Средство защиты информации Secret Net 7
Инструкция по автоматической установке клиента Secret Net 7

Данный документ содержит развернутое описание последовательности действий для выполнения и контроля автоматической установки клиентского ПО Secret Net на компьютерах. Приведенная последовательность применяется и для случаев обновления клиентов предыдущих версий Secret Net на текущую версию, если после обновления компьютеры будут подчинены серверу безопасности с таким же размещением хранилища объектов централизованного управления (или в Active Directory, или вне AD).

Примечание: При необходимости выполнить обновление клиентов на компьютерах, подчиненных серверу безопасности с размещением хранилища объектов ЦУ в AD, с последующим подчинением этих компьютеров серверу безопасности с размещением хранилища объектов ЦУ вне AD — следует использовать другую последовательность действий, которая приводится в документе "Инструкция по обновлению на Secret Net 7". Также в указанном документе приведены особенности обновления при наличии в системе иерархии серверов безопасности версий до 6.5 включительно.

1. На всех компьютерах, где будет установлено программное обеспечение СЗИ Secret Net, должен быть указан русский язык в качестве языка программ, не поддерживающих Юникод. Проверьте выполнение данного требования на компьютерах. Для просмотра и изменения состояния параметра вызовите диалоговое окно "Язык и региональные стандарты" в Панели управления ОС Windows.

2. Выполните начальную установку компонентов СЗИ Secret Net:

1. Если хранилище объектов централизованного управления будет размещаться в Active Directory, выполните модификацию схемы Active Directory.

2. На компьютерах, которые будут функционировать в качестве серверов безопасности, установите компонент "Secret Net 7 — Сервер безопасности" и компонент "Secret Net 7" с подчинением установленному на компьютере серверу безопасности.

3. Установите компонент "Secret Net 7" на рабочем месте администратора безопасности.

4. Установите компонент "Secret Net 7 — Программа управления" на рабочем месте администратора безопасности.

Примечание: Подробные сведения о процедурах модификации схемы Active Directory и установки компонентов см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

3. Создайте папку, которая будет являться общедоступным сетевым ресурсом. В данной инструкции предлагается создать папку \Distrib на контроллере домена. Откройте общий доступ к этой папке. Дополнительно предоставьте права доступа к папке всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или для группы "Прошедшие проверку" ("Authenticated Users"). Необходимые права обеспечиваются установленными разрешениями на чтение, чтение и выполнение и просмотр содержимого.

Примечание: Общедоступный сетевой ресурс можно создать на любом файловом сервере домена. Имя папки не регламентируется. Далее в инструкции в качестве общедоступного сетевого ресурса рассматривается папка \Distrib на контроллере домена.

4. С установочного компакт-диска СЗИ Secret Net скопируйте в папку \Distrib содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft. Если в системе имеются компьютеры, на которых будет использоваться средство аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card, дополнительно скопируйте в папку \Distrib содержимое каталога \Setup\SnTmCard.

5. Создайте файл со сценарием установки, используя доменный компьютер, на котором не установлено клиентское ПО СЗИ Secret Net. Для создания файла сценария войдите в систему с правами локального администратора компьютера и выполните следующие действия:

1. На локальном диске создайте папку C:\ClientSN и с установочного компакт-диска СЗИ Secret Net скопируйте в эту папку содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft.

Примечание: Папку можно создать на любом локальном диске компьютера. Имя и размещение папки не регламентируется. Далее в инструкции рассматривается папка C:\ClientSN.

2. Запустите консоль командной строки (cmd.exe).

3. Введите команду для запуска программы установки в режиме создания файла сценария:

- на компьютере под управлением 32-разрядной версии Windows:
  start C:\ClientSN\Setup\Client\Win32\Setup.exe /script:3
- на компьютере под управлением 64-разрядной версии Windows:
  start C:\ClientSN\Setup\Client\x64\Setup.exe /script:3

4. В программе установки выполните требуемые действия до появления на экране диалога "Готова к установке программы", после чего отмените дальнейшую установку.

5. Убедитесь, что файл сценария SnInstall.script добавлен в каталог размещения дистрибутивных файлов (соответственно C:\ClientSN\Setup\Client\Win32 или C:\ClientSN\Setup\Client\x64).

Примечание: Подробные сведения о создании и редактировании файла со сценарием установки см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

6. Скопируйте файл SnInstall.script в подкаталоги \Setup\Client\Win32 и \Setup\Client\x64 общедоступной папки \Distrib на контроллере домена. После копирования файла можно удалить папку C:\ClientSN на компьютере, который использовался для создания файла сценария.

7. На рабочем месте администратора безопасности запустите программу оперативного управления в режиме конфигурирования. Убедитесь в том, что на сервере безопасности зарегистрировано достаточное число лицензий для запланированного количества клиентов — для этого выберите сервер и перейдите на вкладку "Лицензии". При необходимости зарегистрируйте дополнительные серийные номера.

Примечание: Подробные сведения о работе с программой оперативного управления см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления".

8. Сформируйте в программе структуру оперативного управления — подчините серверу безопасности все компьютеры, на которых будет выполняться автоматическая установка клиента Secret Net.

9. Создайте в доменах безопасности организационные подразделения для группирования компьютеров, на которых будет выполняться автоматическая установка ПО. Для этого на компьютере контроллера домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" выберите последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup";
- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" выберите последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать | Подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup".

Примечание:

Редактирование объектов Active Directory возможно на любом компьютере домена с установленными средствами централизованного управления ОС Windows. На контроллере домена такие средства установлены по умолчанию. Далее в инструкции в качестве компьютера с установленными средствами централизованного управления ОС Windows рассматривается контроллер домена.

