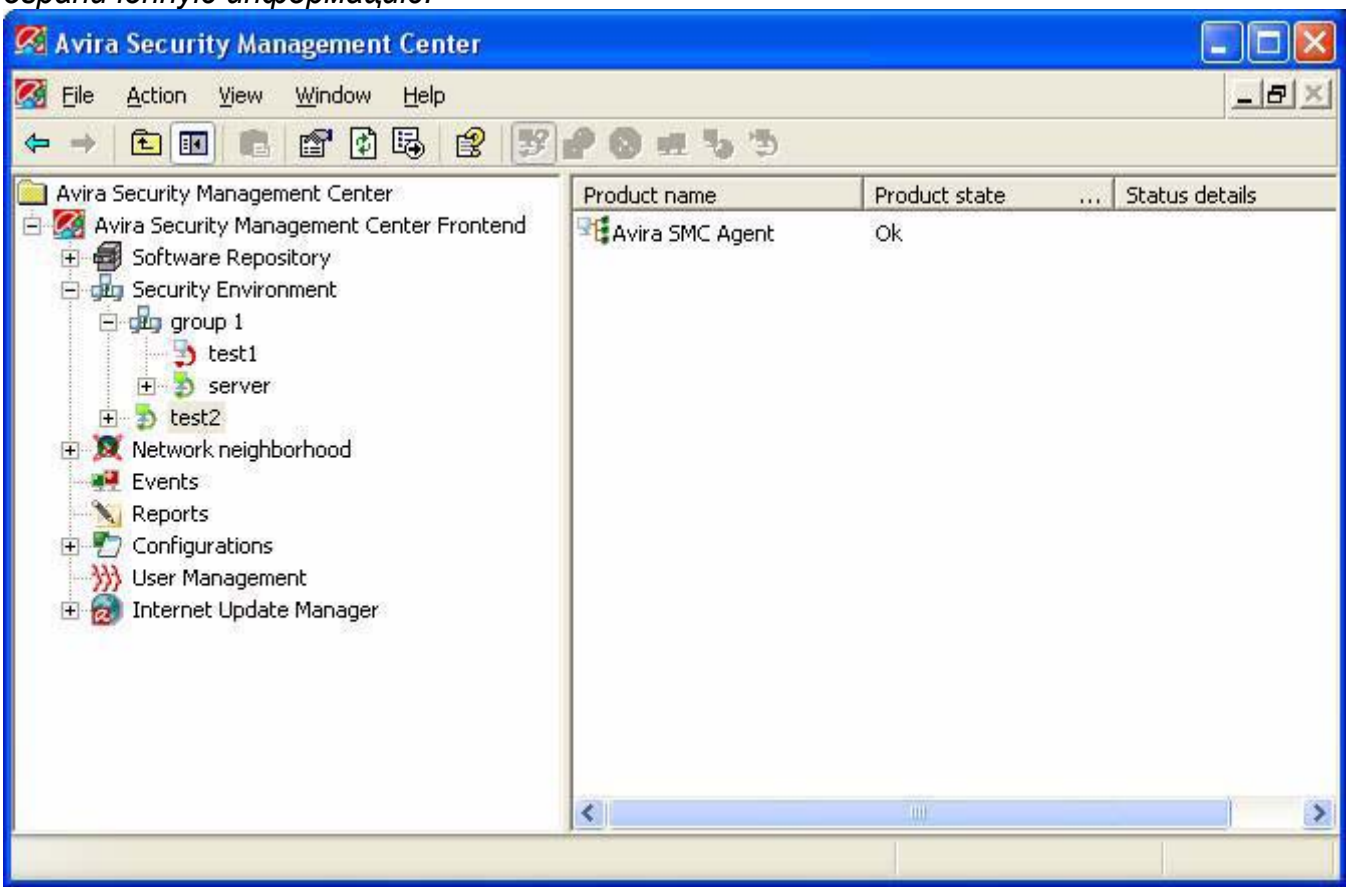
Лицензирование завершено.

4.3 Пользовательский интерфейс SMC Frontend

Используя SMC Frontend, Вы можете настроить и управлять следующими модулями:
- SMC Server и его службами
- SMC Agent в окружении безопасности Security Environment
- продуктами Avira в **Software Repository**
- продуктами Avira на ПК, которые включены в Security Environment.

После полной установки Avira SMC, Вы должны увидеть главное окно.

Avira SMC управляет пользователями с различными правами доступа. Поэтому для определенных пользователей SMC Frontend может отображать ограниченную информацию.



SMC Frontend состоит из двух частей: дерево консоли **Console tree** (левое окно) и панели и панели информации **Details panel** (правое окно). Данные, которые можно развернуть отображаются в виде узлов; например,: узел события **the Events**, группа компьютеров "**group 1**" и т.д.

Вы можете изменить вид панели информации (содержание, колонки и их порядок), используя меню Вид **View**. Изменения будут приняты и остальными группами. Настройки содержимого (например, событий **Events**) сохраняются, но не порядок колонок.

Дерево консоли

Дерево консоли AntiVir Security Management Center Frontend содержит следующие узлы:

Software

Repository (программные пакеты)

Центральная база данных SMC-Server для хранения продуктов AntiVir.

Security
Environment (безопасное окружение/окружение безопасности)

Свободно конфигурируемая, иерархическая структура так называемых виртуальных групп с включенными в них ПК. Группы отражают структуру предприятия или группы пользователей в сети, не только физическую структуру сети.
Внутри окружения безопасности **Security Environment** появляются следующие узлы с дальнейшей информацией:

- узлы групп со всеми ПК, которые включены в эту группу
- узлы ПК и новые ПК с дополнительными узлами, относящимися к продуктам AntiVir и к SMC-Agent

Network
Neighborhood (сетевое окружение)

Рабочие группы и ПК в сетевом окружении Windows. ПК в сети могут отображаться с именами и дополнительно с IP-адресами.

Events (события)

Отображение событий сгенерированных ПК, которые могут быть отсортированы фильтром

Reports (отчеты)

Просмотр шаблонов отчетов и отчетов, которые генерируются ПК.

Configurations (настройки)

Конфигурационные диалоги служб AntiVir SMC.

User
Management (управление пользователями)

Отображение управляемых пользователей

Internet Update Manager	Статус обновления установленных продуктов Avira AntiVir, управляемых при помощи IUM, включая компоненты SMC

Панель информации

Панель информации содержит дальнейшую информацию для выбранных узлов.
Выберите Вид **View**> большие/маленькие значки для отображения маленьких или крупных значков компьютеров, продуктов, задач или событий.
Выберите Вид **View** > таблица> для отображения информации в виде таблицы

Используя опцию **Add/Remove Columns** из меню вид, вы можете настроить вид панели информации. Вы также можете отсортировать таблицу кликнув заголовок колонки.

Software
Repository (программные пакеты)

Информация о сохраненных программных пакетах: имя, файл Setup, файл информации и файл лицензии.

Security

Environment (окружение безопасности/безопасное окружение)
Дополнительная информация о статусе групп или ПК.

Узлы групп На уровне групп (например, отделы), отображается либо информация о подгруппах, либо о ПК: имена продуктов и иконки статуса, версия, статус, операционная система, доступность агента.

Узел компьютер/Новый компьютер В зависимости от выбранного меню вид, отображается следующая информация для каждого ПК:

- **Product status** (статус продукта):

Отображение названий продуктов и иконок статуса, состояния и подробной информации

- **Product version** (версия продукта)**:**

Отображение названий продуктов и версий продукта

- **Events (события)**:

Отображение событий, которые были сгенерированы продуктами AntiVir

- **Tasks** (запланированные задания):

Отображение запланированных заданий, которые выполняются продуктами AntiVir на ПК

- **Pending operations** (ожидающие действия):

Отображение запланированных задач, которые на одном или нескольких ПК еще не могли быть выполнены, так как ПК не был доступен в сети (offline).

- **Error messages** (сообщения об ошибках):

Отображение ошибок (с данными имени продукта и статуса ошибки), продуктов AntiVir

Events (События)
Дополнительная информация отображаемых событий. К списку событий можно применять фильтр, для того чтобы целенаправленном отображались определенные события, например, **критическог уровня** или типа **файл-вирус**.

Reports (отчеты)
Дополнительная информация к настраиваемым шаблонам отчетов и уже готовым отчетам

Configurations (настройки)
Для данного пункта не отображается дополнительной информации. При щелчке на узел открывается диалоговое окно **Configurations (настройки)**
(см. Настройка служб AntiVir).

User Management (управление пользователем)
Дополнительная информация о пользователях: имя, полное имя, описание, адрес электронной почты и дата последнего входа в SMC Frontend

Internet Update Manager Статус обновления всех программных пакетов, включая компоненты: имя продукта и время последнего обновления. При запуске в тестовом режиме, в Internet Update Manager имеется два узла: разрешённые файлы **Approved files** и тестовые файлы **Test files**.

5 Настройка
5.1 Обзор

Настройка главного приложения SMC-Server и служб производятся при помощи графической оболочки SMC-Frontend. После первой установки мы рекомендуем произвести следующие шаги:

- Настройка регистрации в сети и на SMC-Server
- Установка безопасного окружения
- Установка SMC-агентов в безопасном окружении

При необходимости можно настроить службы SMC-Server:

- Настройка служб AntiVir SMC

Кроме того, у Вас есть возможность удобного обновления AntiVir SMC через Интернет, если доступны обновления.

- Обновление AntiVir SMC
- Создание задачи периодического обновления SMC-Server
- Просмотр и редактирование задания по обновлению SMC-Server

Управление пользователями SMC можно настроить, устанавливая доступ и права пользоватеей

- Управление пользователями

Запуск SMC-Frontend

➢ Запустите SMC-Frontend и воидите в SMC-Server (см. Запуск SMC-Frontend и вход на SMC-Server).

5.2 Настройка входа в сеть и на SMC-Server

Вход можно настроить так, чтобы этот процесс при запуске ПК и SMC-Frontend был максимально простым.

После первой установки мы рекомендуем изменить пароль для входа SMC-Frontend на SMC-Server.

У Вас есть следующие возможности настройки:

- Указать учетную запись администратора (или администратора домена) для входа в сеть. Это может быть полезным, если для входа в ПК и в сеть используете разные учетные записи.
- Сохранить имя пользователя для входа в сеть для данной сессии или постоянно. Пароль для входа в сеть не сохраняется.
- Сохранить и изменить пароль для входа в SMC-Server. При первом входе установлен пароль a.

Кроме того, Вы можете создать пользователя и управлять им, устанавливать, изменять и удалять права пользователя, и таким образом управлять входом пользователя на SMC-Server (см. управление пользователями).

Настройка входа

➢ Кликните правой кнопкой мыши на узел AntiVir Security Management Center Frontend и выберите настройки (**settings**)

↳ Откроется диалоговое окно настроек (**settings**).

Введите требуемую информацию в полях закладки Administrator Account и сохраните их. Вы можете выбрать опцию "Use the server's current account" (использовать текущую учётную запись сервера), в случае, если одна административная учётная запись используется для большинства компьютеров в сети. В случае подключения к другим клиентским компьютерам (например, Linux) через SSH, Вы можете активировать опцию "Use SSH public/ private key authentication" и определить ключевой файл, используя кнопку **[...]**.

На закладке **Login** измените пароль для входа на SMC-Server и подтвердите кнопкой **OK**.

↳ Данные будут сохранены

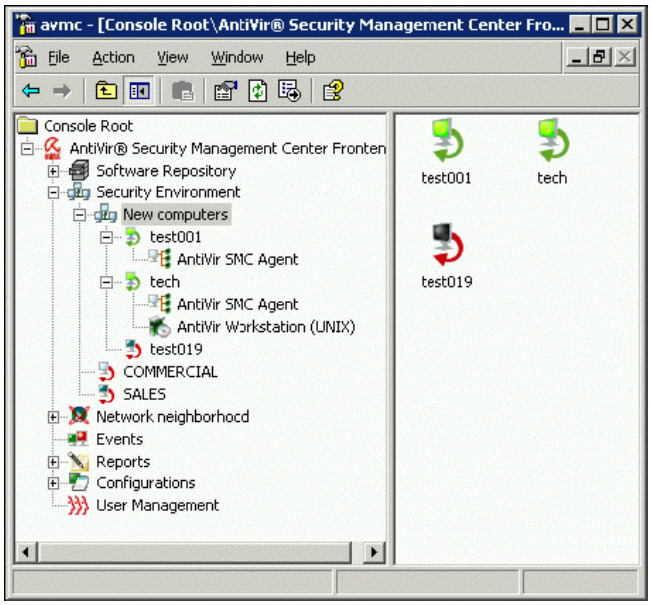
5.3 Установка окружения безопасности

В окружении безопасности программе AntiVir SMC требуются так называемые виртуальные группы ПК, для того, что проводить установку, настройку и контроль. Только ПК, включенные в безопасное окружение, могут управляться при помощи AntiVir SMC.

Узлы окружения безопасности

В окружении безопасности Вы выстраиваете Вашу сеть в иерархической структуре таким образом, чтобы эта структура соответствовала требованиям единой установки и настройки продуктов AntiVir на Ваших ПК.

Для этого Вы создаете в узле безопасного окружения так называемые виртуальные группы, в которых отображаются различные группы пользователей Вашей сети, к примеру, группы ПК отдела продаж или маркетинга, или группы ПК с определенными инсталляциями/настройками (например, продукты на английском языке).
Группы можно также можно делать вложенными. Отдельные группы или несколько групп можно в любое время переместить в другую группу и при этом переподчинить. Имена, с которыми ПК и группы отображаются в безопасном окружении можно выбирать произвольно.



Статус окружения безопасности

Когда SMC-Frontend запущен, статус ПК и групп отображается в виде иконок в зависимости от зарегистрированной учетной записи:

 (монитор зеленый, стрелка зеленая) ПК запущен, SMC-Agent установлен и запущен, возможен полный доступ.

 (монитор голубой, стрелка красная) ПК запущен, SMC-Agent не установлен.

 (монитор голубой, стрелка оранжевая) ПК запущен, SMC-Agent установлен, но доступ невозможен.

 (монитор темный, стрелка оранжевая) ПК выключен или не в сети, SMC-Agent установлен, доступ невозможен.

 (монитор темный, стрелка красная) ПК выключен или не в сети

 (монитор темный/голубой, стрелка оранжевая, красный маркер слева от монитора) **ожидающее действие** (команда или задача SMC) сохранено, так как компьютер выключен, не в сети или нет доступа к SMC-Agent. Действие будет вполнено, как только ПК будет доступен в безопасном окружении.

 ПК или группа ещё не аутентифицирована. AntiVir SMC пытается установить соединение.

 Ошибка в ПК или группе.

 Агент установлен на ПК.

 Программный пакет в базе данных, нет лицензии.

 Программный пакет в базе данных, есть лицензия.

 Программный пакет установлен на ПК.

Создание виртуальных групп

- Кликните в области навигации правой кнопкой мыши на узел **Security Environment** (Окружение безопасности) и выберите **New/Group** (новая/группа).

↳ Откроется диалоговое окно **Create new group** (создать новую группу).

- Введите имя и подтвердите **OK**.

↳ В области навигации под узлом **Security Environment** (Окружение безопасности) появится новая созданная группа

Выбор отображения имени ПК/ IP-адреса

Режим отображение выбирается одновременно для сетевого окружения и окружения безопасности

- Кликните в области навигации правой кнопкой мыши на узел сетевого окружения.
- В контекстном меню кликните левой кнопкой мыши **Display IP Addresses** (отображать IP-адреса).

  ↳ Пункт меню выделится: ПК будут отображаться с IP-адресами.

  ↳ Пункт меню не выделен: ПК отображаются с именами

Добавление ПК в виртуальные группы

Из сетевого окружения

В зависимости от выбранного вида ПК отображаются с именаим или IP-адресами

- Разверните в области навигации узел сетевого окружения и узел Вашей сети (например, сеть Microsoft Windows).

↳ В области результатов отобразятся доступные ПК в сети

- Пертащите ПК и/или группы ПКиз сетевого окружения в группу узла безопасного окружения

– или –

щелкните правой кнопкой мыши на группу и выберите **New/computer (новый/ПК)**

↳ Откроется диалоговое окно **Add new computer (добавить новый ПК)**

- Введите имя, с которым ПК будет представлен в окружении безопасности, а также сетевое имя и подтвердите **OK.**

↳ В области навигации в узле безопасного окружения появится только что добавленный компьютер в выбранной группе

Из узла New Computer

Могут быть компьютеры, на которых установлен SMC-Agent и которые не были добавлены в окружение безопасности Security Environment (например, портативные ПК или компьютеры на которых SMC Agent был установлен вручную). Они автоматически соединятся с SMC Server, как только подключатся к сети.

Кликните в Security Environment (окружении безопасности), New Computer (новый компьютер). Вы увидите новые компьютеры с установленным SMC Agent.

Добавьте нужный компьютер в Security Environment (безопасное окружение), как описано выше

Импорт компьютеров в окружение безопасности Security Environment
Список компьютеров можно также импортировать, используя опцию импорта из контекстного меню. Данное меню предоставляет следующие возможности:

• импорт списка компьютеров
• из сетевого окружения
• Из Active Directory
Для импорта списка ПК:

Создайте список ПК в текстовом редакторе и сохоаните его.
Вы можете дать любое имя фалу (*.txt)
Список имеет следующую структуру:

Group (группа); Name (имя); IP
Marketing; Computer 01; 192.168.146.
Groundfloor; Reception; PC-Reception

Group: имя группы в окружении безопасности, например, Marketing
Name: отображает имя компьютера в окружении безопасности.
IP: IP адрес или сетевое имя компьютера.

- Кликните правой кнопкой на Security Environment и выберите **Import computer list** (импорт списка компьютеров).
- Ведите путь к файлу **[Список компьютеров.txt]** и кликните открыть.

  ↳ Список компьютеров импортирован. Имена компьютеров отобразятся в Security Environment (окружении безопасности).

Для импорта компьютеров из сетевого окружения:
- Кликните **Security Environment** правой кнопкой мыши и выберите **Import/ From network neighborhood**.
  ↳ Список компьютеров из сетевого окружения импортируется в группу **New computers**

*Для импорта компьютеров из **active directory**:*

- Кликните Security Environment правой кнопкой мыши и выберите **Import/ From active directory.**
  ↳ Окно обновления ADS спросит о методе применения новой группы:

- Выберите требуемый метод

↳ Компьютеры из ADS импортированы исходя из Вашего выбора

Переименование виртуальных групп

- Кликните на группе правой кнопкой и выберите Rename (переименовать).
  ↳ Откроется поле ввода имени.
- Измените имя и кликните где-нибудь рядом.
  ↳ Отобразится новое сохраненное имя

Удаление виртуальных групп/ПК

- Кликните правой кнопкой на группу или компьютер и выберите **Delete** (удалить)
  ↳. группа/компьютер будут удалены из окружения безопасности.

5.4 Установка SMC Agent в Security Environment (окружении безопасности)

Для установки Agents в окружении безопасности, Вы должны иметь права администратора на всех ПК.

Убедитесь, что все компоненты продуктов AVIRA обновлены!

AntiVir SMC может контролировать только ПК с установленным SMC Agent. Вам необходимо установить SMC Agent для всего окружения безопасности сразу после установки AntiVir SMC. Если позднее Вы будете добавлять новые группы или ПК в систему, Вы сможете установть SMC Agent для отдельных ПК или групп.

При необходимости Вы межете натроить SMC Agent для всей системы или для отдельных групп или компьютеров после установки и присвоить новые настройки группам или ПК (см. сервис SMC Agent).

Условия для связи между SMC Agent и SMC Server

√ Если установлен firewall, то необходимо открыть следующие порты (TCP): 7000, 7001, 7010, 7020, 7021, 7030. кроме того, необходимо разрешить запросы ICMP и ping.
√ Гостевая учётная запись должна быть отключена
√ Необходимо отключить опцию простого общего доступа
√ SMC Server должен иметь доступ к спрятанному диску C$ (\\<IP \c$\).
√ Для облегчения установки SMC Agent по сети, Вам необходимо использовать административную учётную запись, которая работает на всех ПК.

