FortiClient v5.0

Руководство по администрированию

9 января 2013
04-501-183401-20130109

Техническая документация
docs.fortinet.com
База знаний
kb.fortinet.com
Обслуживания клиентов и поддержки
support.fortinet.com
Услуги по обучению
training.fortinet.com
FortiGuard
fortiguard.com
Документ Обратная связь
techdocs@fortinet.com
Изменения регистрации
Дата
Изменить описание
2012-11-02
Первый релиз.
2012-11-07
Обновлены скрипты глав. Этот документ в настоящее время включают как Windows, и Mac OS X. Это
Важно отметить, что не все функции доступны для Windows, доступны для Mac OS X.
2012-11-15
Обновленный IPsec и SSL VPN-главе.
2012-11-22
Добавлено примечание о FortiClient Лицензия на FortiAuthenticator.
2012-11-27
Обновлен команды сценария, чтобы соответствовать изменениям в FortiClient v5.0 Ссылка XML.

2013-01-09
Обновлено для FortiClient v5.0 релиза патча 1. Удалены XML главе см. в FortiClient v5.0 Справочник по XML для получения дополнительной информации. Удалены FortiClient главе средствах см. FortiClient
Примечания к выпуску для получения дополнительной информации.

Введение

FortiClient была полностью заново разработанный для версии 5.0. FortiClient обеспечивает всесторонний решения сетевой безопасности для конечных точек, в то время как улучшение видимости и контроля. FortiClient позволяет управлять безопасностью нескольких конечных устройств FortiGate от интерфейса.
Этот документ содержит обзор FortiClient v5.0.

Лицензирование

Лицензирования на FortiGate на основе количества зарегистрированных клиентов. FortiGate 40C и выше модели поддерживают 10 (десяти) бесплатно управляемых FortiClient лицензий. Для получения дополнительной управляемых клиентов, обновленная должна быть приобретена лицензия. Максимальное количество управляемых клиентов изменяется в зависимости от модели устройства.

Клиент пределы

Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1 для Mac OS X.
Модель FortiGate
Бесплатная регистрация
FortiClient лицензии на обновление SKU
FortiGate 40, 60, 80 серии, VM00
10
N / A
FortiGate 100, 200, 300, 600, 800 серии, VM01/VM01-Xen, VM02/VM02-Xen
10
1000 регистраций клиентов
FCC-C0103-LIC
FortiGate 1000, 3000, 5000 серий, VM04/VM04-Xen, VM08/VM08-Xen
10
3000 регистраций клиентов
FCC-C0105-LIC
В высокой доступности (HA) конфигураций, всех членов кластера требует лицензионный ключ для обновления.
Для получения дополнительной информации, зайдите в www.forticlient.com.
Fortinet Технологии Инк
FortiClient v5.0 Руководство администратора

Поддерживаемые операционные системы

ОС Windows
Microsoft Windows 8 (32-разрядная и 64-разрядная версия)
Microsoft Windows 7 (32-разрядная и 64-разрядная версия)
Microsoft Windows Vista (32-разрядная и 64-разрядная версия)

Microsoft Windows XP (32-разрядная версия)
Mac OS X
Mac OS X v10.8 Mountain Lion
Mac OS X v10.7 Lion
Mac OS X 10.6 Snow Leopard

Минимальные системные требования

ОС Windows
Microsoft Internet Explorer 8.0 или более поздней
ОС Windows совместимый компьютер с процессором Pentium или эквивалентный
Совместимой операционной системы и минимального ОЗУ: 512 МБ
600 Мб свободного места на жестком диске
Родные Microsoft TCP / IP протокол связи
Родные Microsoft программа дозвона для коммутируемого соединения
Ethernet NIC для сетевых соединений
Беспроводной адаптер для беспроводного подключения к сети
Adobe Acrobat Reader или другой PDF Reader для инструкция
MSI Installer 3.0 или более поздняя версия
Mac OS X
Процессор Intel
256 Мб оперативной памяти
20 МБ на жестком диске (HDD) пространства
TCP / IP протокол связи
Ethernet NIC для сетевых соединений
Беспроводной адаптер для беспроводного подключения к сети.

Пожалуйста, ознакомьтесь с FortiClient v5.0 Патч Release 1 (Windows) или выпуске FortiClient Patch v5.0 Release 1 (Mac OS X) Заметки о выпуске перед обновлением. Текст документа доступен на обслуживание клиентов и поддержка.

Что нового в версии 5.0 FortiClient

Резюме усовершенствования

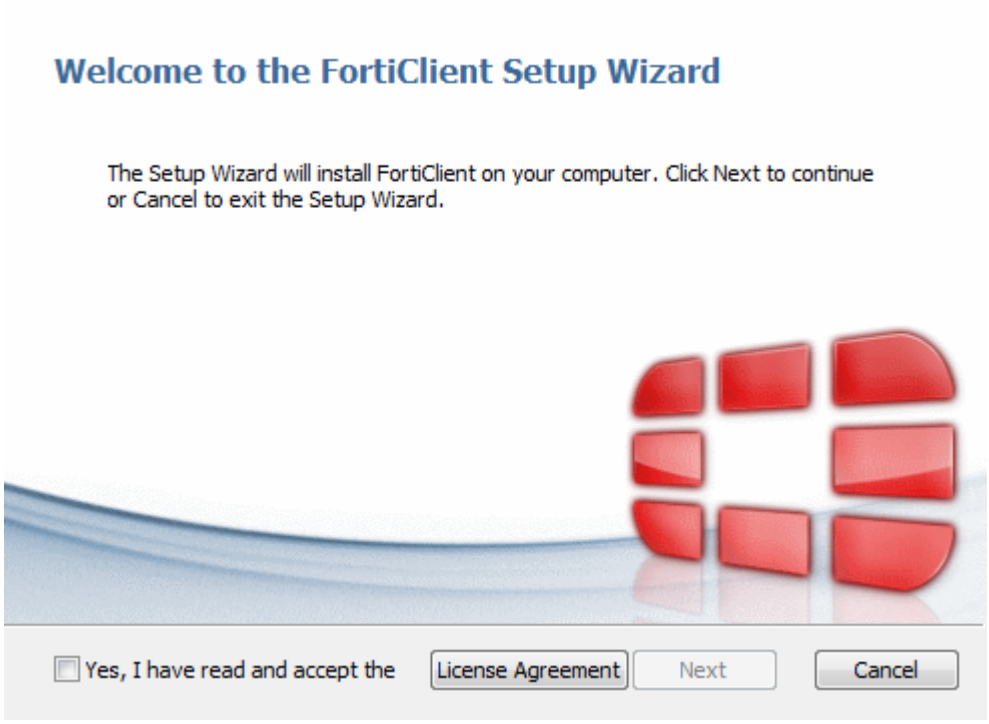
Ниже приведен список усовершенствований в FortiClient v5.0 (включая патч Выпуск 1):
Защита от вирусов и вредоносных
Защиту от новейших вирусов и нежелательных программ (рекламных / опасное) угроз.
Антивирусный клиент, является бесплатным и автоматическое обновление каждые три часа.
Application Firewall
Блок, позволит и контролировать приложения, отправлять трафик на сети.
Bring Your Own Device (BYOD)
Диагностический инструмент
Усовершенствования консоли FortiClient
Управление конечными точками использованием FortiGate, в том числе:
Автоматическая регистрация конечных точек и инициированные пользователем регистрации конечных точек.
Развертывание VPN (IPsec / SSL) конфигурации.
Включить / отключить антивирусную защиту в реальном времени.
Управление / развертывания веб-фильтрации и настройки Application Firewall.

Регистрация по IPsec VPN или SSL-VPN.
FortiGuard Analytics
Автоматически отправлять подозрительные файлы в сети FortiGuard для анализа.
Поддержка локализации
Родительский контроль / Web Filter
Блок, позволяют, предупреждают и мониторинга веб-трафика на основе категорий.
Помните, несколько FortiGates для регистрации Контроль рабочего места.
Удаленный доступ (IPsec и SSL VPN)
Безопасные виртуальные частные сети (VPN) доступ к вашей сети.
Поддержка нескольких шлюзов для одного туннеля.
Поиска и удаления руткитов
Single Sign-On агента мобильности с поддержкой FortiAuthenticator / FSSO Collector агент
Поддержка автоматического выполнения пользовательского сценария партию через туннель IPsec VPN
Поддержка нескольких (максимум 10) Шлюз IP / FQDN в одном конфигурации IPsec VPN
Поддержка XML-конфигурации
VPN из системного трея
Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1 для Mac OS X.
Fortinet Технологии Инк
VPN автоматического подключения / всегда
Поддержите возможность автоматического подключения к туннелю VPN без вмешательства пользователя.
Поддержите возможность настройки VPN, чтобы всегда быть подключены.
Поиск уязвимостей
Определение системы и приложений уязвимости.

Установка FortiClient на компьютере ОС Windows

Следующие инструкции помогут вам хотя установка FortiClient на ОС Windows компьютер.

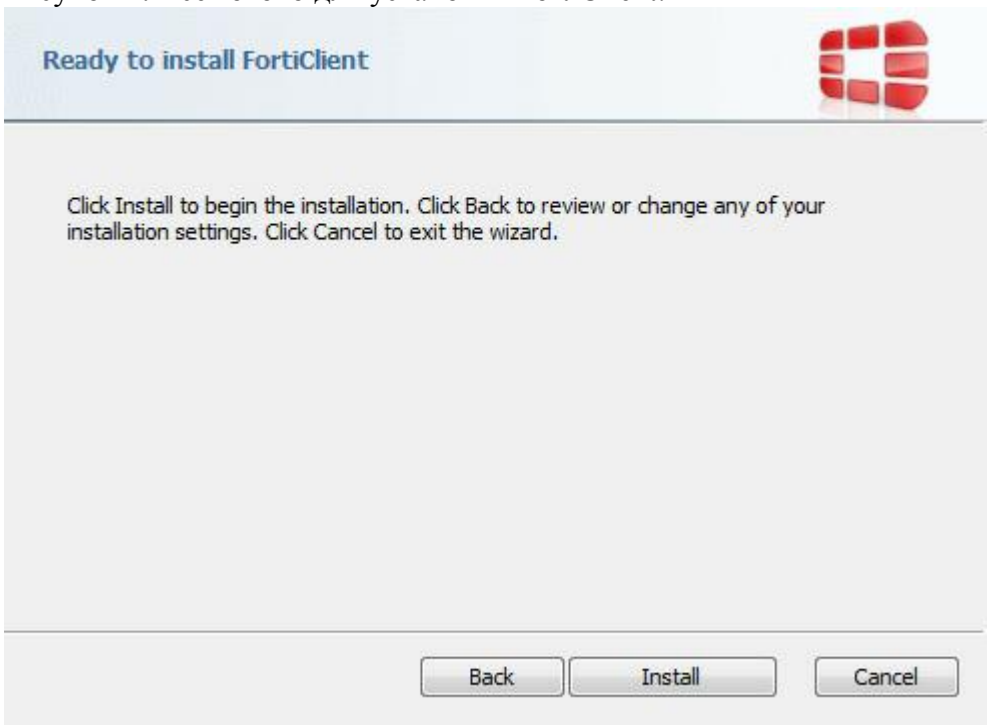
Чтобы установить FortiClient
1. Дважды щелкните на исполняемый файл FortiClient для запуска мастера установки.
Мастер установки
FortiClient установить на ваш компьютер.
Рисунок 1: Экран приветствия.