Имя организационного подразделения не регламентируется. Далее в инструкции рассматривается организационное подразделение с именем "Secret Net Autosetup".

10. Создайте групповые политики автоматической установки для подразделения (подразделений) "Secret Net Autosetup". Политики создаются отдельно для применения на 32- и 64-разрядных версиях ОС Windows. Для создания политик на компьютере контроллера домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" выберите последовательно каждое подразделение "Secret Net Autosetup" и создайте политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды меню "Действие | Создать объект групповой политики в этом домене и связать его" (вариант англоязычного названия: "Create a GPO in this domain, and Link it here");
- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" последовательно вызовите диалоговое окно настройки свойств каждого подразделения "Secret Net Autosetup", перейдите на вкладку "Групповая политика" и создайте политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью кнопки "Создать".

Примечание: Имена групповых политик не регламентируются. Далее в инструкции рассматриваются групповые политики с именами "SNAutosetup Policy Win32" и "SNAutosetup Policy x64".

11. Настройте параметры выполнения сценариев групповых политик. Для этого на компьютере контроллера домена выполните следующие действия:

- В ОС Windows Server 2012/2008:

  1. В оснастке "Управление групповой политикой" последовательно выберите созданные политики (являются подчиненными объектами в организационных подразделениях "Secret Net

Autosetup") и вызовите для каждой из них окно редактора групповых политик с помощью команды меню "Действие | Изменить".

2. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Политики\Административные шаблоны:…\Система\Сценарии". Вызовите диалоговое окно настройки свойств параметра "Указать максимальное время выполнения сценариев групповой политики" ("Specify maximum wait time for Group Policy scripts" для ОС Windows Server 2012 или "Maximum wait time for Group Policy scripts" для ОС Windows Server 2008), установите отметку в поле "Включено" и укажите значение "7200".

3. Вызовите диалоговое окно настройки свойств параметра "Отображать команды сценариев завершения работы во время их выполнения" ("Display instructions in shutdown scripts as they run") для ОС Windows Server 2012 или "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") для ОС Windows Server 2008 и установите отметку в поле "Включено".

- В ОС Windows Server 2003:

1. В оснастке "Active Directory — пользователи и компьютеры" последовательно вызовите диалоговое окно настройки свойств каждого подразделения "Secret Net Autosetup" и перейдите на вкладку "Групповая политика".

2. Последовательно выберите в списке каждую созданную политику и вызовите для нее окно редактора групповых политик с помощью кнопки "Изменить".

3. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Административные шаблоны\Система\Сценарии". Вызовите диалоговое окно настройки свойств параметра "Maximum wait time for Group Policy scripts", установите отметку в поле "Включен" и укажите значение "7200".

4. Вызовите диалоговое окно настройки свойств параметра "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") и установите отметку в поле "Включен".

12. В созданные групповые политики добавьте сценарии завершения работы. Для этого в окне редактора групповых политик (открытом на предыдущем действии) выполните следующие действия:

- В ОС Windows Server 2012/2008:

1. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Политики\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".

2. Добавьте сценарий с помощью кнопки "Добавить". В появившемся диалоге укажите следующие значения:

  - В поле "Имя сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>\Setup.exe
    где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" укажите подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64.
  - В поле "Параметры сценария":
    /autoinstall

- В ОС Windows Server 2003:

1. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".

2. Добавьте сценарий с помощью кнопки "Добавить". В появившемся диалоге укажите следующие значения:

  - В поле "Имя сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>\Setup.exe
    где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" укажите подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64.
  - В поле "Параметры сценария":
    /autoinstall

13. Переместите в подразделение (подразделения) "Secret Net Autosetup" те компьютеры, на которых необходимо выполнить автоматическую установку ПО. Перемещение компьютеров из других контейнеров выполняется в оснастке "Active Directory — пользователи и компьютеры" методом "Drag-and-Drop" или с помощью команды "Переместить" в контекстном меню компьютеров.

Пояснение: Механизм автоматической установки ПО клиента начинает действовать на компьютерах после обновления групповых политик на этих компьютерах. Применение заданных групповых политик осуществляется на компьютерах автоматически в соответствии с установленным режимом обновления политик. Чтобы немедленно применить групповые политики на отдельном компьютере, используйте стандартные средства (например, локальную утилиту gpupdate).

14. На рабочем месте администратора безопасности запустите программу оперативного управления в режиме мониторинга. Используйте программу для контроля процесса установки ПО на компьютерах. После успешной установки и перезагрузки компьютеров соответствующие объекты структуры оперативного управления изменяют свое состояние. В частности, изменяются пиктограммы объектов и признаки состояния.

Примечание: Подробные сведения о работе с программой оперативного управления см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления".

15. После того как установка ПО произошла на всех компьютерах, в оснастке "Active Directory — пользователи и компьютеры" переместите компьютеры из подразделения (подразделений) "Secret Net Autosetup" обратно в исходные контейнеры.

16. После завершения автоматической установки ПО на всех предусмотренных компьютерах удалите объекты, созданные для обеспечения автоматической установки:

1. На контроллере домена удалите папку \Distrib.

2. Удалите подразделение (подразделения) "Secret Net Autosetup" и созданные групповые политики автоматической установки (после перемещения в исходные контейнеры всех компьютеров). Для этого на компьютере контроллера домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" перейдите к разделу "Объекты групповой политики" в иерархии объектов домена и удалите политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды контекстного меню "Удалить". Затем аналогичным образом удалите подразделение (подразделения) "Secret Net Autosetup";
- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" удалите подразделение (подразделения) "Secret Net Autosetup" с помощью команды контекстного меню "Удалить".