

Guardant[®]

Система защиты от компьютерного пиратства

Руководство

системного администратора

Guardant Net

Издание 5.2

© 2007 Компания Актив

Содержание

Комплект поставки	4
На стороне сервера:.....	4
На стороне клиента:.....	4
Порядок установки	5
Концепция Guardant Net	6
Принцип работы Guardant Net	6
Сетевой ресурс ключа	6
Распределение сетевых ресурсов	6
Высвобождение зависших лицензий	7
Система управления лицензиями (LMS).....	7
Поддерживаемые сети и протоколы	8
Работа по протоколу TCP/IP.....	8
Работа по протоколу NetBIOS.....	8
Сервер Guardant Net	9
Загрузка сервера	9
Главное окно сервера Guardant Net	9
Ключи.....	9
Клиенты	10
Строка статуса	11
Сервис Windows Vista/2003/XP/2000.....	11
Установка и запуск сервиса Guardant Net.....	11
Остановка сервера Guardant Net.....	11
Удаление сервиса Guardant Net из системы.....	11
Опции командной строки.....	11
Администрирование сервера ключа	12
Изменение настроек через главное окно сервера Guardant Net	12
Изменение настроек с помощью сетевого монитора GrdMon.exe	12
Изменение настроек сервера с помощью web-браузера	12
Настройка сервера ключа. Файл GrdSrv.ini	13
Клиент Guardant Net	15
Настройка клиента Guardant Net	15
Мониторинг состояния и удаленное администрирование сервера Guardant Net . 17	
Сетевой монитор GrdMon.exe	17
Мониторинг	17
Администрирование	18
Выбор сервера из нескольких доступных	19
Мониторинг и настройка сервера через web-браузер.....	19
Концепция совместимости	20
Решение возможных проблем	21
Приложение не видит сервер ключа	21
Большая загрузка локальной сети.....	21
После выполнения Logoff в Windows Vista/2003/XP /2000/NT сервис не стартует	21
Особенности работы с сетевым ПО Guardant	22

Руководство предназначено для администраторов локальных сетей, в которых используется сетевое программное обеспечение, защищённое электронными ключами Guardant Net III/ Net II/ Net.

Руководство системного администратора содержит рекомендации по установке и настройке сервера электронных ключей Guardant Net, а также советы по устранению возможных неполадок.

Важная информация

Разработчикам настоятельно рекомендуется включать в комплект поставки защищенного ПО данный документ

Комплект поставки

Для нормальной работы защищенного приложения требуется наличие следующих файлов:

На стороне сервера:

GrdSrv.exe – сервер электронных ключей Guardant Net.

GrdSrv.ini – конфигурационный файл сервера, определяющий его основные параметры. Должен находиться в той же директории, что и **GrdSrv.exe**.

Также на сервере (компьютере, к которому присоединен электронный ключ) должны быть установлены драйверы Guardant. Они устанавливаются утилитой **GrdDriversRU.msi**, обычно входящей в комплект поставки защищенной программы. Если по каким то причинам драйверы отсутствуют, их последнюю версию можно загрузить с веб-сайта компании «Актив»: <http://www.guardant.ru/hotline/download/drivers/>.

На стороне клиента:

GnClient.ini – конфигурационный файл клиента. Содержит параметры, которые позволяют настроить защищенное приложение на сервер электронного ключа. Должен находиться в одной директории с исполняемым файлом защищенного приложения.

Порядок установки

Для начала работы с защищенным сетевым программным обеспечением необходимо:

1) Определить компьютер, на котором будет находиться электронный ключ Guardant Net. Это может быть как сервер сети, так и любая рабочая станция.

Важная информация

1. На компьютере должна быть установлена операционная система Windows Vista/ 2003/XP/2000/NT/ME/98 для LPT-ключей и Windows Vista/2003/XP/2000/ME/98 для USB-ключей

2. В локальной сети должны быть установлены и настроены протоколы TCP/IP или любой из интерфейсов NetBIOS. Необходимо контролировать соответствие протоколов. Например, если на клиенте установлен MS эмулятор NetBIOS на TCP/IP, то и на компьютере, на котором загружен сервер ключа, должен стоять тот же интерфейс NetBIOS

2) Установить на этом компьютере драйверы ключа (запустить файл **GrdDriversRU.msi** и следовать указаниям мастера)

3) Подсоединить ключ Guardant Net III/Net II/Net к соответствующему порту компьютера.

4) На этот же компьютер установить сервер ключа (файл **GrdSrv.exe**) и файлы, необходимые для его работы. При необходимости настроить конфигурационный файл сервера - **GrdSrv.ini** (существует возможность дистанционной настройки сервера (службы)). Запустить сервер.

5) Инсталлировать копии защищенного приложения на рабочие станции. При необходимости настроить конфигурационный файл клиента - **GnClient.ini**.

Важная информация

Если разработчик защищенной программы не использует стандартные утилиты системы защиты Guardant, то процесс установки защищённого приложения у конечного пользователя может отличаться от вышеприведенного, например, драйверы могут устанавливаться автоматически, в процессе инсталляции программного обеспечения и т. д.

Концепция Guardant Net

Guardant Net – это технология защиты сетевых приложений с помощью электронных ключей Guardant.

Основными компонентами Guardant Net являются:

Сетевой ключ	Ключ для защиты и лицензирования сетевого приложения
Сервер Guardant Net	Утилита, обрабатывающая и передающая запросы от клиента к ключу и обратно
Клиент	Копия защищенного приложения, которая обращается к серверу ключа с удаленного компьютера
Сетевой протокол	Протокол, по которому происходит обмен между сервером и клиентом

К важным понятиям Guardant Net также следует отнести *сетевой ресурс ключей* и *его распределение* (в том числе, при работе с многомодульными программными комплексами).

Принцип работы Guardant Net

Защищенное приложение обращается к электронному ключу Guardant Net через специальный программный сервер (**GrdSrv.exe**).

