

Outpost Network Security

- Централизованное развертывание и управление
- Защита от сетевых атак и Интернет-угроз
- Антивирус+антишпион с удаленной проверкой
- Блокирование USB-носителей
- Сервер локальных обновлений
- Защита файловых серверов и 64-битных систем



Инструкция по установке Outpost Network Security (ONS) 3.2

Содержание

Архитектура	2
Системные требования	2
Серверная часть:	2
Клиентская часть:	2
Подготовка к установке	3
Подготовка клиентов	3
Подготовка сервера	4
Установка программы	7
Развертывание Outpost Network Security Client на клиентских ПК	10
Устранение неполадок	13
Проблемы клиентской части	13
Проблемы серверной части	14
Наиболее типичные неисправности	15
Инструкция по обновлению с импортированием правил	16

Архитектура

Outpost Network Security (ONS) версии 3.2 подразумевает наличие следующих компонентов:

• Сервер:

Компьютер с установленной Консолью управления и сервером обновлений. Консоль – основной инструмент, позволяющий администратору контролировать клиентские компьютеры в сети и управлять настройками продукта. Сервер обновлений обеспечивает централизованное (однократная загрузка, многократная установка) обновление клиентского ПО.

• Клиент:

Один или более клиентских компьютеров, защищаемых клиентской частью ПО.

Системные требования

Совершенно необязательно устанавливать серверную часть Outpost Network Security на контроллер домена или сервер; она может быть установлена на любой специально отведенной для этой цели рабочей станции.

Серверная часть:

Поддерживаемые платформы (x32 и x64):

- Windows 2000 (SP4 с пакетом обновлений Security Rollup)
- Windows XP SP2 +
- Windows 2003 SP2
- Windows Vista SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

Минимальные требования к оборудованию: процессор 1 ГГц (x86-/x64-/мультиядерный), 512Мб оперативной памяти, 1Гб свободного дискового пространства.

Клиентская часть:

Поддерживаемые платформы (x32 и x64):

- Windows 2000 (SP4 с пакетом обновлений Security Rollup)
- Windows XP SP2+
- Windows 2003 SP2
- Windows Vista SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

Минимальные требования к оборудованию: процессор 1 ГГц (x86-/x64-/мультиядерный), 512Мб оперативной памяти, 450Мб свободного дискового пространства.

Поддерживаемые протоколы и службы электронной почты: POP3, SMTP, IMAP.

Примечание: 64-битный установочный пакет загружается отдельно.

Подготовка к установке

Подготовка клиентов

До установки клиента Outpost Network Security, пожалуйста, убедитесь в отсутствии предыдущих версий на этом ПК. Если предыдущая версия была установлена ранее, пожалуйста, удалите её с помощью стандартных средств Windows и перезагрузите ПК, после чего следуйте дальнейшей инструкции.

1. Для Windows XP:

- **Отключите Windows Firewall** на клиентском ПК.
- Убедитесь, что создана **учётная запись с правами администратора** и для неё задан **пароль**. Это необходимо для получения прав на удалённую установку. В некоторых случаях потребуется указать доменное имя в имени учётной записи администратора: **Имя_домена\УЗ_администратора**.
- Убедитесь, что общая папка **ADMIN\$** доступна. Пожалуйста, откройте **Панель Управления > Администрирование > Управление компьютером** и перейдите в категорию **Общие папки** для просмотра всех общих папок ПК.
- Откройте меню **Панель управления > Администрирование > Локальная политика безопасности > Параметры безопасности** и измените значение политики **Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей с Гостевая - локальные пользователи** удостоверяются как гости на **Обычная - локальные пользователи** удостоверяются как они сами.

2. Для Windows Vista и Windows 7

3. Отключите Windows Firewall на клиентском ПК.

- Убедитесь, что создана **учётная запись с правами администратора** и для неё задан **пароль**. Это необходимо для получения прав на удалённую установку. В некоторых случаях потребуется указать доменное имя в имени учётной записи администратора: **Имя_домена\УЗ_администратора**.
- Убедитесь, что общая папка **ADMIN\$** доступна. Пожалуйста, откройте **Панель Управления > Администрирование > Управление компьютером** и перейдите в категорию **Общие папки** для просмотра всех общих папок ПК.
- Запустите **regedit.exe** и найдите ключ:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

Если параметр **LocalAccountTokenFilterPolicy** отсутствует, щёлкните правой кнопкой мыши на элементе системы и выберите **Новый -> DWORD (32-бит)**. Укажите **LocalAccountTokenFilterPolicy** и установите значение **1**.