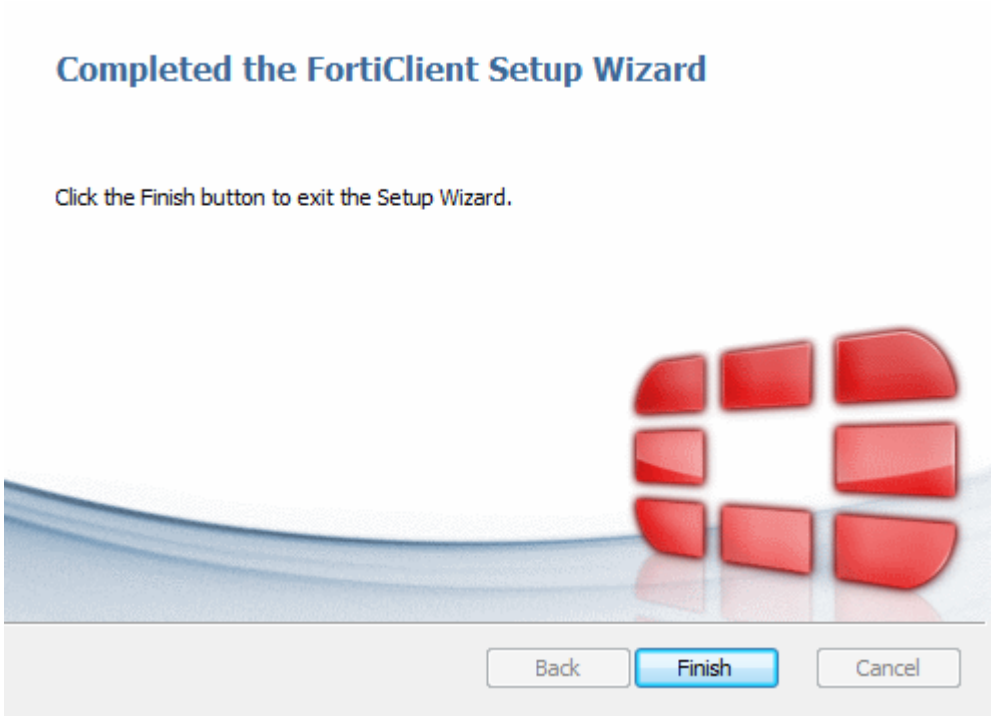
2. Прочитайте лицензионное соглашение и нажмите Далее, чтобы продолжить. У Вас есть возможность распечатать Лицензионное соглашение на этом экране.
Рисунок 2: Лицензионное соглашение.

3. Выберите Изменить, чтобы выбрать альтернативный папку назначения для установки. Выберите Далее, чтобы продолжиться.
Рисунок 3: Выбор папки назначения

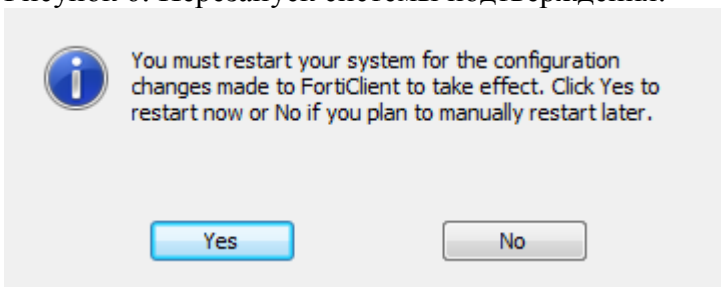
4. Выберите Установить, чтобы продолжить.
Рисунок 4: Все готово для установки FortiClient.



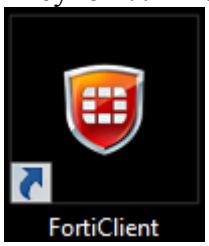
5. Выберите Готово для выхода из мастера установки FortiClient.
Рисунок 5: Установка завершена



6. При новой установке FortiClient, вам не нужно, перезагруживать систему. При обновлении FortiClient версии, вы должны перезагрузить систему для изменения конфигурации FortiClient вступили в силу. Выберите Да, чтобы перезагрузить компьютер сейчас, или Нет, чтобы вручную перезагрузку позже.
Рисунок 6: Перезапуск системы подтверждения.



7. Для запуска FortiClient, дважды щелкните значок на рабочем столе ярлык.
Рисунок 7: Выберите FortiClient ярлык для запуска



Установка FortiClient на компьютере Mac OS X

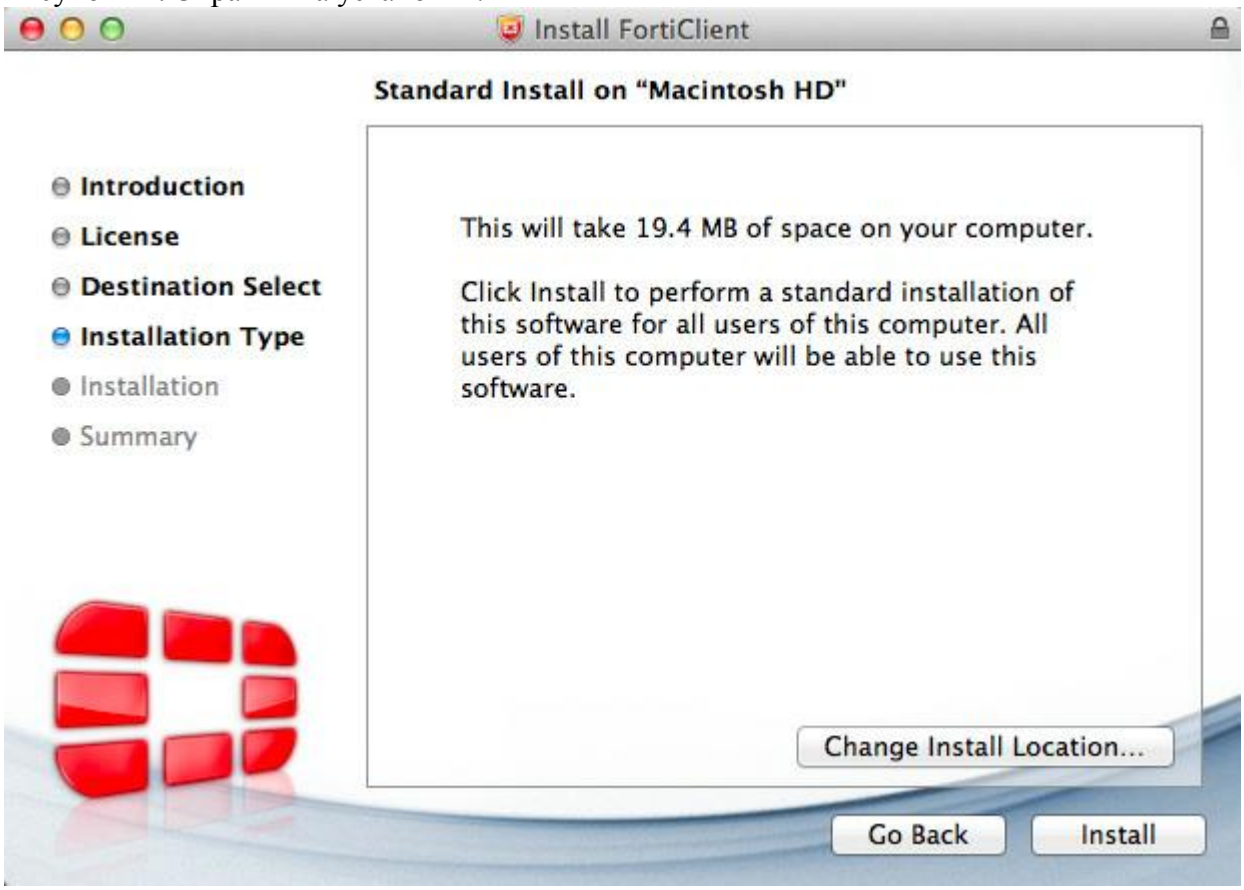
Следующие инструкции помогут Вам для установки FortiClient на Mac OS X компьютер.
Чтобы установить FortiClient
1. Дважды щелкните FortiClient, чтобы запустить установщик FortiClient.
FortiClient Installer установит FortiClient на вашем компьютере. Выберите Продолжить.
Рисунок 8: Экран приветствия

2. Прочитайте лицензионное соглашение и выберите Продолжить. У вас есть возможность распечатать или сохранить соглашение на программное обеспечение на этом экране. Вам будет предложено согласиться с условиями действия лицензионного соглашения.
Рисунок 9: Лицензионное соглашение.

3. Выберите папку для установки.

