

Guardant®

Система защиты от компьютерного пиратства

Руководство

системного администратора

Guardant Net

Содержание

Комплект поставки	3
Порядок установки	4
Принцип работы Guardant Net	5
Механизм высвобождения лицензий	5
Система управления лицензиями (LMS).....	5
Широковещательный поиск	6
Балансировка загрузки сервера.....	6
Концепция совместимости	6
Конфигурирование сервера Guardant Net	7
Секция [NCBs]	7
Секция [CACHE]	8
Секция [TIMEOUT]	8
Секция [PROTOCOLS]	9
Секция [SERVER]	9
Секция [HTTP]	10
Секция [KEY_XX]	10
Конфигурирование клиента Guardant Net	11
Секция [PROTOCOLS]	11
Секция [TIMEOUT]	11
Секция [SERVER]	12
Запуск сервера Опции командной строки	13
Решение возможных проблем	14
Мониторинг сервера Guardant Net	14
Приложение не видит сервер ключа	14
Большая загрузка локальной сети	14
После выполнения Logoff в Windows NT/2000/XP/2003 сервис не стартует	14
Особенности работы с сетевым ПО Guardant	15

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

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

Важно

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:

NnkSrv32.exe — сервер электронных ключей Guardant Net.

Novex32.dll — библиотека, необходимая для работы сервера.
Должна находиться в той же директории, что и NnkSrv32.exe.

NnkSrv32.ini — конфигурационный файл сервера, определяющий его основные параметры.
Должен находиться в той же директории, что и NnkSrv32.exe.

Также на сервере (компьютере, к которому присоединён электронный ключ) должны быть установлены драйверы Guardant. Они устанавливаются утилитой InstDrv.exe, обычно входящей в комплект поставки защищённой 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 защищённого приложения.

Примечание

1. Начиная с версии 2.0, сервер Guardant Net поддерживает протокол TCP/IP (поддержка реализована средствами WINSOCK 1.1 API).
2. Начиная с версии 2.1, сервер Guardant Net дополнен системой управления лицензиями, позволяющей, помимо контроля копий защищённого ПО, также лицензировать и отдельные модули программного комплекса. Кроме того, реализован графический интерфейс, а служба Guardant Net стала интерактивной.
3. Начиная с версии 2.3, клиентская часть Guardant Net поддерживает широковещательный поиск сервера в пределах локальной сети.
4. Начиная с версии 4.5, из конфигурационного файла NnkSrv32.ini исключена секция **[Service]**.

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.

Важно

1. На компьютере должна быть установлена операционная система Windows 95/98/Me/NT/2000/XP/2003 для LPT-ключей и Windows 95 OSR 2.1/98/Me/2000/XP/2003 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 драйверы ключа (запустить файл InstDrv.exe и выбрать кнопку **[Установить драйвер]**) (см. также <http://www.guardant.ru/hotline/instruction/>)

3) Подсоединить ключ Guardant Net к соответствующему порту компьютера.

4) На этот же компьютер установить сервер ключа (файл NnkSrv32.exe) и файлы, необходимые для его работы (см. [Комплект поставки](#)). При необходимости настроить конфигурационный файл сервера - NnkSrv32.ini (существует возможность настройки сервера в интерактивном режиме, если он работает как интерактивный сервис (служба)). Запустить сервер (см. [Опции командной строки](#)).

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

Примечание

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

Принцип работы Guardant Net

Защищенное приложение обращается к электронному ключу Guardant Net через специальный программный сервер (NnkSrv32.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.

Количество рабочих станций, на которых одновременно можно запустить защищенное приложение, равно ресурсу лицензий, определенному разработчиком программы.

Общий и текущий ресурс лицензий можно узнать, открыв либо окно сервера Guardant Net, либо его web-интерфейс.