Процедура установки

В зависимости от операционной системы, SMC Agent имеет различные процедуры установки:

- Удаленная установка через SMC Frontend
- (опционально) ручная установка
- (опционально) скрытая установка в Windows, используя скрипт logon
- (optional) UNIX: ручная установка

5.4.1Установка SMC Agent при помощи SMC Frontend (Windows Vista/2000/XP Professional/UNIX)

ПК/группы должны быть интегрированы в Security Environment (окружение безопасности) и отображаться в виде голубого монитора с красной стрелкой

- ➢ В дереве консоли кликните Security Environment (окружение безопасности) и при необходимости на группы/ПК на которые Вы хотите установить SMC Agent.
- ↳ ПК или группы отобразятся с иконками статуса в области результатов
- ➢ щелкните правой кнопкой мыши группы и выберите Installation/AntiVir SMC Agent/Install.
- ↳ Вы увидите окно установки
- ➢ Кликните **OK**

↳ Программа InstallShield Wizard начнет установку. Вы увидите окошко **Preparing Setup** (подготовка к установке).
↳ SMC Agent будет установлен на требуемых ПК и группах.

- При необходимости перезагрузите ПК
- . запустите SMC Frontend
- Проверьте, чтобы на всех ПК и группах статус SMC Agent был **True** в области результатов Security Environment.

5.4.2 Ручная установка SMC Agent (Win XP Home Edition, опционально: Windows 2000/XP Professional)

Для установки SMC Agent в Windows 98 или Windows XP Home Edition, Вам будет необходим файл AntiVir-Security-Management-Center-Agent.exe. Вы можете найти его на CD-ROM или в локальной папке разархивированного zip-архива.

✓  ПК/группы должны быть интегрированы в Security Environment (окружение безопасности) и отображаться в виде голубого монитора с красной стрелкой.

- Скопируйте файл AntiVir-Security-Management-Center-Agent.exe на ПК, на котором Вы хотите установить SMC Agent.
- Дважды кликните на файле
  ↳ Откроется окно разархивирования и установки
- Кликните Setup.
  ↳ Инсталляционный файл будут разархивирован. Открывается коно InstallShield Wizard appears.
- Кликните **Next (далее)**
  ↳ Откроется окно лицензионного соглашения (**License Agreement**).
- Выберите **I accept...** и кликните **Далее**.
  ↳ Откроется окно данных SMC Server.
- Введите данные и нажмите **Далее**.
  ↳ Следующее окно будет содержать данные настройки SMC Agent.
- Введите данные локального компьютера и нажмите **Далее**.
  ↳ Откроется окно **Path selection** (путь установки).
- При необходимости введите другой путь установки и нажмите **Далее**.
  ↳ Откроется окно **Ready to install** (готовность к установке).
- Кликните **Install**.
  ↳ Будет установлен SMC Agent и откроется окно завершения установки.
- Нажмите **Finished (завершить)**.
  ↳ SMC Agent установлен на локальном ПК.
- Перезагрузите ПК.
- Запустите SMC Frontend

 ПК/группы включены в **Security Environment** (окружение безопасности), иконка статуса: зеленый монитор с зеленой стрелкой. Статус SMC Agent **Yes**.

5.4.3 Скрытая установка Agent в Windows

Если Вы предпочитаете использовать Windows logon скрипт для установки SMC Agents, вместо интерактивной удалённой установки через SMC Frontend, Вы можете запустить установочный скрипт через общую папку. Agent будет установлен без всякого вмешательства пользователя.

√ Убедитесь, что клиентские компьютеры имеют доступ к общей папке, где находится файл установки (по умолчанию: C:\Program Files\Avira\Avira Security Management Center Server\Agent\installagent.bat) .

- Вставьте пакетный файл в logon script, чтобы начать установку Agent в скрытом режиме или используйте следующую команду:

```
setup.exe /serverip=servercomputer /serverport=7000 /
evmgrip=servercomputer /evmgrport=7010 /
upmgrip=servercomputer /upmgrport=7020 /agentip=0.0.0.0
/agentport=7030
```

Примечание:
• параметры должны быть разделены одним пробелом. При ошибке в синтаксисе, начнется интерактивная установка вместо скрытой.
• `/agentip=0.0.0.0` должно быть именем компьютера, которое указано в SMC Frontend. Но так как при использовании logon скриптов, Вы можете использовать здесь "любой" IP. Agent в этом случает получит имя компьютера из операционной системы.
• `servercomputer –` это IP или имя компьютера, на котором установлен SMC.
• если Вы изменили порты по умолчанию, пожалуйста откройте их в FireWall
• если Вы установили Agent на компьютеры вне окружения безопасности Security Environment, они будут добавлены в группу "New computers" (новые компьютеры)

5.4.4 Ручная установка SMC Agent (опционально для систем UNIX)

при необходимости SMC Agent можно установить вручную. Программу установки SMC Agent для систем UNIX можно найти на диске AntiVir CD-ROM или на сайте http://www.avira.com .

- ✓  компьютеры и группы должны быть включены в **Security Environment** (окружение безопасности), иконка статуса: голубой монитор с красной стрелкой.
- ✓ Вы должны знать IP адрес сервера.

➢ Сохраните программу установки UNIX SMC на ПК.
➢ Распакуйте архив:

```
linux:/tmp# tar -xzvf AntiVir_Security_
Management_Center_UNIX_Agent.tgz
```

↳ Файлы распакованы

➢ Смените директорию установки:

```
linux:/tmp# cd AntiVir_Security_
Management_Center_UNIX_Agent.tgz/
```

➢ Установите SMC Agent: Вы должны ввести IP адрес сервера.

```
linux:/tmp/AntiVir_Security_
Management_Center_UNIX_Agent.tgz# ./install [--fast] -
-server=HOST[:PORT] --display-name=<SMC display name>
```

↳ SMC Agent установлен. Появится следующее сообщение:

```
Starting Security Management Center UNIX Agent installation ...
```

↳ Затем сообщение:

```
Installation of the SMC UNIX Agent complete.
```

➢ Смените директорию установки:

```
cd /usr/lib/AntiVir/agent
```

➢ Запустите SMC Agent:

```
/smc-agent.sh start
```

Проверьте, чтобы все ПК и группы имели статус SMC Agent **Yes** в области результатов **Security Environment**.

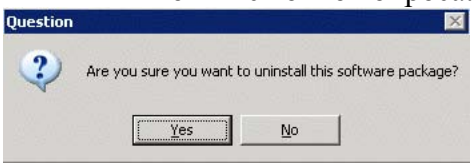
5.4.5 Удаление SMC Agent

Если Вы удалите с ПК SMC Agent, то продуктами AntiVir, установленными на этом ПК, больше нельзя будет управлять при помощи AntiVir SMC. Мы рекомендуем удалять SMC Agent только после того как ПК будет удален из Security Environment и удаления всех продуктов AntiVir.

✓  ПК/группы включены в **Security Environment** (окружение безопасности), иконка статуса: зеленый монитор с зеленой стрелкой.

➢ Кликните правой кнопкой на группе/ПК в Security Environment и выберите **Installation/AntiVir SMC Agent/Uninstall**.

↳ Появится окно вопроса:



➢ Ответьте **Yes**.

↳ SMC Agent удален. Иконка статуса группы/ПК изменилась.

5.5 Настройка AntiVir SMC

В AntiVir SMC входят четыре службы: **Server, Event Manager, Update Manager**, **Alert Manager** и клиентская служба **SMC Agent**. Все службы настраиваются автоматически при установке AntiVir SMC.

Настройка служб по умолчанию и настройка сделанная во время установки AntiVir SMC оптимизированы для данной сети. Мы рекомендуем изменять настройки только в крайнем случае.

Ошибки AntiVir SMC!

Изменения в настройках могут привести к ошибкам AntiVir SMC!
➢ Перед изменениям настроек обратитесь обратитесь в службу поддержки.

Вы можете настраивать службы в окне **Configuration** (настройка), как описано ниже.

5.5.1 Изменение настроек служб

Изменение настройки SMC Agent

√ Компьютеры/группы должны быть включены в окружение безопасности Security Environment, их статус должен быть: зелёный монитор с зелёной стрелкой

- ➢ Кликните правой кнопкой на ПК/группу и выберите **Configuration/Avira SMC Agent/Configure**.
- ↳ Откроется окно конфигурации.
- ➢ Сделайте необходимые настройки

если Вам нужно немедленно применить новые настройки к ПК/группе:

- ➢ Кликните **Send now**.
- ↳ новые настройки будут применены к ПК/группе.

если настройки требуется применить позже:

Кликните **Send later**.
Новые настройки будут сохранены локально. Вы сможете применить их в нужное время.

Изменение настроек компонентов SMC components:
Server, Event Manager, Internet Update Manager, Alert Manager

√ Компьютеры/группы должны быть включены в окружение безопасности **Security Environment**, их статус должен быть: зелёный монитор с зелёной стрелкой

Кликните по Configuration в дереве консоли

В панели результатов отобразятся службы
Дважды кликните нужную службу
Откроется окно настройки
Сделайте изменения в настройках.

Кликните OK.
Появится запрос для перезапуска служб, чтобы принять изменения.

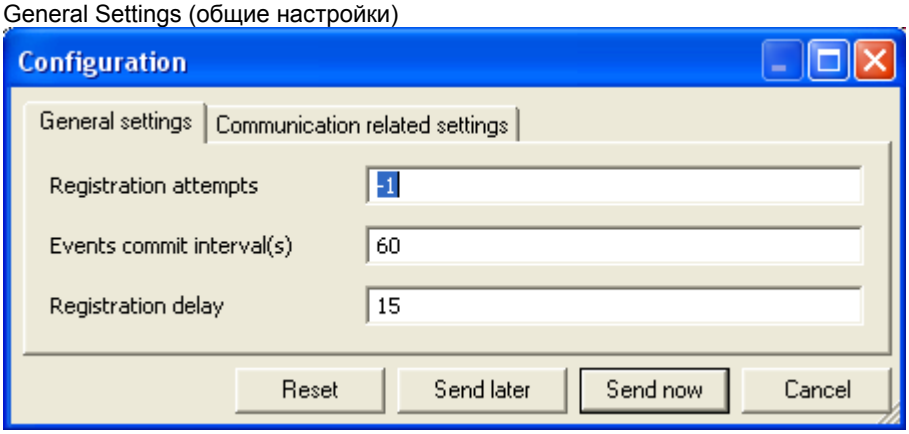
5.5.2 Опции настройки компонентов Avira SMC Components

Настройка SMC Agent

Конфигурация SMC Agent зависит от структуры узлов. Тем не менее, Вы можете поменять настройки для каждого узла. Настройки наследуются от верхнего узла к нижнему, изменения маркируются чёрной рамкой. Все неизменные настройки будут приняты от верхнего узла.

Рекомендуется настраивать SMC Agent, начиная с корневого узла окружения безопасности Security Environment (клик правой кнопкой мыши и выбор Configuration/Avira SMC Agent/Configure). Все ПК в группе унаследуют сделанные настройки. Далее Вы можете сделать необходимые изменения для отдельных ПК или подгрупп: компьютер перепишет настройки унаследованные от корневого узла.

General Settings (общие настройки)

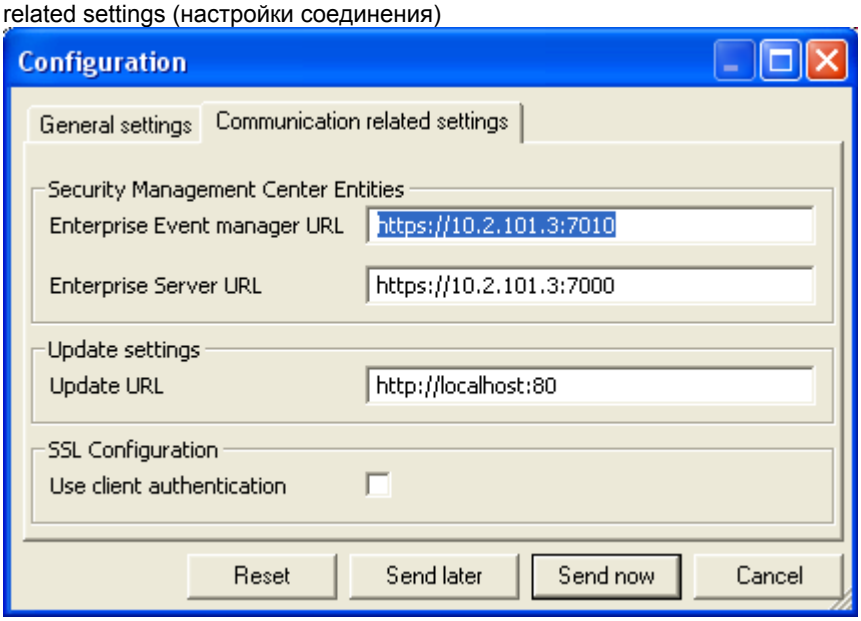


Registration attempts — Количество попыток SMC Agent подключиться к SMC Server.

Events commit interval(s) — Интервал времени за который службы посылают события в Event Manager (менеджер событий). События отсылаются не моментально, а собираются в группы, чтобы не перегружать сетевой трафик.

Registration delay — Интервал времени за который должен запуститься Agent после запуска клиентского компьютера, чтобы предотвратить перегрузку сетевого трафика.

Communication related settings (настройки соединения)



Enterprise Event manager URL — Адрес HTTP и порт используемые службой Event Manager (менеджер событий)

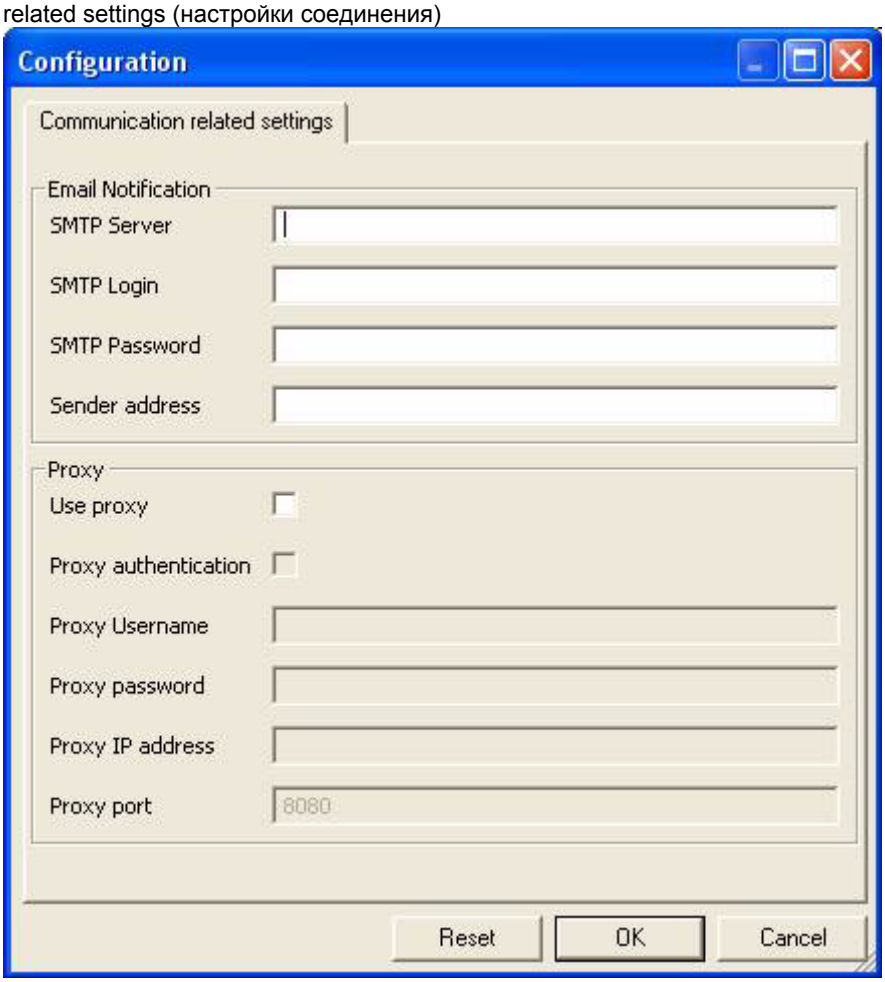
Enterprise Server URL — Адрес HTTP и порт используемые серверной частью SMC

Update URL — Адрес HTTP и порт используемые службой Update

Use client authentication — Аутентификация по протоколу SSL для входа на компьютер

Общие настройки конфигурации

Communication related settings (настройки соединения)



SMTP Server — Имя почтового сервера

SMTP Login, Password — Имя пользователя и пароль для входа на почтовый сервер

Use Proxy — Использование прокси-сервера для подключения SMC Server к Internet

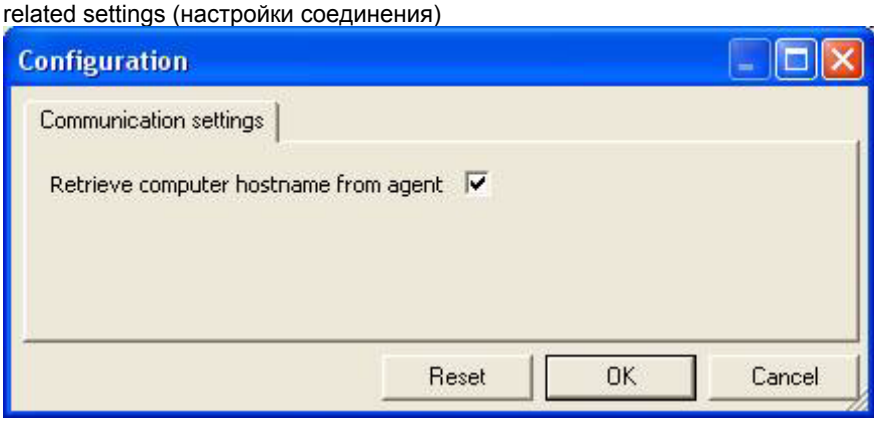
Proxy authentication — Опция для аутентификации на прокси-сервере, если необходимо

Proxy Username, password — Имя и пароль для подключения к прокси

Proxy IP address, port — Адрес и порт прокси

Настройка SMC Server

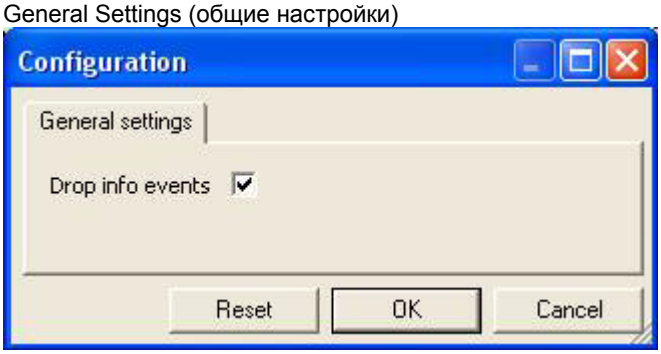
Communication related settings (настройки соединения)



Retrieve ... — Получение имени компьютера из SMC agent: SMC получает адрес IP клиента из агента