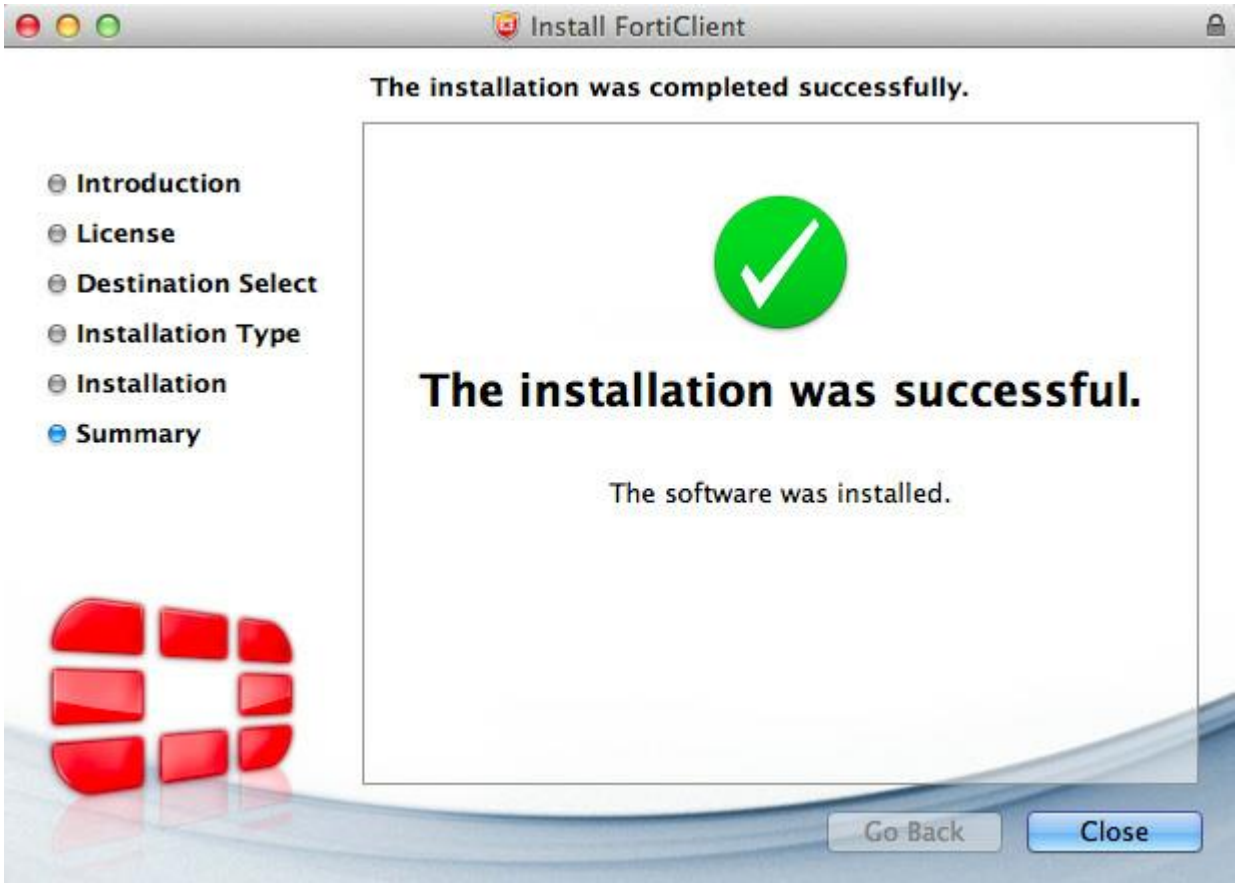
Рисунок 10: направление Выберите экран.

4. Выберите Установить, чтобы выполнить стандартную установку на этом компьютере. Вы можете изменить установки местоположение от этого экрана.
Рисунок 11: Экран типа установки.



5. В зависимости от вашей системы, вам может быть предложено ввести системный пароль.
Рисунок 12: Введите системный пароль, чтобы продолжить

6. Установка прошла успешно. Выберите Закрыть для выхода из программы установки.
Рисунок 13: Установка прошла успешно.



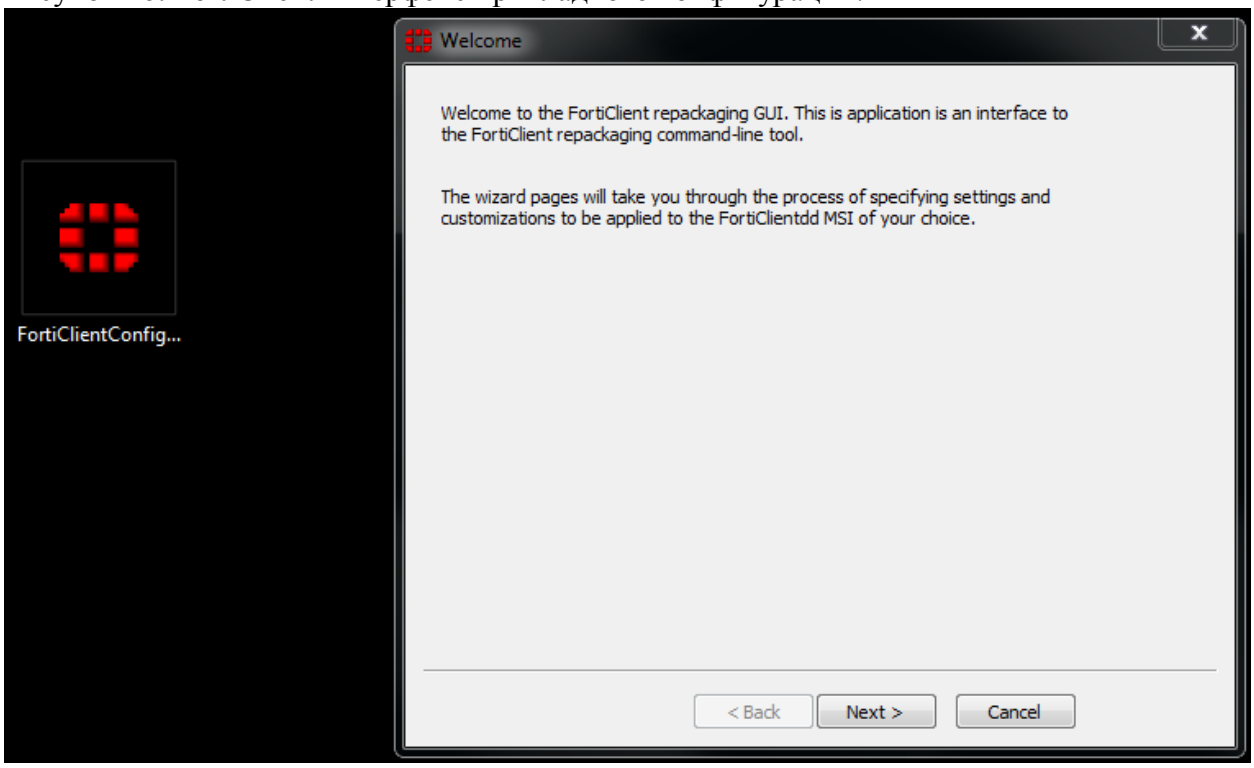
7. FortiClient был сохранен в папку Applications.
Рисунок 14: Папку Приложения.

8. Дважды щелкните FortiClient значок, чтобы запустить приложение. Выберите значок замка в левой нижней части приборной панели, чтобы внести изменения в FortiClient конфигурации.
Рисунок 15: Приборная панель по умолчанию заблокирована FortiClient.

Provisioning FortiClient
FortiClient конфигурации MSI инструмент
FortiClient конфигуратор инструментом является рекомендуемым методом создания индивидуальной установки FortiClient.
Использование
FortiClientConfigurator.exe-м <path к FortiClient.msi file>
[Необязательные параметры]
-M <path к FortiClient MSI файлу (обязательно)
- REGISTRATIONKEY <key>
Используйте для запретить пользователям изменять настройки FortiClient.
- FGTIP <ip:port или fqdn:port>
FortiClient попытается зарегистрируйтесь, чтобы получить эту FortiGate. Если он не может, он будет пытаться зарегистрироваться, чтобы по умолчанию
шлюз.
Пример использования
FortiClientConfigurator.exe-MC: \ Downloads \ forticlient.msi
- REGISTRATIONKEY sercretpassword
Эта команда выше создает следующие каталоги, содержащие файлы готовые для развертывания:
C: \ Downloads \ FortiClient_packaged \ ActiveDirectory \
C: \ Downloads \ FortiClient_packaged \ ManualDistribution \
FortiClient конфигуратор
Инструмент FortiClientConfiguratorGUI это приложение, интерфейс к FortiClient переупаковка инструмент командной строки. Мастер проведет вас через процесс определения параметров, чтобы быть применяется к FortiClient файл MSI.
Этот документ был написан для FortiClient v5.0 Патч Release 1 для Windows. Не все функции описанное в этом документе поддерживаются для FortiClient v5.0 Патч Release 1

для Mac OS X.
Выключатель и параметров чувствительны к регистру.

Рисунок 16: FortiClient интерфейс прикладного конфигурации.



Создание пользовательского файла установки MSI

Вы можете создать собственный файл установщика MSI для вашего специализированного приложение FortiClient:
1. Определите параметры командной строки, для этого нужно для установки настроенной FortiClient.
2. В папке, где вы расширили программу установки. ZIP пакета, выполните следующую команду линия запись:
FortiClientConfigurator.exe-м <path к FortiClient.msi file>
<optional switches>
Новый подкаталог создан, который содержит FortiClient файл MSI.
Развертывание FortiClient использованием Microsoft Active Directory (AD) сервер
Есть несколько способов установить FortiClient к конечной точке устройствами с помощью Microsoft Active
Directory.
Использование Microsoft AD развертывания FortiClient:
На контроллере домена, создайте точку распространения.
1. Войдите на сервер с учетной записью администратора.
Для получения дополнительной информации о конфигурации FortiClient XML см. в FortiClient v5.0 Справочник по XML
Fortinet на сайте технической документации, http://docs.fortinet.com.
Следующие инструкции основаны от Microsoft Windows Server 2008. Если вы используете различные версии сервера Microsoft, ваши или MMC оснастку в местах, могут быть различными.
2. Создание общей сетевой папке, где FortiClient файл установщика MSI будут распространяться с.
3. Установите права доступа к файлам на папку, разрешающие доступ к дистрибутиву. Скопируйте

FortiClient MSI пакет установки в эту общую папку.
4. Выберите Пуск> Администрирование> Active Directory пользователи и компьютеры.
5. После выбора домена, щелкните правой кнопкой мыши, чтобы выбрать новую организационную единицу (OU).
6. Перемещение всех компьютеров, которые необходимо распространять программное обеспечение для FortiClient вновь созданные подразделения.
7. Выберите Пуск> Администрирование> Управление групповой политикой. Групповая политика.
Управление оснастку откроется. Выберите OU вы только что создали. Щелкните правой кнопкой мыши, выберите Создание объекта групповой политики в этом домене и связать его здесь. Дайте новому GPO имя и нажмите ОК.
8. Разверните объект групповой политики и найти контейнер групповой политики, который только что создали. Щелкните правой кнопкой мыши GPO и выберите Изменить. Редактор управления групповой политикой оснастку откроется.
9. Разверните узел Конфигурация компьютера> Политики> Параметры программ. Щелкните правой кнопкой мыши Программное обеспечение
Настройки и выберите New> Package.
10.Выберите на пути к вашей точке распространения и FortiClient файл установки, а затем выберите Открыть. Выбор заданных и выберите ОК. Пакет будет создаваться.
11.Если вы хотите ускорить процесс установки, как на сервере и клиентских компьютерах, принудительно обновить GPO.
12.The программное обеспечение будет установлено на следующей перезагрузки клиентского компьютера. Можно также ожидать клиентском компьютере для опроса контроллера домена для изменения объекта групповой политики и установить программное обеспечение.
Удалите FortiClient использованием Microsoft Active Server каталогов
В этом разделе описывается, как удалить FortiClient с клиентских компьютеров с помощью Active Directory:
1. На контроллере домена, выберите Пуск> Администрирование> Управление групповой политикой.
Управление групповыми политиками оснастку откроется. Развернуть объектов групповой политики контейнер и щелкните правой кнопкой мыши объект групповой политики, созданный для установки и выберите FortiClient Изменить. Редактор управления групповой политикой откроется.
2. Выбор конфигурации компьютера> Политика> Настройки программы> Установка программного обеспечения. Вы будете теперь смогут увидеть пакет, который был использован для установки FortiClient.
3. Щелкните правой кнопкой мыши пакет, выберите Все задачи> Удалить. Выберите Немедленное удаление программное обеспечение от пользователей и компьютеров, или разрешить пользователям продолжать использовать программное обеспечение, но предотвращения новых установок. Нажмите кнопку ОК. Пакет будет удален.
4. Если вы хотите ускорить процесс удаления, как на сервере и клиентских компьютерах, заставить объект групповой политики обновления, как показано в предыдущем разделе.
Программное обеспечение будет удалена со следующей перезагрузки компьютера. Можно также ожидать компьютер для опроса домен контроллера для изменения объекта групповой политики и удаления программного обеспечения.
Развертывание с помощью Microsoft System Center Configuration Manager 2007
Если вы хотели бы использовать системы от Microsoft Center Configuration Manager (SCCM) для развертывания FortiClient, используйте следующий метод:
Эти инструкции предполагают, у вас уже установлен и настроен SCCM. Если у вас нет, пожалуйста, обратитесь к Microsoft онлайн-источники справки для получения информации о выполнении этой задачи.