Механизм высвобождения лицензий

В некоторых случаях на сервере ключа могут «зависать» соединения. Это может произойти, например, при некорректном завершении защищенного приложения, когда в результате сбоя не выполняется операция logout, т. е. сеанс связи с сервером не завершается. В последних версиях сервера электронных ключей (4.5 и выше) реализован обновленный механизм высвобождения «зависших» лицензий, суть которого заключается в следующем:

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

«Сброс» зависших соединений происходит сразу же, в том случае, если приложение было перезапущено с той же рабочей станции, или автоматически через 1 сутки или больше (параметр BadClientKillTimeout в файле NnkSrv32.ini).

Система управления лицензиями (LMS)

Система управления лицензиями (LMS) предназначена для лицензирования отдельных модулей сложных программных комплексов. Все основные настройки в INI-файлах, касающиеся LMS, производятся поставщиком программного обеспечения. Основная задача сетевого администратора - осуществление контроля за распределением лицензий на отдельные модули между компьютерами в локальной сети, в соответствии с рекомендациями поставщика программного обеспечения и количеством приобретенных лицензий.

Информационная консоль сервера Guardant Net версии 2.1 и выше, поддерживающего LMS, 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:

- Сетевые параметры компьютера, на котором загружен сервер ключа
- Общий код доступа
- Ключ
- Модульные и немодульные подключения

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

Широковещательный поиск

Начиная с версии программного обеспечения 2.3 сетевого ПО Guardant, в клиентских приложениях Guardant Net реализован механизм широковещательного поиска сервера ключа. При запуске клиент рассылает по сети периодические широковещательные запросы (датаграммы). На эти запросы откликается сервер Guardant Net, удовлетворяющий заданным параметрам поиска ключа.

Широковещательный поиск значительно сокращает время регистрации клиента на сервере Guardant Net, особенно в Win32-приложениях. При этом, в большинстве случаев, нет необходимости изменять настройки по умолчанию в конфигурационном файле клиента.

Балансировка загрузки сервера

При большом количестве клиентов сильно возрастает нагрузка на сеть и сервер ключа. В этом случае рекомендуется устанавливать несколько ключей и серверов Guardant Net.

В процессе прихода ответов от серверов ключей, клиент формирует список с их координатами (имя и IP-адрес хоста, NetBIOS-имя сервера). Время отклика сервера зависит от его загрузки: раньше отвечает менее загруженный на данный момент сервер. Таким образом, автоматически происходит балансировка загрузки сервера ключа.

Поиск сервера у Win32-клиента происходит быстрее, чем у DOS- и Win16-клиентов:

- По истечению времени рассылки, запроса клиенты DOS и Win16 пытаются поочередно установить связь с каждым найденным сервером, пока один из них не примет клиента. Если зарегистрироваться на серверах, найденных через широковещание, не удалось, или такие не найдены, клиент устанавливает связь с сервером, параметры которого указаны в файле GnClient.ini (IP_NAME, NB_NAME).

Важно

Чтобы сократить время регистрации, рекомендуется отключать в файле GnClient.ini неиспользуемые или некорректно работающие сетевые протоколы.

- У Win32-приложений процесс добавления NetBIOS-имени по LANa, широковещательный поиск по датаграммам и прямой поиск по настройкам файла GnClient.ini происходят параллельно. Как только найден первый сервер Guardant Net, клиент пытается установить с ним связь, и, в случае успеха, прерывает работу всех параллельных процессов, за исключением процесса добавления NetBIOS-имени, который нельзя остановить. Затем клиент получает лицензию и завершает регистрацию на сервере.

Концепция совместимости

Для того чтобы все обновления, реализованные в новых версиях (2.0 и выше) сервера Guardant Net, работали, 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.

Конфигурирование сервера Guardant Net

Конфигурируемые параметры сервера Guardant Net собраны в файле NnkSrv32.ini, который должен находиться в том же каталоге, что и сервер NnkSrv32.exe.

Начиная с версии 4.5, появилась возможность конфигурировать сервер интерактивно. Для этого в меню нужно использовать **Система | Настройки**. При сохранении настроек будет создан новый файл NnkSrv32.ini, содержащий новые установки. Перезапуск сервера в данном случае не требуется.