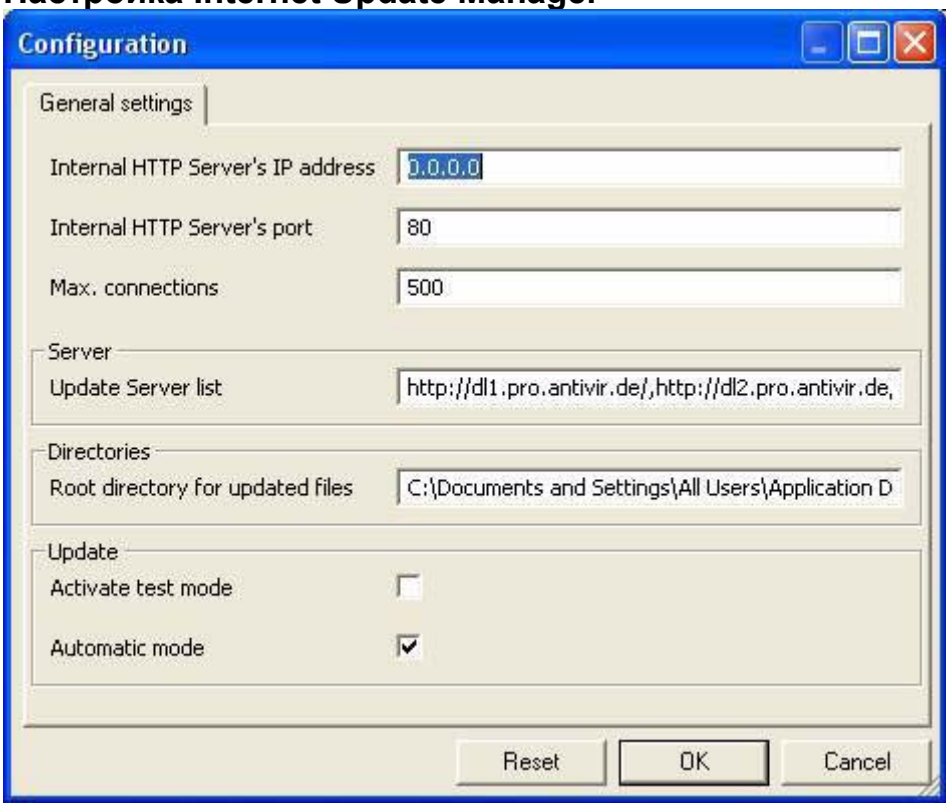
Настройка менеджера событий Event Manager

General Settings (общие настройки)



Drop info events — Запись в файл отчёта только критических событий и предупреждений для предотвращения огромных размеров LOG-файлов

Настройка Internet Update Manager



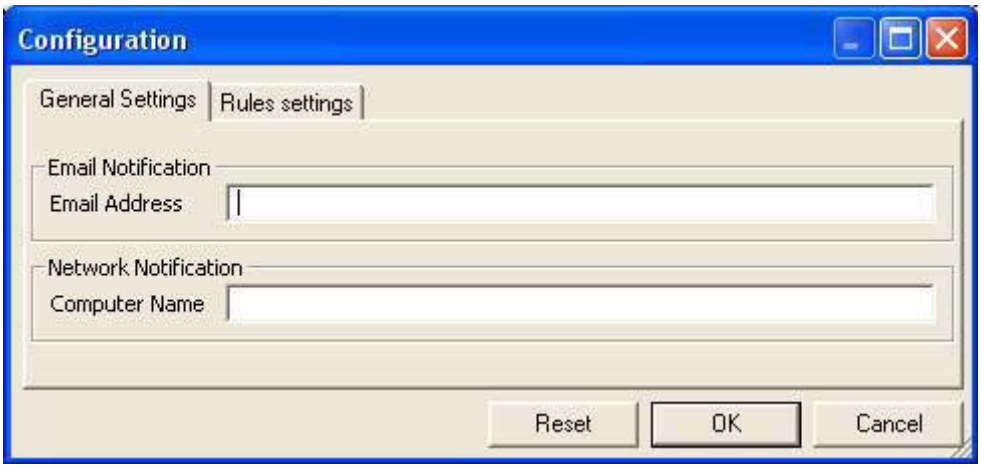
Internal HTTP Server's IP address, port	Адрес и порт сервера Internet для выполнения обновлений Internet Update Manager
Max. connections	Максимальное кол-во одновременных подключений установленных Internet Update Manager к серверу
Update Server list	Список серверов обновления с которых IUM получает пакеты обновлений (по умолчанию: серверы обновления Avira).
Root directory ...	Корневая директория для файлов обновлений: директория, которая зеркально отражает сервер обновлений Avira.
Activate test mode	Новые файлы загружаются в тестовую директорию для проверки. При удачном обновлении они передаются серверу HTTP по умолчанию и распространены в окружении безопасности **Security Environment**.
Automatic mode	Все обновления производятся автоматически модулем Internet Update Manager.

Настройка Alert Manager (менеджер уведомлений)

Менеджер уведомлений Alert Manager является компонентом службы менеджера событий Event Manager. События, посланные продуктами Avira в менеджер событий по сети (например сообщение о вирусной угрозе) может быть передано менеджером уведомлений Alert Manager непосредственно на эл. почту или командой Netsend на ПК в сети. Таким образом, в дополнение к событиям, которые отображаются в SMC Frontend, администратор может напрямую получить информацию о критических событиях.

Настройка Alert Manager производится в окне конфигурации **Configuration window**, которое имеет две закладки, описанные ниже

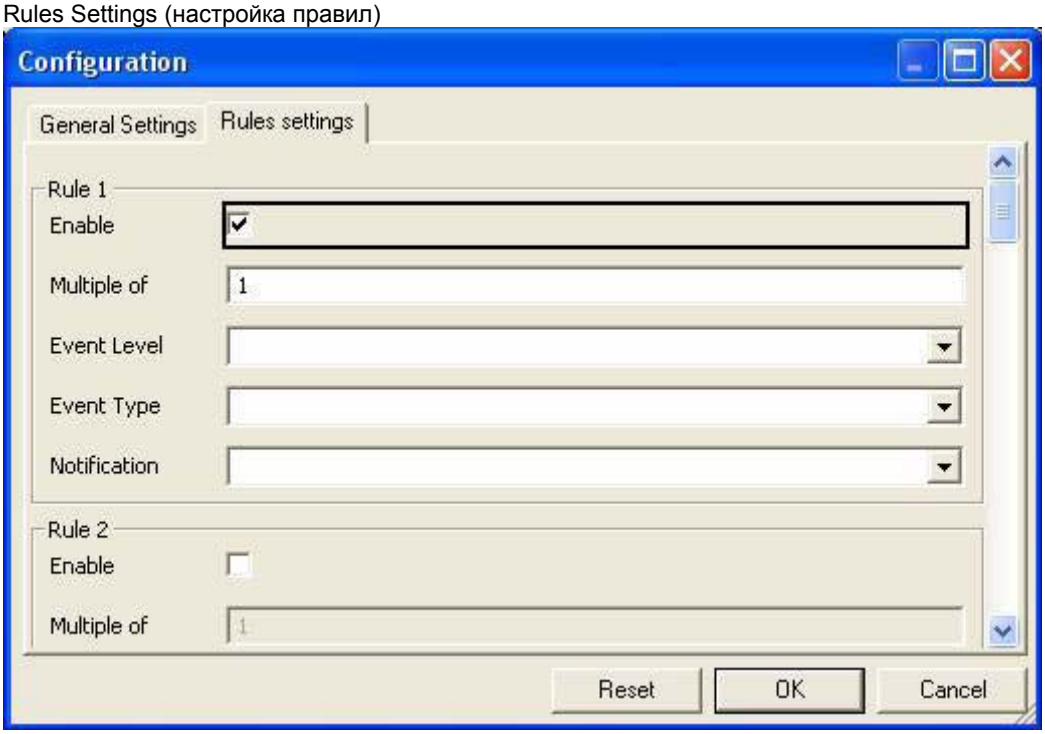
General Settings — На данной закладке Вы вводите адрес электронной почты или адрес компьютера для уведомлений. Определенные типы сообщений и событий будут установлены в закладке Rules Settings (настройки правил).



Email Address — Адрес электронной почты получателя, например администратора или корпоративный адрес группы администраторов

Computer Name — Имя компьютера, на котором должно появиться сообщение, например, компьютер администратора

Rules Settings (настройка правил)



На данной закладке Вы можете настроить (разрешить) до десяти правил сообщений. Доступны следующие опции:

Multiple of — Число событий необходимых для отправки сообщения

Event Level — Сообщение будет отправлено, если встречается любой уровень события (всё, включая информацию) или определенный уровень (критический **Critical**, предупреждение **Warning**).

Event Type — Тип события установлен для всего ПО и не может быть изменен

Notification — Сообщение отсылается на адрес электронной почты (Email) или ПК при помощи команды Netsend (Network), или используя все варианты (All).

5.6 Обновление Avira SMC

Очень важно постоянно иметь обновленное ПО и обращать внимание на совместимость версий компонентов. Вы можете без усилий обновить компоненты Avira SMC: SMC Frontend, SMC Server со всеми службами и SMC Agent. Avira SMC соединяется с открытыми серверами обновлений Avira GmbH и может загружать и устанавливать доступные обновления SMC.

Для выполнения обновлений Avira SMC, Вам необходимо соединение Internet и открыть нужные порты в сетевом firewall.

Во время установки обновлений соединение с SMC Server будет прервано, при этом необходимо закрыть SMC Frontend.

В дополнение к прямым обновлениям, Security Management Center поддерживает автоматические обновления:
• через Internet Update Manager или
• через запланированные задачи обновлений, если автоматический режим не активен

5.6.1 Обновление SMC Server и Frontend

Для выполнеия команд обновления и задач без использования Internet Update Manager Вам необходимо отключить автоматический режим **Automatic mode** в окне настройки сервера ***Server Configuration window***.

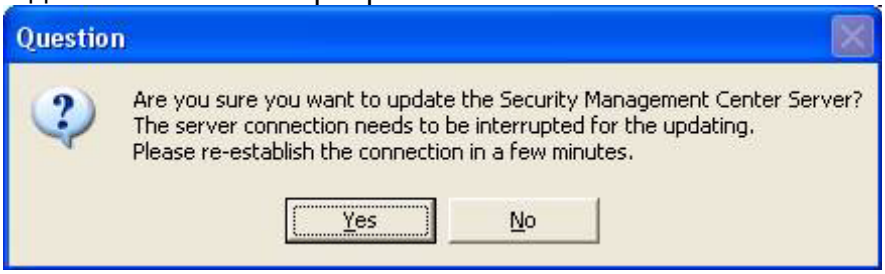
Выполнение прямых обновлений

Кликните правой кнопкой мыши **Avira Security Management Center Frontend** и выберите Обновление **Update**.

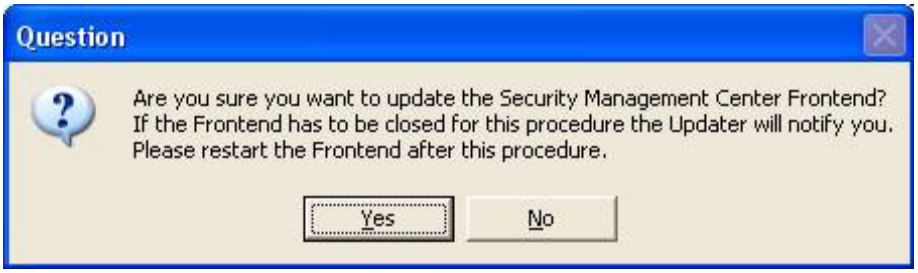
Выберите **Server/Execute** для немедленного обновления сервера

– ИЛИ –

Выберите **Update frontend**.
Появится следующее окно:
– для обновления сервера:



– для обновления **Frontend**:



подтвердите **Yes** и закройте **SMC Frontend** при необходимости.
Соединение с SMC Server будет прервано.
Avira SMC соединится с Internet, загрузит обновления с сервера Avira GmbH и установит их.
Перезапустите SMC Frontend и соединитесь с SMC Server

Обновление через Internet Update Manager

Разверните узел Internet Update Manager, кликните правой кнопкой мыши **Avira Security Management Center Frontend** или **Avira Security Management Center Server** и выберите **Update now**.
 Окно статуса Internet Update Manager покажет процесс обновления.

Создание задачи обновления Server

Вы можете использовать задачи обновлений для периодического обновления SMC Server.

Запланированные задачи обновлениядолжны быть подтверждены администратором.

Кликните правой кнопкой мыши **Avira Security Management Center Frontend** и выберите **Update/Server/Schedule.**
Откроется окно создать задачу **Create a task**.
Введите имя задачи, выберите частоту выполнения **task frequency** и кликниете далее **Next**.
Выберите начальную дату **the start date** и время **time** выполнения задачи и кликните завершить **Finish**.
 Задача запланирована.
Вы можете изменить задачу в любое время из контекстного меню (см. ниже).

5.6.2 Отображение и изменение задач обновлений для SMC Server

Кликните правой кнопкой мыши **Avira Security Management Center Frontend** и выберите **Update/Show tasks**.
 Детали задачи обновления сервера **update server task** отображаются в панели информации
Для изменения задачи:
Дважды кликните задачу **the task**.
 Откроется окно создать задачу **Create a task**.
Сделайте изменения и снова сохраните задачу.

5.6.3 Обновление SMC Agent

Для обновления SMC Agent по всей сети или для определенной группы:

Кликните правой кнопкой мыши **Security Environment** или группу и выберите **Commands/Avira SMC Agent/Update agent**.

Для обновления SMC Agents на определенном ПК:
Кликните правой кнопкой мыши **the Avira SMC Agent** в узле ПК и выберите **Commands/Update agent**.
Обновление SMC Agent можно также запланировать, нажав кнопку **Schedule this command** в окне команд **Commands window**.

Обновление SMC Agents через **Internet Update Manager**:

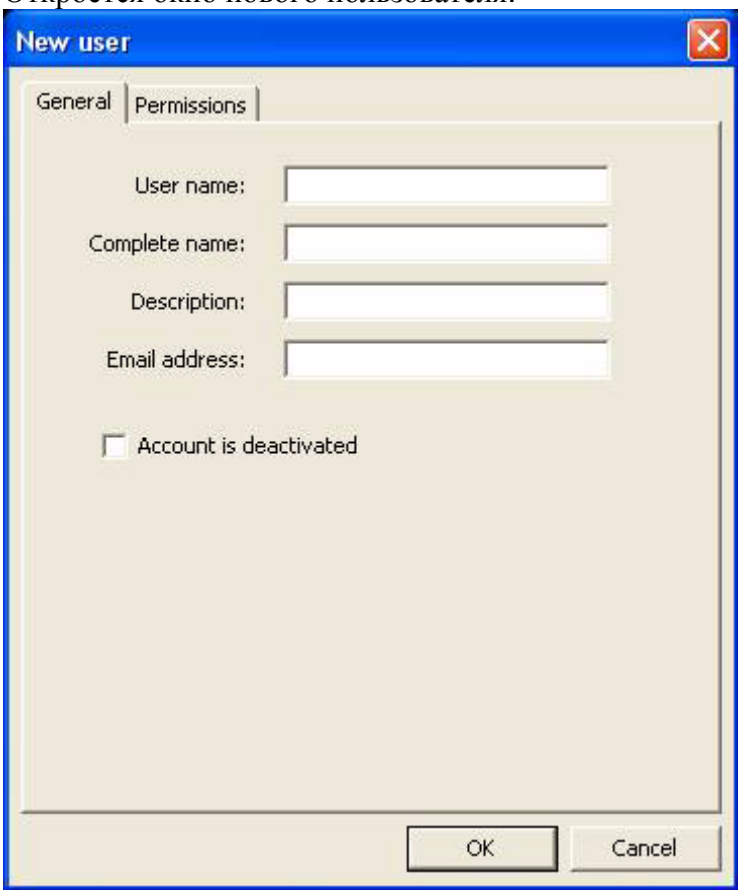
Разверните узел IUM, кликните правой кнопкой мыши **Avira Security Management Center Agent** и выберите обновить сейчас **Update now**.
Окно статуса **Internet Update Manager** покажет процесс обновления.

5.7 Управление пользователями (**User Management)**

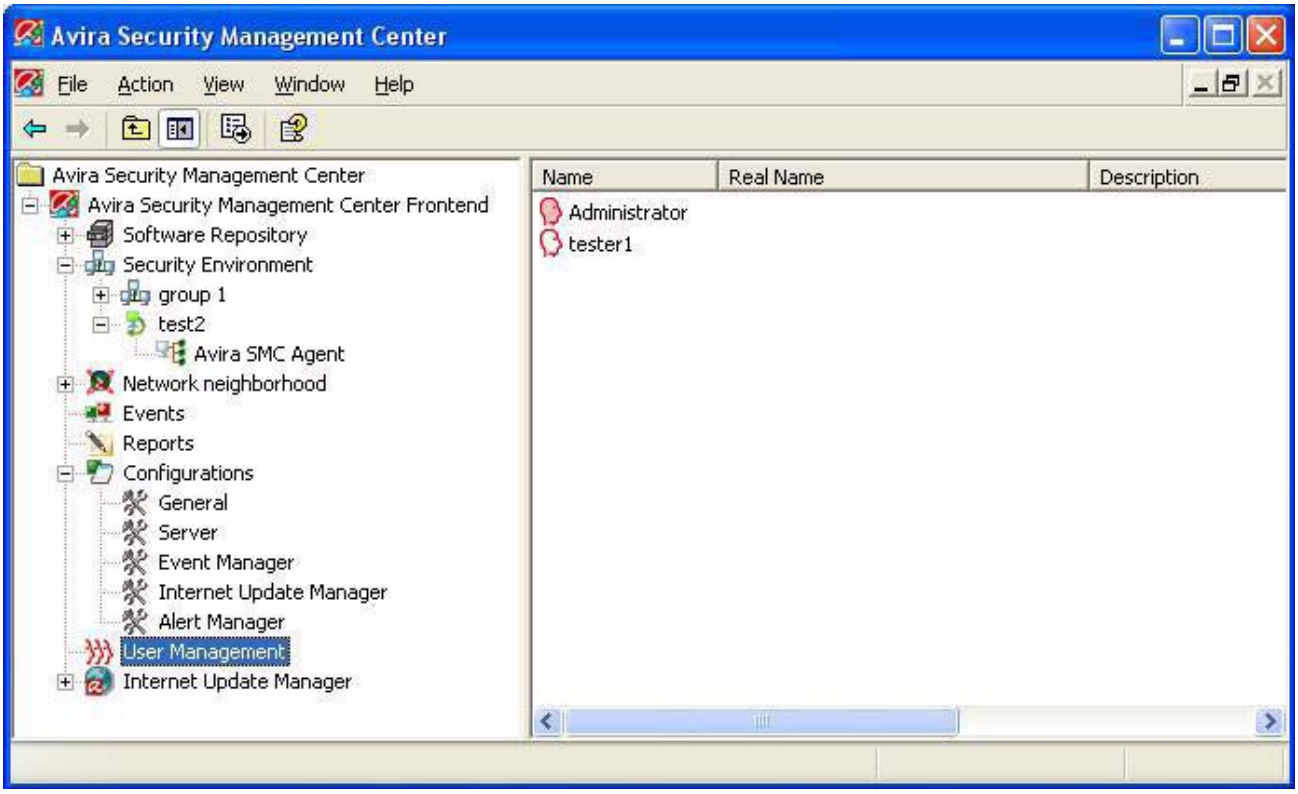
При помощи **User Management** Вы можете создать иерархию с определенными правами доступа. Это помогает администратору эффективно организовать контроль за окружением безопасности **Security Environment** в случае распределения задач IT или на время отпуска. Определенные пользователи SMC смогут подключаться к серверу для просмотра событий и отчётов (**events** или **reports)**, но они не смогут изменять важные настройки безопасности.