Подготовка сервера

- Предназначенный для установки сервера ONS ПК должен иметь статический IP.
- Убедитесь в отсутствии предыдущих версий на этом ПК. Если предыдущая версия была установлена ранее, пожалуйста, удалите её с помощью стандартных средств Windows и перезагрузите ПК.
- Если клиент установлен на том же ПК, что и сервер, пожалуйста, **отключите Windows Firewall**.
- В случае, если на сервере установлено несколько сетевых адаптеров, необходимо включить маршрутизацию между ними. Пожалуйста, найдите следующий ключ реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Если параметр **IPEnableRouter** отсутствует, щёлкните правой кнопкой мыше на элементе системы и выберите **Новый -> DWORD (32-бит)**. Укажите **IPEnableRouter** и установите значение **1**.

1. Для Windows XP

- **Отключите Windows Firewall** на клиентском ПК.
- Убедитесь, что создана **учётная запись с правами администратора** и для неё задан **пароль**. Это необходимо для получения прав на удалённую установку. В некоторых случаях потребуется указать доменное имя в имени учётной записи администратора: **Имя_домена\УЗ_администратора** Make sure that **File and Printer Sharing** is enabled on the computer. Please, open **Control Panel > Network Connections** and select the connection properties. **File and Printer Sharing** component should be present.
- Откройте меню **Панель управления > Администрирование > Локальная политика безопасности > Параметры безопасности** и измените значение политики **Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей с Гостевая - локальные пользователи** удостоверяются как гости на Обычная - **локальные пользователи удостоверяются как они сами**.

2. Для Windows Vista and Windows 7

- С помощью вышеописанных методов убедитесь, что общая папка **ADMIN\$** доступна.
- Убедитесь, что **Доступ к файлам и принтерам** включен на ПК. Пожалуйста, откройте **Панель управления > Сеть** и выберите свойства соединения. **Служба доступа к файлам и принтерам** должна присутствовать.
- Запустите **regedit.exe** и найдите ключ:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

Если параметр **LocalAccountTokenFilterPolicy** отсутствует, щёлкните правой кнопкой мыши на элементе системы и выберите **Новый -> DWORD (32-бит)**. Укажите **LocalAccountTokenFilterPolicy** и установите значение **1**.

- Убедитесь, что создана **учётная запись с правами администратора** и для неё задан **пароль**. Это необходимо для получения прав на удалённую установку. В некоторых случаях потребуется указать доменное имя в имени учётной записи администратора: **Имя_домена\УЗ_администратора** Make sure that **File and Printer Sharing** is enabled on the computer. Please, open **Control Panel > Network Connections** and select the connection properties. **File and Printer Sharing** component should be present.

По умолчанию клиентские станции соединяются с сервером обновлений по порту 80 ТСП. Если на ПК работают иные приложения, использующие этот порт, например, IIS, необходимо назначить другой порт для сервера обновлений. Список используемых портов можно получить, запустив команду **netstat** из командной строки. Пожалуйста, следуйте инструкции для переназначения порта сервера обновлений:

1. Закройте консоль управления.
2. Остановите службу Agnitum Administration Server в меню **Панель управления > Администрирование > Службы**.
3. Также остановите службу Agnitum Update Server в том же меню.
4. Откройте файл **C:\Program Files\Agnitum\Outpost Network Security\update_config.ini** и найдите параметр **ServerHTTPPort=** - по умолчанию указан порт 80.
5. Измените значение параметра **ServerHTTPPort=** на необходимое и сохраните изменение.
6. Перезапустите службу Agnitum Update server.
7. Перезапустите службу Agnitum Administration Server.
8. Установите клиентов.