Чтобы начать работу, клиентское приложение должно зарегистрироваться на сервере ключа. В ходе регистрации сервер проверяет, подсоединен ли к компьютеру ключ с запрашиваемыми параметрами, и уменьшает на 1 значение ресурса лицензий ключа. Если регистрация прошла успешно, приложение нормально работает, в противном случае клиенту возвращается соответствующая ошибка.

При завершении работы приложение снимает свою регистрацию с сервера, при этом производится увеличение на 1 значения ресурса лицензий ключа.

Общий и текущий ресурс лицензий можно узнать с помощью утилиты GrdMon.exe, либо через стандартный web-интерфейс.

Сетевой ресурс ключа

Число одновременно работающих клиентских приложений ограничивается сетевым ресурсом ключей Guardant Net III/ Net II/ Net.

Реальный сетевой ресурс программируется разработчиком перед передачей защищенного приложения и ключа конечному пользователю. Значение реального сетевого ресурса равно числу оплаченных конечным пользователям лицензий на использование приложения.

Распределение сетевых ресурсов

В программном обеспечении Guardant версий 5.x сетевые лицензии могут распределяться по рабочим станциям или по копиям приложения.

Распределение сетевых ресурсов по рабочим станциям

При распределении сетевых ресурсов ключа по рабочим станциям:

1. Сетевой ресурс ключа уменьшается на 1 только при запуске первой копии защищенного приложения. Если с этого же компьютера запускать новые копии того же приложения (либо другие приложения, привязанные к тому же ключу), сетевой ресурс ключа уже не будет уменьшаться
2. Сетевой ресурс ключа возвращается (увеличивается на 1) только по завершении работы последней копии защищенного приложения, запущенной на данном компьютере. При этом порядок, в котором были запущены копии, не имеет значения.
3. Если компьютер с запущенным на нем защищенным приложением «завис», то лицензия, выделенная компьютеру, на 15 минут останется закрепленным за ним. С этого компьютера приложение по-прежнему можно будет запускать, однако это уже не повлечет за собой изменения сетевого ресурса ключа.

Распределение сетевых ресурсов по копиям приложения

При распределении сетевых ресурсов ключа по копиям приложения:

1. Сетевой ресурс ключа уменьшается на 1 при запуске каждой копии защищенного приложения, независимо от того, запущены ли несколько копий на одном или на нескольких компьютерах.
2. Сетевой ресурс ключа возвращается (увеличивается на 1) по завершении работы любой копии защищенного приложения, запущенной на любом компьютере в сети. При этом порядок, в котором были запущены эти копии, не имеет значения.
3. Если защищенная копия приложения «зависла», то лицензия, захваченная этой копией, на 15 минут останется закрепленной за ней. С этой рабочей станции приложение по-прежнему можно будет запускать, причем это влечет за собой уменьшение сетевого ресурса ключа (каждая запущенная копия захватывает 1 лицензию).

Важная информация

При распределении сетевых ресурсов ключа по копиям приложения необходимо иметь в виду, что запуск нескольких копий одного приложения на одном компьютере может привести к неоправданному расходованию сетевых ресурсов.

Высвобождение зависших лицензий

Зависание лицензий на сервере ключа — это распространенная ситуация, при которой единица сетевого ресурса на время остается закрепленной за рабочей станцией или копией приложения после их зависания или некорректного завершения работы. В этом случае в результате сбоя не выполняется операция GrdLogout, и сеанс связи с сервером не прекращается после фактического завершения работы приложения.

В сетевом ПО Guardant реализован механизм высвобождения зависших лицензий. Клиентское приложение производит регулярный, как минимум, один раз в 5 минут, опрос сервера Guardant Net. Сеанс связи с приложением, не отправившим данные в течение 3-х интервалов между опросами, прекращается, а данный клиент помечается в консоли сервера как «неактивный» (выделяется серым цветом). Т. о. лицензия становится свободной уже через 15 минут после зависания, но при этом информация о неактивном подключении остается в списке клиентов.

Лицензия, использовавшаяся неактивным клиентом, либо возвращается прежнему клиенту при повторной регистрации на сервере, либо передается новому клиенту, если тому не хватает свободной лицензии.

Важная информация

1. Необходимо учитывать, что в окне сервера помимо текущих активных подключений также отображаются все неактивные клиенты с момента запуска сервера. Это не означает, что каждый неактивный клиент занимает в данный момент единицу сетевого ресурса. В данном случае, это всего лишь своеобразная история подключений к серверу.
2. Удаление информации о зависших соединениях происходит автоматически через 1 сутки или больше (см. параметр BadClientKillTimeout в файле GrdSrv.ini).

Система управления лицензиями (LMS)

Для лицензирования многомодульных программных комплексов предназначена *система управления лицензиями*.

В этом случае, помимо общего (реального) сетевого ресурса ключа отдельный сетевой ресурс назначается каждому модулю программного комплекса.

При использовании таблицы лицензий происходит двухуровневый контроль лицензий:

1. Общее количество рабочих станций или число одновременно запущенных копий приложения (в зависимости от способа распределения), ограничивается реальным сетевым ресурсом ключа
2. Количество рабочих станций, на которых одновременно используется определенный модуль программы, или одновременно запущенные копии определенного модуля (в зависимости от способа распределения сетевого ресурса), ограничивается ресурсом этого модуля (значение соответствующего байта таблицы лицензий)

При этом значение реального сетевого ресурса может не совпадать с суммой ресурсов лицензий всех модулей.

Поддерживаемые сети и протоколы

Сетевые ключи Guardant могут работать в любых локальных сетях с интерфейсами NetBIOS и TCP/IP. Однако следует учитывать, что сервер Guardant Net является Win32-приложением, поэтому он должен быть загружен на сервере или рабочей станции, работающей под управлением ОС семейства Windows.