Важно

Если файл NnkSrv32.ini не будет найден, всем параметрам соответствующего сервера будут присвоены значения по умолчанию.

Параметры, записанные в файле NnkSrv32.ini распределены по секциям:

Секция [NCBs]

В секции [NCBs] собраны параметры, позволяющие настроить сервер на работу с большим или меньшим количеством клиентов. Секция [NCBs] актуальна только для соединений по протоколу NetBIOS.

По умолчанию сервер Guardant Net имеет конфигурацию, вполне достаточную для одновременного обслуживания порядка 10 клиентов, и не требует дополнительной настройки. Вмешательство может потребоваться, если в окне состояния сервера Guardant Net пиковое значение параметра NCB приближается к максимальному, либо если сервер выдает сообщения о необходимости увеличить эти параметры.

TotalNCB=XX

;Maximum NCB number (1..256, 50 by default)

TotalNCB=50

Параметр задает максимальное количество NCB, которые одновременно может создать сервер Guardant Net при работе с клиентами (или, иначе, максимальное количество сетевых пакетов, которое может получать/передавать сервер). На каждого клиента сервер может "потратить" до 2 NCB одновременно, поэтому значение TotalNCB косвенно характеризует и максимальное количество клиентов, которых (теоретически) способен обслужить сервер в один момент времени. Допустимые значения параметра — от 1 до 256, по умолчанию 50.

NCBInLANA=XX

;Maximum number of NCBs in each LANA (1..9, 3 by default)

NCBInLANA=6

При работе по протоколу NetBIOS большое значение имеет параметр LANA. Количество LANA на одной рабочей станции зависит от числа интерфейсов NetBIOS, загруженных на ней. После загрузки сервер ждет запросов от новых клиентов по всем доступным ему LANA, а реальное общение с каждым клиентом происходит только по какому-то одному LANA. Параметр NCBInLANA задает количество NCB, которые выделяются сервером для ожидания запроса от нового клиента на каждом LANA. Иными словами, этот параметр показывает, сколько новых клиентов может быть (теоретически) зарегистрировано сервером на каждом LANA в один момент времени. Допустимые значения параметра — от 1 до 9, по умолчанию 3. Для нормальной работы сервера на рабочей станции необходимо, чтобы значение параметра TotalNCB было, как минимум, на 2 больше, чем значение параметра NCBInLANA, помноженное на количество LANA на данной рабочей станции. То есть должно выполняться условие: $TotalNCB > NCBInLANA * LANAs + 2$, где LANAs — количество LANA на данной рабочей станции.

Секция [CACHE]

В секции [CACHE] собраны параметры, задающие конфигурацию кэша сервера Guardant Net. Кэш используется для того, чтобы уменьшить время ответа сервера Guardant Net при выполнении наиболее часто используемой операции — чтения памяти ключа. Кэш наиболее эффективно влияет на работу сервера Guardant Net с большим количеством клиентов и значительно повышает устойчивость работы сервера в моменты пиковых нагрузок.

CacheMode=On|Off

;Enable (On) or disable (Off) cache (On by default)
CacheMode=On

Параметр позволяет включить (On) или выключить (Off) кэш сервера Guardant Net. Если кэш выключен, остальные параметры секции [CACHE] не используются. По умолчанию включен (On).

Секция [TIMEOUT]

В секции [TIMEOUT] собраны параметры, задающие величину таймута блокирования электронных ключей, а также таймаутов на отправку и прием данных (в секундах). При работе на медленных линиях (независимо от протокола) значения можно увеличивать, чтобы клиент не отключался по истечении TIMEOUT'a.

LockTimeout=XX

;Dongle lock timeout in seconds (1..600, 60 by default)
LockTimeout=60

Если по каким-то причинам ключ остается заблокированным в течение длительного времени, он будет автоматически разблокирован по истечении времени таймута. Диапазон задаваемых значений таймута — от 1 до 600 секунд, по умолчанию 60 секунд.