Если клиенты уже были установлены, необходимо отредактировать файл **machine.ini** на клиентском ПК по следующей инструкции:
Запустите графический интерфейс клиента ONS, правым щелчком мыши по иконке продукта выберите приостановку защиты до перезапуска, после чего выйдите из программы с остановкой службы. Откройте файл **C:\Program Files\Agnitum\Outpost Security Suite Pro\machine.ini** и найдите секцию **[Update]**

Отредактируйте параметр **server**, добавив номер порта, например:
server=http://192.168.7.249:8080
Сохраните изменение.

9. Запустите графический интерфейс клиента, восстановите защиту и переключите в фоновый режим при необходимости.

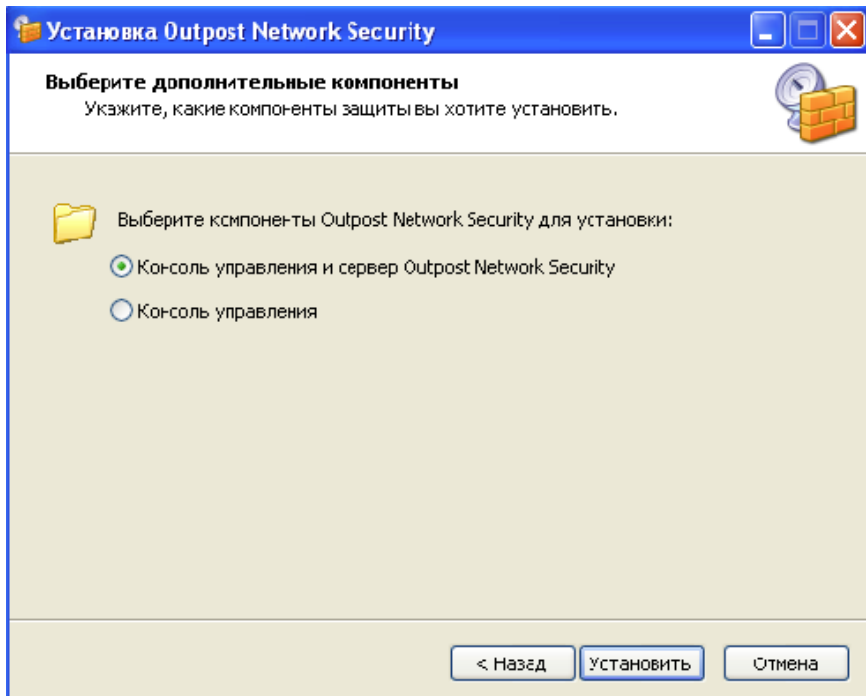
Также возможно указать IP-адрес сервера обновлений. Так как по умолчанию используется адрес 0.0.0.0, сервер слушает все интерфейсы по одному порту. Привязка сервера к определённомu IP-адресу даст возможность использовать один и тот же порт для разных служб. Для привязки необходимо после установки серверной части проследовать инструкции:

1. Закройте Консоль управления.
2. Остановите службу Agnitum Administration Server.
3. Остановите службу Agnitum Update Server.
4. Измените значение ServerBindIP= в файле C:\Program Files\Agnitum\Outpost Network Security\update_config.ini на нужный IP-адрес и сохраните изменения.
5. Перезапустите службу Agnitum Update server.
6. Перезапустите службу Agnitum Administration Server.

Примечание: Необходимо привязать к определённому адресу не только сервер обновлений, но и службу, использующую тут же порт. Для этого обратитесь к документации соответствующей службы.

Установка программы

Чтобы начать установку Outpost Network Security, запустите файл установки. Процедура установки проста и похожа на большинство программ под Windows. Просто следуйте шагам мастера установки и он установит все необходимые компоненты на ваш компьютер.



Мастер установки. Шаг 1 – выбор компонентов установки

Важно: И Консоль управления, и службы следует устанавливать на компьютер со статическим IP-адресом.

Во время установки в папку **C:\Program Files\Agnitum\Outpost Network Security\clients** будет скопирован установочный пакет Outpost Network Security Client, к папке будет автоматически дан общий доступ, чтобы установочный пакет был доступен всем клиентам в сети.

После копирования файлов мастер установки запросит номера портов, которые будут использоваться клиентскими компьютерами для соединения с сервером, а также пароль доступа к Консоли управления.

Мастер установки Outpost Network Security

Укажите настройки сервера
Пожалуйста, укажите сетевые настройки и пароль администратора.

Порты служб
Укажите порты, которые будут использоваться клиентами для соединения со службами Outpost Network Security.