Важная информация

В большинстве случаев можно рекомендовать отключение протокола NetBIOS в конфигурационных файлах клиента и сервера и работу только по протоколу TCP/IP.

В локальной сети должен быть настроен хотя бы один из указанных протоколов, в противном случае сервер ключа выдаст ошибку типа «Протокол не найден».

Работа по протоколу TCP/IP

Сетевое программное обеспечение Guardant не налагает ограничений на работу по протоколу TCP/IP. Доступности клиента по сети могут препятствовать только настройки сетевых экранов, маршрутизаторов и т. п. оборудования, а также настройки сетевых политик безопасности.

Таким образом, допускается работа с Guardant Net по Интернет (удаленные филиалы, корпоративная VPN), однако эта возможность является побочной, она не тестировалась досконально.

Работа по протоколу NetBIOS

В тех ситуациях, когда использование NetBIOS является единственной возможностью (например, при работе с сетевым DOS-приложением), следует учитывать особенности этого сетевого интерфейса.

По умолчанию, клиент, работающий по протоколу NetBIOS, «видит» сервер Guardant Net только в пределах одного сегмента сети, поскольку этот протокол является немаршрутизируемым. Когда возникает необходимость организовать работу защищенного приложения в сложной сети, состоящей из нескольких сегментов, можно воспользоваться одной из следующих рекомендаций:

1. Установить ключ и сервер Guardant Net на компьютер (например, Windows-сервер), доступный сразу из нескольких сегментов сети.
2. Разрешить межсегментный обмен пакетами. Для этого нужно установить или переконфигурировать маршрутизатор и/или коммутатор.
3. Установить в каждом сегменте сетевой ключ и сервер Guardant Net.
4. Использовать на компьютерах, входящих в другие сегменты, локальные ключи.

Сервер Guardant Net

Сервер Guardant Net (файл GrdSrv.exe) обеспечивает связь между защищенным сетевым приложением и ключом сетевым Guardant в ЛВС. Один сервер GrdSrv.exe может обслуживать запросы к нескольким сетевым электронным ключам Guardant.

Загрузка сервера

Сервер Guardant Net должен быть загружен на том же компьютере, к которому подсоединен сетевой электронный ключ.

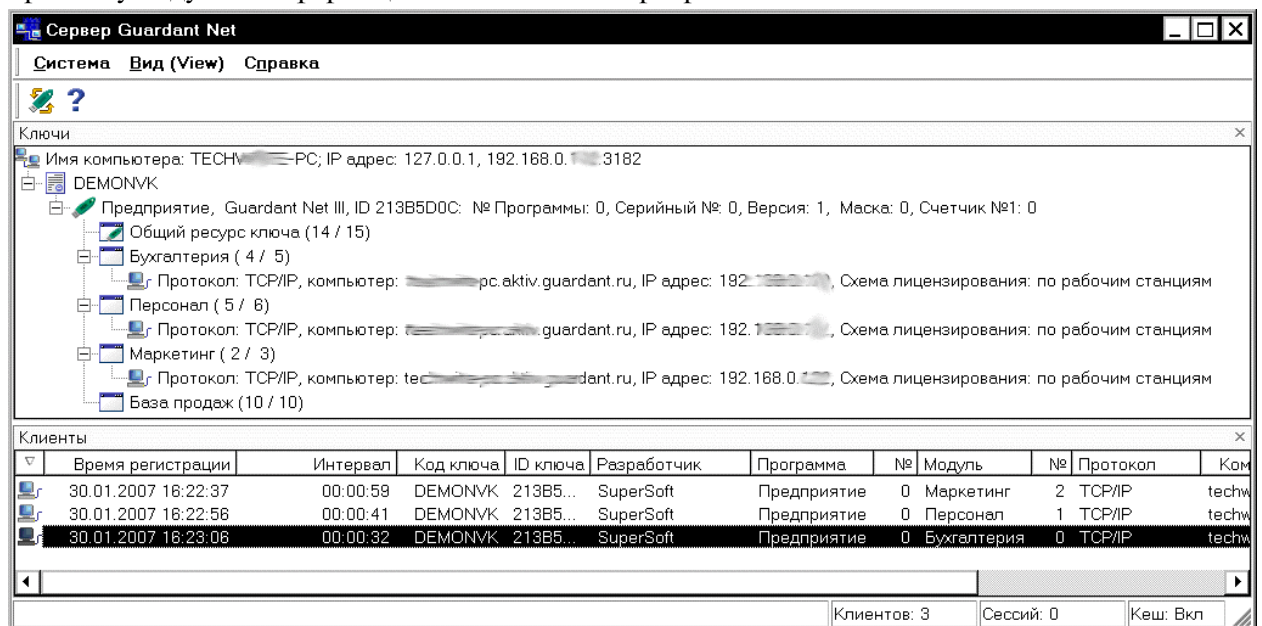
В пределах локальной сети можно запускать несколько серверов Guardant Net. Они должны находиться на разных компьютерах и обладать уникальными NetBIOS-именами (NetBIOS-имя и другие параметры сервера задаются в GrdSrv.ini). Запуск двух серверов (сервера и сервиса, двух сервисов) на одном компьютере невозможен.

Главное окно сервера Guardant Net

Информационная консоль сервера Guardant Net имеет интуитивно понятный графический интерфейс, и разбита на два взаимосвязанных горизонтальных окна, позволяющие отслеживать распределение лицензий.

В верхнем окне отображается древовидная структура по каждому зарегистрированному на данном сервере ключу.

Нижнее окно служит для отображения информации о клиентах по ключу в целом, либо по конкретному модулю. Информация может быть отсортирована.



