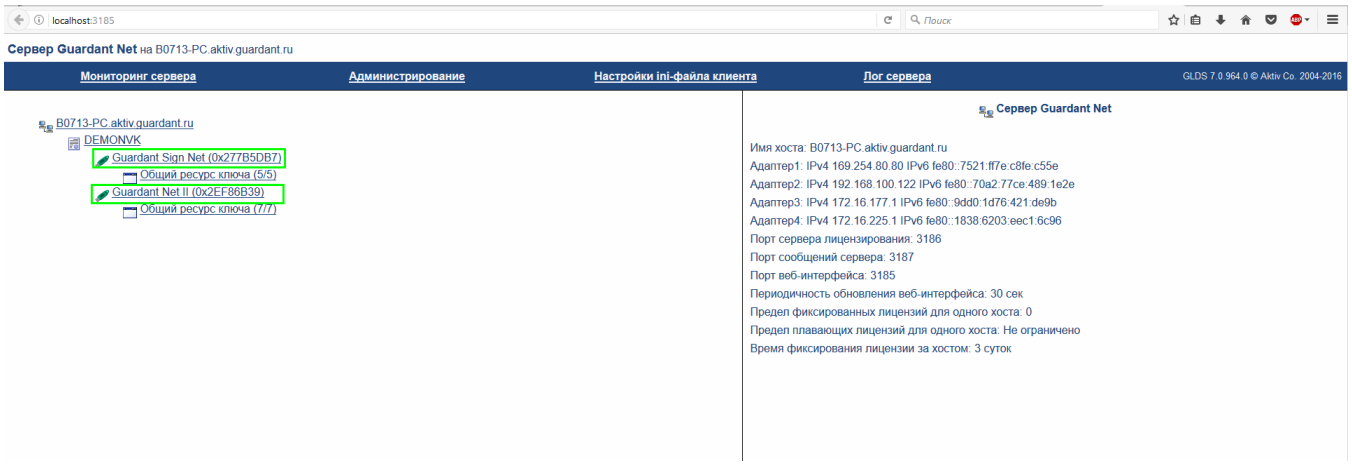
0010

Диагностика сетевых ключей

Перед диагностикой необходимо убедиться в том, что мы имеем дело с сетевым ключом. Как определить модель ключа можно узнать в этой стат ье.

Теперь убедимся, что ключ определяется утилитой диагностики (а, следовательно, исправен).

Далее обратим внимание на сервер сетевых ключей. При корректно сформированных полях памяти сетевого ключа, ключ и его текущий сетевой ресурс будут отображаться в мониторе сервера сетевых ключей. В нормальном случае в интерфейсе монитора должна быть похожая картина.



Важно!

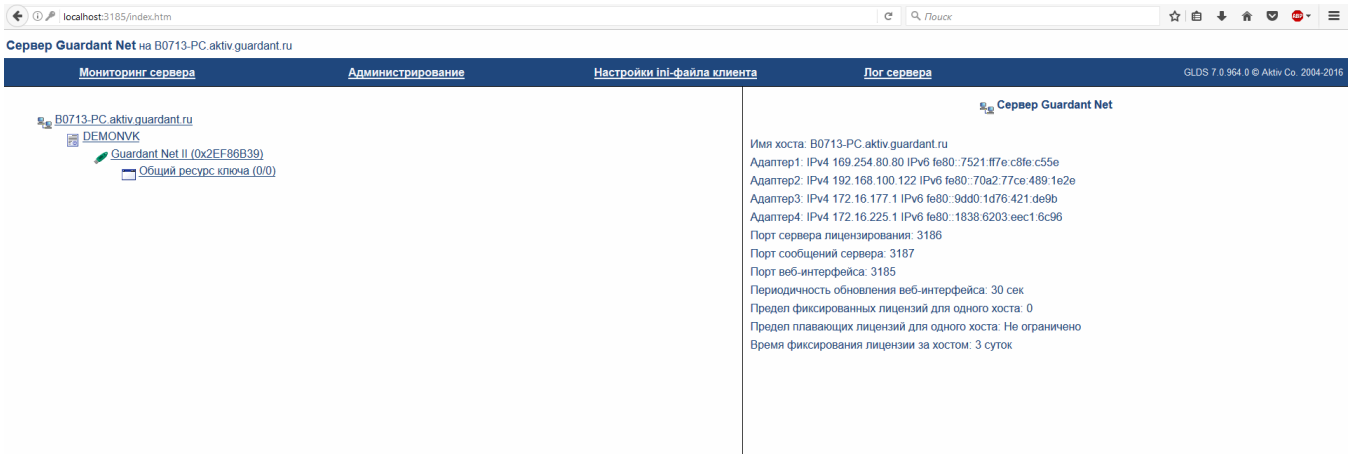
Для некоторых устаревших моделей ключей семейства Stealth, а также для софтверных ключей SP Net сетевой ресурс будет отображаться в мониторе сервера сетевых ключей только после первого удачного обращения защищенного приложения к сетевому ключу.