Порт службы конфигурации: 1112
Порт службы обновлений: 1113

Безопасность
Укажите пароль, который будет контролировать доступ к Консоли управления.

Пароль:
Подтвердите:

< Назад Далее > Отмена

Мастер установки. Шаг 2 – Конфигурация сервера (Порты служб и Безопасность)

По завершении мастера установки укажите параметры подключения к серверной части и параметры доступа для запуска Консоли управления. Введите IP-адрес, DNS-имя или NetBIOS-имя компьютера, на котором установлены службы Outpost Network Security или выберите его из списка. Если серверная часть установлена на локальном компьютере, выберите **localhost** (по умолчанию).

Также укажите порт для службы конфигурации и параметры доступа (пароль, указанный во время установки серверной части).

Соединение с сервером

Agnitum Outpost Network Security
Введите параметры доступа.

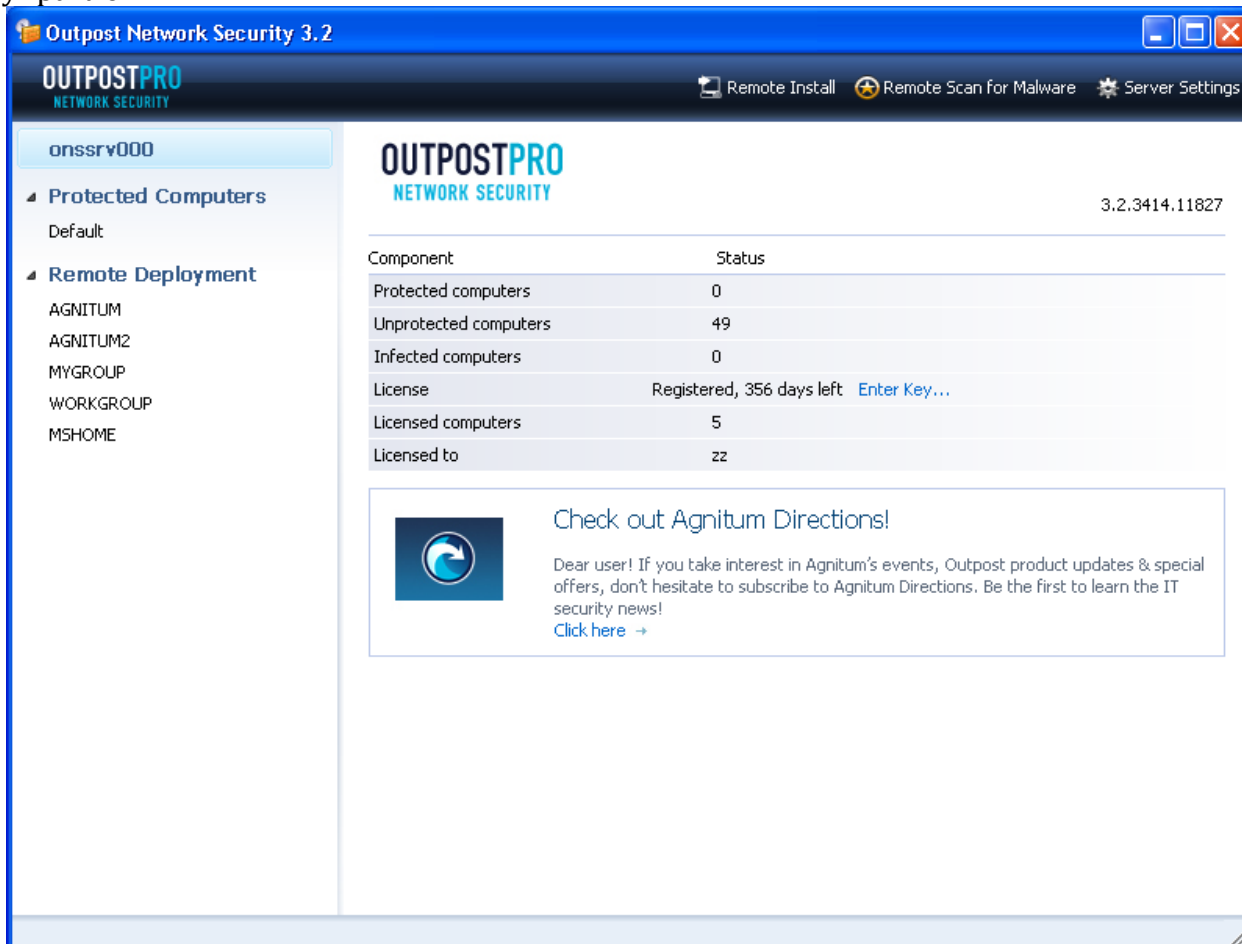
Сервер: localhost
Порт: 1112
Имя пользователя: Administrator
Пароль:

ОК Отмена

Соединение с сервером – окно “Введите параметры доступа”

Примечание: Outpost Network Security не устанавливает Outpost Network Security Client на консоль. Клиентское ПО может быть установлено на компьютере с установленной Консолью управления или службами Outpost Network Security вручную или с помощью процедуры, описанной в главе [Развертывание Outpost Network Security Client на клиентских ПК](#). Однако, если на этом компьютере уже установлено какое-либо средства безопасности, убедитесь, что соединение с портом, указанным в качестве порта службы конфигурации, не заблокировано. В противном случае, клиенты будут не в состоянии получать настройки и работать надлежащим образом.

Введите параметры доступа, щелкните **OK** и откроется главное окно Консоли управления.



Консоль управления ONS– Главное окно.

Развертывание Outpost Network Security Client на клиентских ПК

При небольшом числе компьютеров вы можете установить клиента Outpost Network Security на каждую рабочую станцию вручную (установочный пакет, **OutpostNetworkSecurityClientInstall.exe**, находится в папке **C:\Program Files\Agnitum\Outpost Network Security\clients**, которая становится доступной при установке).

Outpost Network Security позволяет устанавливать клиентское ПО на рабочие станции автоматически.

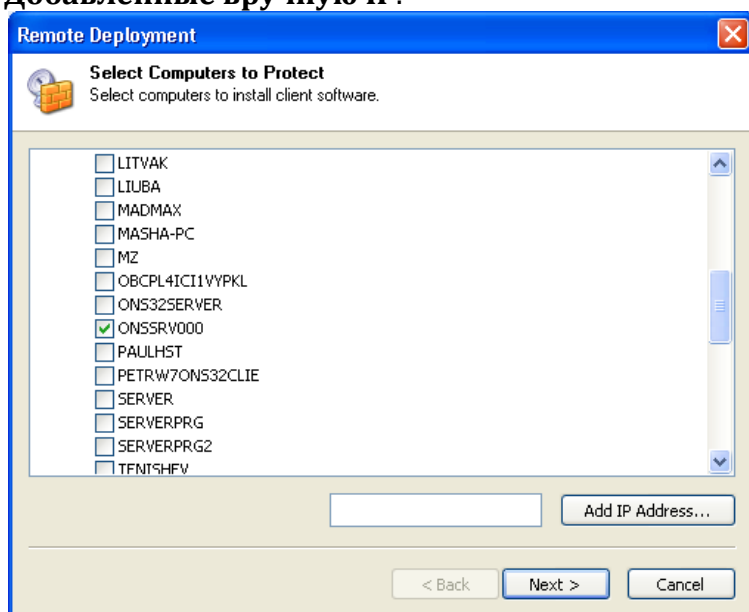
Все рабочие станции в вашей сети отображаются в ветке **Удаленное развертывание** в левой панели главного окна Консоли управления. Они объединены по доменам и рабочим группам, представленным подузлами данной ветки в соответствии с инфраструктурой вашей сети.

С помощью команды **Обновить сетевое окружение**, доступной в контекстном меню узла вы можете обновить информацию в левой панели.

Примечание: Консоль управления ONS определяет ПК, которые видны в Сетевом Окружении Windows. Если ПК в сети не виден через Windows Explorer, Консоль управления ONS не сможет его определить.

Чтобы автоматически установить клиентскую часть на рабочие станции, щелкните **Удаленная установка** на панели инструментов Консоли управления или выберете **Установить Outpost Network Security** в контекстном меню узла или конкретного компьютера и следуйте шагам Мастера удаленного развертывания.