Ключи




В окне Ключи с помощью древовидной структуры представлена информация о компьютере, на котором установлен ключ (ключи) и сервер, а также основные данные о клиентах:

Уровень вложенности	Что отображается	Описание
Основание древа	Информация о компьютере	Имя компьютера
		IP-адрес
		NetBIOS-имя
1-й	Общий код ключа	Идентификатор разработчика

Уровень вложенности	Что отображается	Описание
2-й	Информация о ключе	Модель ключа
		Название приложения
		Битовая маска
		ID ключа
		Номер программы
		Серийный номер
		Версия программы
		Значение счетчика GP
3-й	Информация о реальном сетевом ресурсе и модулях защищенного приложения	Значение реального сетевого ресурса ключа: текущий / максимальный
		Название модуля таблицы лицензий, его ресурс лицензий: текущий/ максимальный
4-й	Информация о клиенте	Сетевой протокол, по которому выполнено соединение
		Имя и IP-адрес компьютера, на котором запущен клиент
		Схема распределения сетевых ресурсов

Зарегистрированный на сервере сетевой ключ Guardant может быть доступным, заблокированным или недоступным.

Статус ключа отражают специальные символы рядом с пиктограммой ключа:

Пиктограмма	Статус ключа
	Ключ заблокирован операцией GrdLock
	Ключ недоступен (отсоединен)
	Отсутствие пометок означает, что ключ доступен, т. е. подсоединен к порту компьютера и не заблокирован.




Клиенты

Окно Клиенты служит для получения оперативной информации о зарегистрированных на сервере ключа клиентах. Окно организовано в виде таблицы, строки которой образуют характеристики клиентов, а столбцы – перечень клиентов:

Столбец	Характеристика клиентского приложения	
Время регистрации	Время регистрации клиентского приложения на сервере ключа в формате день.месяц.год часы:минуты:секунды	
Интервал	Время, прошедшее с момента последнего обмена данными с клиентом в формате часы:минуты:секунды	
Код ключа	Общий код (Public Code) ключа, используемого клиентом	
ID ключа	Идентификатор ключа, используемого клиентом	
Разработчик	Название фирмы-разработчика	Если используется таблица лицензий
Программа	Название клиентского приложения	
№	Порядковый номер клиентского приложения	
Модуль	Название модуля из состава многомодульного клиентского приложения	
№	Номер модуля из состава многомодульного клиентского приложения	
Протокол	Протокол, используемый клиентом для связи с сервером	
Компьютер	hostname / NetBIOS-имя компьютера, на котором запущено клиентское приложение	
IP-адрес	IP-адрес компьютера, на котором запущено клиентское приложение	
Версия	Версия клиента Guardant	
Платформа	Платформа, для которой написано клиентское приложение: Win32, Win16, DOS	

Данные о клиентах можно сортировать по возрастанию или убыванию по любому из параметров. Направление сортировки указывается стрелкой-индикатором в заголовке выбранного столбца

Зарегистрированный на сервере клиент может быть активным, неактивным и заблокированным. Статус клиента отражают специальные символы:

Пиктограмма	Статус клиента
	Активный клиент
	Неактивный, зависший клиент
	Клиент заблокирован операцией GrdLock

Строка статуса

В строке статуса сервера отображаются следующая статистическая информация о его работе:

Параметр	Описание
Клиенты: xx	Число клиентов, которых обслуживает сервер в данный момент
Сессии: xx	Количество сессий (сеансов связи), открытых с клиентами
Кэш: Вкл. /Выкл.	Состояние кэша сервера

Сервис Windows Vista/2003/XP/2000

Сервер Guardant Net может работать не только как обычное оконное приложение, но и как сервис (служба) Windows Vista/2003/XP/2000.

Преимущества сервиса состоит в том, что он запускается самой операционной системой во время ее загрузки, для его запуска не нужно выполнять процедуру регистрации на компьютере, и пользователю доступны специальные средства Windows по управлению сервисом.

Установка и запуск сервиса Guardant Net

Для установки сервиса запустите сервер из командной строки с опцией /i: **GrdSrv.exe /i**

Для установки и запуска сервиса запустите сервер с опцией /s: **GrdSrv.exe /s**

Это действие нужно произвести только один раз. После того как сервис Guardant Net будет успешно запущен, защищенные приложения получают доступ к сетевым ключам Guardant. Сервис будет запускаться автоматически при каждом старте ОС.

Остановка сервера Guardant Net

Работу сервиса Guardant Net можно временно приостановить. Для этого нужно зайти в **Панель управления | Службы** (для Windows NT) или **Панель управления | Администрирование | Службы** (для Windows Vista/2003/XP/2000) и щелкнуть правой кнопкой мыши на строке «Guardant Net service». В появившемся меню нужно выбрать «Стоп». Сервис останется установленным в систему, однако перестанет обрабатывать запросы к сетевым ключам. Для возобновления его работы нужно выполнить старт сервиса из Панели управления или командой **GrdSrv.exe /s**.

Важная информация

Остановка сервиса не предполагает его выгрузки из списка сервисов, т. е. при перезагрузке компьютера сервис Guardant Net будет снова загружен.

Удаление сервиса Guardant Net из системы

Для удаления сервиса Guardant Net нужно запустить GrdSrv.exe с опцией /r: **GrdSrv.exe /r**

Опции командной строки

Сервис Guardant Net поддерживает следующие опции командной строки:

GrdSrv.exe /i [q]	Установить сервис (службу) Guardant Net. Взаимодействие с рабочим столом отключено
GrdSrv.exe /s [q]	Стартовать службу Guardant Net, предварительно установив ее, если до этого она не была установлена
GrdSrv.exe /e [q]	Остановить службу Guardant Net
GrdSrv.exe /r [q] (или GrdSrv.exe /u)	Остановить и удалить службу Guardant Net
GrdSrv.exe /?	Краткая справка

Дополнительная опция /q отключает вывод диагностических сообщений. Код ошибки помещается в LASTERROR.

Администрирование сервера ключа

Настройки сервера Guardant Net хранятся в файле GrdSrv.ini.

