

Обновление ViPNet Administrator с версии 3.1.x до версии 3.2.x

Приложение к документации ViPNet CUSTOM 3.2

1991–2012 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00006-05 90 12

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: <http://www.infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	4
О документе	5
Для кого предназначен документ	5
Терминология документа	5
Соглашения документа.....	5
Обратная связь	7
Глава 1. Обновление ViPNet Administrator с версии 3.1.x до версии 3.2.x	8
Особенности обновления.....	9
Подготовка к обновлению	12
Порядок проведения обновления.....	13
Процесс обновления ViPNet Administrator.....	15
Конвертация ключей на внешнем устройстве	16
Формирование списков отозванных сертификатов.....	19
Приложение А. Возможные неполадки в процессе обновления и способы их устранения.....	21
Не проверяются сертификаты пользователей в своей сети ViPNet.....	22
Не проверяются сертификаты пользователей в доверенных сетях ViPNet	23
Приложение В. Глоссарий	24



Введение

О документе	5
Обратная связь	7

О документе

Настоящий документ описывает особенности и порядок обновления программного обеспечения ViPNet Administrator, установленного на рабочем месте администратора сети ViPNet, с версии 3.1.x до версии 3.2.x.

Для кого предназначен документ

Документ предназначен для специалистов, имеющих квалификацию администратора сети ViPNet (подтвержденную соответствующим документом) и обладающих знаниями и опытом в области конфигурирования, эксплуатации и управления сетью ViPNet.

Терминология документа

Представленный документ ориентирован на терминологию, используемую в программе ViPNet Administrator версии 3.2.3 и выше. Отличия терминологии данной версии по сравнению с версиями 3.2.2 и ниже представлены в таблице.




Таблица 1. Различия терминологии

Термин ViPNet Administrator 3.2.2 и ниже	Термин ViPNet Administrator 3.2.3 и выше
Ключевая информация	Ключи
Справочно-ключевая информация	Справочники и ключи
Ключевой диск	Ключи пользователя
Ключевой набор	Ключи узла
Дистрибутив справочно-ключевой информации	Дистрибутив ключей

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 2. Условные обозначения

Указатель	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «ИнфоТеКС». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- Описание комплекса ViPNet CUSTOM <http://www.infotecs.ru/products/line/custom.php>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.
- Информация о решениях ViPNet <http://www.infotecs.ru/solutions/vpn/>.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами компании «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки hotline@infotecs.ru.
- Форма запроса по электронной почте в службу поддержки <http://www.infotecs.ru/support/request/>.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).



1

Обновление ViPNet Administrator с версии 3.1.x до версии 3.2.x

Особенности обновления	9
Подготовка к обновлению	12
Порядок проведения обновления	13
Процесс обновления ViPNet Administrator	15
Конвертация ключей на внешнем устройстве	16
Формирование списков отозванных сертификатов	19

Особенности обновления

В программном обеспечении ViPNet Administrator версии 3.2.x реализовано много новых функциональных возможностей по сравнению с ViPNet Administrator предыдущей версии 3.1.x. Особенно много значительных доработок и изменений появилось в компоненте ViPNet Administrator — программе ViPNet Удостоверяющий и ключевой центр. Со списком изменений и доработок, сделанных в УКЦ версии 3.2.x, можно ознакомиться в документе «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора», во введении, в разделе «Новые возможности».

Вследствие некоторых доработок УКЦ процесс обновления программного обеспечения ViPNet Administrator до новой версии имеет ряд особенностей и требует проведения дополнительных операций, а именно:

- В новой версии УКЦ используется другой формат ключей. Если в УКЦ версии 3.1.x ключи для входа в программу хранились на внешнем устройстве, то после обновления программного обеспечения ViPNet Administrator до версии 3.2.x потребуется их конвертация в новый формат. Подробнее см. раздел [Конвертация ключей на внешнем устройстве](#) (на стр. 16).



Внимание! Для проведения конвертации ключей программное обеспечение ViPNet Administrator требуется обновить до версии не ниже 3.2.9. Приложение, которое используется для конвертации ключей, входит в конфигурацию УКЦ, начиная с данной версии. При его отсутствии провести конвертацию ключей будет невозможно.

- В УКЦ версии 3.1.x, независимо от количества зарегистрированных администраторов и количества сертификатов подписи у каждого из них, может быть сформирован и использоваться только один список отозванных сертификатов (СОС). В данный СОС в случае отзыва или приостановления действия попадают все сертификаты, изданные в УКЦ, независимо от того, каким администратором они были изданы и каким сертификатом администратора были заверены.