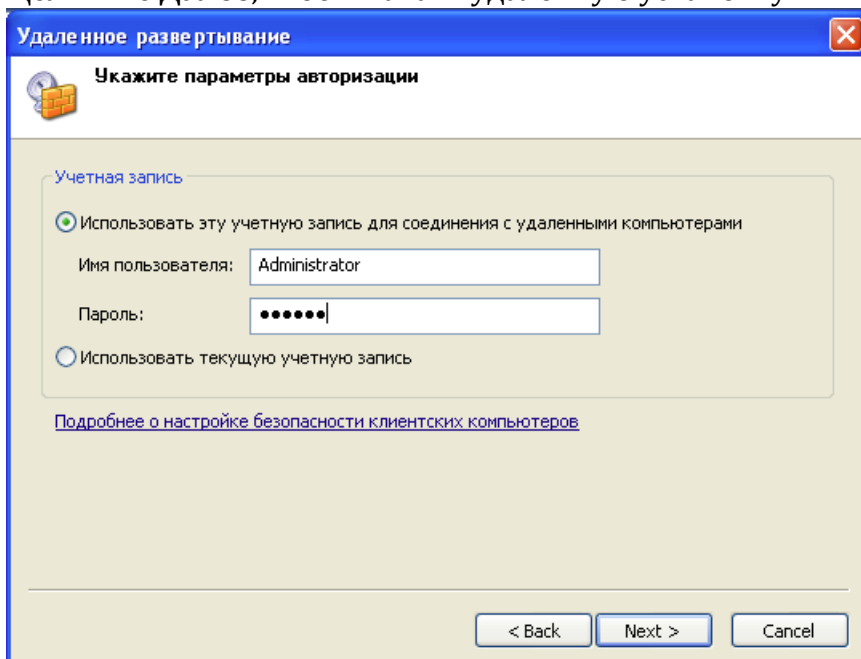
Первый шаг мастера позволяет выбрать компьютеры в вашей сети, на которые вы собираетесь устанавливать клиентское ПО. Вы также можете указать IP-адреса компьютеров вручную в специально отведенном текстовом поле внизу окна, если не видите имя компьютера в списке. Щелкните **Добавить IP-адрес** и IP появится в ветке **Добавленные вручную IP**.



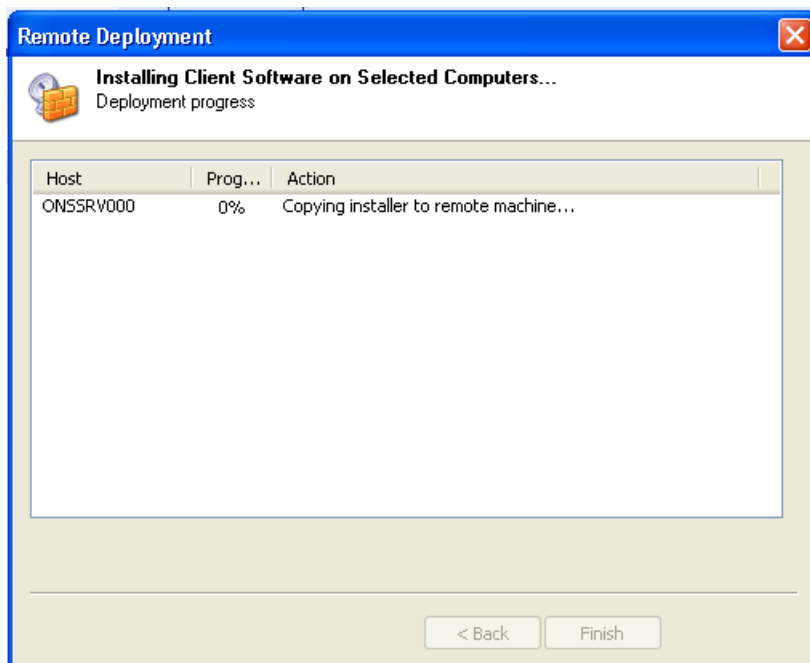
Удалённое развёртывание. Шаг 1 – выбор компьютеров для защиты.

Щелкните **Далее**. Мастер запросит параметры подключения к выбранным компьютерам. Указанная учетная запись должна обладать правами администратора на всех компьютерах.

Щелкните **Далее**, чтобы начать удаленную установку.