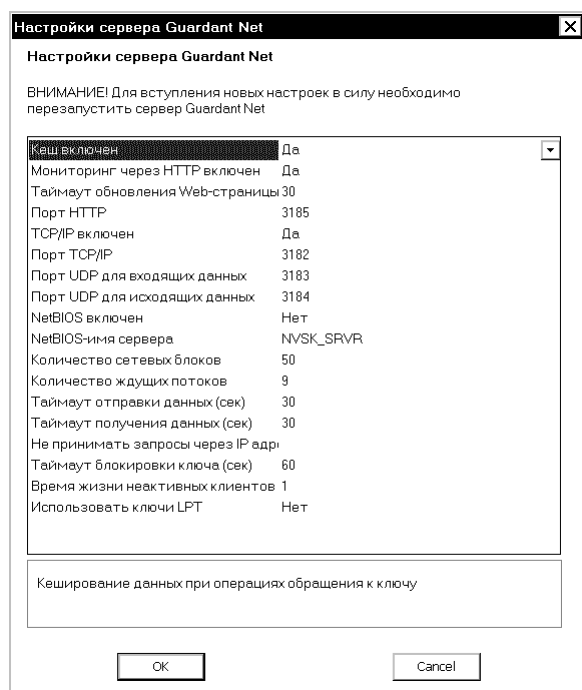
Управлять настройками сервера (службы) Guardant Net можно следующими способами:

Способ администрирования	Особенности	Сервер Guardant Net	
		Сервис	Приложение
Редактирование файла настроек GrdSrv.ini	Только локально	-	
Из главного окна сервера	Только локально, когда сервер работает как приложение	-	+
С помощью монитора GrdMon.exe	Удаленно, с любого компьютера	+	
Через web-интерфейс		+	

Изменение настроек через главное окно сервера Guardant Net

Запустите сервер GrdSrv.exe как приложение и выполните команду меню **Система | Настройки**.

На экране появится окно, в котором будут доступны для редактирования настройки сервера:



Более подробно о настройках см. пункт Настройка сервера ключа. Файл GrdSrv.ini.

Изменение настроек с помощью сетевого монитора GrdMon.exe

См. раздел [Сетевой монитор GrdMon.exe](#).

Изменение настроек сервера с помощью web-браузера

См. разделы [Мониторинг и настройка сервера через web-браузер](#) и [Сетевой монитор GrdMon.exe](#).

Настройка сервера ключа. Файл GrdSrv.ini

Файл GrdSrv.ini должен находиться в том же каталоге, что и сервер ключа. Если этот файл не будет найден, всем параметрам сервера ключа будут присвоены значения по умолчанию.

Секция	Параметр и его значение по умолчанию	Возможные значения	Описание
[NCBs]	TotalNCB=50	1 – 256	Максимальное количество сетевых пакетов, которое может получать/ передавать сервер
	NCBInLANA=3	1 – 9	Число новых клиентов, которое может быть зарегистрировано сервером на каждом LANА в один момент времени. Для нормальной работы сервера должно выполняться условие: TotalNCB > NCBInLANA*LANAs + 2, где LANAs – количество LANА на данной рабочей станции.
[CACHE]	CacheMode=On	On/Off	Кэш уменьшает время ответа GrdSrv.exe при выполнении чтения памяти ключа. Наиболее эффективно влияет на работу сервера с большим количеством клиентов и повышает устойчивость работы сервера в моменты пиковых нагрузок.
[TIMEOUT]*	TO_SEND=30	1 – 120 [сек]	Таймаут на посылку данных клиентом серверу ключа.
	TO_RECEIVE=30	1 – 120 [сек]	Таймаут на прием данных клиента сервером ключа.
	TO_SEARCH=5	1 – 120 [сек]	Таймаут на широковещательный поиск сервера ключа.
	BadClientKillTimeout=1	0 – 365 [суток]	Таймаут удаления информации о неактивных клиентах. 0 – не очищать
[PROTO- COLS]	TCP_IP=1	0, 1, 2	Используемые сетевые протоколы: 1, 2 – протокол используется, 0 – протокол не используется
	NETBIOS=2		
[SERVER]	TCP_PORT=3182	Любой доступный порт	Номер TCP/IP-порта, по которому происходит обмен между сервером и клиентом Guardant
	UDP_PORT_CLIENT=3183		Номер UDP-порта, через который клиент рассылает датаграммы серверам
	UDP_PORT_SERVER=3184		Номер UDP-порта, через который сервер отвечает клиенту
	NB_NAME=NVS_K_SRVR	Любое	NetBIOS-имя сервера Guardant Net. Не должно совпадать с host name компьютера
	IGNORED_IP=XXX.XXX.XXX.XXX	Список игнорируемых IP-адресов	Блокирование запросов нежелательных сетевых интерфейсов, при использовании нескольких сетевых карт. IP-адреса в списке разделяются запятыми
	UseLPTDongles=Off	On/Off	Использовать / не использовать LPT-ключи
	Dongles=x	По числу описаний	Число описаний ключей (только если используется система управления лицензиями)
[HTTP]	HttpService=On	On/Off	Мониторинг состояния службы Guardant Net через web-браузер
	HttpRefresh Timeout=30	Любое допустимое	Интервал обновления страницы web-браузера
	HttpPort=3185	Любой	Номер порта для приема http-запросов

* Увеличение таймаутов необходимо при работе по медленной линии или большой загрузке сервера ключа, чтобы клиент, ожидающий ответ, не отключался по истечении таймаута.

Секция [KEY_xx]

При использовании системы управления лицензиями в GrdSrv.ini добавляются секции вида [KEY_xx], где xx – номер секции. В этих секциях находятся описания ключей для различных многомодульных приложений – данные таблицы лицензий и параметры поиска ключа.