Добавление новых пользователей

Кликните правой кнопкой мыши на узел **User Management** и выберите **Create new user**.
Откроется окно нового пользователя:



Введите имя пользователя, полное имя **complete name** и опционально описание и адрес электронной почты **email address.**
Если Вы не хотите активировать учетную запись, кликните опцию **Account is deactivated**.
Настройте права пользователя на закладке **Permissions**.
Кликните **OK** для сохранения настроек.
Новый пользователь появится в панели информации



Настройка учётной записи пользователя

Следующие настройки доступны для каждой учетной записи:
• password: введите пароль входа пользователя Avira SMC
• properties: введите имя пользователя **user name**, полное имя **complete name**, описание **description** и адрес электронной почты **email address**
• permissions: установка прав доступа к Avira SMC

Все пользователи могут просматривать окружение безопасности **Security Environment.**

Для каждого пользователя можно установить следующие права:
• **display Network neighborhood** отображение сетевого окружения
• **display reports** отображение отчетов
• **modify/delete reports** редактирование/удаление отчетов
• **manage users** управление пользователями
• **display events** отображение событий
• **delete events** удаление событий
• **display software packages** отображение программных пакетов
• **change login password** смена пароля входа
• **configure SMC** настройка SMC
• **configure IUM** настройка IUM

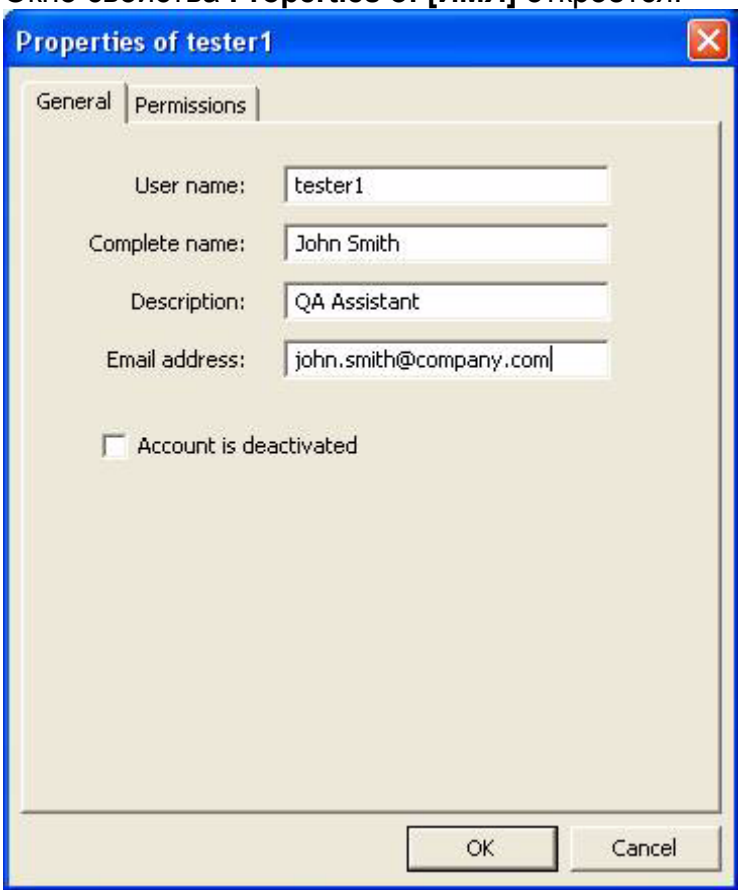
Установка пароля

Кликните правой кнопкой мыши иконку пользователя в управлении пользователями **User Management** и выберите установить пароль **Set password.**
Откроется окно ввода пароля
Введите пароль, подтвердите его и кликните **OK**.
Доступ к учётной записи пользователя теперь защищен паролем

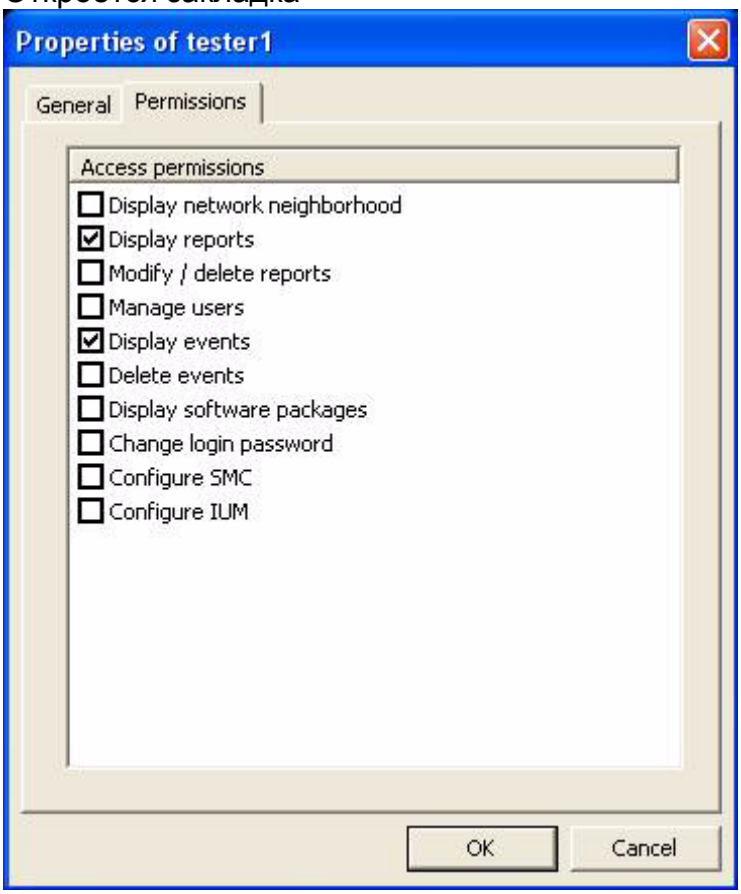
Настройка свойств и прав

 Кликните правой кнопкой мыши иконку пользователя в управлении пользователями **User Management** и выберите свойства **Properties.**

Окно свойства **Properties of [ИМЯ]** откроется.



Внесите изменения в свойства
Кликните закладку разрешения **Permissions**.
Откроется закладка



Выберите или деактивируйте права пользователя и подтвердите **OK**.
Удаление пользователя

Кликните правой кнопкой мыши иконку пользователя и выберите удалить **Delete**.
Ответьте **Yes** на запрос.
Пользователь удален

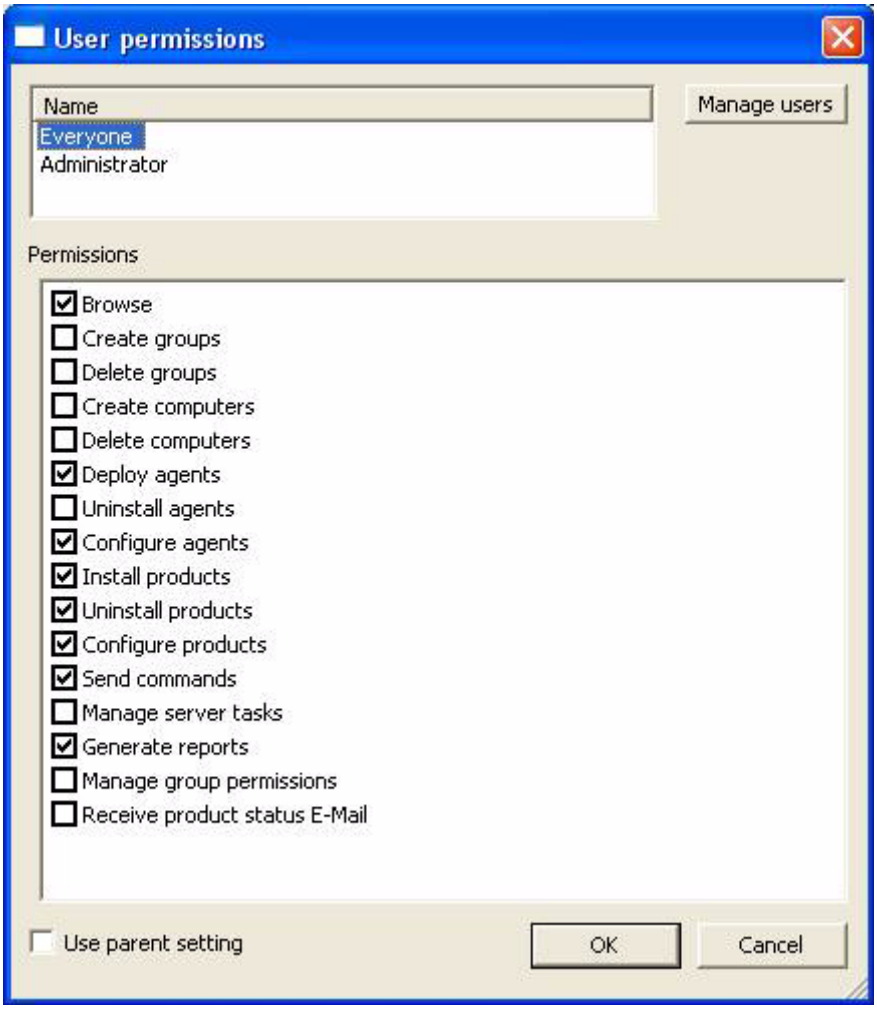
Настройка прав пользователей в виртуальных группах

Вы можете установить права и доступ к виртуальным группам или компьютерам в окружении безопасности **Security Environment** для всех пользователей. Эти права назначаются в каскадной форме и наследуются сверху вниз в иерархичной структуре виртуальных групп.
Таким образом, для каждого узла Вы можете назначить авторизованного пользователя и установить для них права доступа или дать унаследовать права с вышестоящего узла.

Для каждой группы или пользователя доступны следующие права:
• **browse** просмотр
• **create/delete groups** создать/удалить группы
• **add/delete computers** добавить/удалить компьютеры
• **deploy/uninstall/configure agents** развернуть/удалить/настроить агентов
• **install/uninstall/configure products** установить/удалить/настроить продукты
• **send commands** послать команды
• **manage server tasks** управлять задачами сервера
• **generate reports** генерировать отчеты
• **manage group permissions** управлять разрешениями группы
• **receive product status emails** получать уведомление эл. письмом о статусе продукта

Права для учётной записи **Administrator** изменить нельзя*.*

Кликните правой кнопкой мыши узел ПК или виртуальной группы и выберите права доступа пользователей **User permissions**.
Откроется окно **User permissions**



Выберите пользователя и настройте права

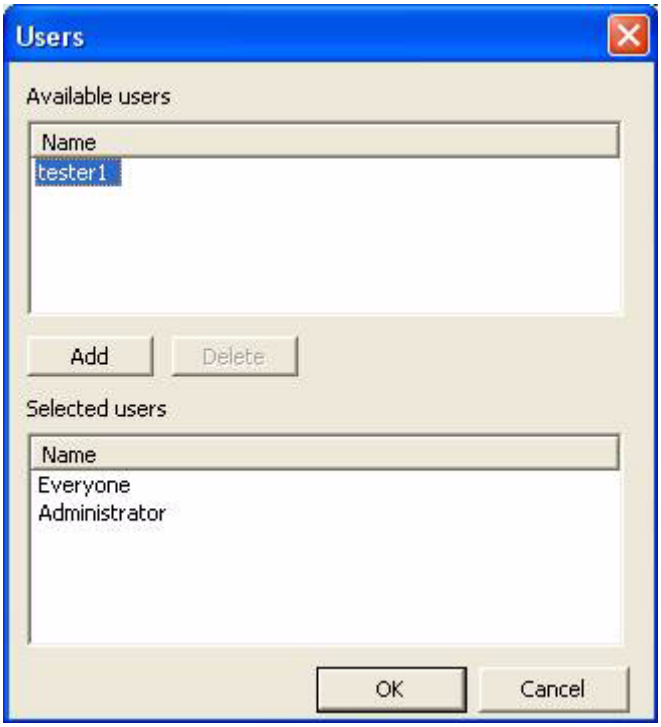
Управление пользователями

Вы можете настроить пользователей и их права для каждого узла. Когда настройки наследуются с вышестоящего узла, части окна отображаются серым цветом (не активны).

При необходимости деактивируйте опцию **Use parent settings** (использовать родительские настройки).

Кликните **Manage users** управление пользователями.

Откроется следующее окно



В поле доступные пользователи **Available users**, выберите пользователей, которые должны иметь доступ к узлу и подтвердите **Add**

– ИЛИ –

Выберите пользователей, которые не должны иметь доступа к узлу и подтвердите кнопкой **Remove.**
Пользователи добавлены/удалены

Использовать родительские настройки

Для наследования родительских настроек с вышележащего узла: выберите опцию использовать родительские настройки **Use parent settings.**
 Пользовательские настройки наследуются

6 Использование программы

6.1 Обзор

Эта глава описывает функции AntiVir SMC. В зависимости от операционной системы и версии MMC функции программы могут немного отличаться.
Вы можете управлять продуктами AntiVir используя следующие функции AntiVir SMC:

- Сохранять, устанавливать, удалять и настраивать программные пакеты
- Запускать или планировать действия установленных продуктов AntiVir (например, поиск вирусов или обновления).
- Отображение различной информации о ПК в окружении безопасности **Security Environment** после установки программных пакетов: Просмотр информации о ПК\Группах в безопасном окружении
- Отображение и фильтрация сообщений AntiVir SMC после установки и настройки программных пакетов: просмотр событий
- Просмотр статуса установленных программных пакетов, событий и сообщений в окружении безопасности **Security Environment**:
- Распределение и запуск файлов и утилит AntiVir tools в сети внутри окружения безопасности **Security Environment**:

Регистрирование всех действий AntiVir SMC в log-файлах (опционально). Это помогает быстрее обнаружить ошибки установки программ
Программные пакеты можно обновлять, используя запланированные задачи обновления, а также выполнять задачи периодического обновления установленных продуктов AntiVir:

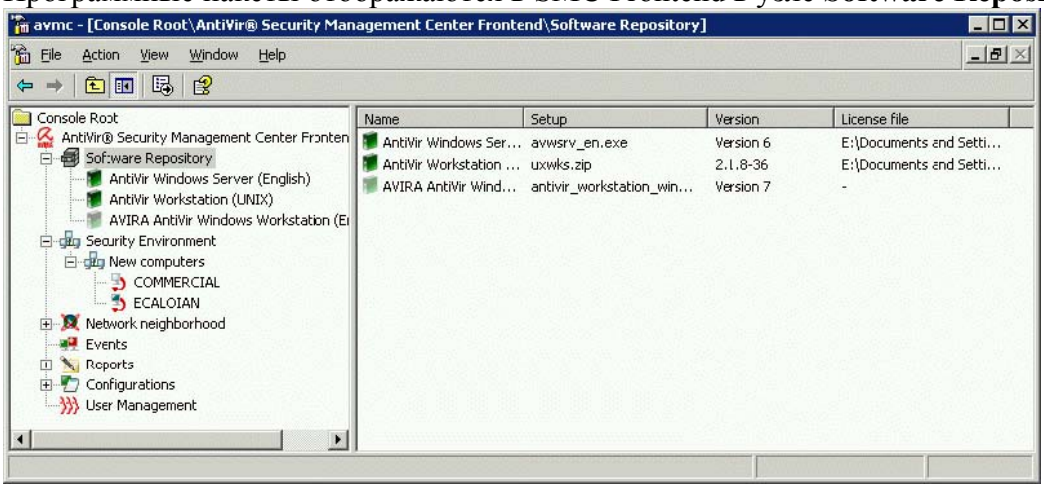
Запуск SMC Frontend
См. главу Запуск SMC-Frontend и регистрация на SMC-Server

6.2 Управление программными пакетами

При помощи AntiVir SMC Frontend можно легко и удобно устанавливать, настраивать и удалять продукты AntiVir в виртуальных группах окружения безопасности **Security Environment**. AntiVir SMC хранит продукты AntiVir в виде так называемых программных пакетов (**software packs**) в собственной базе данных.

Узел Software Repository Node

Программные пакеты отображаются в SMC Frontend в узле **Software Repository**.



В области результатов отображается общая информация о пакетах: имя продукта AntiVir, имя файла setup и info-файла, а также файл лицензии.

6.2.1 Создание и удаление программного пакета

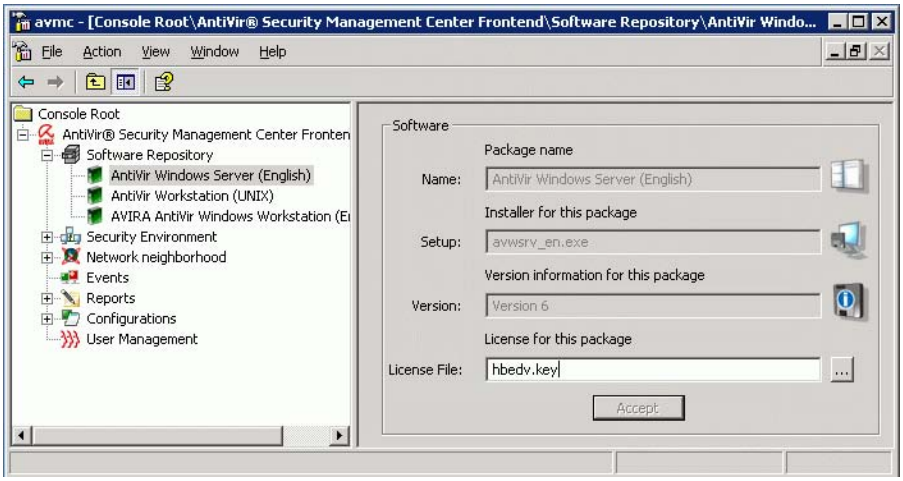
Пример продукта AntiVir product в папке **Software Repository**: AntiVir Windows Workstation. Программный пакет содержит все программные файлы продукта AntiVir product info-файл, все архивированные и самораспаковывающиеся файлы и хранится в базе данных AntiVir SMC.

Программные пакеты нельзя сохранить дважды в AntiVir SMC - SMC Server не позволяет сделать этого.

Вы не сможете установить в сети программный пакет, если у Вас не будет лицензии AntiVir GmbH. Информацию о лицензировании Вы сможете найти в документации продукта AntiVir.

Создание программного пакета

- ✓ Продукт AntiVir сохранен на ПК в локальной сети.
  - ➢ Кликните правой кнопкой на Software Repository и выберите New/Software.
    - ↳ Откроется окно выбора программного пакета.
  - ➢ Выберите путь к программному пакету и кликните **Open**.
    - ↳ Программный пакет будет сохранен.
    - ↳ В области результатов отразятся данные, содержащиеся в Info-файле.
  - ➢ Кликните **[…]**, введите путь к файлу лицензии и кликните **Open**.
    - ↳ В области результатов отобразится путь к файлу лицензии.
  - ➢ Кликните **Accept**.
    - ↳ ПО лицензировано и отображается в **Software Repository.**
    - ↳ В области результатов отображается информация о ПО



Пожалуйста, обратите внимание что данный файл лицензии используется только для (пере-) установки. Для того чтобы расширить лицензию для конкретного продукта, Вам необходимо загрузить файл лицензии используя функцию ***Copy files****.*

Удаление программного пакета

Мы рекомендуем не удалять существующие программные пакеты, так как случайно Вы можете удалить связанные файлы с жесткого диска сервера.

- Разверните узел **Software Repository**.
  ↳ Отобразятся сохраненные программные пакеты
- Кликните правой кнопкой на **программный пакет** и нажмите удалить **Delete**.
  ↳ ПО будет удалено из базы данных AntiVir SMC

6.2.2 Установка, удаление и изменение программного пакета

Пожалуйста, прочитайте файл README.TXT в корневой директории AntiVir SMC.

Установка и удаление программных пакетов на ПК в окружении безопасности, используя AntiVir SMC, происходит в безопасном режиме, это означает, что процесс не может быть прерван или отменен.
Установка и удаление программных пакетов будет выполнена при условии, что все ПК в окружении безопасности находятся в сети, имеются права администратора и запущены SMC агенты.
В случае, если ПК недоступны в сети, действия или команды (например, установка программного пакета) будут сохранены и автоматически сразу выполнены после того, как ПК/группы будут доступны в сети. У ПК будут статус ожидающей операции: темный монитор с оранжевой стрелкой и красным маркером слева

Установка программных пакетов требует настройки продуктов AntiVir. Настройка установленных продуктов AntiVir требует хороших знаний параметров настройки. Пожалуйста прочитайте и следуйте инструкциям по настройке продуктов AntiVir перед выполнением удаленной установки/настройки при помощи AntiVir SMC.