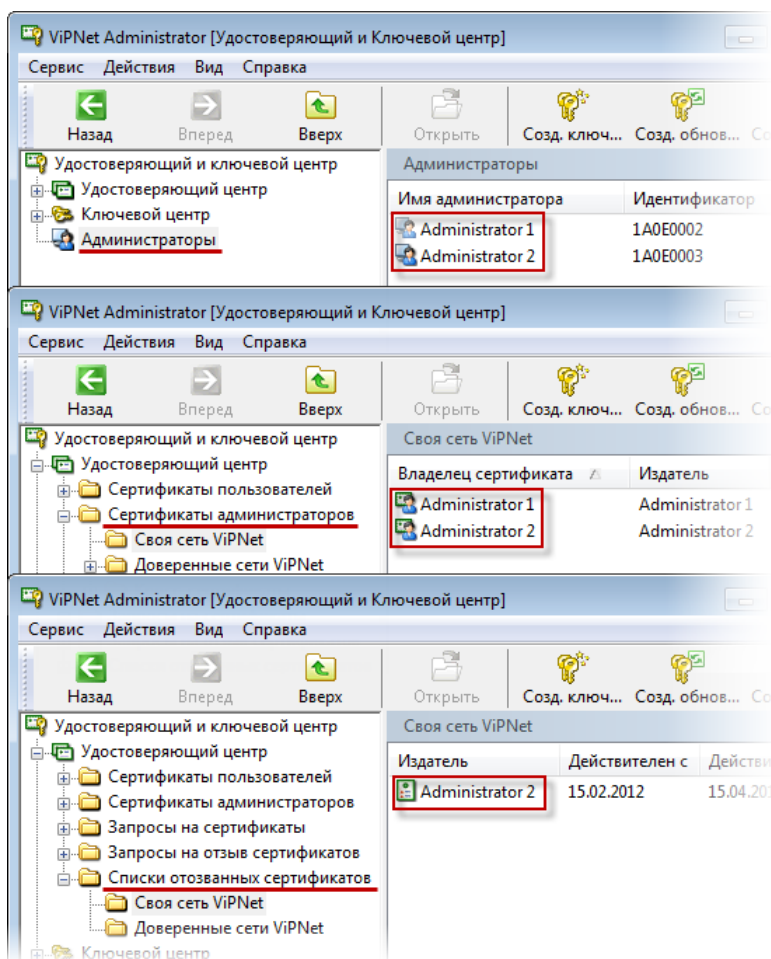


Рисунок 1: Списки отозванных сертификатов в УКЦ версии 3.1.x

В УКЦ версии 3.2.x изменен порядок работы с СОС. Формирование СОС в новой версии осуществляется для каждого сертификата администратора, вследствие этого каждому сертификату администратора соответствует конкретный СОС.