Возможные параметры поиска ключа расположены в секции по убыванию приоритета, т. е. ID ключа имеет абсолютный приоритет, а битовая маска – самый низкий. Уровень более приоритетного параметра выше суммы всех менее приоритетных.

При запуске сервер Guardant Net считывает информацию из подсоединенных ключей и подбирает для каждого ключа наиболее подходящее из описаний, содержащихся в ini-файле. Подходящим описанием считается такое, в котором суммарный приоритет параметров поиска, удовлетворяющих данному ключу, больше суммарного приоритета других описаний. Если в ini-файле есть несколько секций описаний с одинаковым суммарным приоритетом, то будет использоваться первая из них.

Параметры секции [KEY_xx]:

Параметр	Описание
PublicCode=xx	Общий код ключа
ID=xx	Идентификационный номер ключа. Параметр имеет абсолютный приоритет. Если указан ID ключа, то описание будет присвоено только данному ключу
VendorName=xx	Название компании-разработчика. Данные таблицы лицензий
ProgramName=xx	Название защищенного программного комплекса. Данные таблицы лицензий
ProgramNumber=xx	Номер программы. Дополнительный параметр поиска описания для ключа
Version=xx	Версия. Дополнительный параметр поиска описания для ключа
Mask=xx	Битовая маска. Дополнительный параметр поиска описания для ключа
SerialNumber=xx	Серийный номер. Дополнительный параметр поиска описания для ключа
Module0=xx	Имя 1-го модуля программного комплекса. Данные таблицы лицензий
ModuleN=xx	Имя N-го модуля программного комплекса. Данные таблицы лицензий

Клиент Guardant Net

Чтобы начать работу, клиентское приложение должно зарегистрироваться на сервере ключа. При старте сетевой клиент запрашивает сервер Guardant Net и продолжает работать только после успешной регистрации на сервере.

Клиент ищет сервер, как с помощью встроенных механизмов Guardant API, так и используя настройки файла конфигурации GnClient.ini: широковещательный поиск и указание прямого IP-адреса.

Широковещательный поиск включен в конфигурационном файле GnClient.ini по умолчанию. В этом случае при запуске клиент рассылает по сети периодические широковещательные запросы (датаграммы). На запросы откликается сервер Guardant Net, удовлетворяющий заданным параметрам поиска ключа. Широковещательный поиск может значительно сократить время регистрации клиента на сервере Guardant Net, особенно в Win32-приложениях.

Однако в некоторых случаях требуется указывать IP-адрес компьютера, на котором установлен ключ и запущен сервер.

При большом количестве клиентов сильно возрастает нагрузка на сеть и сервер ключа. В этом случае, рекомендуется устанавливать несколько ключей и серверов Guardant Net. Время отклика сервера зависит от его загрузки: раньше отвечает менее загруженный на данный момент сервер. Таким образом, автоматически происходит балансировка загрузки сервера ключа.

Настройка клиента Guardant Net

Конфигурируемые параметры клиента Guardant Net собраны в файле GnClient.ini. Этот файл должен находиться в одной директории с копией защищенного приложения. Для сетевого клиента JAVA конфигурационный файл может также располагаться в системном каталоге.

При отсутствии GnClient.ini всем параметрам сервера Guardant Net присваиваются значения по умолчанию. В этом случае клиент будет искать сервер со стандартным именем (NVSK_SRVR) и только по протоколу NetBIOS.

Секция	Параметр и его значение по умолчанию	Возможные значения	Описание
[PROTO-COLS]	TCP_IP=1	0, 1, 2	Используемые сетевые протоколы: 1, 2 – протокол используется, 0 – протокол не используется
	NETBIOS=2		
[TIMEOUT]**	TO_SEND=30	1 – 120 [сек]	Таймаут на посылку данных клиентом серверу ключа
	TO_RECEIVE=30	1 – 120 [сек]	Таймаут на прием данных клиента сервером ключа
	TO_SEARCH=5	1 – 120 [сек]	Таймаут на широковещательный поиск сервера ключа

** Увеличение таймаутов необходимо при работе по медленной линии или большой загрузке сервера ключа, чтобы клиент, ожидающий ответ, не отключался по истечении таймаута.

Секция	Параметр и его значение по умолчанию	Возможные значения	Описание
[SERVER]	TCP_PORT=3182	Любой доступный порт	Номер TCP/IP-порта, по которому происходит обмен между сервером и клиентом Guardant Net
	UDP_PORT_CLIENT=3183		Номер UDP-порта, через который клиент рассылает датаграммы серверам
	UDP_PORT_SERVER=3184		Номер UDP-порта, через который сервер отвечает клиенту
	BC_ADDR=255.255.255.255	-	Адрес широковещания. Константу 255.255.255.255 рекомендуется использовать при рассылке широковещательных пакетов. Фактически это означает, что при любой маске подсети все станции получают пакет.
	IP_NAME=127.0.0.1	Реальный IP-адрес или host name	IP-адрес компьютера, на котором установлены сетевой ключ и сервер Guardant Net. Если в сети используются динамические IP-адреса (DHCP-сервер), то вместо IP-адреса следует указывать host name компьютера.
	NB_NAME=NVSK_SRVR	Любое	NetBIOS-имя сервера Guardant Net. Не должно совпадать с host name компьютера.
	SEARCH=On	On/Off	Включение/выключение широковещательного поиска

Мониторинг состояния и удаленное администрирование сервера Guardant Net

Для мониторинга состояния сервера (или службы) Guardant Net и его настройки по сети можно использовать, как специальную утилиту **GrdMon.exe**, так и обычный web-браузер.

И сетевой монитор и web-браузер предоставляют одинаковую информацию по серверу ключа и одинаковые возможности по его настройке.

Сетевой монитор GrdMon.exe

Сетевой монитор **GrdMon.exe** предназначен для получения оперативной информации о серверах и сетевых электронных ключах Guardant в пределах ЛВС, а также администрирования серверов Guardant Net. Сетевой монитор можно запускать с любой рабочей станции.