Шаг 1: создать пакет

1. Запуск вашей консоли Configuration Manager GUI и расширить следующее: Компьютер Управление> Программные пакеты дистрибутива>.
2. Щелкните правой кнопкой мыши и выберите пакеты Создать> Пакет из контекстного меню. Мастер открыть.
3. Заполните пакеты свойствами, как вы хотите на вкладке Общие.
4. На вкладке Источник данных выберите Этот пакет содержит исходные файлы коробку, а затем выберите Установить кнопку, чтобы указать источник SCCM пакет. SCCM попросит вас указать путь к исполняемый файл установки. Выбор этого пути, а затем выберите OK.
5. Установите флажок рядом с обновление точек распределения по расписанию, а затем установите планировать, как часто вы хотите.
6. Настроить параметры доступа к данным в случае необходимости.
7. На вкладке Параметры распространения, установить приоритет передачи. Высокая рекомендуется.
8. Под вкладку Отчетность, оставьте настройки по умолчанию.
9. Под вкладке Безопасность установить права для класса пакета и прав экземпляре.
10.Review ваш пакет выборы под вкладку Сводка, затем выберите Далее. Мастер завершить.

Шаг 2: Создание программы для вашего пакета.

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:
Управление компьютером > Распространение программного обеспечения> пакеты. Выберите только что созданную FortiClient пакета. Щелкните правой кнопкой мыши этот пакет и выберите Создать > Программа из контекстного меню.
2. На вкладке Общие, заполнить соответствующие подробности. Для автоматической установки, убедитесь, что вы использовать MS-переключатель под параметров командной строки.
3. На вкладке Требования установите флажки рядом с клиентских платформах вы хотите установить для (Windows Vista, Windows XP и т.д.).
4. Установите переменные окружения. Рекомендуется, чтобы выбрать, что программа могла работать.
5. Вы можете оставить Расширенный и Windows Installer вкладки по умолчанию.
6. Если вам требуется уведомление, направленное Microsoft Operations Manager (MOM), выберите соответствующие параметры на вкладке обслуживание.
7. Как и на предыдущем этапе, рассмотреть Ваше резюме, а затем создать вашу программу.

Шаг 3: реклама вашего пакета на клиентские компьютеры.

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:
Управление компьютером> Распространение программного обеспечения > Объявления. Щелкните правой кнопкой мыши и выберите Объявления Новое объявление > из контекстного меню.
2. При запросе нет распределительных пунктов, выберите Да. Мы будем обновлять распределения указывая позже в процессе.
3. По расписанию вкладке установите дату вы хотите. Установите уровень приоритета (рекомендуется установка "High"). Выберите на желтом звездочкой для указания обязательных параметров.
4. На вкладке Точки распространения, выберите "Загрузить содержимое с точки распространения и запустить локально как для все настроек.
5. При взаимодействии вкладке, вы можете использовать это, чтобы предупредить

зарегистрированным пользователям, что программа будет запустить и обеспечить таймер обратного отсчета до завершения исполнения.
6. Под вкладке Безопасность установить права для класса пакета и прав экземпляре.
7. Просмотрите выбранные параметры пакета под вкладку Сводка, затем выберите Далее. Мастер завершить.

Шаг 4: Создание и обновлять точки распространения

1. Стартовая конфигурация вашего менеджера интерфейс консоли и раскройте следующие:
Управление компьютером > Распространение программного обеспечения > пакеты.
Расширен пакет, созданный и щелкните правой кнопкой мыши Точки распространения.
Щелкните правой кнопкой мыши Точки распространения и выберите Создать точки распространения из контекстного меню. Откроется окно мастера.
2. Выберите SCCM сервер из списка доступных серверов и выберите Далее. Вы увидите резюме и мастера будет завершена.
3. Теперь вам необходимо обновить точки распространения, который был только что создан с пакета. Щелкните правой кнопкой мыши Точки распространения и теперь выбрать распространения обновлений
Очки из контекстного меню. Всплывающем окне появится. Подтвердите обновление, Да выбора.

Использование Microsoft SCCM 2007 удалить FortiClient:

1. Откройте консоль Configuration Manager:
System Center Configuration Manager> База данных сайта> Управление компьютером> Распространение программного обеспечения> Пакет> Реклама.
2. Выберите FortiClient пакет, который вы хотите удалить, затем выберите для каждой системы удаления. Обеспечивать
выбран правильный коллекции границы. Укажите, когда реклама будет вещать членов целевой коллекции.
3. Завершите работу мастера. Убедитесь, что вы удалите начальные Реклама установке вы использовали для установки FortiClient для предотвращения SCCM от FortiClient переустановки.

Управление конечными точками

Введение

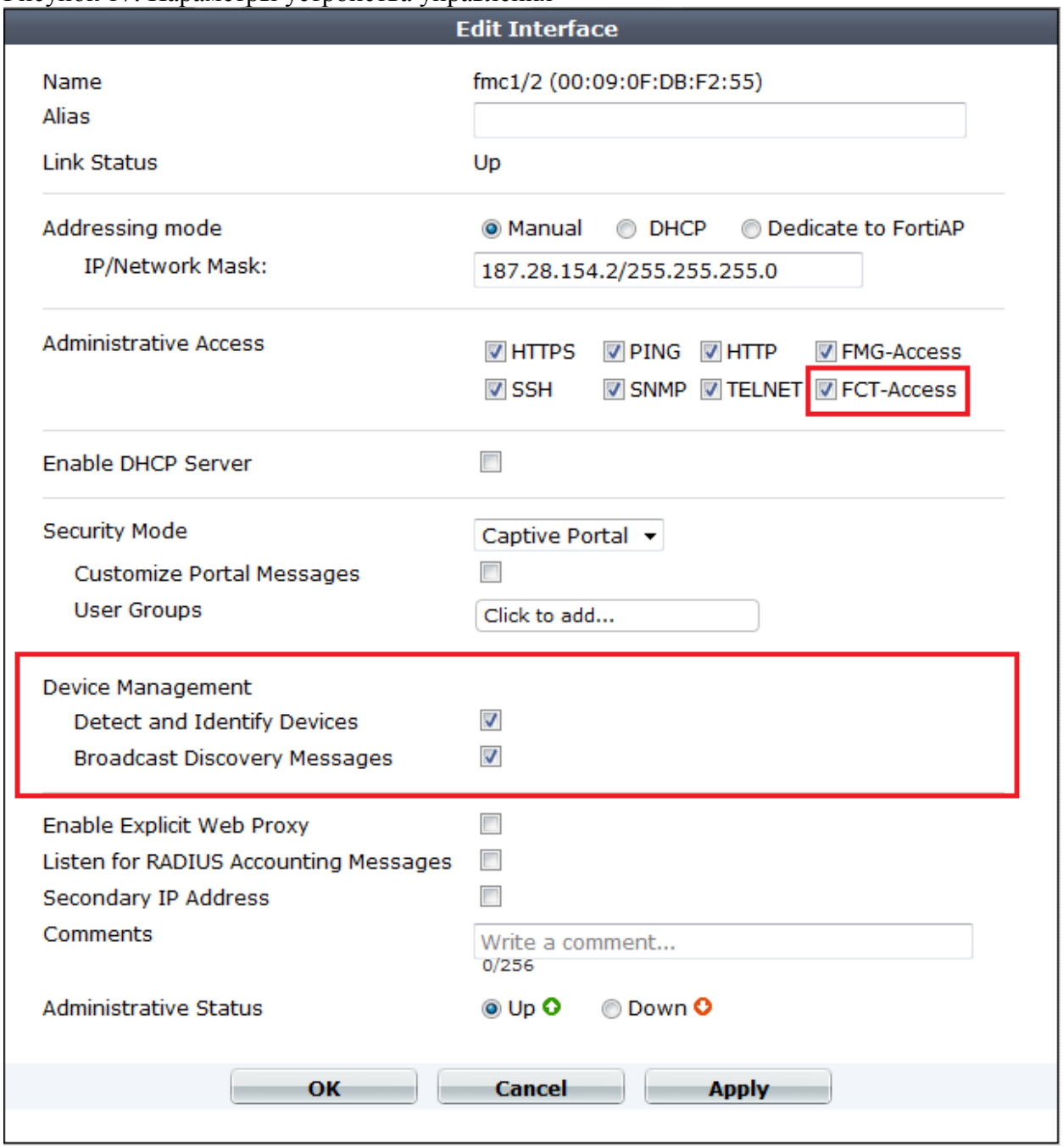
Целью этого раздела является предоставление базовой инструкции по настройки, развертывания и FortiClient управлять конфигурациями от FortiGate.
Настройка Управление конечными точками
В FortiOS v5.0, настройку и управление FortiClient агентов конечной точки теперь можно обрабатываются FortiGate. Можно настроить устройство FortiGate открыть для себя новые устройства сети, соблюдение FortiClient регистрации, и развернуть предварительно сконфигурированных конечной точке профиля подключенными устройствами. Конечная точка профиля могут быть развернуты на устройства в сети и более соединение VPN.
Чтобы настроить Управление конечными точками на FortiGate, выполните действия, перечисленные ниже.

Шаг 1: Включить управление устройствами и трансляция сообщений обнаружения

Для настройки устройства управления, выберите Система > Сетевой интерфейс>, выберите интерфейс, а выберите Правка на панели инструментов. На странице интерфейса редактирования можно по желанию включить обнаружение и идентификации устройств. Для включения трансляции сообщений обнаружения (опция) необходимо сначала включить FCT-Access под правами администратора. Нажмите кнопку Применить, чтобы сохранить настройки.
FortiOS Перевозчик GA v5.0.0 или более поздней версии.
Управление конечными точками доступно на FortiGate 40C и выше устройств.