TO_SEND=XX

;Send operation timeout in seconds (1..120, 20 by default)
TO_SEND=20

Максимальный таймат на отправку данных клиентом серверу ключа. Диапазон значений таймута — от 1 до 120 секунд, по умолчанию 20 секунд. Не рекомендуется уменьшать значение по умолчанию, т. к. это может привести к ошибкам соединения.

TO_RECEIVE=XX

;Receive operation timeout in seconds (1..120, 20 by default)
TO_RECEIVE=20

Максимальный таймат на прием данных клиента сервером ключа. Диапазон значений таймута — от 1 до 120 секунд, по умолчанию 20 секунд. Не рекомендуется уменьшать значение по умолчанию, т. к. это может привести к ошибкам соединения.

При работе по медленной линии или большой загрузке сервера значения таймаутов TO_SEND и TO_RECEIVE рекомендуется увеличивать, чтобы клиент, ожидающий ответ, не отключался по истечении таймута.

BadClientKillTimeout=XX

;Expired client kill timeout in days(1..365, 1 by default, 0-do not kill clients)
BadClientKillTimeout=1

Таймат сброса «зависших» клиентов, связь которых с сервером была потеряна. Диапазон значений таймута — от 1 до 365 суток, по умолчанию 1 сутки.

Секция [PROTOCOLS]

В секции [PROTOCOLS] собраны параметры, с помощью которых определяются используемые сетевые протоколы и их приоритет. Протокол TCP/IP поддерживают только клиенты для Win16 и Win32.

TCP_IP=X

NetBIOS=X

Возможные значения параметра:

0 - протокол не используется

1 - протокол используется первым

2 - протокол используется вторым

Примечание

В текущей версии Win32-клиента очередность использования протоколов утратила свое значение, так как опрос по всем протоколам происходит параллельно. Таким образом, если это значение не ноль - протокол используется. (эта особенность сохранена только для Win16)

DOS-приложения не используют протокол TCP/IP, из файла NnkSrv32.ini им требуется информация только о NetBIOS: имя сервера (NB_NAME) и таймауты (TO_SEND, TO_RECEIVE).

Секция [SERVER]

В секции [SERVER] собраны параметры, с помощью которых задается NetBIOS-имя сервера и адрес TCP/IP-порта.

NB_NAME=NVSK_SRVR

NVSK_SRVR — имя сервера по умолчанию

TCP_PORT=XXXX

3182 — номер TCP/IP-порта по умолчанию

DONGLES=X

X — число описаний ключей (если используется система управления лицензиями)

UDP_PORT_CLIENT=XXXX

Номер UDP-порта, через который клиент рассылает датаграммы серверам, 3183 — номер порта по умолчанию.

UDP_PORT_SERVER=XXXX

Номер UDP-порта, через который сервер отвечает клиенту, 3184 — номер порта по умолчанию.

IGNORED_IP= XXX.XXX.XXX.XXX, XXX.XXX.XXX.XXX, ...

Список IP-адресов сетевых адаптеров компьютера с установленным сервером Guardant Net, запросы на которые не будут приниматься.

IP-адреса разделяются запятыми. Иногда на компьютере, где установлен сервер Guardant Net, используется более одного сетевого интерфейса, каждый со своим IP-адресом. Эта опция используется в тех случаях, когда нужно блокировать запросы с нежелательных интерфейсов, например, когда этот интерфейс направлен в глобальную сеть.

Секция [HTTP]

Параметры, секции [HTTP] служат для настройки мониторинга состояния сервера Guardant Net через web-интерфейс (т. е. через web-браузер).

HttpService=On|Off

Обработка http-запросов включена (Off — выключена)

HttpRefreshTimeout=XX

Интервал перезагрузки страницы в секундах. Значение по умолчанию — 30 сек.

HttpPort=XXXX

Номер порта для приема http-запросов. Значение по умолчанию — 3185.

Секция [KEY_XX*]

Данная секция не предназначена для пользовательского конфигурирования сервера и заполняется разработчиком, использующим при защите своего ПО технологию LMS.