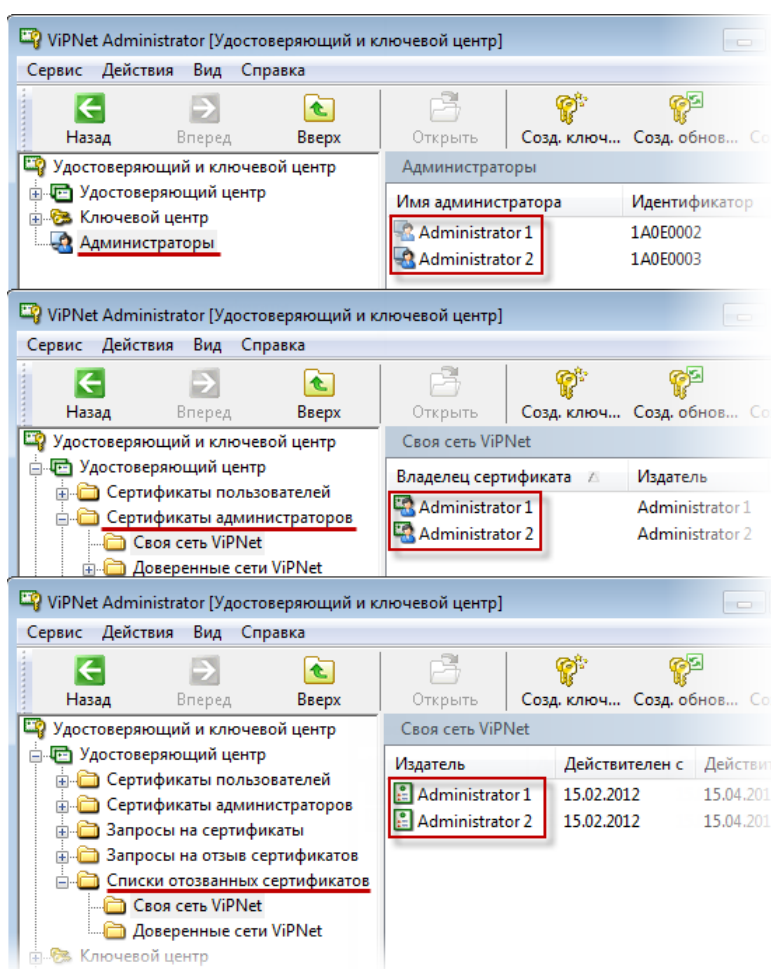


Рисунок 2: Списки отозванных сертификатов в УКЦ версии 3.2.x

В связи с данной функциональностью по завершении процесса обновления требуется вручную для сертификатов всех зарегистрированных администраторов сформировать соответствующие СОС. Подробнее см. раздел [Формирование списков отозванных сертификатов](#) (на стр. 19).



Примечание. Формировать СОС следует только для действительных сертификатов администраторов. Для имеющихся в программе недействительных сертификатов администраторов СОС формировать не требуется.

Подготовка к обновлению

Прежде чем начать обновление программного обеспечения ViPNet Administrator:

- 1 Внимательно прочтите настоящую инструкцию. Для успешного обновления, во избежание проблем, строго соблюдайте последовательность действий, указанных в документе.

Если результат операций по какому-либо разделу данной инструкции не соответствует указанному, не выполняйте дальнейших действий, так как это может привести к нарушению работоспособности всей защищенной сети. При возникновении ошибки приостановите дальнейшую работу и обратитесь в службу технической поддержки компании «ИнфоТеКС» (см. «[Обратная связь](#)» на стр. 7).

- 2 В обязательном порядке сделайте резервную копию содержимого папки, в которой установлено программное обеспечение ViPNet Administrator версии 3.1.x. Настоятельно рекомендуется полностью сохранить папку InfoTeCS.

Совет. Перед созданием резервной копии желательно:

- В программе ViPNet Центр управления сетью сформировать справочники и создать архив конфигурации сети.
- В программе ViPNet Удостоверяющий и ключевой центр создать резервную копию текущей конфигурации.
- Завершить все операции по обмену справочниками и ключами между ЦУСом и УКЦ.
- Завершить работу с ЦУСом и УКЦ.
- Завершить работу модуля ViPNet MFTP для предотвращения обработки служебных конвертов от программы [ViPNet Registration Point](#) или [ViPNet Publication Service](#) в момент обновления либо временно заблокировать IP-трафик средствами программы ViPNet Монитор.



- 3 Удалите содержимое вложенных папок FOR_NCC, FROM_NCC, \NCC\ARC, \NCC\S, \NCC\R, \KC\ARCHIVES, \KC\Restore папки установки ViPNet Administrator (в том числе удалите все файлы с расширением *.dmp, *.err, *.log, *.var, *_rem.sgn, *_spr.* при их наличии).

Порядок проведения обновления

Для успешного проведения процедуры обновления требуется выполнить все действия из приведенного ниже списка.

Действие	Ссылка
<input type="checkbox"/> Выполните подготовку к обновлению.	Подготовка к обновлению (на стр. 12)
<input type="checkbox"/> Если требуется, на всех узлах сети ViPNet обновите программное обеспечение ViPNet Client и ViPNet Coordinator до версии 3.1.x и выше, ViPNet CryptoService до версии 3.2.x. Если на узлах после обновления ViPNet Administrator будет использоваться программное обеспечение ниже указанных версий, работоспособность таких узлов и сети в целом может быть нарушена!	Документ «Обновление ПО ViPNet Client/Coordinator с версии 2.8.x до версии 3.1.x» Документ «ViPNet CryptoService. Руководство администратора»
<input type="checkbox"/> Выполните обновление программного обеспечения ViPNet Administrator до версии 3.2.x.	Процесс обновления ViPNet Administrator (на стр. 15)
<input type="checkbox"/> Если до обновления ViPNet Administrator ключи для входа в программу ViPNet Удостоверяющий и ключевой центр хранились на внешнем устройстве, то выполните их конвертацию в новый формат.	Конвертация ключей на внешнем устройстве (на стр. 16)
<input type="checkbox"/> В УКЦ для каждого действительного сертификата каждого зарегистрированного администратора вручную сформируйте соответствующий список отозванных сертификатов.	Формирование списков отозванных сертификатов (на стр. 19)
<input type="checkbox"/> Создайте обновления ключей узлов и отправьте их на все узлы сети ViPNet.	Документ «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора»
<input type="checkbox"/> При наличии межсетевых взаимодействий сформируйте и отправьте в соответствующие доверенные сети ViPNet экспорт, предварительно выполнив в УКЦ экспорт справочников (меню Сервис > Экспорт справочников).	Документ «ViPNet Administrator Центр управления сетью. Руководство администратора»

