Часто задаваемые вопросы

В: Какие шлюзы SMS поддерживаются?
Вы можете отправлять SMS-сообщения через подключенный модем WaveCom или Siemens, а также через провайдера SMS-шлюза Интернет; подробности см. **SMS Gateways**.

В: Не следует ли отправлять одноразовый код-пароль в процессе аутентификации?

Данный подход считается кардинально неправильным из-за следующих проблем:

1. Доставка SMS-сообщения задерживается

Несмотря на то, что текстовые SMS-сообщения передаются за секунды, они могут задерживаться из-за перегрузки сети. SMS-трафик не работает сквозным методом: сообщения выстраиваются в очередь, после чего передаются на нужную ячейку сети, где также установлена очередь, после чего передаются на телефон конечного пользователя. Такая очередность становится причиной задержек в пиковые периоды; по сведениям мобильных операторов 96% всех SMS-сообщений доставляются за 20 секунд. Это означает, что 4% пользователей, пытающихся аутентифицироваться, не смогут этого сделать, и будут обращаться в службу поддержки для получения аварийного доступа. Таким образом, для разворачивания 5000 пользователей, аутентифицирующихся ежедневно, служба технической поддержки получит 200 звонков в день!

2. Зоны отсутствия сигнала

Сигналы сотовых операторов не всегда доступны, особенно в зданиях с широкими наружными стенами, в подземных сооружениях или в компьютерных залах, где генерируются высокие уровни радиочастот. Следует учитывать пользователей, пытающихся аутентифицироваться в таких местах. Сначала придется ввести идентификационный номер пользователя и PIN-код, но после этого код аутентификации получен не будет. После этого придется переместиться в зону приема сигнала, получить код аутентификации, вернуться в первоначальное местоположение для ввода кода-пароля; ВСЕ нужно сделать в течение 2 минут.

Пользователи в данных зонах будут вынуждены обращаться в службу технической поддержки за помощью для аварийного доступа.

3. Мобильный телефон используется для выхода в Интернет.

В большинстве случаев, когда сотовый телефон создает подключение к данным, он не может принимать SMS-сообщения. Пользователи, пытающиеся использовать сотовый телефон как средство выхода в Интернет, не будут получать коды-пароли до отключения от получения данных. Конечным пользователям потребуется начать аутентификацию пользовательского идентификационного номера и PIN-кода, отключить соединение с Интернет, дождаться SMS-сообщения, подключиться повторно, повторно ввести свой идентификационный номер, PIN-код и код-пароль в течение 2 минут.

Продукт SecurAccess не использует SMS-сообщения по требованию. Сначала пользователь вводит свой идентификационный номер, потом вводит пароль Windows и добавляет свой 6-значный код-пароль, уже сохраненный в мобильном телефоне, который был прислан при осуществлении последней аутентификации. Подход, при котором в процессе аутентификации предварительно загружается следующий необходимый код-пароль, разрешает все проблемы, связанные с задержкой доставки SMS-сообщений, кратковременной потерей сигнала и наличием соединений для передачи данных.

Данная методика устраняет любые проблемы с задержкой доставки SMS-сообщений, поскольку, как правило, конечный пользователь не запрашивает следующий код-пароль до следующего рабочего дня. Такая продолжительность – более чем достаточна для любых задержек SMS и дает конечному пользователю достаточно времени для перемещения в зону приема сигнала, например, когда он перемещается с места или на место работы. SecurEnvoy также поддерживает отправку 3 действующих кодов-паролей в рамках каждого кода-пароля SMS. Данная методика обеспечивает до 3 действующих аутентификаций до запроса получения следующего SMS-сообщения.