Установка программного пакета

Используя AntiVir SMC Вы можете одновременно устанавливать продукты AntiVir с одинаковыми настройками более чем на один ПК. Поэтому виртуальные группы окружения безопасности должны быть структурированы по принципу одинаковых требований к настройкам.

Если на ПК, на котором Вы хотите установить программный пакет, не установлен SMC Agent, то автоматически сначала будет установлен SMC Agent.

Во время установки откроется диалоговое окно установки конкретного продукта, в котором можно ввести необходимые параметры

✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment** иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

- Кликните правой кнопкой на ПК/группу, в которой Вы хотите установить ПО.
- Выберите **Installation/[имя ПО]/Install**.
- ↳ Откроется окно: **Installation- Setup Configuration**.
- Сделайте настройки продукта AntiVir и кликните **OK**.
- ↳ SMC Agent устанавливает программный пакет.
- ↳ Могут открыться программные диалоги и сообщения
- В дереве консоли кликните ПК или группу, где была произведена установка.
- ↳ Область результатов отобразит дальнейшую информацию по установленному на ПК продукту AntiVir product

Удаление программного пакета

 ПК/группы должны быть интегрированы в окружение безопасности **Security Environment** иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

- Кликните правой кнопкой на ПК или группу, которая содержит ПО для удаления
- В контекстном меню выберите **Installation/[имя ПО]/Uninstall**.
- Кликните **Yes**.
- ↳ Программный пакет будет удален
- ↳ Записи о данном пакете будут удалены из свойств ПК в области результатов

Изменение программного пакета

Вы можете удалять или добавлять отдельные модули для некоторых продуктов AntiVir через программу установки.

 ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой

- Кликните правой кнопкой на ПК или группу
- В контекстном меню выберите **Configuration/[software name]/Configure**.
- ↳ Откроется окно установки продукта
- Следуйте диалогу установки для добавления или удаления программных модулей

6.2.3 Изменение настроек продукта AntiVir

Настройка установленного продукта AntiVir специфична для каждого узла, это означает, что Вы можете сделать настройки для каждого узла. Настройки наследуются сверху вниз для каждого узла, изменения отмечаются черной рамкой в окне настройки. Все неизмененные настройки будут унаследованы от верхнего узла.

Рекомендуется начинать настройку продукта AntiVir с самого верхнего узла **Security Environment**. Все компьютеры группы унаследуют настройки. Затем Вы сможете сделать изменения для отдельных ПК и подгрупп: компьютер перепишет настройки, наследованные из корневого узла.

Во время настройки каждого продукта AntiVir, для каждого продукта будут открываться свои диалоговые окна: **Installation- Setup Configuration**, где можно указывать параметры
Для дополнительной информации используйте руководство пользователя продукта AntiVir .


При установке и настройке программного пакета на ПК из окружения безопасности ***Security Environment*** *открывается панель настройки продукта. Настройки доступные в данном окне аналогичны настройкам в самом продукте. В Avira SMC данные настройки отображаются в иной форме.*


Если ПК недоступны в сети, то действия и команды (например, настройка установленного продукта AntiVir) будут сохранены в режиме ожидания в SMC и запущены автоматически, после того как ПК/группы будут доступны в сети. Иконка статуса ПК будет показывать ожидающую операцию: темный монитор с оранжевой стрелкой, красный маркер с левой стороны

Настройка продукта AntiVir

✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой

- Кликните правой кнопкой на ПК/группу
- Выберите **Configuration/[software name]/Configuration.**

Откроется окно настройки продукта

- Сделайте настройки продукта

Если необходимо сразу применить настройки к ПК/группе:

- Кликните **Send now**.

Новые настройки применены к ПК/группе.
Если необходимо применить настройки к ПК/группе позже:

- Нажмите **Send later**.

AntiVir SMC сохранит настройки для каждого узла локально. Вы сможете применить эти настройки к ПК/группе позже

6.3 Просмотр информации о ПК/Группах в окружении безопасности

6.3.1 Просмотр информации об узле/ПК

Вы можете просмотреть основную информацию о ПК или группе, кликнув правой кнопкой.

Информация о виртуальной группе:

- Число ПК в группе
- Активные ПК: число ПК подключенных в данный момент к Anti-Vir SMC.
- Продукт и количество: имя и количество продуктов, установленных в группе .

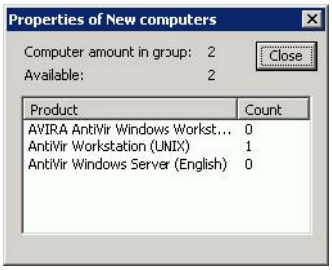
Информация о ПК:

- Отображение имени: имя ПК в окружении безопасности.
- Сетевое имя/IP: имя хоста или сетевой адрес IP.

Свойства виртуальной группы

➢ Кликните правой кнопкой мыши на виртуальную группу в **окружении безопасности** и выберите **Properties** (свойства).

↳ Откроется окно свойств:



Свойства ПК

➢ Кликните правой кнопкой на ПК в **окружении безопасности** и выберите **Properties** (свойства).

↳ Откроется окно свойств:

6.3.2 Просмотр информации в области результатов

AntiVir SMC сохраняет различную информацию о ПК или группе в окружении безопасности **Security Environment**, которую можно отобразить и отсортировать в области результатов.

При выборе ПК правой кнопкой меню позволяет выбрать различные ржимы отображения:

Для группы: **Status** (статус), **Tasks** (задачи), **Error Messages** (сообщения об ошибках) и **Pending operations** (ожидающие операции).
Для ПК: **Products status** (статус продукта), **Events** (события), **Tasks** (задачи), **Error Messages** (сообщения об ошибках) и **Pending operations** (ожидающие операции).

Настройки и сортировка отображаемой информации

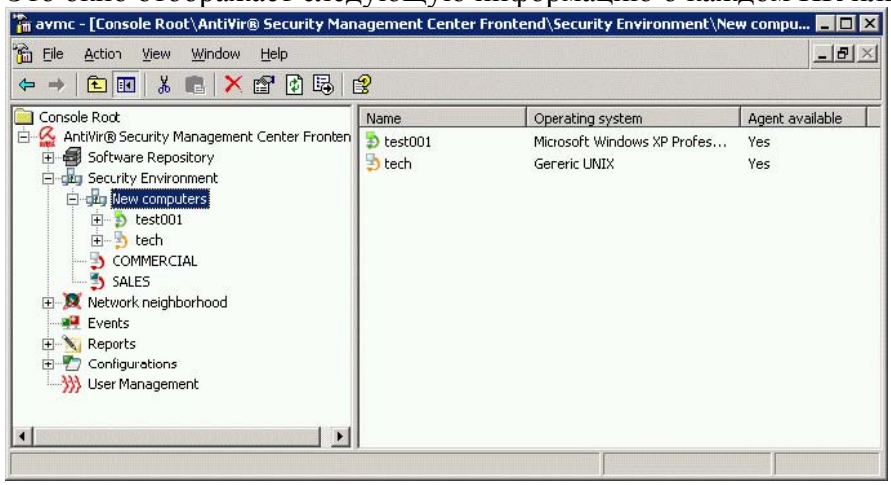
✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой

- Кликните правой кнопкой на ПК/группу, для которых требуется информация.
- Выберите требуемый вид: **Status (**статус**)**, **Products** (продукты), **Events** (события), **Tasks** (задачи) или **Pending operations** (ожидающие операции).
  - ↳ Требуемая информация отобразится в области результатов
- Кликните на заголовок колонки, например: **Level** (уровень) или **Time** (время), для сортировки событий.

Отсортированные события отобразятся в области результатов.

Просмотр статуса

Это окно отображает следующую информацию о каждом ПК или группе:

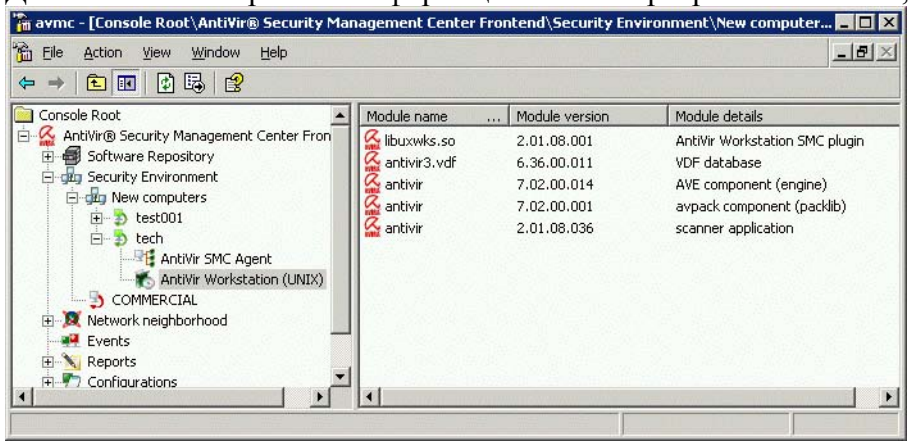


Computer Status	Информация о компьютере: в сети **"Online"**, в сети, агент не установлен **"Online, no agent installed"** или не доступно **"N/A".**
Hostname/ IP	Имя хоста или сетевой адрес IP
Configuration	Настройки Agent наследуются или настраиваются вручную
Name	имя ПК.
Operating System	информация об операционной системе.

Если Вы выбираете компьютер в окружении безопасности **Security Environment**, статус продукта **the Product Status** будет отображать информацию о: имени продукта **product name**, состоянии продукта **product state**, деталях статуса **status details**.

Просмотр продуктов

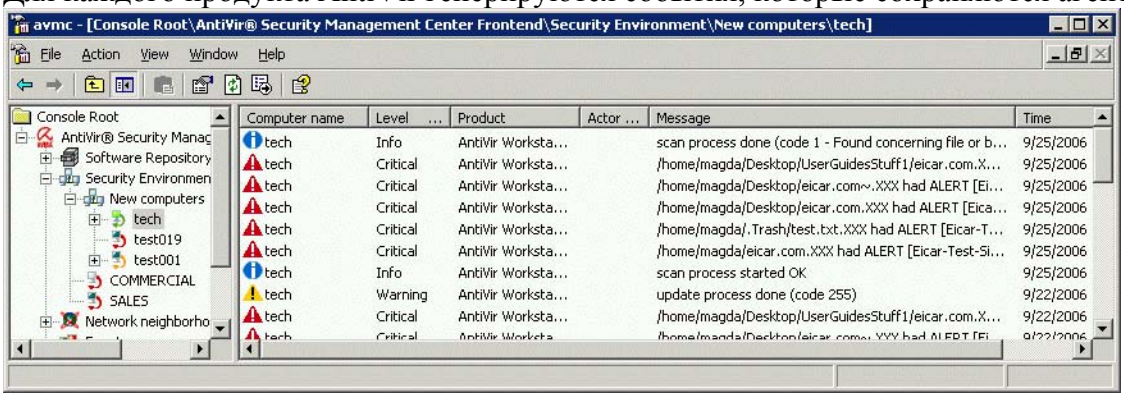
Данное окно отображает информацию о всех программах AntiVir, установленных на ПК:



Module name список установленных на ПК продуктов AntiVir
Module Version Информация о версии файла
Module Details описание файла

Просмотр событий

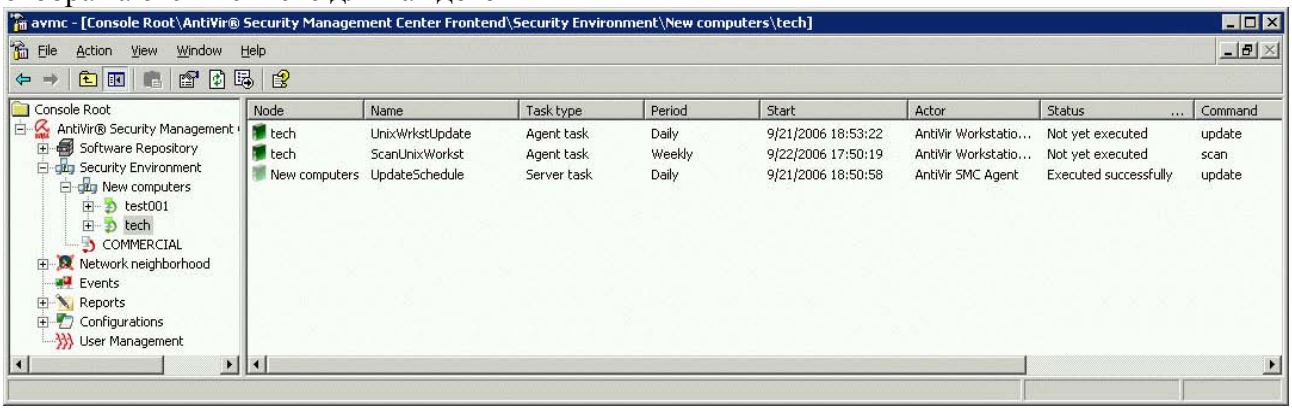
Для каждого продукта AntiVir генерируются события, которые сохраняются агентом SMC Agent:



Computer name Имя ПК на котором сгенерировано событие продуктом AntiVir.
Level Для каждого события продукты AntiVir присваивают уровни (степень важности), например: **Critical** (критический), **Warning** (предупреждение) или **Info** (информация).
Product Имя продукта AntiVir, который сгенерировал событие.
Actor Имя программного компонента сгенерировавшего событие.
Message Специфичный для каждого продукта текст события.
Time Дате/время события.
Type Продукты AntiVir присваивают каждому событию тип, например: **General** (общий), **Error** (ошибка), **File virus** (заражен файл), **Email virus** (заражено эл.сообщение) .

Просмотр задач

Для каждого продукта AntiVir существуют свои команды (например, поиск или обновление). Используя AntiVir SMC, эти команды можно запланировать, как регулярно выполняющиеся задачи. Для каждого ПК или группы можно просмотреть задачи. Задачи групп также отображаются в списке для каждого ПК

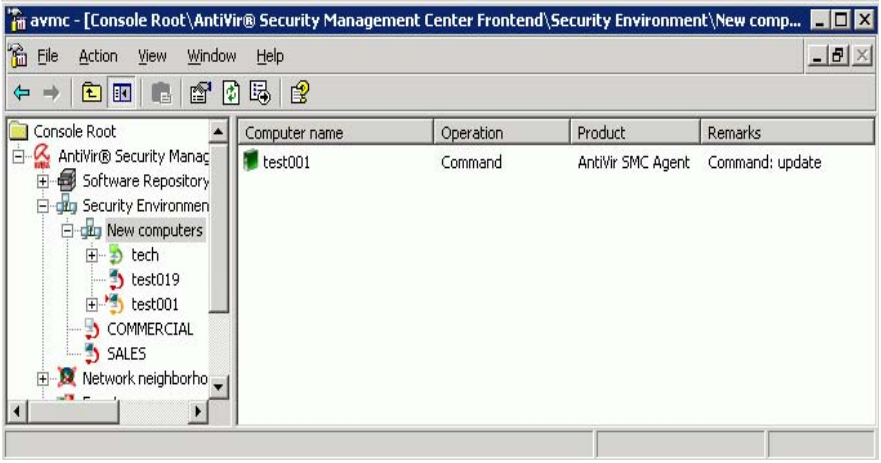


Запланированные задачи отображаются как ожидающие операции до момента запуска

Node Имя ПК или группы.
Name Имя задачи.
Task type **Server Task**: задача SMC. **Agent Task**: задача SMC Agent
Period Выбранная частота.
Start Выполнение первого запуска
Actor Продукт AntiVir выполняющий задачу
Status Информация о статусе задачи.
Command Конкретная для каждого продукта команда задачи. Параметры здесь не отображаются.

Просмотр ожидающих операций

Для каждого продукта AntiVir существуют свои команды (например, поиск или обновление). Используя AntiVir SMC, эти команды можно запланировать, как регулярно выполняющиеся задачи. Если задача не может быть выполнена из-за отсутствия ПК в сети, SMC сохраняет команду или задачу как ожидающую операцию. Эти операции будут выполнены, как только ПК будут доступны в сети. Ожидающие операции можно просмотреть для каждого ПК или группы



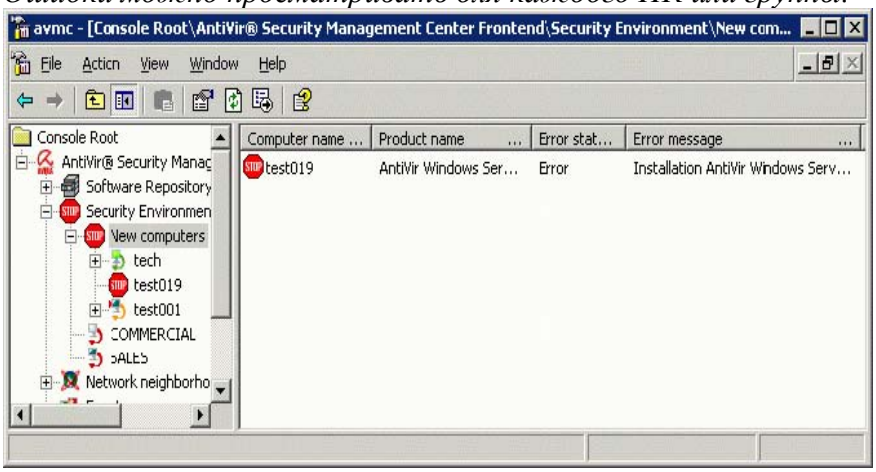
Computer name	Имя ПК, на котором должно выполняться задание
Operation	Тип задания (к примеру, установка или команда
Product	Продукт относящийся к задаче
Remarks	Информация об ожидающей задаче, например тип команды.

Просмотр ошибок

Если во время установки, настройки или удаления программного пакета, или во время действия продукта AntiVir на ПК в окружении безопасности **Security Environment**, или во время выполнения задач или команд произошла ошибка, AntiVir SMC может показать в SMC Frontend log-файлы продуктов AntiVir и служб SMC.

Ошибки всегда возникают на уровне ПК, поэтому узлы не могут генерировать ошибки, так как они не представляют физическую сеть

Ошибки можно просматривать для каждого ПК или группы.



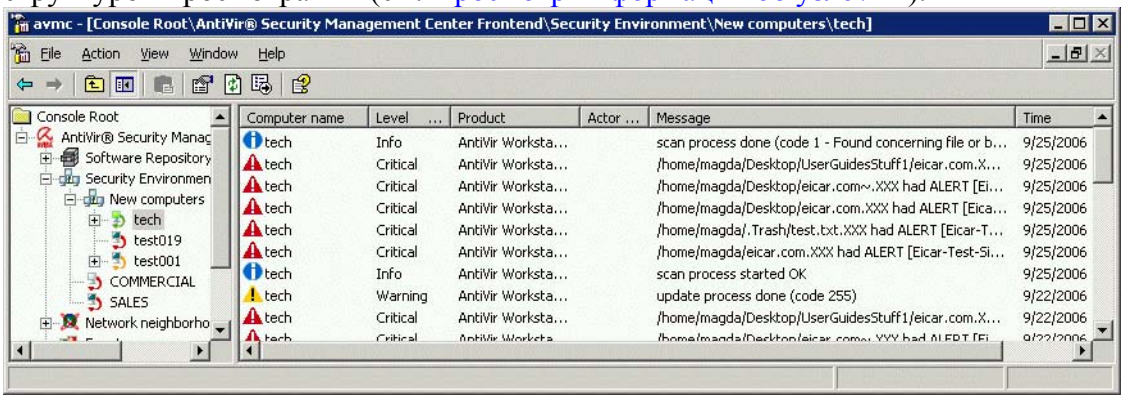
ComputerName	Имя ПК, на котором возникла ошибка
Product Name	Имя продукта, который сообщил об ошибке
Error Status	статус ошибки
Error Message	Содержание сообщения об ошибке
Created	Время и дата собития

6.4 Просмотр событий

Каждый продукт AntiVir создает особые события, которые собираются AntiVir SMC и отображаются SMC Frontend. Сначала SMC Agent собирает события продуктов AntiVir и сохраняет их в локальной базе данных.
Позже Вы сможете просмотреть эти события в SMC Frontend:

- Вы можете просматривать и сортировать события, которые произошли на каждом из ПК в окружении безопасности **Security Environment**
- Вы можете просматривать и сортировать события, которые произошли на всех ПК в окружении безопасности **Security Environment** в узле **Events**. Только в узле **Events** Вы можете сортировать события по определенным критериям.

