Инструкция по эксплуатации 1С и ключей защиты HASP

1. УСТАНОВКА КЛЮЧА HASP.

Компании "1С" для защиты своих продуктов использует аппаратный ключ защиты HASP4, присоединяемый к USB или LPT порту компьютера. Для установки ключа HASP4 на операционные системы Win 98, ME, NT4, 2000, XP(x86/x64), 2003 Server(x86/x64), 2008 Server(x86/x64) или Vista(x86/x64) Вам необходимо скачать и **установить драйвер** версии 4.116. Если Вы планируете работать под управлением ОС Windows 7(x86/x64) и выше, то рекомендуется использовать актуальную версию драйвера. (**ВНИМАНИЕ!**) Так как HASP4 не имеет официальной поддержки современных ОС, начиная с Windows 7 и выше, то работа защищённого с помощью HASP4 ПО в этих ОС не гарантируется! Для успешной установки драйвера Вам потребуются привилегии локального администратора, рекомендуется отключите любое защитное ПО (антивирус, брандмауэр).

Драйвера устанавливаются в консольном режиме, для этого необходимо запустить драйвер с параметром " -i". В случае если, на этом компьютере уже использовались ключи HASP – рекомендуется удалить предыдущую версию драйвера, запустив инсталляцию с ключом " -r".

Возможные проблемы:

Если во время установки драйверов возникли проблемы – рекомендую выполнить следующую последовательность действий:

- Удалите все компоненты HASP через «Панель управления - Установка/удаление программ»;
- Остановите все службы, которые содержат в названии «Hasp» или «HLServer»;
- Удалите все файлы aks*.*, «hardlock.sys» и «haspnt.sys» из папки c:\windows\system32\drivers» (если они не используются другими приложениями);
- Изменение драйверов в «Диспетчере устройств»:
  - Зайдите в «Панель управления»\«Система»;
  - Перейдите на вкладку «Оборудование» и откройте «Диспетчер устройств»;
  - Выберите в меню «Показать скрытые устройства»;
  - Раскройте пункт «Драйверы устройств не Plug and Play»;
  - Удалите каждый из следующих пунктов, если они присутствуют: «Hardlock», «Haspnt», «HASP fridge».
- Попробуйте еще раз удалить драйверы с помощью команды «haspdinst –purge», а затем установить с помощью «haspdinst –i».

Ключи бывают в виде LPT и USB реализаций. В случае, если необходимо установить LPT-ключ HASP4 на компьютере, где **отсутствует LPT-порт**, можно установить PCI-плату расширения с LPT портом. При установке PCI-платы с LPT-портом необходимо учитывать, что базовый адрес LPT-порта, установленного на PCI-шине, отличается от общепринятых значений для интегрированных портов (это 378h, 3BCh и 278h), поэтому установку драйвера следует запускать со следующими параметрами: "*hinstall -i -lpt1=x*", где x - базовый адрес порта. Посмотреть его значение можно в менеджере устройств. Пример для данных адресов: "*hinstall -i -lpt1=0x378*" или "*hinstall –i -lpt1=0x3BC*".

К сожалению, ключи не работают на переходниках PCMCIA-LPT или USB-LPT. Это связано с особенностями работы драйвера ключа. Также, технически возможна замена LPT-ключа на аналогичный USB-ключ, для этого необходимо обратиться в компанию 1С. В случае отсутствия портов USB их можно добавить с помощью плат расширения PCI или PCMCIA. Мы гарантируем работоспособность LPT и USB ключей HASP только с платами расширения предлагаемыми компанией Aladdin.

При использовании LPT-ключей стоит проверить, что порт задействован на уровне BIOS'а материнской платы и выключены энергосберегающие режимы. Режим работы порта имеет значение только в случае совместного использования с какой-либо периферией. В таких случаях, мы рекомендуем использовать режим SPP.