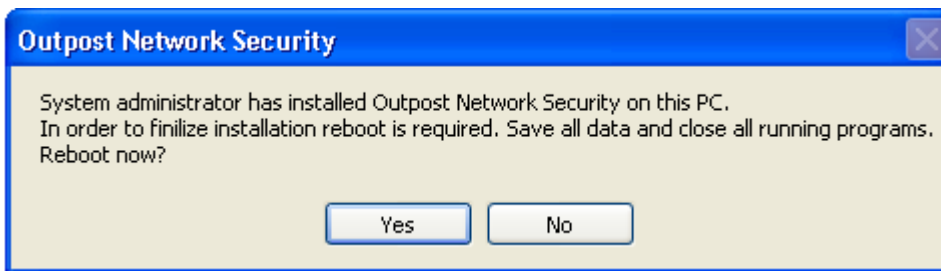


Удалённое развёртывание. Шаг 2 – указание параметров авторизации



Удалённое развёртывание. Шаг 3 – Установка клиентского ПО на выбранные ПК – развёртывание в процессе.

Клиенты информируются о необходимости перезагрузки. На клиентских ПК появляется соответствующее предупреждение. Необходимо убедиться, что ПК перезагружен.



Установка клиента Outpost Network Security – предупреждение о перезагрузке

Кнопка завершения в окне удалённого развёртывания становится доступной после установки клиентской части.

После установки клиента все компьютеры, на которые он был успешно установлен, появятся в **Основной группе** узла **Защищенные компьютеры**. Выбрав группу в левой панели, вы увидите список компьютеров, принадлежащих ей.

Устранение неполадок

При обнаружении неполадок, пожалуйста, свяжитесь со [Службой поддержки Agnitum](#). Используйте следующую инструкцию для сохранения необходимой технической информации.

Проблемы клиентской части

- 1) Откройте Консоль управления через меню Пуск - Программы - Agnitum - Outpost Network Security - Outpost Network Security.
- 2) Правой кнопкой мыши щёлкните по группе, в которой находится клиентский ПК (по умолчанию группа Default) и выберите Настройки.
- 3) Откройте Журналы, включите опцию 'Регистрировать отладочную информацию' и установите уровень лога 2. Сохраните изменения.
- 4) Перезапустите клиента.
- 5) Воспроизведите проблему.
- 6) Сразу после воспроизведения проблемы, правой кнопкой мыши щелкните на иконку Outpost в системном трее и выберите 'Сохранить файлы журнала'. После этого откроется папка 'Feedback'.
- 7) Пришлите нам feedback.zip из этой папки, а так же файлы Вашей конфигурации:
 - 1) *configuration.conf*
 - 2) *ons_conf.ini*
 - 3) *machine.ini*

находящиеся в папке установки Outpost

(По умолчанию *C:\Program Files\Agnitum\Outpost Security Suite Pro*).

Возможно, понадобится включить отображение расширений файлов в меню "Панель управления - Свойства папки - Вид". Необходимо снять галочку с опции "Скрывать расширения зарегистрированных типов файлов".

Проблемы серверной части

- 1) Откройте Консоль управления через меню Пуск - Программы - Agnitum - Outpost Network Security - Outpost Network Security.
- 2) Выберите меню Настройки сервера - вкладка Дополнительно.
- 3) Установите уровень лога 4 и сохраните изменения.
- 4) Перезагрузите компьютер и воспроизведите проблему.
- 5) Сразу после воспроизведения проблемы скопируйте и заархивируйте папку *C:\Program Files\Agnitum\Outpost Network Security\log*
- 6) Вышлите её вместе со следующими файлами:
 - 1) *administrative.stg*
 - 2) *configuration.conf*
 - 3) *machine.ini*
 - 4) *ons_con.ini*
 - 5) *ons_con.stg*
 - 6) *shuttle.ini*
 - 7) *update_config.ini*

Как правило одновременно требуются отладочные файлы сервера и клиента.