Узел Events (события)
Панель результатов узла **Events** отображает детально все события, которые произошли в окружении безопасности **Security Environment**.
Структура просмотра событий всего окружения безопасности **Security Environment** сходна со структурой просмотра ПК (см. Просмотр информации об узле\ПК).



Сортировка событий
Вы можете отфильтровывать события и отображать только требуемые результаты. Возможны следующие варианты:

- **All**: отображение всех событий базы данных;
- **Level**: отображение событий определенного уровня (**Critical**/критическое, **Warning**/предупреждение или **Info**/информация);
- **Type**: отображение событий выбранного типа;
- **Product**: отображение событий определенного продукта AntiVir. Продукты доступные для фильтрации содержатся в меню **Filter/Product**;
- **String**: отображает события, которые содержат определенное выражение

Просмотр и фильтрация событий

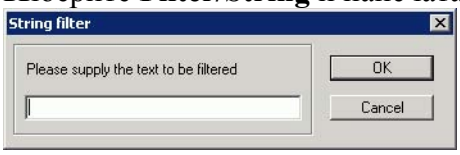
Узел **Events** показывает события, полученные SMC Agent из продуктов AntiVir окружения безопасности **Security Environment**, например, события сгенерированные при поиске вируса.

➢ Кликните **Events**
↳ Панель результатов отобразит все события окружения безопасности **Security Environment** (фильтр выключен)
➢ Если кликнуть на заголовок колонки, то данные будут отсортированы по критерию колонки, например, **Level** или **Time**.
➢ Кликните правой кнопкой на **Events**
➢ Выберите **Filter** и выберите нужные параметры фильтрации.

↳ Вы увидите отфильтрованные данные в области результатов

– ИЛИ –

выберите **Filter/String** и напечатайте в окне String filter:



- После набора текста кликните **OK**.
  ↳ Требуемые данные отобразятся в области просмотра

Удаление событий

Со временем список событий разрастается и Вам может потребоваться удалить его для сохранения места на диске

- Кликните правой кнопкой на **Events** и выберите **Delete all**.

6.5 Выполнение команд и планирование задач

Для каждого продукта AntiVir существуют различные возможности выполнения таких действий, как поиск вирусов и выполнение обновлений, используя особые параметры или планирование. Вы можете настроить, активировать и запланировать эти действия, используя AntiVir SMC для ПК и групп в окружении безопасности **Security Environment**. Действие, инициированное AntiVir SMC (например, поиск), считается командой **command**, а запланированное однократно или многократно повторяющееся называется задачей **Task** (например, еженедельное обновление).

Задачи могут быть на основе SMC или на основе Agent:

- Задачи SMC сохраняются в SMC. Это обеспечивает выполнение задач на ПК, которые будут включены в группу позднее
- Задачи на основе Agent сохраняются на ПК, на котором они будут выполнены при установленном агенте. Это обеспечивает выполнение периодических задач, таких как поиск вирусов, на ПК, который находится не в сети, например, ноутбук.

AntiVir SMC может запускать все команды, которые возможно выполнить на установленных продуктах AntiVir.

Дополнительную информацию о командах и параметрах AntiVir Вы получите в документации продукта AntiVir.

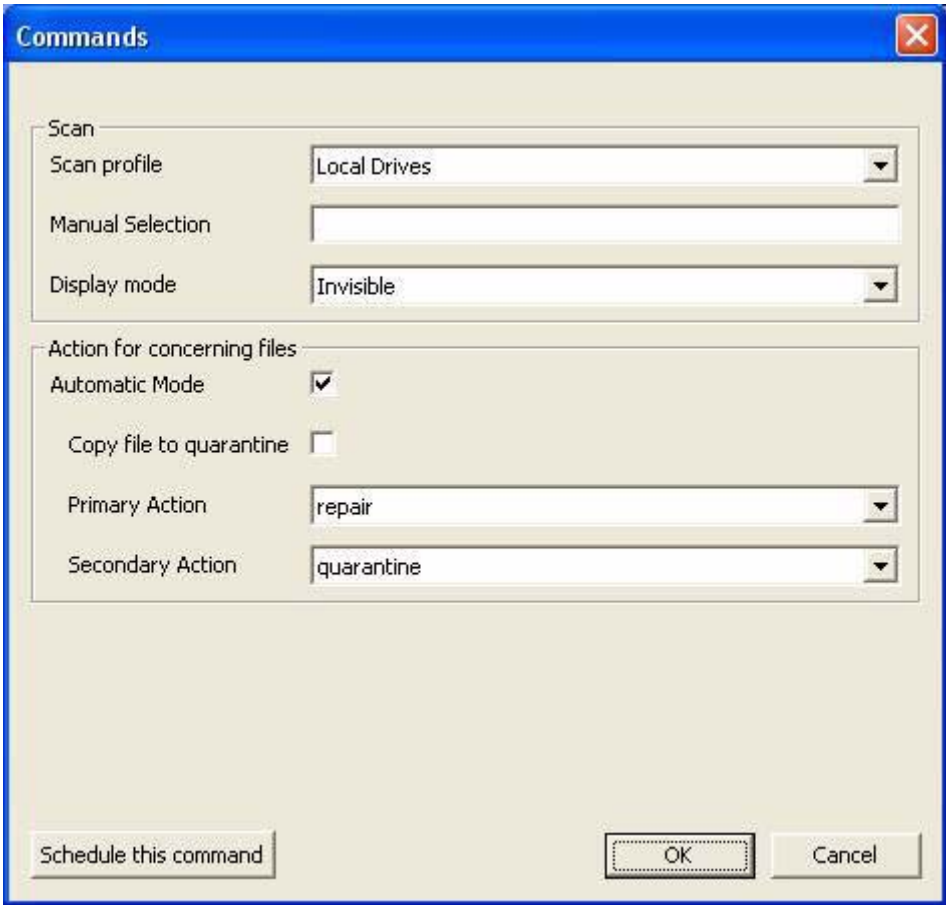
- Внимательно прочитайте все инструкции перед выполнением команд AntiVir SMC и планированием задач.

Результат команды или задачи можно увидеть в области результатов узла **Events** или узла группы или ПК.
Если ПК недоступны в сети, то действия и команды (например, настройка установленного продукта AntiVir) будут сохранены в режиме ожидания в SMC и запущены автоматически, после того как ПК/группы будут доступны в сети. Иконка статуса ПК будет показывать ожидающую операцию: темный монитор с оранжевой стрелкой, красный маркер с левой стороны

Выполнение команд

ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

- Кликните правой кнопкой ПК/группу и выберите **Commands**.
  ↳ Подменю отобразит установленные продукты AntiVir products и все их команды.
- Выберите команду (например, поиск).
  ↳ Если команда допускает параметры, то откроется окно ввода пути к приложению и параметров.



- Введите параметры и нажмите **OK**.
  - ↳ Команда запущена и результаты отражены в узле **Events** области результатов.

Планирование задач на основе Agent

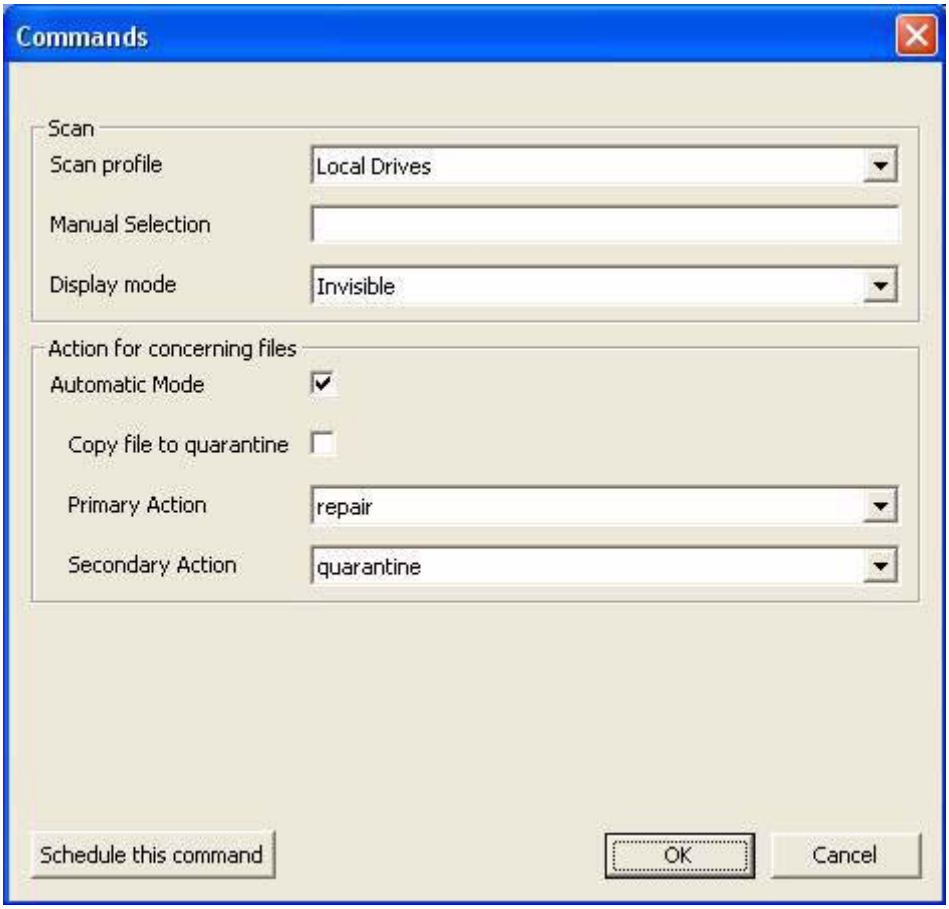
Эта процедура рекомендована специально для ПК, которые не постоянно находятся в сети, например ноутбуки.

Все доступные команды могут быть запланированы на определенное время. Такие команды называются задачами.

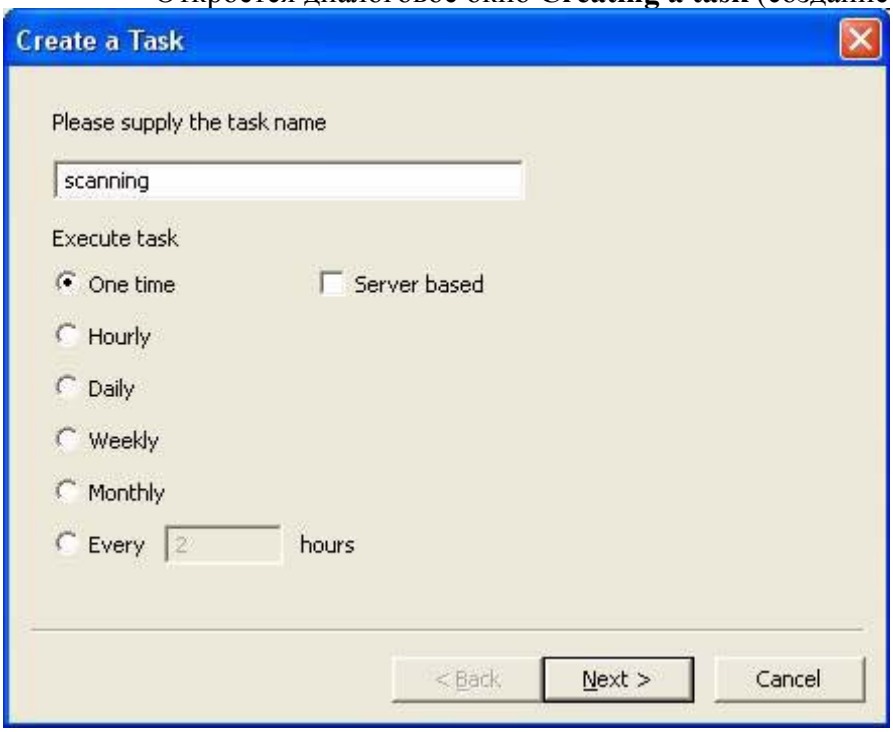
✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

Кликните правой кнопкой ПК/группу и выберите **Commands**.

- Кликните правой кнопкой ПК/группу и выберите **Commands**.
  - ↳ Подменю отобразит установленные продукты AntiVir products и все их команды.
- Выберите команду (например, поиск).
  - ↳ Если команда допускает параметры, то откроется окно ввода пути к приложению и параметров.

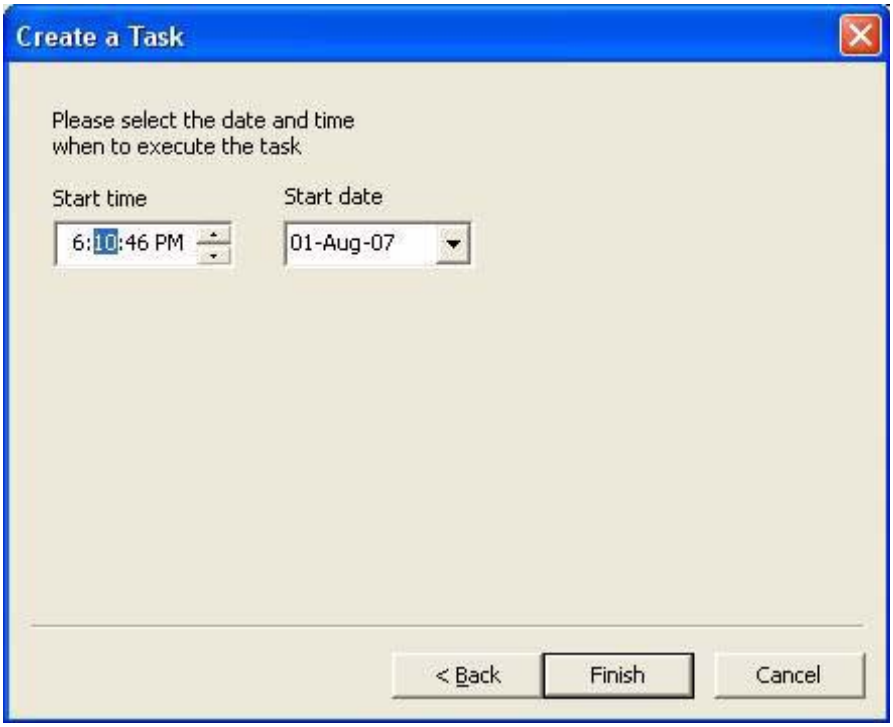


- Введите параметры и нажмите **Schedule this command** (запланировать команду).
  ↳ Откроется диалоговое окно **Creating a task** (создание задачи):



- Введите имя задачи и выберите частоту выполнения.
- Убедитесь, что опция **Server based** не активна.
- Нажмите **Next** (далее).

Откроется окно установки времени и даты:

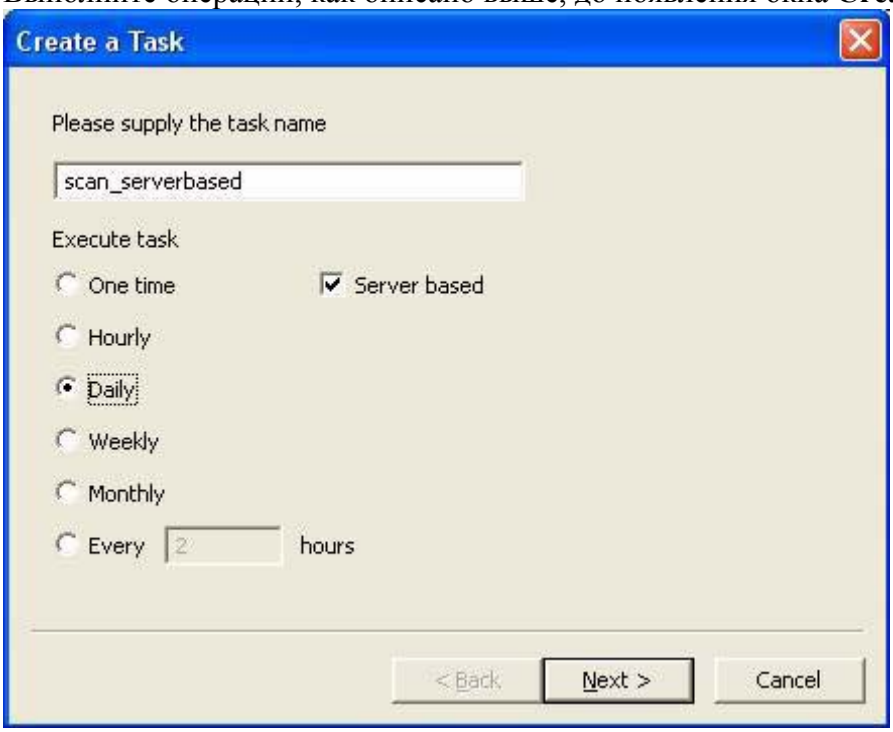


- Выберите время и дату запуска и нажмите **Finish** (завершить).

↳ Задача установлена и отображается в области результатов ПК/группы

Планирование задач на основе SMC

Выполните операции, как описано выше, до появления окна **Creating a task**:



- Введите имя задачи и выберите частоту выполнения
- Активируйте опцию **Server based**.
- Затем продолжайте, как описано в разделе **Планирование задач на основе** Agent

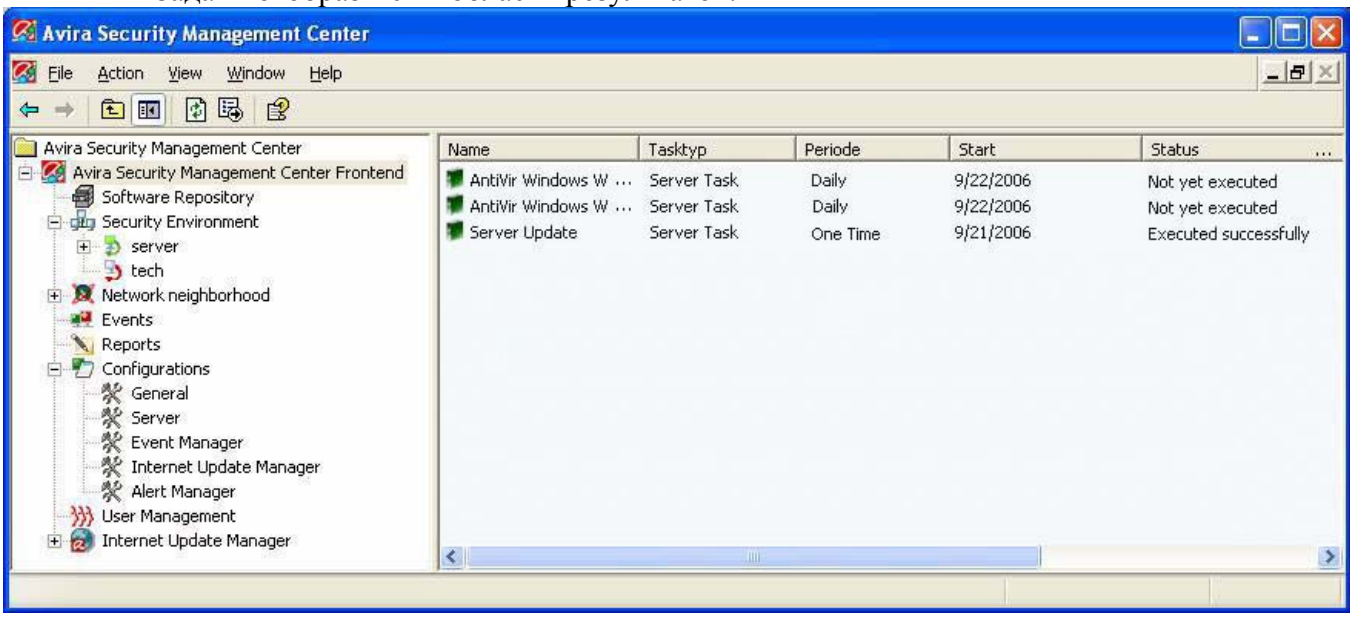
Отображение задач или ожидающих операций

Запланированные задачи отображаются в области результатов ПК/группы, в которых они запланированы.