В: Какова разница между одноразовым кодом и дневным кодом?
В «одноразовом» режиме введенный код-пароль можно использовать только один раз, аналогично токенным системам таких компаний, как RSA. Новый одноразовый код отправляется пользователю после каждой попытки аутентификации – удачной или неудачной. Любая попытка повторить уже введенный код закончится неудачей, потому что аутентифицированный код-пароль уже заблокирован: его можно ввести только один раз. Такой режим эксплуатации идеален для удаленных пользователей «вредоносных» систем, домашних ПК или при аутентификации в общественных местах. Данные пользователи аутентифицируются в виртуальную частную сеть VPN, где используется ключ сеанса, т.е. один или максимум два раза за день. В среднем удаленные пользователи аутентифицируются два раза в неделю; некоторые могут аутентифицироваться раз в месяц или еще реже. Следует помнить, что данным пользователям не потребуется локальная аутентификация, поскольку они будут подключаться с «чужой» системы или домашнего ПК. В «дневном» режиме многократно используемый код-пароль передается ежедневно (или через определенное количество дней, например, каждую неделю), и данный код можно использовать в течение указанного или следующего дня, поэтому риск атаки при повторе ограничивается двумя днями, что значительно более надежно, нежели пароль на 30 дней (без учета выходных). При неиспользовании дневного кода он не известен другим лицам и не может быть перехвачен, поэтому заменяющий дневной код передается, только если он использовался ранее. Такой режим эксплуатации идеален для корпоративных пользователей настольных компьютеров, которые аутентифицируются несколько раз в день, поскольку он требует только одного кода-пароля SMS в день или реже, если пользователь, например, находится в отпуске и не использует ежедневный код. Поэтому риски можно спрогнозировать и сократить затраты на SMS в соответствии с пользовательскими требованиями и рабочей средой.

В: У некоторых моих пользователей нет мобильных телефонов. Как я могу использовать данное решение?
У этих пользователей может не быть корпоративных телефонов, но у них наверняка есть личные телефоны, и по статистике мобильных телефонов больше, чем взрослого населения. При отсутствии личных мобильных телефонов программа SecurAccess может передать код-пароль на стационарный телефон или даже на прямой номер местной АТС.

В: Что делать, если конечные пользователи не хотят использовать свой личный телефон?
Вопрос в том – почему они не хотят пользоваться личными телефонами? Ведь на их телефоны не нужно устанавливать дополнительное программное обеспечение. Таким пользователям просто отправляется бесплатное SMS-сообщение. В некоторых случаях проблема кроется в том, что они не хотят получать телефонные звонки от коллег. Номера личных сотовых телефонов хранятся зашифрованными: узнать их могут только администраторы SecurEnvoy, и другие сотрудники не могут по ним звонить. Что неудобнее для пользователя, – носить токен в кармане или пользоваться виртуальным пространством на сотовом телефоне?

В: Каков охват GSM на телефоне?
Общая сеть GSM состоит из более чем 860 сетей в 220 странах/регионах мира. Карты охватов представлены на веб-сайте: http://www.gsmworld.com/roaming/gsminfo/index.shtml.

В: В месте моего проживания охват GSM очень некачественный или отсутствует совсем. Что делать?
Если вы часто находитесь в зоне с неустойчивым сигналом, то можно воспользоваться предусмотренной в программе опцией дневного кода. Это означает, что код-пароль можно использовать многократно от 1 до 99 дней. Поскольку SecurEnvoy работает по принципу предварительной загрузки, то пользователь может всегда иметь на телефоне действующий код. Альтернативно, сервер безопасности можно настроить на отправку 3 одноразовых кодов в каждом SMS-сообщении. Наконец, SecurAccess может передать код-пароль на стационарный телефон или на прямой номер местной АТС.

В: Как сервер отправляет SMS-сообщения?
Существует два способа отправки SMS-сообщений.

Первый – воспользоваться выходным GSM-модемом Wavecom достаточной пропускной способности. Данная опция позволяет клиенту использовать существующий контракт с поставщиком мобильных телекоммуникационных услуг. Последний может предложить пакет, в котором вызовы (и SMS) между корпоративными телефонами – бесплатные, либо включить в контракт значительное количество минут и SMS в месяц. С помощью данного метода клиент может пользоваться службой практически бесплатно. С другой стороны, можно выбрать однопользовательский контракт с ведущим провайдером.

Второй вариант – подписаться на обслуживание одним из шлюзов Web SMS. В принципе, это – HTTPS-подключение к шлюзу Web SMS, с которого провайдер отправляет вам сообщения. Данная опция – более гибкая, чем модем GSM, но возможно обойдется дороже.