При запуске монитор находит по сети все доступные серверы Guardant Net, устанавливает с ними связь и выдает на экран полученную информацию о первом найденном сервере.

Монитор GrdMon.exe поддерживает 2 режима работы: *мониторинг* и *администрирование* сервера. Переключение между режимами происходит при помощи панели управления, расположенной в верхней части окна монитора.

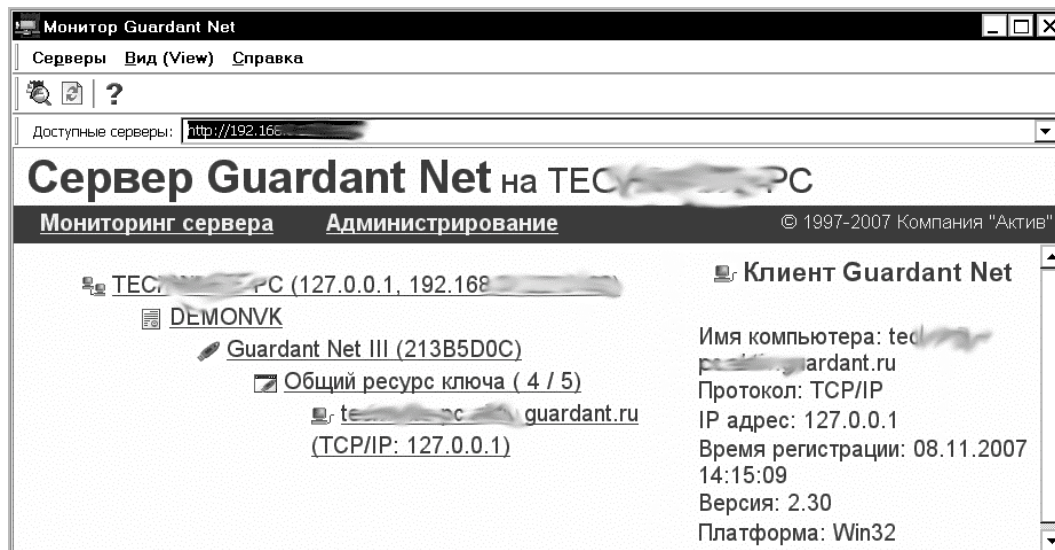
Окно монитора делится на две части:

Название	Что отображается
Рабочая область	Серверные объекты в виде древовидной структуры: информация о компьютере, на котором установлены ключ и сервер, а также основные данные о клиентах (режим мониторинга)
	Консоль администрирования сервера (режим администрирования)
Окно состояния выбранного объекта	Подробная информация по ранее выбранному в режиме мониторинга серверному объекту

Мониторинг

В рабочей области окна GrdMon.exe в режиме мониторинга отображается древовидная структура с информацией о параметрах и состоянии выбранного сервера и сетевого ключа Guardant. Эта информация идентична той, которую выдает в окне **Ключи** сам сервер GrdSrv.exe.

Подробная информация о любом серверном объекте (ключе, модуле LMS, зарегистрированном клиенте) отображается справа, в окне состояния, после выделения нужного объекта курсором мыши.



Администрирование

При переключении в режим администрирования происходит запрос пароля:

Доступные серверы:

Сервер Guardant Net на ТЕС...

Мониторинг сервера **Администрирование**

Пожалуйста, введите пароль администрирования

<input type="text"/>	Подтвердить
----------------------	-------------

Имя
ТЕС
Тай
(1..
Тай
(1..

Пароль по умолчанию: **admin**.

Важная информация

Чтобы сменить пароль или отказаться от его использования, необходимо загрузить сервер Guardant Net как приложение, выполнить команду меню **Система | Смена пароля администратора** и указать необходимое значение

После успешного ввода пароля в рабочей области отображаются настройки сервера, доступные для редактирования:

Монитор Guardant Net

Серверы Вид (View) Справка

Доступные серверы:

Сервер Guardant Net на ТЕС...-PC

Мониторинг сервера **Администрирование** © 1997-2007 Компания "Актив"

Пересчитать ключи	Выполнить
Таймаут отправки данных (1..120 сек)	<input type="text" value="30"/>
Таймаут получения данных (1..120 сек)	<input type="text" value="30"/>
<input checked="" type="checkbox"/> TCP/IP включен	
Не принимать запросы через локальные IP адреса	<input type="text"/>
Порт TCP/IP	<input type="text" value="3182"/>
Порт UDP для входящих данных	<input type="text" value="3183"/>
Порт UDP для исходящих данных	<input type="text" value="3184"/>
<input type="checkbox"/> NetBIOS включен	
NetBIOS-имя сервера	<input type="text" value="NVSK_SRVR"/>
Количество сетевых блоков (1..256)	<input type="text" value="50"/>
Количество ждущих потоков (1..9)	<input type="text" value="9"/>

Сервер Guardant Net

Имя компьютера: ТЕС... PC
Таймаут отправки данных (1..120 сек): 30
Таймаут получения данных (1..120 сек): 30
IP адрес: 127.0.0.1, 192.1...
Порт TCP/IP: 3182
Порт UDP для входящих данных: 3183
Порт UDP для исходящих данных: 3184
Кеш включен: Да
Использовать ключи LPT: Нет
Таймаут блокировки ключа (1..600 сек): 60
Время жизни неактивных сеансов (1..49 суток): 1
Периодичность обновления Web-страницы (сек): 30

Подробное описание настроек и параметров см. в пункте [Настройки сервера Guardant Net. Файл GrdSrv.ini](#).

Новые настройки подтверждаются нажатием на кнопку **[Принять изменения]** и сопровождаются перезагрузкой сервера без рестарта процесса.