При установке двух и более ключей защиты программного обеспечения HASP **на один компьютер** следует учитывать, что ключи, имеющие разные серии, будут работать нормально. Серия - это пять латинских букв и цифр, нанесенных на этикетку либо на корпус. Ключи одной серии не

будут работать совместно на одном компьютере, будет виден только один из них: либо ближний к порту (в случае с LPT-ключами), либо размещенный на порту с младшим адресом (в случае с USB-ключами).

Возможные решения данной проблемы:

- Замена нескольких ключей защиты программ HASP на один, с бОльшим количеством лицензий (необходимо обратиться к производителю программного обеспечения).
- Установка ключей защиты на разные компьютеры с последующей установкой и настройкой Менеджеров лицензий при каждом ключе.

Ключ HASP не должен быть установлен на машине, где используются **терминальные службы**. Некоторое время назад разработчики специально внесли несовместимость драйвера с различным терминальным ПО (Terminal Server, Citrix Winframe/Metaframe и т.д.). Это было сделано с целью предотвращения неконтролируемой утечки лицензий через открытые терминальные соединения. Для решения данной проблемы можно:

- Остановить сервисы и приложения терминального ПО на машине, где установлен ключ.
- Если ключ сетевой, то можно установить ключ на любую другую машину данной сети, где нет активного терминального ПО.

2. РАБОТА С КЛЮЧАМИ ПО СЕТИ

Для работы с сетевыми ключами, кроме установки драйверов, Вам еще потребуется **установить License Manager**(Менеджер лицензий) при каждом сетевом ключе. Менеджер лицензий - это утилита, которая служит связующим звеном между сетевым ключом и "1С", запускаемой на удаленной машине.

Скачать менеджер лицензий можно по следующим ссылкам:

- Менеджер лицензий для Windows
- Менеджер лицензий для Linux
- Менеджер лицензий для Mac OS

Для работы защищенного приложения на удаленной рабочей станции, необходимо **обеспечить беспрепятственный проход UDP- и TCP-пакетов по 475 порту в обе стороны**. Также, должны проходить и **broadcast**-пакеты. Если последнее требование по каким-либо причинам не выполняется, необходима настройка приложения через файл nethasp.ini (должен находиться в одной директории с исполняемым файлом) с целью отключения broadcast-механизма поиска ключа и явного указания IP-адреса машины, обслуживающей ключ.

Пример файла nethasp.ini:

```
---------- nethasp.ini ----------
 [NH_COMMON]
NH_TCPIP = Enabled
...
[NH_TCPIP]
NH_SERVER_ADDR = 168.192.1.10 // ip-адрес компьютера, где расположен Менеджер лицензий.
NH_TCPIP_METHOD = TCP
NH_USE_BROADCAST = Disabled
----------
```

Если часть маршрута между запускаемой программой и ключами HASP **проходит через Интернет** или на ключе более 100 лицензий, могут возникнуть проблемы с тайм-аутами при доставке пакетов. Время ожидания ответа можно регулировать с помощью параметров NH_SESSION и NH_SEND_RCV. По умолчанию они закомментированы, и их значение составляет 30 и 5 секунд соответственно. Таким образом, делается 6 попыток найти ключ по 5 секунд каждая. При необходимости Вы можете увеличить эти параметры.

Для корректной работы Менеджера лицензий не рекомендуется устанавливать его на компьютер с **2-мя и более сетевыми интерфейсами**, так как это может вызвать некорректное функционирование Менеджера. Для решения данной проблемы:

- Перенести Менеджер лицензий на другую машину в сети;
- Отключить остальные сетевые интерфейсы;
- Также, можно попробовать изменить метрики в свойствах протокола tcp/ip (первым будет использован интерфейс с меньшей метрикой), но результат в данном случае гарантировать нельзя.

При установке в сети двух и более Менеджеров лицензий их необходимо настроить для корректной работы. Иначе в сети может возникать коллизия из-за имен Менеджеров лицензий - при старте они принимают одно и то же имя по умолчанию, и в результате в сети присутствует несколько ресурсов с одинаковыми именами. Стоит отметить, что нередко Менеджеры нормально работают и без настройки. Тем не менее, следует иметь в виду, что возможно возникновение проблемы. Кроме того, настройка может понадобиться, например, чтобы разделить клиентов по разным Менеджерам лицензий.