При успешном выполнении всех вышперечисленных действий обновление можно будет считать законченным, и вы сможете возобновить работу с программным обеспечением ViPNet Administrator в обычном режиме.

Процесс обновления ViPNet Administrator



Внимание! Приведенные ниже действия описывают обновление компонентов программного обеспечения ViPNet Administrator: ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр, установленных на одном узле.

Для обновления программного обеспечения ViPNet Administrator:

- 1 Двойным щелчком запустите программу установки `setup.exe`

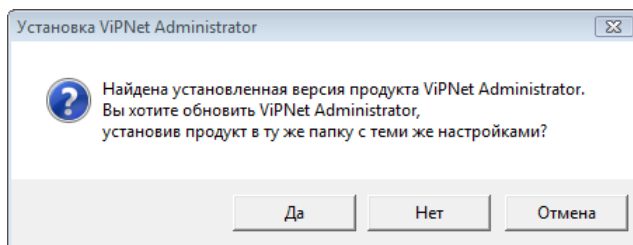


Рисунок 3: Сообщение о наличии ранее установленного программного обеспечения

- 2 В появившемся окне с сообщением о том, что обнаружена установленная ранее версия ViPNet Administrator, нажмите кнопку **Да**, чтобы начать обновление. При нажатии на кнопку **Нет** обновление не произойдет, и будет запущен мастер для установки программы в другую папку.
- 3 Дождитесь завершения процесса обновления.
- 4 При успешном окончании обновления перезагрузите компьютер.
- 5 Запустите УКЦ. При использовании внешнего устройства для входа в УКЦ выполните конвертацию ключей, хранящихся на данном устройстве (см. «[Конвертация ключей на внешнем устройстве](#)» на стр. 16).

Совет. После завершения процесса обновления рекомендуется:



- В ЦУСе сформировать справочники и создать архив конфигурации сети.
 - В УКЦ выполнить проверку текущих данных и создать резервную копию конфигурации.
-

Конвертация ключей на внешнем устройстве

Программа ViPNet Удостоверяющий и ключевой центр версии 3.2.x не поддерживает старый формат ключей, поэтому после обновления программного обеспечения ViPNet Administrator до этой версии, при использовании для входа в УКЦ устройств хранения с ключами в старом формате, следует выполнить конвертацию данных ключей.



Внимание! Для проведения конвертации ключей программное обеспечение ViPNet Administrator должно быть обновлено до версии не ниже 3.2.9. Конвертер, который используется для конвертации ключей, входит в конфигурацию УКЦ, начиная с данной версии. При его отсутствии провести конвертацию ключей будет невозможно.

Чтобы преобразовать ключи, хранящиеся на внешних устройствах в старом формате, в новый формат, выполните следующие действия:

- 1** Вручную запустите конвертер ключей. Для этого дважды щелкните по файлу `converterad.exe` из папки установки УКЦ. По умолчанию папка установки УКЦ: `\InfoTeCS\ViPNet Administrator\KC`.
- 2** В окне **Конвертер ключей ViPNet**, в списке **Устройство** выберите внешнее устройство хранения данных, на котором хранятся ключи в старом формате. Если список пуст, значит устройство не подключено либо для него неправильно установлены драйверы.
- 3** В поле **Введите ПИН-код** укажите ПИН-код выбранного внешнего устройства хранения данных.
- 4** Далее в списке **Ключи ViPNet на устройстве** напротив каждого из ключей в старом формате в столбце **Действие** выберите **Конвертировать**. На внешнем устройстве кроме ключа защиты, который используется непосредственно для входа в УКЦ, может находиться закрытый ключ подписи. В этом случае закрытый ключ также должен быть переконвертирован в новый формат.