Трансляция сообщений обнаружения является дополнительной конфигурации. При включении этой функции будет FortiGate рассылать сообщения компьютерной сети, позволяя клиентских подключений обнаружить FortiGate для FortiClient регистрации. Без эта функция включена, пользователь может ввести IP-адрес или адрес FortiGate для завершения регистрации.

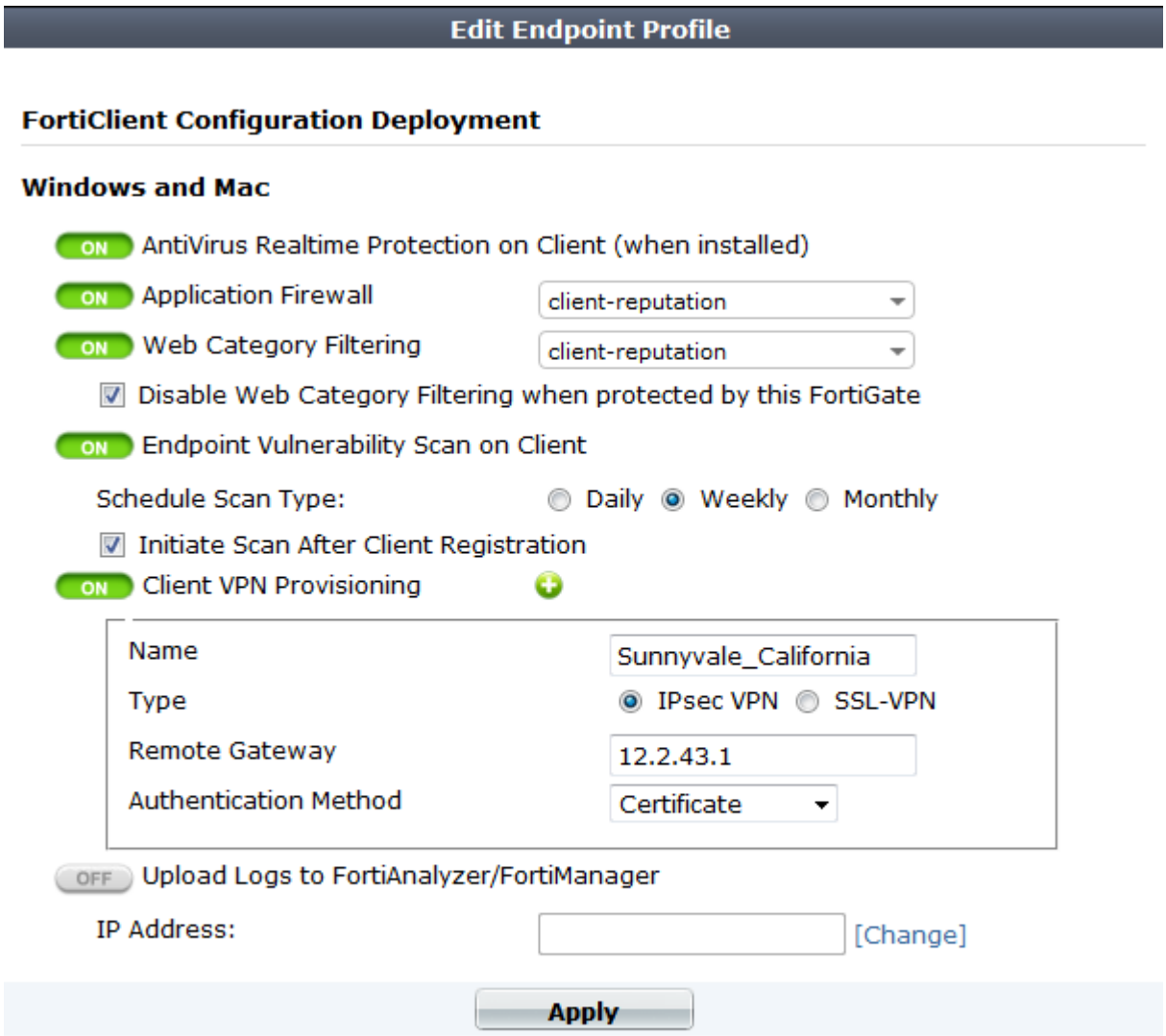
Рисунок 17: Параметры устройства управления



Шаг 2: Настройте клиентский профиль Endpoint

Чтобы настроить клиентский профиль Endpoint, Перейти к пользователю и устройства> Устройство> Endpoint профиля. Редактировать как требуется. Нажмите кнопку Применить, чтобы сохранить настройки.

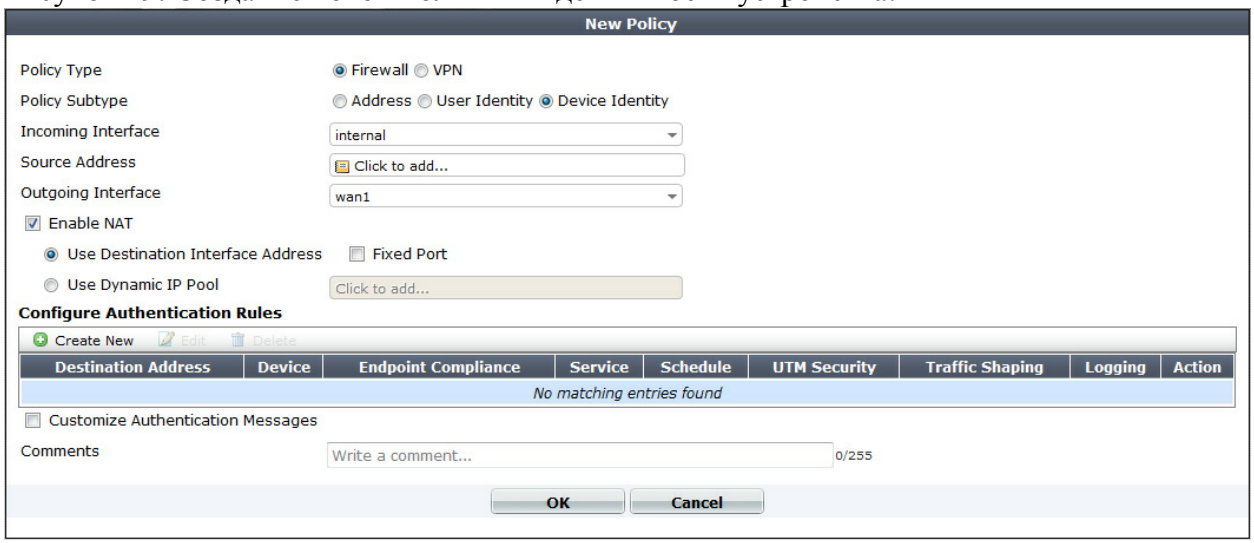
Рисунок 18: конечная точка Редактировать профиль.



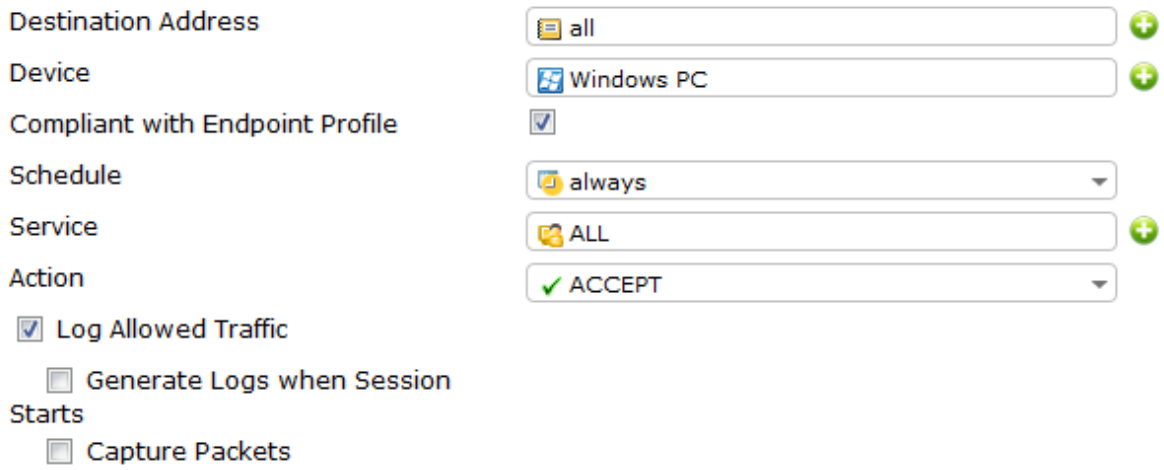
Шаг 3: Настройка политик брандмауэра

Чтобы настроить политику брандмауэра для Endpoint управления, перейдите в Политика > Политика. Политика > и выберите Создать новую на правой панели инструментов. Для политика Класс, выберите идентичность устройства.

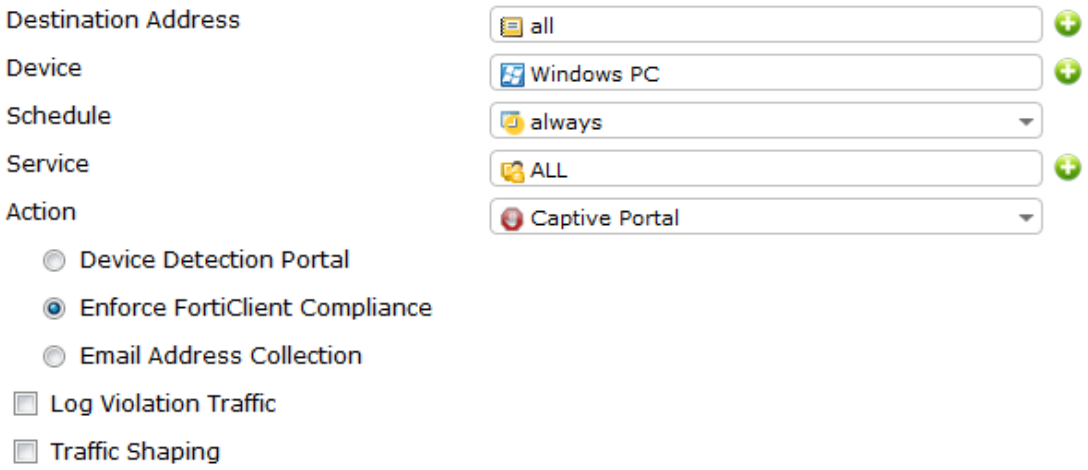
Рисунок 19: Создание новой политики идентичности устройства.