Основная идея настройки в данном случае – назначить каждому Менеджеру свое имя и сообщить каждой копии 1С эти имена. Задать имя Менеджеру можно через файл nhsrv.ini, он должен находиться в одном каталоге с Менеджером лицензий (по умолчанию - C:\Program Files\Aladdin\HASP LM). Если Менеджер лицензий установлен как сервис, то данный файл необходимо скопировать в каталог Windows\System32 (для 64-разрядных ОС - Windows\SysWOW64). Имя должно состоять из алфавитно-цифровых символов (только английские буквы!), и не должно быть длиннее 7 символов.

Пример настройки:

```
------------------- nhsrv.ini #1-----------------------------
[NHS_SERVER]
NHS_SERVERNAMES = LM1
-----------------------------------------------------------------
------------------- nhsrv.ini #2-----------------------------
[NHS_SERVER]
NHS_SERVERNAMES = LM2
-----------------------------------------------------------------
```

Также вы можете указать диапазон IP-адресов, которым будет разрешено взаимодействовать с Менеджером лицензий. За это отвечает параметр NHS_IP_LIMIT и по умолчанию он закомментирован. Запросы с адресов, которые не указаны в этом параметре будут проигнорированы. С помощью параметра NHS_USERLIST можно указать максимальное число одновременных подключенный к менеджеру лицензий, по умолчанию его значение равно 250.

Сообщить защищенному приложению имена Менеджеров лицензий можно через файл nethasp.ini, он должен находиться в одном каталоге с защищенным приложением (для 1С – каталог Bin) либо в каталоге Windows\System32(для 64-разрядных ОС - Windows\SysWOW64):

```
------------------- nethasp.ini -----------------------------
[NH_COMMON]
NH_TCPIP = Enabled
[NH_TCPIP]
NH_SERVER_ADDR = 168.192.1.41, 168.192.1.11
NH_SERVER_NAME = LM1, LM2
-----------------------------------------------------------------
```

Параметры "адрес" и "имя" должны соответствовать друг другу, т.е. на машине с адресом 168.192.1.41 должен быть запущен Менеджер с именем LM1. Адреса даны для примера, следует указывать реальные IP адреса машин, где установлены соответствующие Менеджеры лицензий. В параметре NH_SERVER_ADDR можно через запятую указать несколько компьютеров, где расположены Менеджеры лицензий. Если по первому адресу менеджер лицензий окажется недоступен или на нем не окажется свободных лицензий, то запрос будет перенаправлен к следующему менеджеру лицензий, который был указан в NH_SERVER_ADDR.

При использовании UDP в качестве протокола передачи данных возможна **100% загрузка одного из ядер процессора** или массовые ошибки **"receive problem error 10038"** и **"receive problem error 10054"** в журнале License Manager. Причина сбоев в работе Менеджера лицензий – «битые» пакеты, приходящие по UDP. Поскольку обмен при помощи UDP-дейтаграмм не предусматривает контроля успешной доставки пакета, данный протокол надежно работает только в сетях, построенных на высококачественном оборудовании. Единственный способ разрешить эту проблему, не учитывая замену оборудования на более качественное, – это переход на обмен посредством TCP-пакетов. В этом случае контролируется успешная доставка каждого пакета, и работа с ключом становится более надежной.