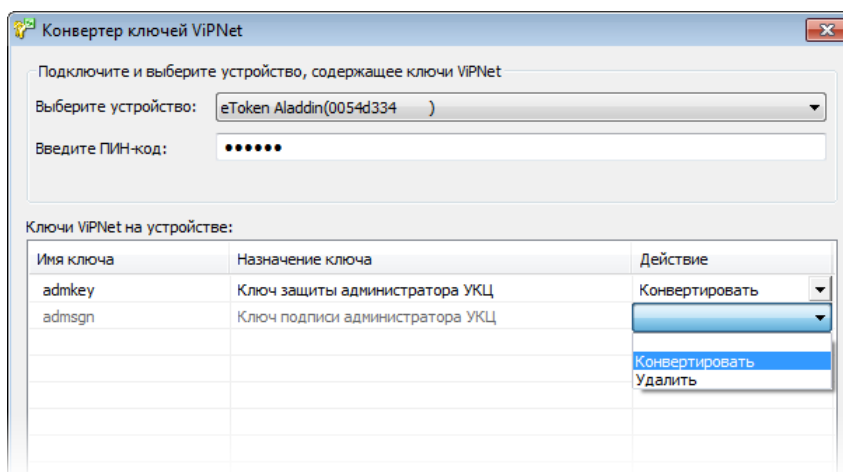


Рисунок 4: Выбор действия **Конвертировать** для ключей старого формата

- 5 Введите пароль доступа к ключу.



Внимание! Если вы не знаете пароль к какому-либо ключу, узнайте пароль у администратора или выберите для него действие **Удалить**. Действие должно быть указано для каждого ключа, иначе кнопка **Конвертировать** будет неактивна.

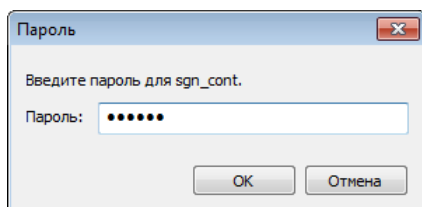


Рисунок 5: Окно ввода пароля

Если на устройстве уже имеется ключ с тем же именем и в новом формате, появится предупреждение об этом.

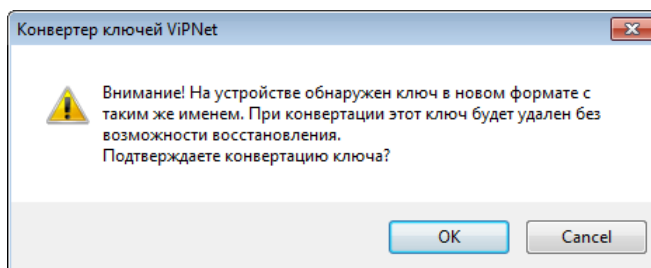


Рисунок 6: Предупреждение о совпадении имен ключей



Внимание! Если на устройстве уже имеется ключ в новом формате с точно таким же именем, что и ключ в старом формате, то при конвертации старого ключа ключ в новом формате будет удален без возможности восстановления.

6 Нажмите кнопку **Конвертировать**.



Внимание! Если в процессе конвертации ключей в новый формат произошел сбой, есть возможность продолжить процесс конвертации. Для этого повторно откройте **Конвертер ключей ViPNet**, запустив файл `converterad.exe` в папке установки программы. Нажмите кнопку **Да** в ответ на вопрос, хотите ли вы продолжить выполнение оставшихся действий.

Формирование списков отозванных сертификатов

В связи с тем, что в программе ViPNet Удостоверяющий и ключевой центр версии 3.2.x изменился порядок работы со списками отозванных сертификатов (СОС), после обновления программного обеспечения ViPNet Administrator до версии 3.2.x требуется выполнить дополнительную операцию — для каждого действительного сертификата каждого зарегистрированного администратора вручную сформировать соответствующий СОС (см. раздел [Особенности обновления](#) (на стр. 9)). В результате данной операции количество СОС должно стать равным количеству всех действительных в УКЦ сертификатов администраторов.

Чтобы сформировать нужное количество СОС, в УКЦ последовательно назначьте текущим каждый действительный сертификат каждого администратора, который не имеет соответствующего ему СОС.



Примечание. Если в УКЦ зарегистрировано несколько администраторов, то изменить текущий сертификат администратора можно при условии, что сам администратор является текущим.

Чтобы назначить текущим сертификат администратора:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** дважды щелкните по учетной записи текущего администратора.
- 2 В появившемся окне **Свойства администратора** на вкладке **Сертификаты** нажмите кнопку **Сертификаты**.
- 3 В окне **Сертификаты администратора <имя администратора>** в списке выберите сертификат, который должен стать текущим, и нажмите кнопку **Назначить текущим**.