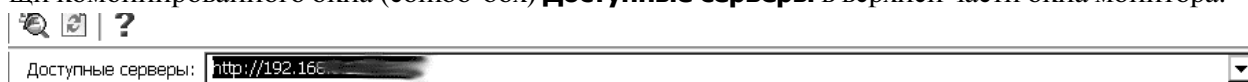
Важная информация

При удаленном администрировании строго не рекомендуется включать/отключать сетевые протоколы во избежание некорректной работы сервера Guardant Net!

Выбор сервера из нескольких доступных

Монитор находит все доступные в ЛВС серверы ключей. По умолчанию в главном окне монитора отображается первый найденный сервер Guardant Net.

Если найдено несколько серверов ключей, то переключение между ними происходит при помощи комбинированного окна (combo-box) **Доступные серверы** в верхней части окна монитора:



Кроме того, комбинированное окно **Доступные серверы** предназначено для задания IP-адреса компьютера, на котором запущен сервер ключа, вручную.

Мониторинг и настройка сервера через web-браузер

Для получения о сервере и изменения его настроек можно также воспользоваться стандартным web-интерфейсом, набрав в строке поиска браузера реальный IP-адрес (или host name) компьютера, на котором установлен сервер и сетевой ключ Guardant, и указав порт, по которому сервер ключа принимает http-запросы (по умолчанию 3185):

Например, **http://192.168.0.x:3185/**

Необходимо также удостовериться, что в файле настроек сервера GrdSrv.ini включена поддержка http-запросов (параметр **HttpService=On**).

Интерфейс и возможности для настройки сервера при помощи web-браузера такие же, как интерфейс и возможности сетевого монитора (см. описание [GrdMon.exe](#)).

Концепция совместимости

Чтобы использовать все возможности, реализованные в новых версиях сервера Guardant Net, бывает недостаточно просто заменить старую версию сервера.

Разработчик программного обеспечения должен перекомпилировать приложение с новыми объектными модулями и предоставить конечному пользователю соответствующее обновление.

Следует также помнить, что новые сетевые клиенты работают только с новыми версиями сервера (соответствующей им или более свежей версии). Совместимость старых клиентов с более новыми версиями сервера Guardant Net поддерживается.

Решение возможных проблем

Приложение не видит сервер ключа

1. Проверить соответствие установок в INI-файлах: протоколы, имя сервера.
2. Проверить правильность указания IP-адреса или NetBIOS-имени сервера в клиентском файле конфигурации.
3. Проверить наличие в системе сетевых протоколов, указанных в конфигурационных файлах, при необходимости переустановить их.

Большая загрузка локальной сети

1. **Использовать USB ключи.** При этом обмен данными происходит значительно быстрее (защищенное приложение «не тормозит»), существенно меньше используются ресурсы центрального процессора, нет проблем с захватом порта (конфликт разделения ресурсов, например, с периферией).
2. **Использовать несколько серверов.** Например, если у вас 50 рабочих мест и программа активно используется в течение рабочего дня всеми сотрудниками или по сети пересылается значительный объем данных, возможны некоторые перегрузки. Рекомендуется договориться с поставщиком, чтобы он выделил 2 электронных ключа по 25 лицензий вместо одного на 50. Если загрузка очень большая, например, постоянно шифруются какие-либо данные, возможно стоит поставить даже 3 ключа (10, 20 и 20 лицензий).

После выполнения Logoff в Windows Vista/2003/XP /2000/NT сервис не стартует

Данная ситуация является следствием особенностей функционирования интерактивных сервисов. Если необходимо постоянно выполнять Logoff, имеет смысл в свойствах сервиса Guardant Net, на вкладке «Вход в систему», снять флаг «Разрешить взаимодействие с Рабочим столом». В этом случае информационная консоль будет недоступна, и для контроля за состоянием сервера можно будет применять только web-интерфейс сервера Guardant Net.

Особенности работы с сетевым ПО Guardant

- Для использования сервера Guardant Net в сетях отличных от Windows (Novell, Unix, Linux и др.) достаточно запустить сервер ключа защиты на любой Windows-рабочей станции сети и убедиться в наличии поддерживаемых протоколов.
- Не рекомендуется без острой необходимости запускать сервер на компьютере с внешним IP адресом, поскольку в этом случае есть угроза несанкционированного использования лицензий. Если такая необходимость есть, то следует позаботиться о безопасности. Во всех остальных случаях рекомендуется запрещать обращение к порту сервера из внешних сетей. Запросы с «внешнего» интерфейса можно игнорировать, записав его IP-адрес в параметр IGNORED_IP в файле GrdSrv.ini.
- Не рекомендуется включать защищенное сетевое приложение на автозапуск при загрузке компьютера - при этом также резко возрастает вероятность пиковой перегрузки сервера. Типичный пример - когда с началом рабочего дня в какой-нибудь крупной организации одновременно включается сотня терминалов, и с них со всех практически одновременно поступают запросы к ключу.
- Не устанавливайте слишком больших значений конфигурируемых параметров в INI-файле сервера Guardant Net. Это не принесет ожидаемого адекватного эффекта (увеличения быстродействия, стабильности работы при пиковых нагрузках на сервер и т.п.) - просто сервер станет потреблять неоправданно много системных ресурсов (оперативной памяти и процессорного времени). Умолчательные значения параметров являются оптимальными для сетей с малым и средним количеством рабочих станций, увеличивать их имеет смысл лишь в каких-то серьезных случаях, например, при работе сервера с большим числом ключей в крупных сетях, и должно сопровождаться соответствующей коррекцией конфигурации самого протокола NetBIOS. Кстати, в случае если ресурсов, задаваемых конфигурируемыми параметрами, станет не хватать, сервер сам сообщит об этом, выдав на экран соответствующее сообщение.
- Для локальной работы с сервером Guardant (если отсутствует сетевой адаптер) по протоколу NetBeui в ОС Win'9x необходимо установить Dialup Adapter (Контроллер удалённого доступа).