В: Насколько хорошо сервер SecurEnvoy масштабируется?
Ответ: очень хорошо. SecurEnvoy масштабируется напрямую с Active Directory, поскольку, это – его база данных, и, поэтому, вопрос должен быть поставлен так: «Насколько хорошо масштабируется существующая AD?». Microsoft потратила много времени и средств на совершенствование репликации между серверами контроллеров доменов. SecurEnvoy только выиграла от этой репликации, поскольку сервер напрямую интегрируется с AD или с другими серверами LDAP, например, с eDirectory.

В: Что происходит, если пользователь удаляет SMS-сообщение?
Просто введите свое имя пользователя и завершите процесс регистрации без кода-пароля; система рассмотрит данную ситуацию как неправильный вход и отправит новый код-пароль. Этот вариант будет срабатывать до тех пор, пока не будет достигнуто заданное количество последовательных неправильных входов в систему; в этом случае учетная запись будет деактивирована.

В: Как узнать, каким кодом-паролем пользоваться?
При активации в системе будет автоматически направлен первый код-пароль; предварительная загрузка кодов будет обслуживать любые задержки доставки SMS. После аутентификации будет направлен новый код-пароль, и на большинстве моделей сотовых телефонов новый код перепишет старый. Таким образом, на телефоне отобразится только один код.

В: Как узнать, что хакер пытается получить мои регистрационные данные?
Если хакер пытается выяснить логин с указанным корректным идентификационным номером, тогда вы получите следующий необходимый код-пароль. Получение данного SMS-сообщения играет роль предупреждения, что кто-то пытается подключиться по вашей учетной записи.

В: Как SecurEnvoy интегрируется с сетевыми устройствами типа RAS и NAS?
SecurEnvoy использует сервер Radius, поэтому поддерживается любое приложение, поддерживающее основной пароль аутентификации RADIUS. Кроме того, SecurEnvoy имеет инструкции по интеграции для большинства обычных поставщиков служб SSL/VPN, IPsec VPN и по телефонному набору. Приложения на базе веб, установленные на веб-сервере Microsoft IIS, например, OWA и Citrix, можно аутентифицировать через агент SecurEnvoy IIS Agent.

В: Существуют ли отзывы или описания примеров применения?
На нашем веб-сайте описаны многие примеры применения, охватывающие различные рыночные вертикали.

В: Расскажите вкратце об основателе SecurEnvoy.
Г-н Кемшелл – один из ведущих европейских специалистов по двухфакторной аутентификации. Как соучредитель SecurEnvoy г-н Кемшелл является изобретателем следующего поколения систем аутентификации без токенов. Он был одним из первых технических сотрудников компании RSA Europe с номером 0005. 8 лет он работал в компании RSA, в основном, представителем по работе с клиентами. За это время он напрямую взаимодействовал более чем с 500 основными клиентами RSA Security. «Мне стало ясно, что рынок продуктов аутентификации страдает от отсутствия решения без токенов на базе сотового телефона, и что большинству клиентов совсем не нравилась стоимость внедрения аппаратных средств с токенами», – говорит г-н Кемшелл.

В: Я удалил код-пароль с телефона, что делать?
Просто введите свое имя пользователя и завершите процесс регистрации без кода-пароля; система рассмотрит данную ситуацию как неправильный вход и отправит новый код-пароль. Этот вариант будет срабатывать до тех пор, пока не будет достигнуто заданное количество последовательных неправильных входов в систему; в этом случае учетная запись будет деактивирована.

В: В некоторых зонах в офисе сигнал не принимается; как получить код-пароль?
Предварительная загрузка кодов-паролей при наличии сигнала дает достаточно времени на получение кода-пароля. Либо можно воспользоваться дневными кодами: в этом случае один код используется для заданного количества дней, либо сервер безопасности можно сконфигурировать на отправку 3 одноразовых кодов в каждом SMS-сообщении.