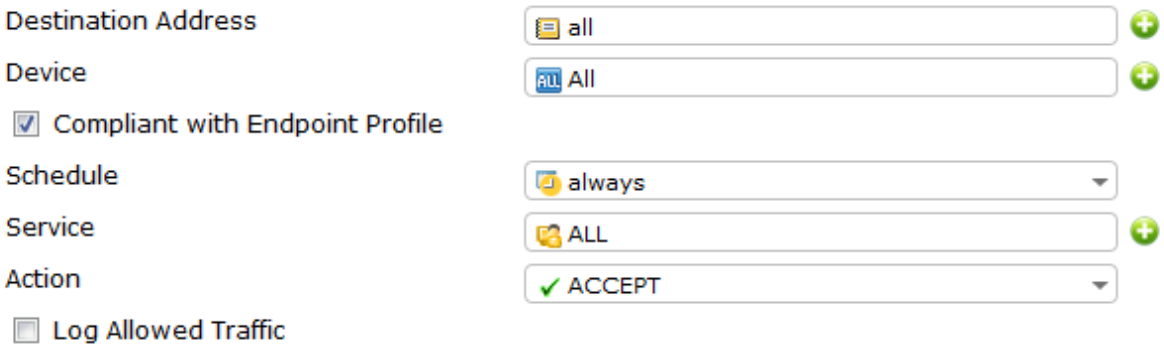
Добавить Примите аутентификации правило для всех совместимая с Windows-ПК-клиентов. Это правило позволит Windows, клиенты, которые установили FortiClient и быть зарегистрированными на данной FortiGate к передачи трафика.
Рисунок 20: принять правила для аутентификации совместимая с Windows-ПК-клиентов.



Добавить Captive Portal правила аутентификации для всех не-совместимая с Windows-ПК-клиентов. Это правило перенаправления всех клиентов Windows (через веб-браузер) на специальный портал, где они могут скачать. После регистрации в FortiGate, конечная точка профиля будет назначена.
Рисунок 21: Пленница правила аутентификации портал для Windows-PC устройств.

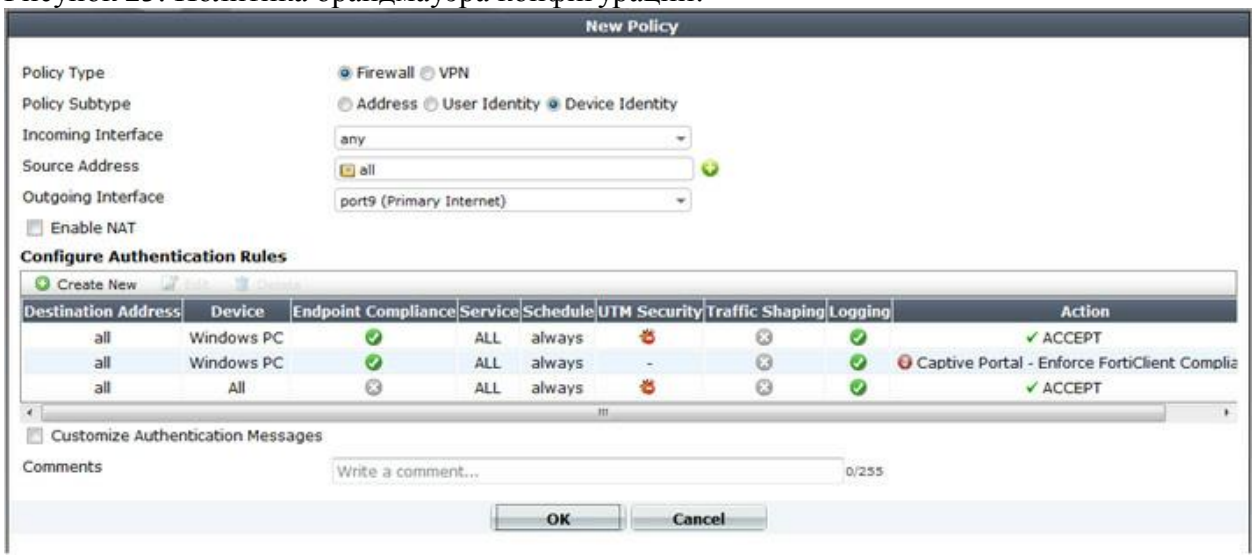


(Необязательно) Добавьте правило Accept аутентификации, чтобы разрешить трафик от всех других устройств для передачи трафика без соблюдения FortiClient соответствия.
Рисунок 22: Принять Правило проверки подлинности для всех других устройств.

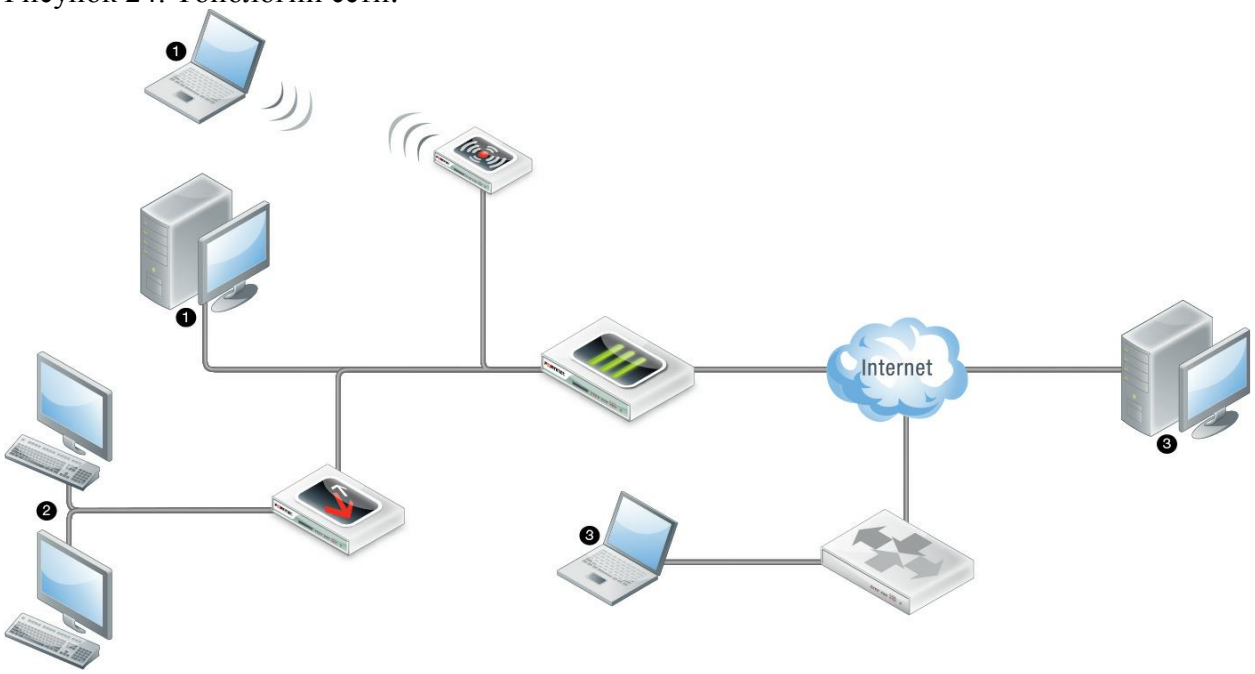


Как только эти три правила аутентификации настроен, выберите ОК, чтобы сохранить новые настройки политики.

Конфигурацию клиента готово к развертыванию.
Рисунок 23: Политика брандмауэра конфигурации.



После FortiGate конфигурация была завершена, вы можете приступить к FortiClient конфигурации. Настройте Windows PC в корпоративной сети со шлюзом по умолчанию установлены в IP из FortiGate.
FortiClient Endpoint топологии сети.
Следующий профиль FortiClient Endpoint топологий поддерживаются:
Клиент напрямую связано с FortiGate, либо к физическому порту, порту коммутатора или WiFi SSID.1
Эта топология регистрации клиента, настройка синхронизации и конечной точки профиля органов.
Клиент подключен к FortiGate, но находится за маршрутизатором NAT или device.2
Эта топология регистрации и настройки клиента синхронизации.
Клиент подключен к FortiGate через VPN connection.3
Эта топология регистрации клиента, настройка синхронизации и конечной точки профиля органов.
Рисунок 24: Топологии сети.



Чтобы настроить FortiClient Endpoint для управления, выполните действия, перечисленные ниже.

Шаг 1: Загрузите и установите FortiClient

Откройте веб-браузер на рабочей станции и попытка открыть веб-страницы, которая будет направлено на Captive Portal. Следуйте инструкциям на портале, чтобы загрузить и установить FortiClient.

Рисунок 25: Captive Portal блоке страницы отображается.

Endpoint Security Required

The use of this security policy requires that the latest FortiClient Endpoint Security software is working properly. Please make sure

- *FortiClient is installed and running,*
- *FortiClient is registered with FortiGate and currently in "online" status, and*
- *the "Disable configuration sync with FortiGate" option in FortiClient settings is turned off.*

Installing FortiClient requires that you have administrator privileges on your computer. If you do not, please contact your network administrator to have FortiClient installed.

The installer may be downloaded using the following link:
FortiClientInstaller-Windows-Enterprise-5.0.0.exe

Installation instructions:

- *For Internet Explorer:*
  1. Click the above link to download the installer
  2. When Internet Explorer asks what action you would like to take, click "Run"
- *For Firefox:*
  1. Click the above link to download the installer
  2. Save the installer and note the location it is saved to
  3. Open the folder containing the installer and run it

FortiClient installation may take a few minutes. Thank you for your patience.

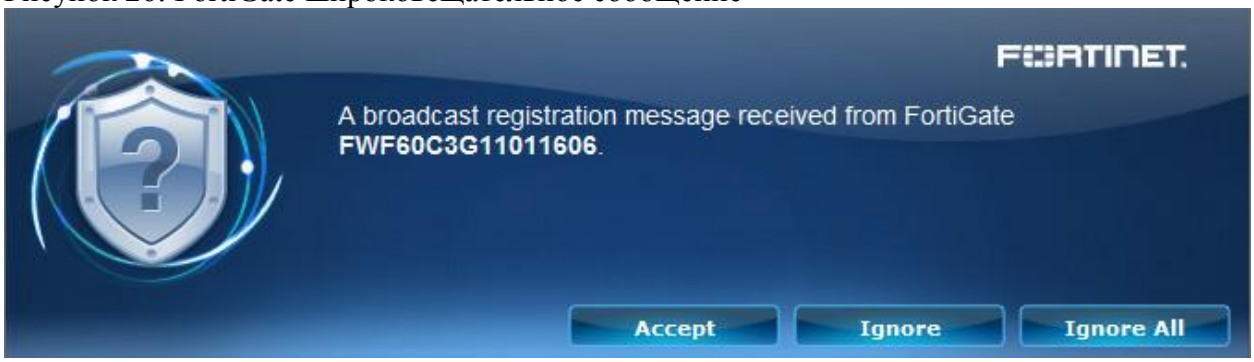
Шаг 2: FortiClient регистрации

После FortiClient завершает установку FortiClient запустится автоматически.
Устройство FortiGate для регистрации. Есть три способа, которыми FortiClient / FortiGate связи инициируется:

1. FortiClient подключается к предпочтительный IP-адрес (если имеется).
2. Если 1. не удается, FortiClient будет пытаться подключиться к IP-адрес шлюза по умолчанию.
3. Если 2. не удается, FortiClient будет ожидать FortiGate сообщений базовой станции.