После того как сертификат администратора будет выбран в качестве текущего, для него автоматически будет сформирован соответствующий СОС. В СОС будут помещены только сертификаты с отозванным и приостановленным действием, которые при издании были заверены сертификатом администратора, соответствующим этому СОС.



Внимание! Если операция по формированию СОС не будет выполнена (или СОС будут сформированы не для каждого действительного сертификата администратора), то после принятия обновлений ключей на узлах своей сети и после принятия экспорта в доверенных сетях ViPNet возникнут проблемы с проверкой сертификатов пользователей (см. [«Возможные неполадки в процессе обновления и способы их устранения»](#) на стр. 21).



Возможные неполадки в процессе обновления и способы их устранения

Не проверяются сертификаты пользователей в своей сети ViPNet

После обновления программного обеспечения ViPNet Administrator до версии 3.2.x и рассылки обновлений ключей на узлы сети перестали проверяться сертификаты пользователей по причине недействительного списка отозванных сертификатов (СОС).

Причинами возникновения данной проблемы могут быть следующие:

- Версии программного обеспечения ViPNet Client либо ViPNet CryptoService, установленного на таких узлах сети, не соответствуют версиям, рекомендованным к применению: ViPNet Client (Coordinator) версии не ниже 3.1.x, ViPNet CryptoService 3.2.x.
- Сертификаты пользователей заверены сертификатами администраторов, для которых в программе ViPNet Удостоверяющий и ключевой центр после обновления не были созданы соответствующие СОС.

Возможные варианты решения проблемы в зависимости от причины ее возникновения:

- На узлы сети с помощью программы ViPNet Центр управления сетью вышлите обновление программного обеспечения до последней актуальной версии либо рекомендуйте пользователям обновить программное обеспечение вручную.
- В УКЦ сформируйте СОС для соответствующих сертификатов администраторов и отправьте их на узлы в составе обновлений ключей (см. раздел [Формирование списков отозванных сертификатов](#) (на стр. 19)).

Не проверяются сертификаты пользователей в доверенных сетях ViPNet

После обновления программного обеспечения ViPNet Administrator до версии 3.2.x и рассылки экспорта в доверенные сети ViPNet сертификаты вашей сети перестали проверяться в доверенных сетях по причине недействительного списка отозванных сертификатов (СОС).

Причинами возникновения данной проблемы могут быть следующие:

- Перед отправкой экспорта в доверенные сети не был произведен экспорт справочников в программе ViPNet Удостоверяющий и ключевой центр (меню **Сервис > Экспорт справочников**).
- В доверенной сети функционирует устаревшая версия программного обеспечения ViPNet Administrator либо программного обеспечения ViPNet, установленного на клиентских местах.

Возможные варианты решения проблемы в зависимости от причины ее возникновения:

- Отправьте в УКЦ доверенной сети с помощью программы ViPNet Деловая почта либо средствами файлового обмена нужный СОС, предварительно экспортированный из УКЦ вашей сети (файл с расширением *.crl), либо сообщите администратору УКЦ доверенной сети точку распространения (см. [«Точка распространения данных»](#)) ваших актуальных СОС и корневых сертификатов администраторов.
- Рекомендуйте обновить соответствующее программное обеспечение на рабочем месте администратора доверенной сети ViPNet либо на клиентских местах до последней актуальной версии.



В

Глоссарий

V

ViPNet Publication Service

Программное обеспечение для публикации сертификатов пользователей, издателей (администраторов) и СОС в общедоступных хранилищах данных.

См. также: [Список отозванных сертификатов \(СОС\)](#).

ViPNet Registration Point

Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

См. также: [Дистрибутив ключей](#), [Пользователь ViPNet](#), [Сертификат открытого ключа подписи пользователя](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

С

Сертификат издателя

Сертификат, с помощью закрытого ключа которого подписывается другой сертификат.

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором Удостоверяющего центра и на данный момент недействительны.

См. также: [Уполномоченное лицо \(администратор\) Удостоверяющего центра](#).

Т

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, FTP или LDAP), используемый для размещения сформированной в Удостоверяющем центре информации (сертификатов издателей и списков отозванных сертификатов).

См. также: [FTP \(File Transfer Protocol\)](#), [LDAP \(Lightweight Directory Access Protocol\)](#), [Сертификат издателя](#), [Список отозванных сертификатов \(СОС\)](#), [Удостоверяющий центр](#).