Если необходимо зарегистрировать на сервере несколько ключей от разных производителей, следует объединить в одном файле NnkSrv32.ini информацию обо всех этих ключах. Информация копируется блоками типа [KEY_00], [KEY_01], [KEY_02] (пример см. ниже) и т.д. без внесения каких-либо изменений в параметры, установленные производителем программного обеспечения.

[KEY_00]

PublicCode=DEMONVK

ID=18ab8215

VendorName=Software Co.

ProgramName=Business enterprise

ProgramNumber=1

Version=16

Mask=0

SerialNumber=2

Module0=Production

Module1=Accounts

Module2=Finances

Module3=Banks

* XX — номер секции

Конфигурирование клиента Guardant Net

Конфигурируемые параметры клиента Guardant Net собраны в секциях [PROTOCOLS], [TIMEOUT] и [SERVER] файла GnClient.ini. Этот файл должен находиться в одной директории с копией защищенного приложения.

Секция [PROTOCOLS]

В секции [PROTOCOLS] собраны параметры, с помощью которых определяются используемые сетевые протоколы и их приоритет. Сеть должна работать по протоколу TCP/IP или любому из интерфейсов NetBIOS.

TCP_IP=X

NetBIOS=X

Возможные значения параметра:

0 — протокол не используется

1 — протокол используется первым

2 — протокол используется вторым

Примечание

В текущей версии Win32-клиента очередность использования протоколов утратила свое значение, так как опрос по всем протоколам происходит параллельно. Таким образом, если это значение не ноль - протокол используется. (эта особенность сохранена только для Win16)

DOS-приложения не используют протокол TCP/IP, из файла GnClient.ini им требуется информация только о NetBIOS: имя сервера (NB_NAME) и таймауты (TO_SEND, TO_RECEIVE).

Секция [TIMEOUT]

В секции [TIMEOUT] собраны параметры, задающие величину таймаутов на посылку и прием данных (в секундах):

TO_SEND=XX

Максимальный таймаут на посылку данных клиентом серверу ключа. Диапазон значений таймаута — от 1 до 120 секунд, по умолчанию 20 секунд. Не рекомендуется уменьшать значение по умолчанию, т. к. это может привести к ошибкам соединения.

TO_RECEIVE=XX

Максимальный таймаут на прием данных клиента сервером ключа. Диапазон значений таймаута — от 1 до 120 секунд, по умолчанию 20 секунд. Не рекомендуется уменьшать значение по умолчанию, т. к. это может привести к ошибкам соединения.

При работе по медленной линии или большой загрузке сервера значения таймаутов TO_SEND и TO_RECEIVE рекомендуется увеличивать, чтобы клиент, ожидающий ответ, не отключался по истечении таймаута.

TO_SEARCH=XX

Таймаут на широковещательный поиск сервера ключа. Диапазон значений таймаута — от 1 до 120 секунд, по умолчанию 5 секунд (для версии сетевого ПО от 2.3 и выше).

Секция [SERVER]

В секции [SERVER] собраны параметры, с помощью которых задается NetBIOS-имя компьютера, на котором установлен сервер Guardant Net, его IP-адрес или host name, адрес TCP/IP-порта.

TCP_PORT=XXXX

3182 — адрес TCP/IP-порта по умолчанию

IP_NAME=XXX.XXX.XXX.XXX

Если в сети используется динамическое распределение IP-адресов (DHCP-сервер), и есть вероятность смены IP-адреса компьютеров, то вместо IP-адреса следует указывать HOST NAME компьютера, на котором установлен сервер ключа. Это необходимо для сокращения времени поиска сервера клиентом, т.е. при отсутствии информации о IP-адресе сервера, клиент будет принудительно искать его только по имени хоста и NetBIOS имени сервера Guardant Net.
127.0.0.1 — IP-адрес сервера ключа по умолчанию.

NB_NAME=NVSK_SRVR

NVSK_SRVR — имя сервера ключа по умолчанию.

SEARCH=On|Off

Включение/выключение широковещательного поиска. Значение по умолчанию — On.