На рисунке 26 показан пример сообщения вещания прислал FortiGate и полученных FortiClient. Выберите Принять, чтобы зарегистрироваться в этом устройстве FortiGate. После регистрации FortiGate назначен Endpoint профиль FortiClient.

Рисунок 26: FortiGate широковещательное сообщение



Шлюз по умолчанию вашего персонального компьютера IP должны быть настроены на IP Set
FortiGate интерфейс.

Рисунок 27 показывает поведение FortiClient на первоначальной настройке. FortiClient выполнит поиск доступных.

Устройства FortiGate для завершения регистрации. Выберите FortiGate значок на приборной панели, чтобы повторить поиск.

Рисунок 27: FortiClient будет искать доступные FortiGate.

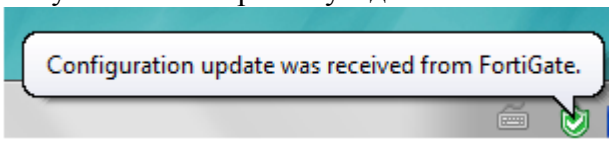
Если FortiClient не может обнаружить устройство FortiGate, введите IP-адрес или URL устройства и выберите кнопку Повторить, как показано на рисунке 28.
Рисунок 28: Введите FortiGate IP или URL

Когда FortiClient находит FortiGate, вам будет предложено подтвердить регистрацию в как показано на рисунке 29. Нажмите кнопку Подтвердить для завершения регистрации.
Рисунок 29: Подтверждение регистрации окна.

После успешной регистрации, FortiGate развернет конфигурации конечной точки.
Рисунок 30: Регистрация завершена.

Шаг 3: FortiGate развертывает Endpoint профиля FortiGate развернет Endpoint после завершения регистрации. Профиль позволит трафик через FortiGate. Значёк системном трее появится.

Рисунок 31: Настройка уведомлений об обновлениях сообщение.



FortiClient консоли будет отображаться, что она успешно зарегистрирован в FortiGate. Endpoint профиля устанавливается на FortiClient.

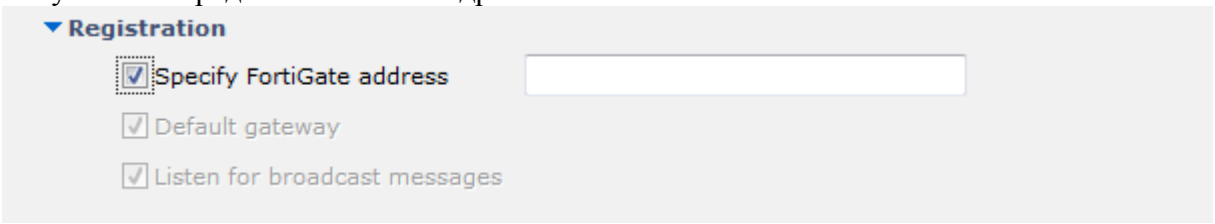
Рисунок 32: Зарегистрированные консоли FortiClient.

Развертывание Endpoint профиля с клиентами через VPN

Можно развернуть Endpoint профиль клиентам через соединение VPN.

1. На приборной панели FortiGate, выберите Настройки> File. При регистрации выберите Указать FortiGate-адрес и введите IP-адрес и номер порта (если необходимо) в FortiGate

Внутренний интерфейс.
Рисунок 33: Предпочтительный адрес FortiGate.

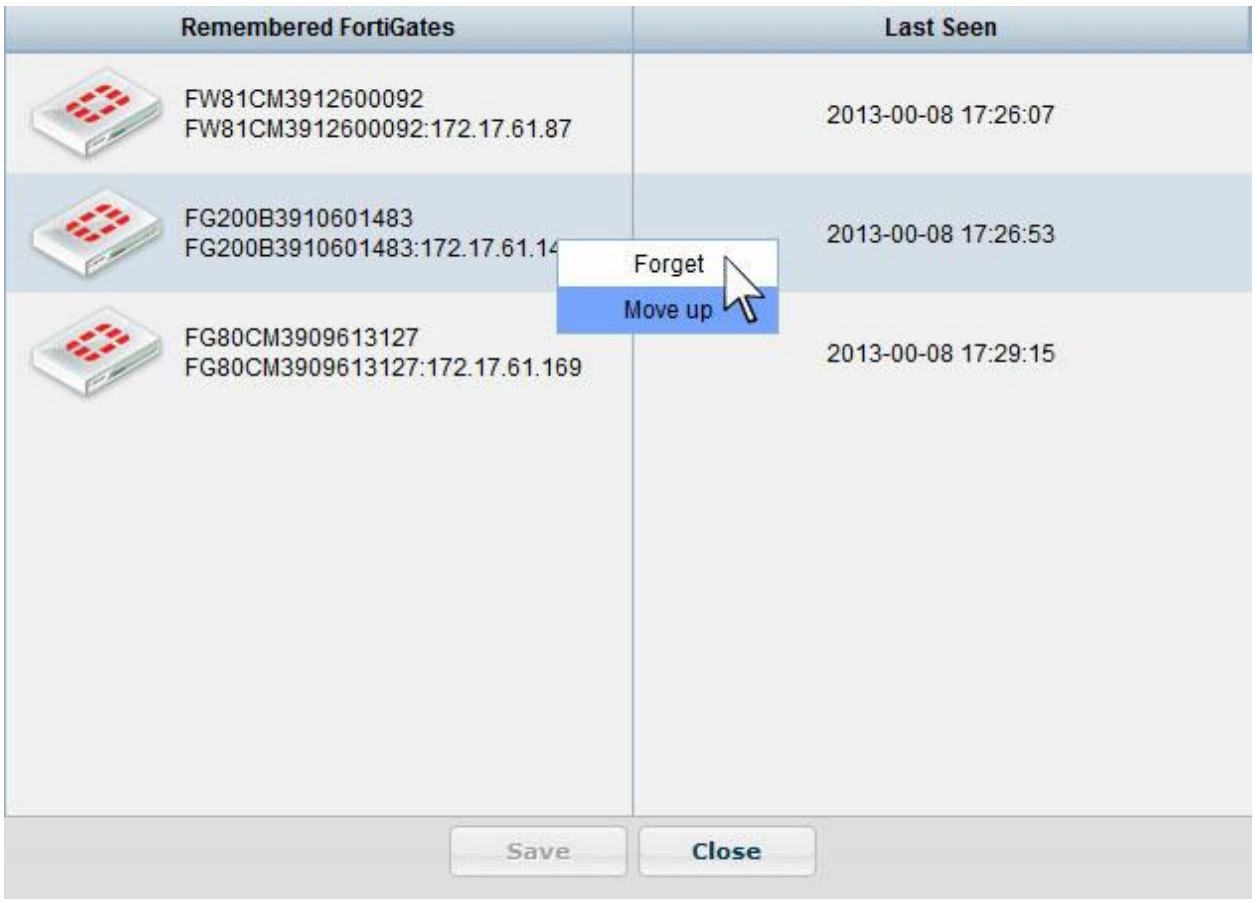


2. Настройка соединения IPsec VPN от FortiClient к управлению FortiGate. Для получения дополнительной информация о настройке IPsec VPN см. раздел «Создание нового IPsec VPN соединения".
3. Подключение к VPN.
4. Теперь вы можете искать для FortiGate шлюз. См. "Шаг 2: FortiClient регистрация" для получения дополнительной информации.
5. После регистрации, клиент имеет возможность получить Endpoint профиля.
Fortinet Технологии Инк
FortiClient v5.0 Патч Release 1 добавляет возможность помнить при принятии FortiGate транслироваться сообщение о регистрации.
Рисунок 34: Вариант помнить FortiGate.

Выберите значок Регистрация на приборной панели для просмотра информации о текущем зарегистрированных
устройства, включая имя компьютера, домен, серийный номер и IP-адреса.
Рисунок
35

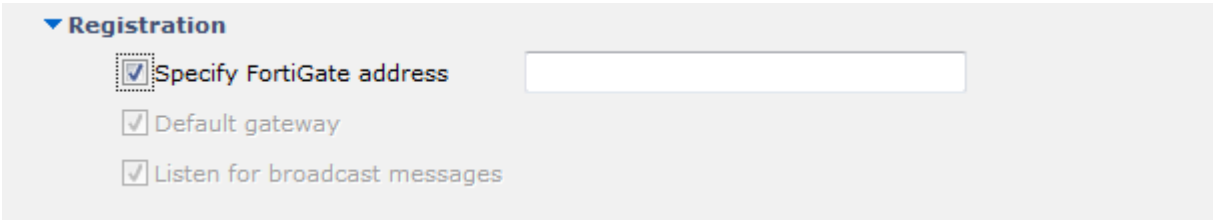
Эта функция будет улучшена в будущих выпусках патч, чтобы FortiClient для автоматического переключения между различными устройствами запоминающийся. Выберите список устройств FortiGate, что имеет FortiClient ранее зарегистрированных. Вы также можете изменить порядок устройств в этом списке с помощью контекстного меню.

Рисунок 36: Показать устройств.

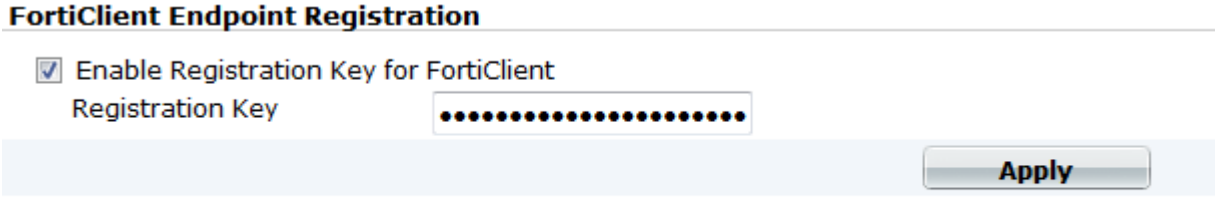


Посмотреть FortiClient регистрации на веб-FortiGate-администратора
Вы можете просмотреть все FortiClient зарегистрированных на FortiGate веб-администратора. В каждом новом регистрация будет автоматически добавляться в таблице устройств. Для просмотра зарегистрированных устройств Пользователь & Устройства > Устройство > определение устройства.
Рисунок 37: Устройство FortiGate.