Наиболее типичные неисправности

Case	Troubleshooting steps
Клиенты не могут получить ответ от сервера	<p>Убедитесь, что соответствующие порты доступны. Это можно сделать с использованием утилиты telnet. В Windows Vista и Windows 7 эта утилита требует предварительной активации в меню Панель управления > Программы и компоненты, включите компоненты Windows, выберите Telnet нажмите ОК</p> <p>В командной строке введите telnet <IP сервера ONS> 1113 для проверки соединения. Если утилита отображает текст "connecting..." без прогресса, это означает заблокированный порт. Отключите Windows Firewall в таком случае.</p>
Клиенты не обновляются	<p>Сервер закачивает полную базу данных с серверов Agnitum, что занимает значительное время. Пожалуйста, удостоверьтесь, что сервер обновился полностью, подождав ~40 минут перед обновлением клиентов.</p>
Невозможно удалённо установить клиентов	<p>Убедитесь, что клиенты подготовлены согласно инструкции и управляются из-под учётной записи администратора. Контроль за учётными записями (UAC) должен быть отключен.</p>

Инструкция по обновлению с импортированием правил

Рекомендуется устанавливать новую версию с нуля и создавать новую конфигурацию. Однако если существует необходимость сохранить настройки групп, отдельных клиентов и правил для приложений, пожалуйста, используйте следующую инструкцию:

1) Сделайте резервную копию конфигурации сервера путём копирования следующих файлов из каталога C:\Program Files\Agnitum\Outpost Network Security:

- 1) *administrative.stg*
- 2) *ons_con.stg*
- 3) *machine.ini*
- 4) *ons_con.ini*
- 5) *shuttle.ini*
- 6) *update_config.ini*

2) Сохраните копию конфигурации клиентской станции (на каждом ПК с особыми правилами для приложений): файл *configuration.conf* из папки C:\Program Files\Agnitum\Outpost Security Suite Pro

3) Затем удалите клиентское приложение через апплет "Установка и удаление программ" и перезагрузите клиентский ПК.

4) Удалите сервер обновлений и консоль управления, перезагрузите ПК и установите новую версию консоли управления и сервера обновлений, загрузив её с <http://www.agnitum.ru/products/networksecurity/index.php>

5) Запустите консоль управления. Все защищаемые ПК временно находятся без защиты, требуется ручной перевод клиентских станций на новую версию.

6) Пожалуйста, импортируйте старую конфигурацию следующим образом:

- Закройте консоль управления.
- Откройте "Панель управления - Администрирование - Службы"
- Остановите службы Agnitum Administration Server и Agnitum Update Server.
- Скопируйте файлы конфигурации сервера в папку C:\Program Files\Agnitum\Outpost Network Security с перезаписью существующих в ней.
- Запустите службы Agnitum Update server и Agnitum Administration Server service.
- Откройте консоль администрирования и проверьте присутствие своих правил для групп защищаемых ПК.

Консоль администрирования определит наличие клиентских ПК, но посчитает их выключенными, так как на клиентских ПК не установлены соответствующие станции. Пожалуйста, удалите эти записи. При этом сохранятся настройки для группы.

После этого обновите сетевое окружение, щёлкнув правой кнопкой на группе незащищённых ПК и выбрав соответствующий пункт. После этого клиентские ПК появятся в списке незащищённых ПК, и на них можно установить ONS через консоль администрирования.

В настоящей реализации ONS клиентские станции информируются о необходимости перезагрузки с выдачей предупреждения на клиентском ПК. Пожалуйста, убедитесь, что клиенты были перезапущены.

После установки клиентов кнопка окончания процесса будет доступна. Клиентские ПК с настройками по умолчанию могут быть перемещены в группы с Вашими настройками.

Индивидуальное импортирование конфигурации для приложений

Если существуют особые правила для приложений на клиентских ПК, которые необходимо импортировать, пожалуйста, сделайте следующее:

- 1) Запустите клиентскую станцию из "Пуск - Программы - Agnitum Outpost Security Suite Pro - Outpost Security Suite Pro".
- 2) Приостановите защиту на 5 минут.
- 3) Выйдите из Outpost, нажав правой кнопкой мышки на иконке программы в системном лотке, выбрав "Выход", и выберите опцию "Выйти из Outpost и остановить службу"
- 4) Скопируйте ранее сохранённый файл configuration.conf в C:\Program Files\Agnitum\Outpost Security Suite Pro с перезаписью существующего файла.
- 5) Запустите клиентскую станцию и восстановите внутреннюю защиту.