В современных ключах за хранение сетевого ресурса отвечает таблица лицензий. Если разработчик не добавил таблицу лицензий в ключ, в отчете утилиты диагностики отобразится соответствующая информация, а в мониторе сервера сетевых ключей такой ключ отображаться не будет.

Информация о системе	**21.02.2017 17:36:02**
Процессор	Intel(R) Core(TM) i5-2320 CPU @ 3.00GHz
Материнская плата	ASUSTeK Computer INC. P8H67-M PRO
Операционная система	Microsoft Windows 10 Enterprise Edition (Build 10586)
Тип системы	64-разрядная операционная система
Версия .Net Framework	v1.0.3705, v1.1.4322, v2.0.50727, v3.0, v3.5, v4.0.30319
Версия драйвера Guardant	7.0.190

Поиск установленных ключей Guardant	**21.02.2017 17:36:02**		
Модель	Guardant Sign Net USB		
Идентификационный номер	277B5DB7h (662396343d)		
Коды доступа	DEMONVK		
Дата и время выпуска	27 Nov 2009 11-45-46		
Поддержка	Windows, Net, GSII64, PI, TRU, AES, ECC		
Номер продукта	0	Версия ключа	0.1
Версия продукта	1	Тип микроконтроллера	08
Серийный номер	1	Номер программы	1, 0, 0, 23
Маска	0	Версия драйвера	7.0.190
Счётчик запусков	0	Максимальный сетевой ресурс	10
Таблица лицензий	Нет		
Состояние микропрограммы	OK		
Ключ в режиме обновления	Нет		

В устаревших моделях ключей (ключи семейства Stealth) текущий сетевой ресурс учитывается значением поля в ключе Счётчик № 2. Информация о значении Счётчика № 2 в отчете утилиты диагностики не отображается. Однако, если разработчик не указал отличное от нуля значение в поле Счётчик № 2, в мониторе сервера сетевых ключей текущий сетевой ресурс будет равен нулю.



Важно!

Особое внимание следует уделить версии устанавливаемого сервера сетевых ключей. Мы рекомендуем использовать последнюю версию сервера сетевых ключей 7.x, которую можно скачать на нашем сайте. Однако некоторые разработчики до сих пор пользуется версией сервера 5.x. Информацию о версии сервера, для которой производилась защита приложения, конечный пользователь может уточнить у разработчика, если тот в свою очередь не указал такую информацию в документации к своему приложению. Важно помнить, что версии 5.x и 7.x между собой не совместимы. Сервер сетевых ключей версии 5.x является устаревшей технологий, ограничен по функционалу в сравнении с версией 7.x, а также не тестировался на совместимость и стабильную работу в современных операционных системах. Сервер сетевых ключей версии 5.x также доступен для скачивания на нашем сайте.