Для того, чтобы настроить 1С на работу через TCP-пакеты, необходимо сконфигурировать файл nethasp.ini:

```
-------------------- nhsrv.ini -------------------------------
[NH_COMMON]
NH_TCPIP = Enabled
...
```

[NH_TCPIP]
NH_SERVER_ADDR = 168.192.1.41
NH_TCPIP_METHOD = TCP

Далее следует отключить в Менеджере лицензий прослушивание UDP-протокола, оставив только TCP, для этого в nhsrv.ini требуется прописать:

---------- nhsrv.ini ----------
[NHS_IP]
NHS_USE_UDP = disabled
NHS_USE_TCP = enabled

1С 8.x работает только по UDP. Однако ее можно заставить использовать TCP неявно. Для этого, помимо того, что описано выше, необходимо разрешить в свойствах протокола TCP/IP (Properties - Advanced - WINS) поддержку NetBios over TCP/IP на рабочих станциях, где работает защищенное приложение и на машине, где установлен ключ. Конфигурационные файлы приложения необходимо настроить следующим образом:

---------- nethasp.ini ----------
[NH_COMMON]
NH_TCPIP = Disabled
NH_NETBIOS = Enabled
...
[NH_NETBIOS]
NH_USELANANUM =

Значение параметра Num можно взять из лога Менеджера лицензий, - там указывается, какие каналы Менеджер слушает по NetBios'y. Если номеров несколько, переберите их по очереди, пока 1С не запустится. При такой настройке 1С в качестве транспорта по-прежнему будет использовать TCP/IP, но работать с ним будет через интерфейс NetBios. Причем при передаче пакетов будет использоваться именно TCP-механизм, в силу особенностей реализации NetBios over TCP/IP.

При нештатном завершении работы 1С, когда оно не успевает освободить лицензию, могут образовываться **"зависшие" лицензии**. В этом случае новые копии приложения не будут запускаться до тех пор, пока не будут удалены "зависшие" лицензии. По истечению таймаута, который составляет 36 часов с момента последнего обращения со стороны защищенного приложения, лицензии будет освобождены самим Менеджером лицензий. Раньше этого срока освободить лицензию можно только перезапустив Менеджер лицензий (перезагружать компьютер нет необходимости). Обратите внимание, что в этом случае, другие пользователи должны будут так же перезапустить приложение. Если таймаут равен 0, значит лицензия уже освобождена. Просто запись об этом осталась в журнале Менеджера лицензий. По мере наступления новых событий, подлежащих журналированию, эта запись будет затерта.

3. ДИАГНОСТИКА

Утилита **Aladdin Monitor** разработана для осуществления централизованного администрирования приложений HASP License Manager и ключей сетевых ключей HASP.

Aladdin Monitor позволяет:

- Проверять наличие и свойства ключей HASP4 Net в сети;
- Отслеживать наличие и свойства Менеджеров лицензий в сети;
- Останавливать и запускать локальный Менеджер лицензий;
- Отслеживать лицензии, которые используются в данный момент.

Стоит учитывать, что сам по себе Aladdin Monitor может показать только наличие Менеджера лицензий на том или ином адресе. Ключ он сможет увидеть только после того, как защищенное приложение успешно откроет хотя бы одну сессию с ключом. Кроме того, Aladdin Monitor работает только по протоколу UDP, порт 475. Таким образом, отсутствие данных о ключе в мониторе еще не означает, что ключ недоступен для приложения.

Утилита HASP Admin Control Center (устанавливается вместе с драйверами от ключей Sentinel HASP v.5.*) не предназначена для работы с ключами, которые использует “1С”, поэтому они ей в ней отображаться не будут – воспользуйтесь утилитой Aladdin Monitor.

Утилита **Aladdin DiagnostiX** реализует механизм обратной связи. Ее главная задача - диагностика работоспособности локальных и сетевых ключей, работающих в системе. Кроме того, она позволяет настраивать конфигурацию для сетевых ключей HASP и генерировать отчеты, включающие всю информацию, связанную с устройствами Aladdin. При обращении в службу технической поддержки рекомендуется прикреплять подобный отчет, это поможет сформировать более полную картину о сложившейся проблеме.

Вы всегда можете получить техническую поддержку по ключам HASP, задав вопрос через сайт http://safenet-sentinel.ru , по электронной почте: support-ru@gemalto.com *, либо позвонив по телефону +7-(495)-783-2878.*