В: Как произвести обновление с пробной лицензии на постоянно действующую?
Очень просто. Запустите администраторский интерфейс (Admin GUI), выберите меню «config», скопируйте новый ключ действующей лицензии в поле, обозначенное «License». Если планируется использование шлюза Web SMS, запустите «Advanced Config», перейдите на Web SMS Gateway и введите действующий идентификационный номер пользователя и пароль, предоставленный вам компанией службы Web SMS Gateway.

В: Как настраивать множественные серверы SecurEnvoy Security для обеспечения резервирования?
Множественные серверы безопасности должны иметь одинаковый шифровальный ключ безопасности (config.db). Всякий раз при установке новой копии сервера безопасности будет появляться подсказка с вопросом: «Is this the first server or any additional server?» (это – первый или дополнительный сервер?). При выборе дополнительного (additional) появится подсказка с просьбой загрузки файла config.db с первого сервера.

В: Телефонный шлюз 1 (Phone Gateway1) не инициализируется.
1. Убедитесь, что на модеме Wavecom мигает красный светодиод. Если светодиод не мигает, проверьте питание и SIM-карту.
2. Остановите выполнение службы SecurEnvoy Phone Gateway1, откройте Microsoft Hyperterm (Start/Programs/Accessories/Communications). Откройте Com-порт, к которому подключен модем. Измените com-порт и скорость в бодах для достижения подключения. Отметьте Wavecom defaults to 9600 8 No Stop Bits 1. Введите ATI, вы должны получить «WAVECOM MODEM».
3. Проверьте мощность сигнала, запустите Hyperterm. Введите «AT+CSQ», вы должны получить «+CSQ: 22,0», где 22 – число от 0 до 31, определяющее мощность сигнала.
4. Извлеките SIM-карту из Wavecom и установите в обычный телефон GSM. Убедитесь, что с данной SIM-карты можно отправлять SMS-сообщения на международные номера.
5. Установите настройку в реестре HKLM\SOFTWARE\SecurEnvoy\Phone Gateway1. После внесения изменений перезапустите SecurEnvoy Phone Gateway1.
6. Перед запуском службы SecurEnvoy Phone Gateway1 убедитесь, что последовательный COM-порт не используется другой программой.

В: Мой сервер SecurEnvoy Radius Server дает сбой с сообщением «Error Opening Local Port» (ошибка при открытии локального порта). Как устранить данную проблему?
Убедитесь, что порт Radius (1812) не используется другой программой. Остановите выполнение службы SecurEnvoy Radius и подождите 60 секунд. В окне CMD (командной строке) введите «netstat -a -p UDP». Строка «UDP xxxx:radius *:*» НЕ должна отображаться, где xxxx – имя системы. Если отображается данная строка, то, возможно, установлен Microsoft Internet Authentication Manager (IAM); в этом случае имеет место ошибка в определенной версии Windows, потому что IAM по-прежнему использует порт Radius даже при остановке и деинсталляции! Рекомендуется сменить порты IAM, заданные по умолчанию, чтобы высвободить порт Radius.

В: Если для локального администрирования я использую IE7, запускаю справку и потом закрываю окно справки, почему машина выдает необходимость повторной аутентификации?
Это – известный дефект Microsoft IE7. Файлы cookies сеанса удаляются при закрытии 2-го окна. На данный момент эта ошибка Microsoft не исправлена. Однако, как правило, могут помочь следующие действия. Измените настройки IE7 в Tools/Internet Options/General/Browser History Settings на «Everytime I visit the web page» (когда я захожу на веб-страницу».

В: Почему локальный администратор повторно аутентифицирует каждую страницу?
Браузеры IE6 и IE7 не возвращают cookie аутентификации, если в имени хоста содержится знак «_». Переименуйте хост-машину или воспользуйтесь Firefox как браузером по умолчанию.

В: Вы поддерживаете серверы 64-битовых ОС?
Да, сервер и агент IIS поддерживают 64-битовые ОС.

В: Вы поддерживаете сервер Windows 2008R2
Да, в версии 5.2 и выше мы поддерживаем Windows 2008 и Windows 2008R2 как на 32-, так и на 64-битовых системах.