Для корректной работы сервера сетевых ключей и сетевого приложения необходимо обеспечить беспрепятственное прохождение сетевого трафика по следующим портам:

Порт веб-интерфейса	PORT=3185	Порт TCP/UDP	Порт для web-мониторинга сервера ключа
Порт сервера лицензирования	PORT=3186	Любой подходящий порт TCP/UDP	TCP/UDP-порт, который использует сервер для обслуживания клиентов
Порт сообщений сервера	PORT=3187	Любой подходящий порт TCP/UDP	TCP/UDP-порт, который используется для сообщений сервера

Указанные сетевые порты используются «по умолчанию» и могут быть изменены через раздел «Администрирование» в мониторе или в конфигурационном файле «grdsrv.ini».

Проверить, какие порты открыты на вашей рабочей станции можно с помощью команды:

netstat –a. Команду необходимо выполнить в командной строке, запущенной от имени администратора.

Также проверить, открыт ли порт, можно с помощью команды **telnet**. Для этого запустите командную строку от имени администратора, и введите команду

telnet имя_сервера номер_порта

или:

telnet IP_сервера номер_порта

Если команда вернет ошибку, значит порт закрыт. Если же на экране появится приглашение сервера (или окно станет полностью пустым), порт открыт.

Обратите внимание! В ряде случаев антивирусы, файровлы и другие средства проактивной защиты могут препятствовать корректной работе сервера сетевых ключей и защищенного приложения, поэтому на этапе тестирования работы сервера сетевых ключей и приложения мы рекомендуем отключать все средства проактивной защиты.

Убедитесь, что рабочая станция с установленным сервером сетевых ключей доступна в локальной сети, где будет использоваться защищенное приложение. Сделать это можно используя команду **ping**. Важно удостовериться, что ICMP пакеты ходят в обе стороны (приложение – сервер, серевер – приложение)

Как пользоваться командой **ping**

«**Ping**» — это утилита, с помощью которой можно проверить доступность сервера с компьютера.

Как запустить **ping** в Windows

в меню Пуск выберите пункт Выполнить или просто нажмите сочетание клавиш «Win» + «R»;

в открывшемся маленьком окошке наберите команду «**cmd**» и нажмите кнопку OK;

в открывшемся окне терминала наберите команду:
ping имя_сайта
или
ping IP_сервера

Если команда **ping** выявляет потерю пакетов, или же отсутствие связи с удаленной рабочей станцией, обратитесь к вашему сетевому администратору для решения данной проблемы. Проблемы прохождения трафика могут быть вызваны не корректно настроенной маршрутизацией сети, или же наличием файерволов и других средств, осуществляющих контроль сетевого трафика.

Если были соблюдены все вышеописанные условия и проведены проверки, а сетевое приложение не занимает лицензию, то нужно протестировать работу сервера сетевых ключей и защищенного приложения по следующему алгоритму:

1) Взять два ПК полностью отключенных от общей ЛВС;

2) На одном установить драйвер, подсоединить ключ и запустить сервер Guardant Net, а на другом установить защищенное приложение;

3) Соединить данные две машины, прямым (без использования хабов или маршрутизаторов), кроссовер (cross-over) патчкордом;

4) Вручную настроить стандартную (вида: 192.168.x.x) подсеть между данными компьютерами;

5) Выключить абсолютно все средства проактивной защиты запущенные на обоих компьютерах;

6) Настроить (конфигурационный файл gnclient.ini для защищенного приложения нужно выгрузить из web-интерфейса по ссылке "Настройки ini-файл клиента") и запустить защищенное приложение на ПК-клиенте.

Если во время тестирования так и не удалось сделать однозначный вывод о работоспособности сетевого ключа или сервера сетевых ключей, то можно составить обращение в техническую поддержку нашей компании и направить его по электронному адресу hotline@guardant.ru. В письме необходимо указать следующую информацию:

1. Данные о системе где установлен сервер сетевых ключей и электронные ключ и о системе того компьютера, на котором установлено защищенное приложение.
2. Отчет утилиты диагностики ключей
3. Версия сервера сетевых ключей (приложенная разработчиком, и использующаяся в данный момент)
4. Версия операционной системы
5. Файл с настройками для сервера сетевых ключей (grdsrv.ini)
6. Файл с настройками для поиска сервера сетевых ключей (gnclient.ini)
7. Файл с логом сервера сетевых ключей (glds_log.txt)