- Кликните правой кнопкой мыши на ПК/группу и выберите **Tasks (задачи)** или **Pending operations** (ожидающие операции).
  ↳ Вы увидите задачи с дополнительной информацией

Отображение задач для программных пакетов Software Packs или SMC Server
Запланированные задачи обновления компонентов **SMC Server** или программных пакетов отображаются в узле **Events** Security Management Center Frontend.

- Кликните правой кнопкой **AntiVir Security Management Center Frontend** и выберите **Update/ Show tasks**.
  ↳ Задачи отобразятся в области результатов:



Name Имя задачи

Task type На основе Server: задачи для программных пакетов и SMC Server всегда на основе SMC

Period Выбранная частота выполнения

Start Время первого запуска

Status Информация о выполнении задачи

6.6 Создание и просмотр отчетов

Вы можете создавать отчеты для отдельных ПК/групп в окружении безопасности **Security Environment**, используя SMC Agent.

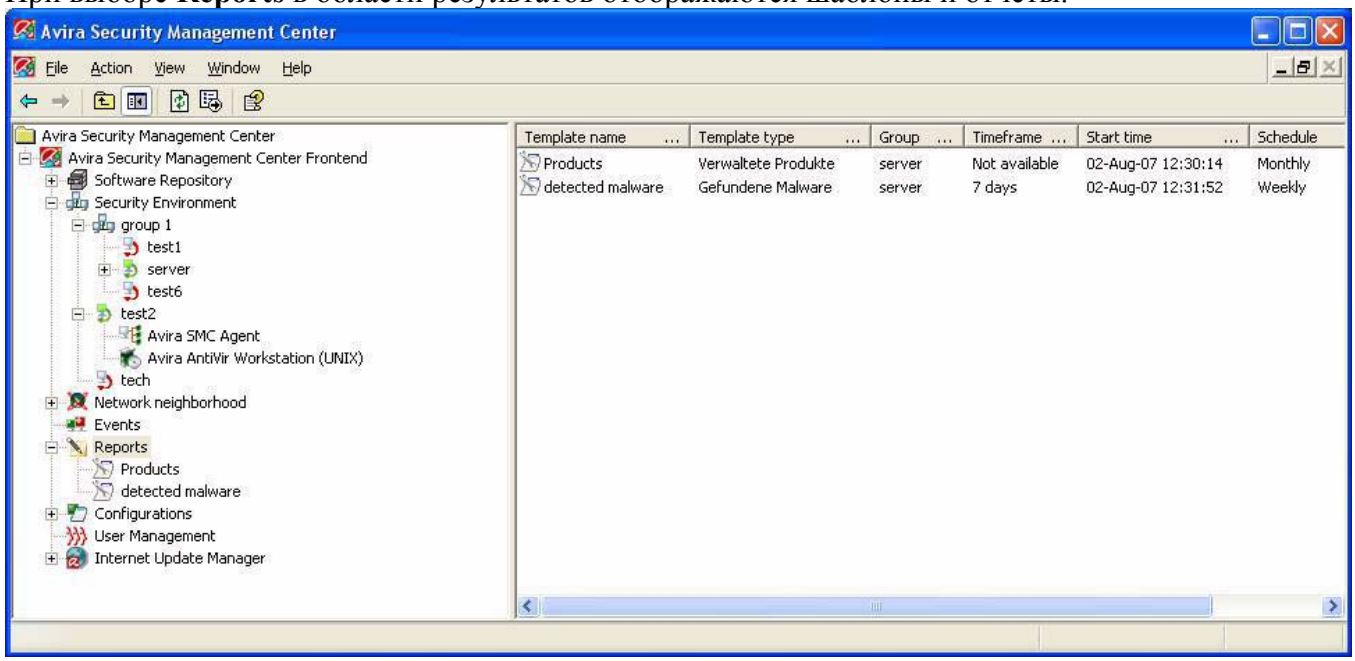
Сначала Вам необходимо создать шаблон для конкретного типа отчета. AntiVir SMC поддерживает все типы отчетов, которые поддерживаются продуктами AntiVir, установленными в окружении безопасности **Security Environment.**

Дополнительную информацию о типах отчетов Вы найдете в документации продукта AntiVir product.

- Пожалуйста, прочитайте внимательно все инструкции, относящиеся к типу отчетов, перед созданием и планированием отчетов AntiVir SMC.

SMC Agent создаст отчет на основе шаблона и пошлет его в SMC Server.

Узел Reports (отчеты)
При выборе **Reports** в области результатов отображаются шаблоны и отчеты.

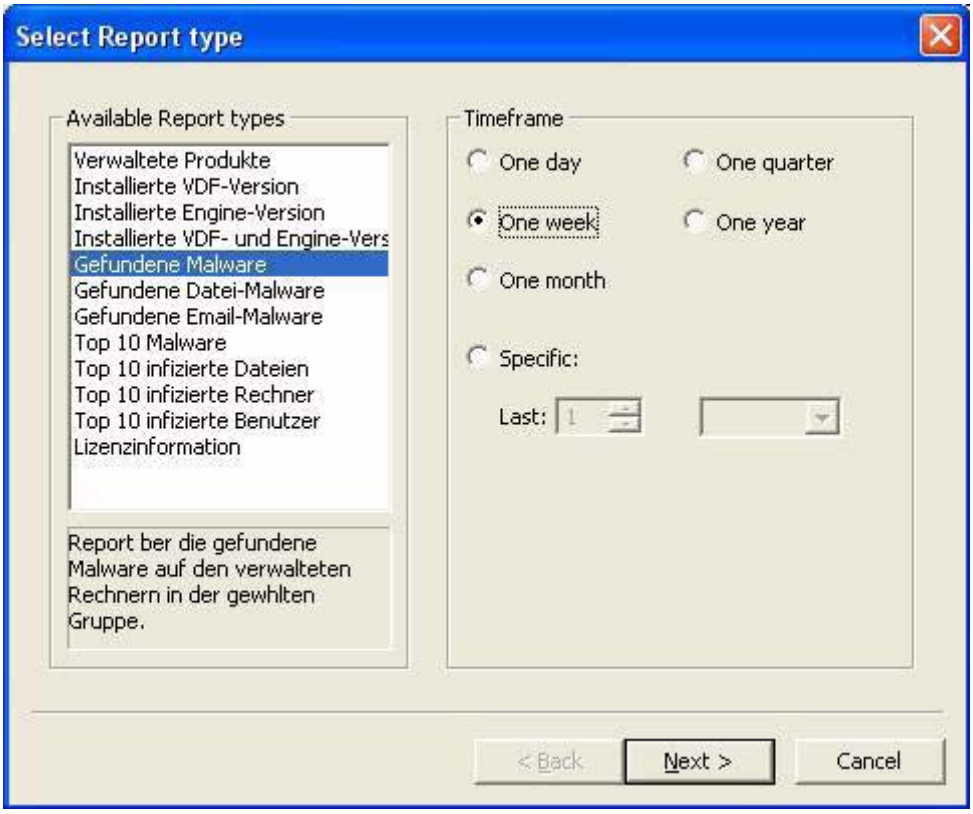


Template name	Имя отчета, определенное пользователем
Template type	Выбранный тип отчета
Group	Виртуальный ПК/группа, на котором запущен отчет.
Timeframe	Частота отчета (где возможно).
Start time	Время первых отчетов.
Schedule	Выбранный временной интервал отчета

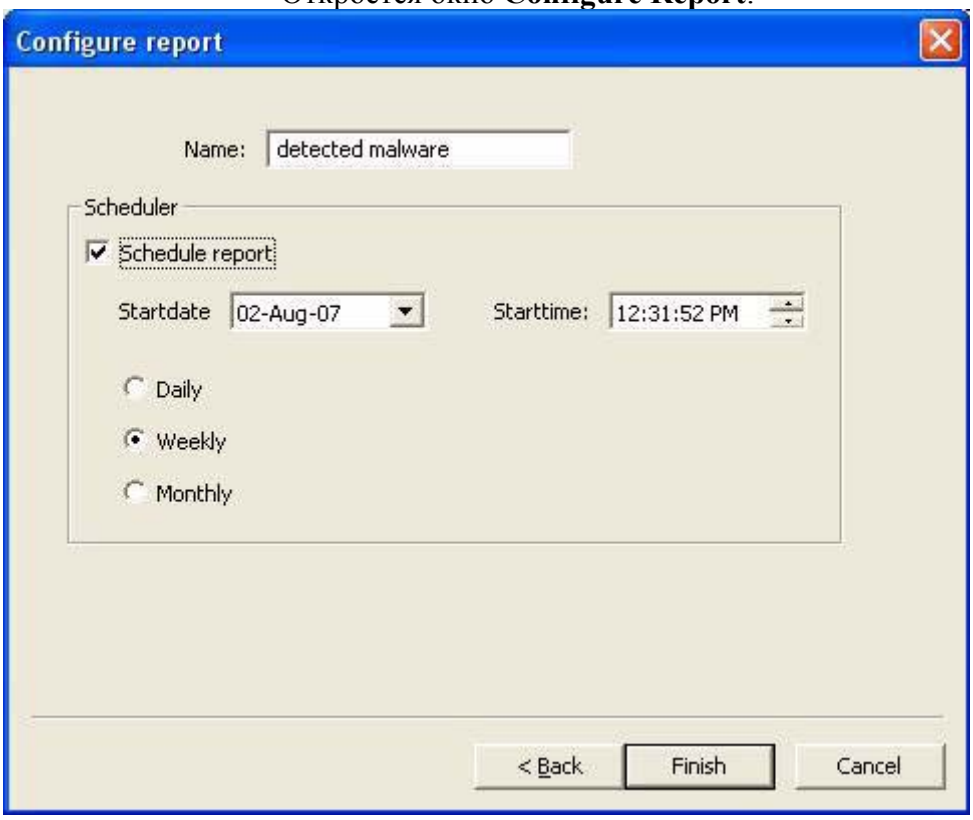
Создание шаблонов отчетов


ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой

- Кликните правой кнопкой на ПК/группу и выберите **Create report**.
  ↳: откроется окно следующего вида:



- Выберите тип отчета и интервал времени отчета и нажмите **Next/далее**.
  - ↳ Откроется окно **Configure Report**:



- Введите имя шаблона отчета

Если Вам необходимо запускать отчет регулярно:

- Выберите опцию **Schedule report**, введите дату, время и частоту запуска отчета
- Нажмите завершить **Finish**.

Создан шаблон отчета. Отчет будет создан немедленно или будет запланирован для периодического выполнения и отображается в узле **Reports**.

Редактирование шаблонов отчетов

В шаблоне нельзя менять тип отчета
Если Вы хотите изменить тип отчета, Вы должны создать новый шаблон

- Кликните правой кнопкой на шаблон в узле **Reports** и выберите **Properties**.
  ↳ Откроется окно **Select Report Type**/выбор типа отчета.
- Здесь Вы можете редактировать промежуток времени, кликните **Next**/далее.
  ↳ Откроется окно **Configure Report**/настройка отчета.
- Вы можете изменить имя, настройки планировщика; нажмите **Finish/завершить**.
  ↳ Изменения сохранены.
  ↳ Измененный шаблон отчета отобразится в области результатов.

Просмотр отчета

Отчеты SMC Agent можно просматривать в виде таблиц или файлов HTML.

- Разверните узел **Reports** дерева консоли.

↳ Панель результатов отобразит имеющиеся шаблоны.

- Кликните правой кнопкой шаблон отчета

↳ Вы увидите созданные отчеты с датой/временем начала и конца

- Кликните правой кнопкой нужный отчет и выберите **List** или **HTML**.

↳ Отчет отобразится в области результатов

Печать отчетов

AntiVir SMC создает отчеты в виде HTML-страниц, используя редактор HTML Вашей операционной системы (например, Microsoft Word или Microsoft Internet Explorer).

- Выберите отчет
- Кликните правой кнопкой и выберите **Print/печать**.
  ↳ Отчет откроется в редакторе HTML editor.
- Используйте команду печати редактора.

6.7 Распределение и выполнение файлов/программ в безопасном окружении

Вы можете распределять только определенные программы, сертифицированные Avira между ПК в окружении безопасности ***Security Environment****.*

AntiVir SMC имеет две возможности распределения и запуска файлов или приложений (сертифицированных Avira) удаленно на всех ПК окружения безопасности **Security Environment.**

- Вы можете распределить любой файл или программу (возможно с параметрами запуска или командой) среди ПК или групп, например, специальные утилиты удаления вирусов, файлы лицензии и т.д., а также немедленно их запустить.
- Вы можете удаленно настроить SMC Agent для запуска программ на других ПК, а также запланировать все эти задачи

При открытии общего доступа (share) файлы копируются в директорию установки продукта AntiVir, который Вы выбрали (\\<smc server>\C:\Program Files\AntiVir Security Management Center Agent). Эта директория будет корневой для такого рода действий в AntiVir SMC. Вы можете также создать поддиректорию (например,...\New-VDF-files) для более быстрого поиска файлов. Для открытия программы удаленно она должна находиться в папке SMC Agent (\\Client\C:\Program Files\AntiVir Security Management Center Agent).

Если Вы хотите использовать данную функцию чаще, рекомендуется создать стандартную директорию для скопированных файлов. Пример: ***…\Shared Files.***

Возможна потеря данных при неправильной настройки программы!

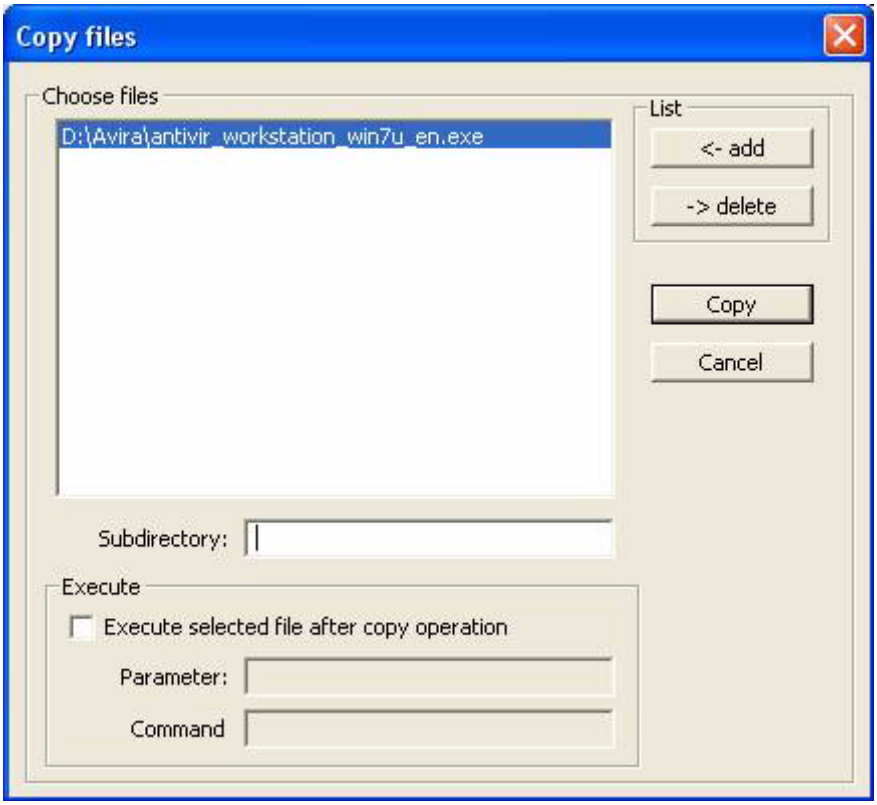
При распределении исполнимых файлов:
Пожалуйста, внимательно прочитайте инструкцию к программам, командам и параметром перед их применением в AntiVir SMC.

Если программы не ноль, то в SMC Agent посылается событие ошибки. Это будет отображено в **Events**.
Если ПК недоступны в сети, то действия и команды (например, настройка установленного продукта AntiVir) будут сохранены в режиме ожидания в SMC и запущены автоматически, после того как ПК/группы будут доступны в сети. Иконка статуса ПК будет показывать ожидающую операцию: темный монитор с оранжевой стрелкой, красный маркер с левой стороны

Распределение и открытие файлов/программ

ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

➢ Кликните правой на ПК/группу и выберите **Installation/[AntiVir product]/ Copy files**.
↳ Откроется окно копирования файлов:



- Кликните **Add** и выберите файл(ы)/программу(ы) для копирования.
- Для скопированных файлов Вы можете создать подкаталог

Если Вы хотите немедленно открыть скопированные файлы:

- Выберите **Execute …** и введите нужные параметры или команду.

Общий доступ к файлам лицензий

Для продления лицензии продуктов Avira Вам необходимо новый файл лицензии, используя функцию **Copy files**.

Обновите файл лицензии в **Software Repository** для использования его для дальнейших установок.

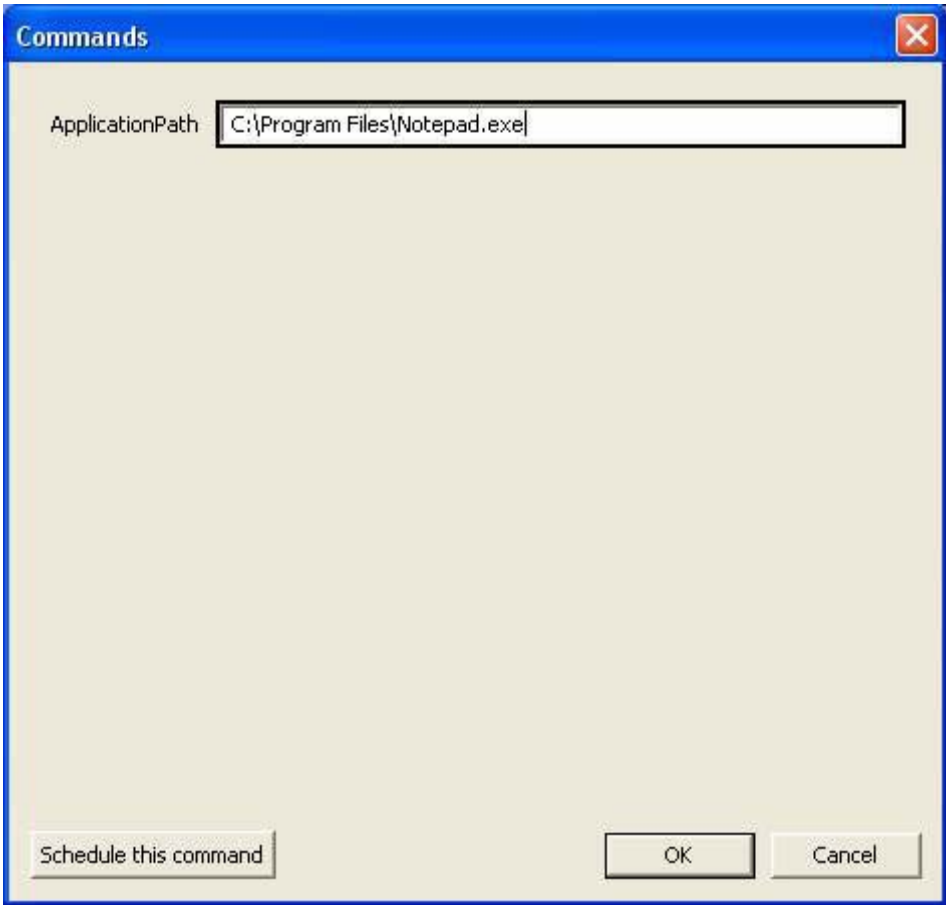
Кликните правой кнопкой мыши по крупе или ПК, на котором установлен продукт AVIRA в окружении безопасности **Security Environment**, выберите **Installation/[Avira product]/Copy files** и выполните операцию описанную выше.