BC_ADDR=XXX.XXX.XXX.XXX

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.

UDP_PORT_CLIENT=XXXX

Номер UDP-порта, через который клиент рассылает датаграммы серверам, 3183 — номер порта по умолчанию.

UDP_PORT_SERVER=XXXX — начиная с версии 2.3

Номер UDP-порта, через который сервер отвечает клиенту, 3184 — номер порта по умолчанию.

Запуск сервера

Опции командной строки

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. Запуск двух серверов (сервера и сервиса, двух сервисов) на одной рабочей станции невозможен. Сервер Guardant Net может работать не только как обычное оконное приложение, но и как сервис (служба) Windows NT/2000/XP.

Преимущества сервиса 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.

Следует обратить внимание, что сервер Guardant Net, начиная с версии 2.1 и выше, работающий как сервис, имеет информационную консоль, позволяющую следить за состоянием сервера, а также проинформировать об остановке сервиса. Младшие версии сервера Guardant Net такой консоли не имеют.

Для того чтобы разрешить запуск сервера Guardant Net в качестве сервиса, нужно задать значение "On" в параметре "ServiceMode" файла NnkSrv32.ini. После этого сервер можно будет запускать и как обычное приложение, и как сервис. В противном случае утилита NnkSrv32.exe сможет работать только как обычное оконное приложение. Для установки сервиса нужно запустить сервер Guardant Net с опцией /i или /ii.

NnkSrv32.exe /i [q]	Установить сервис (службу) Guardant Net. Взаимодействие с рабочим столом отключено.
NnkSrv32.exe /ii [q]	Установить сервис (службу) Guardant Net. Взаимодействие с рабочим столом включено.
NnkSrv32.exe /s [q]	Стартовать сервис (службу) Guardant Net, предварительно установив его, если до этого он не был установлен.
NnkSrv32.exe /e [q]	Остановить сервис (службу) Guardant Net
NnkSrv32.exe /r [q]	Остановить и удалить сервис (службу) Guardant Net
NnkSrv32.exe /?	Короткая справка

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

Установку сервиса (службы) Guardant Net нужно произвести только один раз. После того, как сервис Guardant Net будет успешно запущен, защищенные приложения получают доступ к ключам Guardant Net. Сервис будет запускаться автоматически при каждом старте Windows NT/2000/XP.

Важно

Следует помнить, что остановка сервиса из опций меню информационной консоли не предполагает его выгрузки из списка сервисов, т. е. при перезагрузке компьютера сервис Guardant Net будет снова загружен.

Решение возможных проблем

Мониторинг сервера Guardant Net

Наблюдать за состоянием сервера Guardant Net можно двумя способами:

- Если сервер запущен как обычное приложение с оконным интерфейсом, или как интерактивный сервис (служба), то информацию о сервере на локальном компьютере отображается в окне сервера.
- Если сервер запущен в качестве сервиса (службы) Windows NT/2000/XP/2003 без оконного интерфейса, или если информацию о сервере нужно получить с удаленного компьютера, то можно воспользоваться web-интерфейсом, открыв в браузере URL [http://\[IP/hostname сервера\]:\[порт сервера\]](http://[IP/hostname сервера]:[порт сервера]). Если в файле NnkSrv32.ini http-порт установлен по умолчанию, то номер порта 3185.

Приложение не видит сервер ключа

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

Большая загрузка локальной сети

- **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).
- **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 NT/2000/XP/2003 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 локальной работы с сервером Guardant (если отсутствует сетевой адаптер) по протоколу NetBeui в ОС Win'9x необходимо установить Dialup Adapter (Контроллер удалённого доступа).
- В Win16-системе необходимо наличие файлов Winsock.dll (только для работы с TCP/IP), ToolHelp.dll. Эти библиотеки входят в дистрибутив Windows по умолчанию и линкуются динамически.
- Для использования сервера Guardant Net в сетях отличных от Windows (Novell, Unix, Linux и др.) достаточно запустить сервер электронного ключа 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 NnkSrv32.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.