Запуск программ

- ✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

- ✓ Программные файлы хранятся в каталоге установки ПК/ группы.

- Кликните правой кнопкой ПК/группу и выберите **Command/AntiVir SMC Agent/ execute**.
  ↳ Откроется окно **Commands**



- Введите путь и имя файла (например, **Shared Files/Notepad.exe**).
- Если Вы хотите запустить программу немедленно:нажмите **OK**.
  - ↳ Программа будет запущена

– ИЛИ –

Если Вы хотите запускать программу периодически: кликните **Schedule this command** (запланировать данную команду) The task is displayed in the computer/group Details pane.

6.8 Устранение ошибок

Если во время установки, настройки, удаления программных пакетов или во время действий продуктов AntiVir на ПК или группах или во время выполнения команды и задачи возникают ошибки, AntiVir SMC может отобразить log-файлы продуктов AntiVir и служб SMC в SMC Frontend.

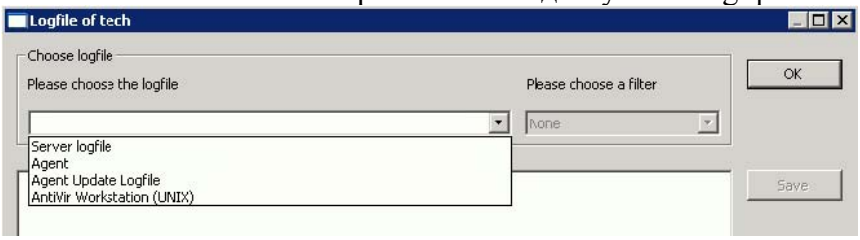
Ошибки всегда возникают на уровне компьютера, поэтому узлы не могут создавать ошибки, так как они не создают физическую сеть.

Для решения проблем мы рекомендуем сначала проверить log-файлы продуктов AntiVir и при необходимости сохранить их для обращения в службу поддержки

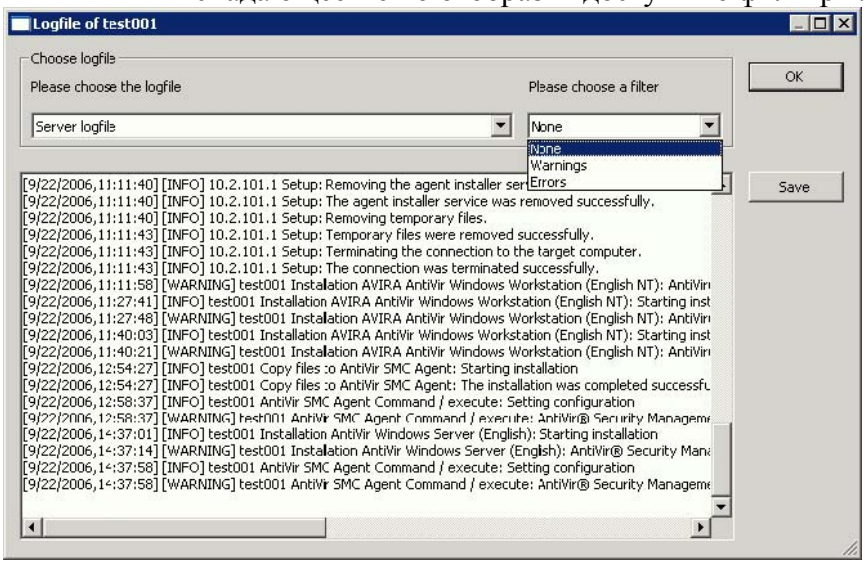
6.8.1 Просмотр Log-файлов

✓  ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой

➢Кликните правой кнопкой на ПК и выберите **View logfile**.
↳Откроется окно **Logfile of [имя ПК]**.
➢Кликните на стрелку ниспадающего меню в поле **Choose logfile**
↳ Меню отобразит список доступных log-файлов:



➢ Выберите log-файл.
↳ Log-файл отобразится в окне
➢ Кликните на стрелку ниспадающего меню **Choose a filter**.
↳ Ниспадающее меню отобразит доступные фильтры:



➢ Выберите фильтр
↳ Log-файл будет отфильтрован и отобразится в окне

6.8.2 Сброс статуса ошибки

При возникновении ошибки в Avira SMC соответствующие разделы **Security Environment** отмечаются красным значком **Stop** в дереве консоли.

√  Значок ошибки рядом с узлом ПК или группы.

Выберите вид сообщение об ошибке **Error messages** для группы или ПК в окружении безопасности **Security Environment.**

Проверка Log-файла Сначала проверьте log-файл узла, как описано выше, для определения и устранения ошибки

Удаление ошибки Для предотвращения удаления сообщения об ошибке: кликните правой кнопкой на ошибку и выберите **Delete**.

- Подтвердите **Yes**.
  - ↳ Сообщение об ошибке удалено

Сброс статуса ошибки Если Вы решили проблему:сбросьте статус ошибки:

- Кликните правой клавишей и выберите **Reset error state**.

7 Обновление продуктов Avira

Avira SMC предлагает несколько путей обновления продуктов Avira:

Вы можете обновлять как программные пакеты, так и уже установленные продукты Avira автоматически, используя **Internet Update Manager**, который интегрирован в Avira SMC и является частью программы установки SMC (setup).

-ИЛИ-

Если Вы отключили автоматический режим **Automatic mode** в узле **Server Configuration**, на закладке **Update settings**:

- Вы можете обновить программные пакеты **software packs** в **Software Repository** через интернет (при помощи команды или запланированной задачи).
- Вы можете обновить программные пакеты, используя удаленные команды обновления, которые тоже могут быть запланированы.

В зависимости от настроек задачи обновления каждого продукта AntiVir, Вы можете обновлять продукты AntiVir, установленные на ПК в окружении безопасности ***Security Environment*** *через Интернет или локальную сеть. Эти обновления выполняются каждым ПК отдельно. Программные пакеты таким образом обновлять нельзя.*

- Пожалуйста, прочитайте и следуйте процедурам обновления, описанным в инструкциях к продуктам AntiVir, перед выполнением обновлений через AntiVir SMC.

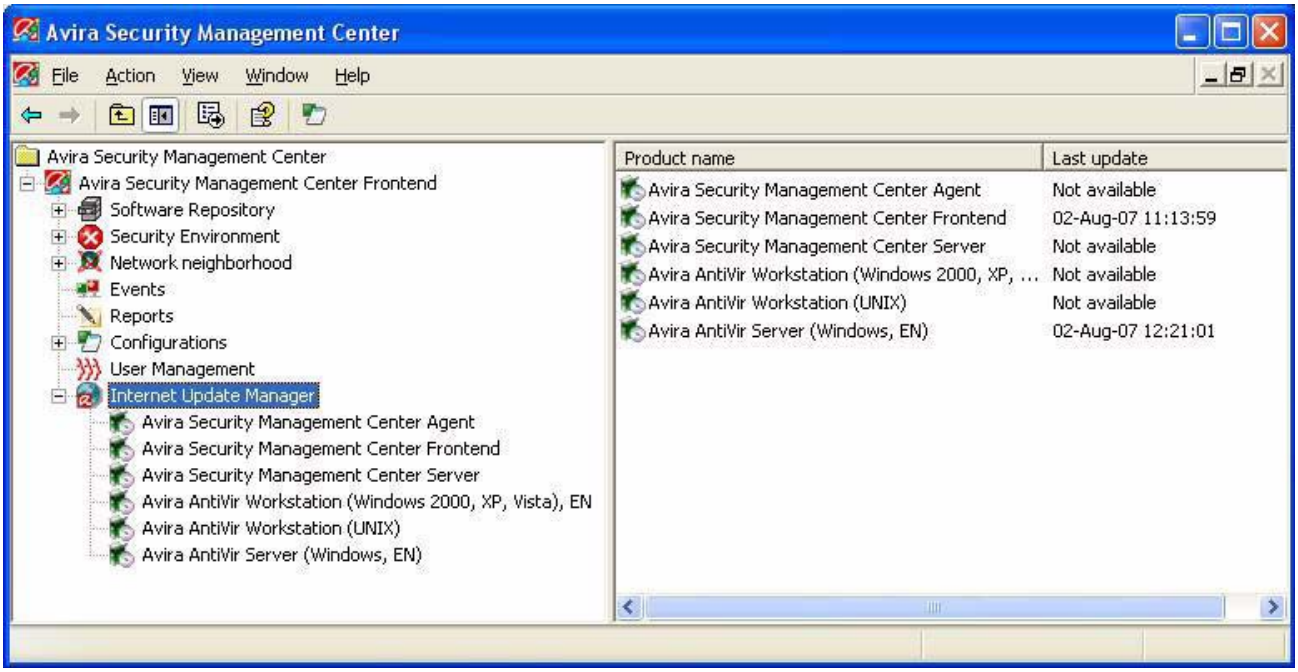
При обновлении программных пакетов, продукты AntiVir, установленные в окружении безопасности **Security Environment** не обновляются.

7.1 Использование Internet Update Manager

Служба Internet Update Manager является частью SMC Server и выполняет функцию обновления продуктов ANTIVIR в сети. Модуль IUM имеет уже настройки по умолчанию и не требует дальнейшего вмешательства. Кроме того, данный модуль позволяет раздать обновления по всей сети, не используя подключение Интернет на каждом компьютере.

Internet Update Manager использует следующие файлы обновлений:

• SMC Agent update files
• SMC Server update files
• SMC Frontend update files
• SMC Software Repository files (product packs)
• Product binaries of all Avira products

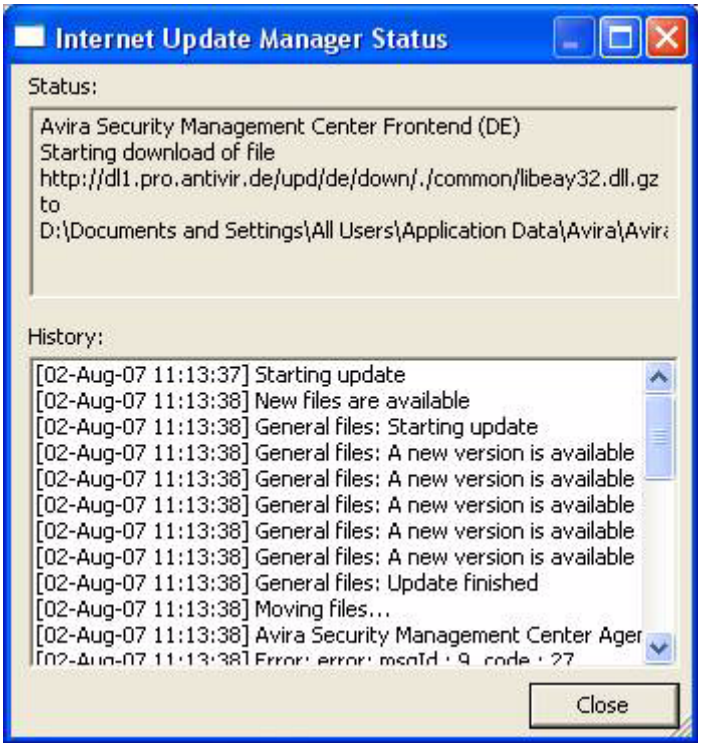


Основные опции IUM (меню щелчком правой кнопкой мыши):

• Status: возвращение информации статуса всех продуктов
• Update now: исполнение команд обновления
• Schedule Updates: планирование периодических задач обновления
• Cancel update: остановка процесса обновления
• Freeze current files: задачи обновления не будут выполнены для этих файлов.

Internet Update Manager сохраняет в log-файлы события обновлений и отправляет электронные письма с уведомлениями об ошибках **errors**, предупреждениях **warnings** или удачных обновлениях **successful updates.**

Для обновления продуктов Avira через IUM:
Кликните правой кнопкой мыши по **Internet Update Manager** или по конкретному продукту и выберите **Update now.**
Окно статуса отобразит процесс обновления:



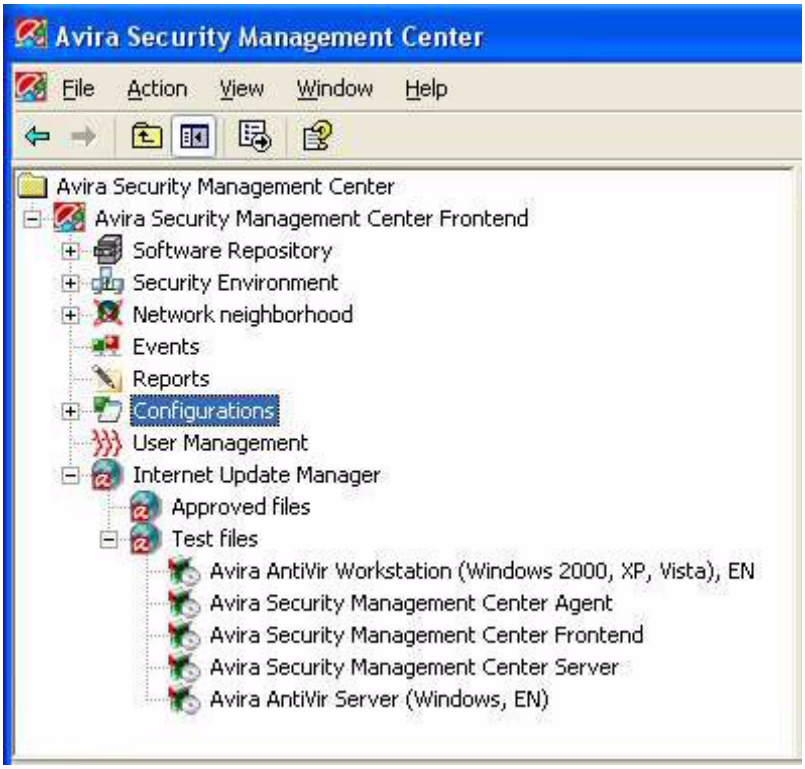
-ИЛИ-

Если Вы хотите запланировать задачу обновления для всех продуктов, включённых в IUM:

Кликните правой кнопкой мыши по Internet Update Manager или по конкретному продукту и выберите запланировать обновления **Schedule Updates**.

Откроется окно создать задачу **Create a task**, где Вы сможете установить интервал и время обновлений:

Вы также можете использовать IUM в тестовом режиме (который можно активировать в окне настроек). В тестовом режиме новые файлы загружаются в специальную тестовую директорию (**Test files**), в которой они проверяются на совместимость. Если файлы прошли проверку (**Approved files**), они могут использоваться основным HTTP сервером.



Параметры командной строки IUM:

`IUM.exe –uninstall`	Удаляет службу IUM из SMC
`IUM.exe -u`	
`IUM.exe –install`	Регистрирует службу IUM в SMC
`IUM.exe -i`	
`IUM.exe –start`	Запускает (зарегистрированную) службу
`IUM.exe –stop`	Останавливает (зарегистрированную) службу
`IUM.exe –restart`	Перезапускает (зарегистрированную) службу
`IUM.exe –run`	Запускает службу из консоли
`IUM.exe –checkstatus`	Возвращает информацию о текущем статусе IUM

7.2 Обновление пакетов в Software Repository

Для выполнения команд и задач обновления без использования Internet Update Manager Вам необходимо отключить автоматический режим **Automatic mode** в окне настроек *сервера* ***Server Configuration window***.

Ручное обновление программных пакетов

- Кликните правой кнопкой **Software Repository** и выберите **Update Software Repository/ Execute**

– ИЛИ –

Кликните правой кнопкой на отдельный программный пакет в **Software Repository** и выберите **Update/Execute**.

↳ AntiVir SMC соединится через Интернет с сервером Avira GmbH server, загрузит доступные обновления и сохранит их в узле **Software Repository**

Планирование регулярного обновления программных пакетов

В SMC Server можно также запланировать задачи регулярного обновления программных пакетов. Через узел **Software packs** можно обновить все программные пакеты или выбрать отдельные программные пакеты.

- Кликните правой кнопкой на **Software Repository** и выберите **Update Software Repository/ Schedule**

– ИЛИ –

Кликните правой кнопкой на отдельный программный пакет и выберите **Update/Schedule**.

↳ Откроется окно **Create a task**

- Введите название задачи, выберите частоту выполнения и нажмите **далее/Next**.

↳ Следующие два окна запросят дату и время

- Выберите дату и время и нажмите **Finish**/завершить.

↳ задача сохранена

Вы можете редактировать задачу в любое время, используя меню правой клавиши

7.3 Обновление продуктов AVIRA

Вы можете запланировать задачи обновления продуктов AntiVir, установленных на ПК в окружении безопасности **Security Environment.**

ПК/группы должны быть интегрированы в окружение безопасности **Security Environment**, иконка статуса должна показывать зеленый монитор с зеленой стрелкой.

- Кликните правой кнопкой на группу или ПК и выберите **Commands/[AntiVir product]/ Update**.

↳ Продукт AntiVir запускает процесс обновления и устанавливает программные файлы

8 Решение проблем

Убедитесь, что все компоненты SMC и продуктов Avira обновлены, это позволит обеспечить надёжную и эффективную работу окружения безопасности ***Security Environment.***

8.1 Необходимые условия для связи между SMC Agent и SMC Server

√ В firewall должны быть открыты следующие порты (TCP): 7000, 7001, 7010, 7020, 7021, 7030. Должны быть разрешены запросы ICMP и ping.
√ Гостевая учётная запись должна быть отключена
√ Простой общий доступ должен быть отключен
√ SMC Server должен иметь доступ к клиентскому общему диску C$ (\\<client's IP address>\c$\).
√ Для облегчения установки SMC Agent по сети Вам необходимо использовать административную учётную запись, общую для всех ПК.

8.2 Резервные копии SMC Server Files

Для создания резервной копии для SMC Server, кликните правой кнопкой мыши узел **Avira SMC Frontend** и выберите **Backup server files**.
Окно проводника Windows позволит выбрать имя и место сохранения резервной копии в виде .zip file.
По завершении процесса резервного копирования откроется сообщение описывающее процесс использования резервной копии:

8.3 Ошибка MMC при установке SMC Agent

Причина
Активирована опция **Использовать простой общий доступ к файлам** в меню панель управления/свойства папки/вид, дополнительные параметры
Эта опция устанавливает флаг **Force Guest** значение=1. При этом отсутствуют права администратора и SMC Agent не может быть установлен.
Решение
Деактивируйте данную опцию

8.4 Идентификационные номера программных пакетов **Software Pack IDs**

Если Frontend отображает сообщение "Missing software package with ID...", это означает что SMC обнаружил продукт Avira на клиентском ПК, который не интегрирован в Software Repository или имеет устаревшую версию.

ПО имеет следующие ID:
3 SMC Agent
30 AntiVir Windows Server German
31 AntiVir Windows Server English
51 UNIX Server
71 UNIX Workstation
91 UNIX MailGate
111 UNIX WebGate
121 UNIX Updater for SMC
200 AntiVir Windows Workstation German
201 AntiVir Windows Workstation English

9 Продукты, поддерживаемые AntiVir SMC
9.1 Поддерживаемые продукты AntiVir

AntiVir Security Management Center в данный момент поддерживает следующие продукты AntiVir, которые приобретаются отдельно. Для дополнительной информации посетите сайт: http://www.avira.com.

• Avira SmallBusiness Suite
• AntiVir Windows Workstation
– AntiVir Guard (On-Access Scanner)
– AntiVir MailGuard
AntiVir Windows Server 2000/2003
AntiVir UNIX Server (Linux)
AntiVir UNIX Workstation (Linux)
AntiVir UNIX MailGate (Linux)
AntiVir UNIX WebGate (Linux)

10 Сервис
10.1 Поддержка

Сервис поддержки	www.avirus.ru
Форум	http://forum.avirus.ru