Настроить IP предпочтительным FortiGate на FortiClient для регистрации
FortiClient пользователя администратор может указать предпочтительный FortiGate IP адрес для регистрации и управление конфигурации клиента. Когда незарегистрированной FortiClient запускается, он сначала ищет предпочтитаемым FortiGate. Если предпочтительный FortiGate недоступен, она будет выглядеть для подключения к шлюз по умолчанию. Если оба предпочтительным FortiGate и шлюз по умолчанию не доступны, FortiClient будет принимать широковещательное сообщение от FortiGate.
Чтобы настроить предпочтительный FortiGate IP адрес на FortiClient, перейдите в меню Файл > Настройки. Выбирать
Регистрация расширить выпадающее меню. Введите IP-адрес и номер порта (если требуется) внутреннего интерфейса FortiGate автора.
Рисунок 38: Настройка предпочтительного FortiGate на FortiClient



Включить FortiClient Endpoint регистрации (опционально)
Чтобы включить FortiClient Endpoint. Регистрация на FortiClient, выберите Система> Конфигурация> Дополнительно.
Выберите Включить ключ регистрации на FortiClient, ввести регистрационный ключ и выберите Применить.
Рисунок 39: Включить FortiClient Endpoint Регистрация на FortiGate.



FortiClient пользователю нужно будет ввести тот же регистрационный ключ для успешной регистрации FortiClient к FortiGate.

Антивирус

FortiClient Antivirus

FortiClient v5.0 включает в себя модуль антивирус для сканирования системных файлов, исполняемых файлов, DLL. FortiClient также поиска и удаления руткитов.
В этом разделе описывается, как включить антивирус и параметров конфигурации.

Включить / отключить антивирус

Чтобы включить или отключить FortiClient защита в реальном времени, переключите [Enable / Disable] в меню FortiClient приборной панели.

Уведомления

Выберите FortiClient приборной панели, чтобы просмотреть все уведомления. Когда вирус был обнаружен, восклицательный появится значок антивируса в дереве меню вкладки. Значок изменится с серого на желтый. Выберите Все, чтобы просмотреть все уведомления Antivirus события.
Рисунок 40: Уведомления окна.

Scan Now

Для выполнения сканирования по требованию антивируса, выберите кнопку Scan Now на FortiClient приборной панели. В раскрывающемся меню выбрать вариант Выборочная проверка, Полная проверка, Быстрая проверка.

Приборная панель отмечает дату последнего сканирования выше кнопки.

Выборочное сканирование работает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Выборочное сканирование позволяет выбрать определенную папку, файл на вашем локальном жестком диске (HDD) для сканирования на наличие угроз.

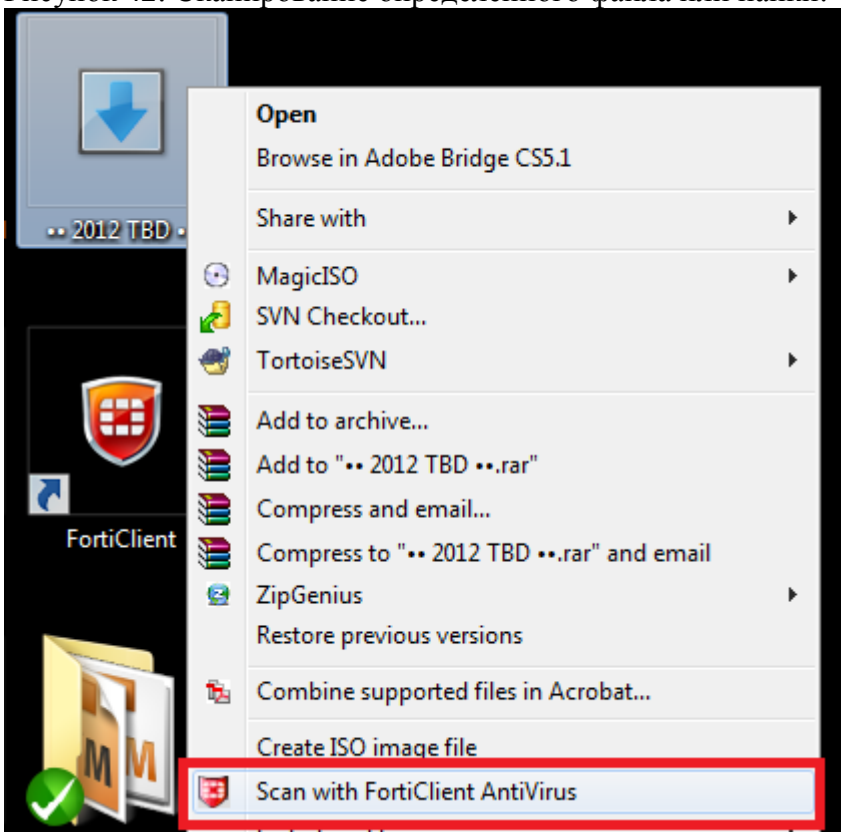
Полная проверка запускается двигатель обнаружения руткитов для обнаружения и удаления руткитов. Полное сканирование затем выполняет полную проверку системы, включая все файлы, исполняемые файлы, библиотеки DLL и драйверы для угроз.

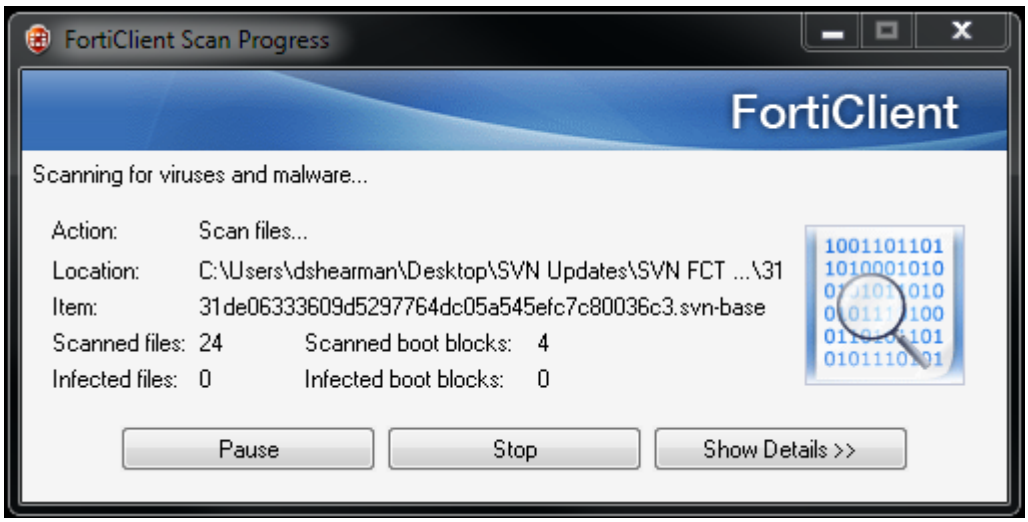
Быстрое сканирование системы запускает двигатель обнаружения руткитов для обнаружения и удаления руткитов.

Быстрое сканирования проверяет только исполняемые файлы, DLL, драйверы, которые в настоящее время работают на наличие угроз.

Рисунок 41: Антивирусный сканирующий варианты.

Проверить файл или папку.
Чтобы выполнить проверку на вирусы определенного файла или папки, щелкните правой кнопкой мыши файл которую необходимо поверить и нажмите Проверить.
Рисунок 42: Сканирование определенного файла или папки.



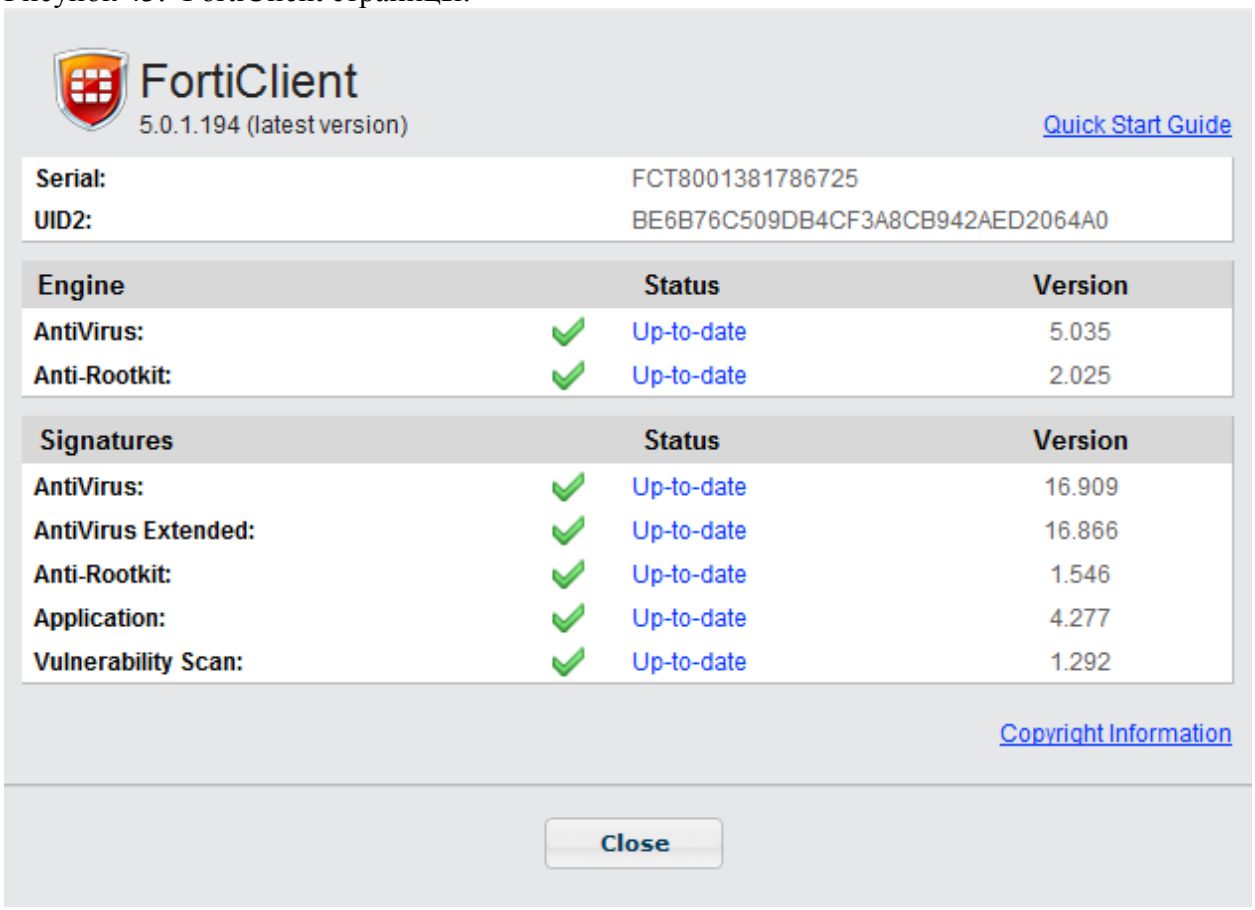


Обновить сейчас

Для выполнения по требованию обновление FortiClient версии, двигатели, а также подписи, выберите Обновить сейчас кнопку на панели содержимого. Содержание области заметок дате последнего обновления выше кнопки.

Для просмотра текущей версии FortiClient, двигатель, и подпись информацию, выберите Справка в панели инструментов на выпадающее меню.

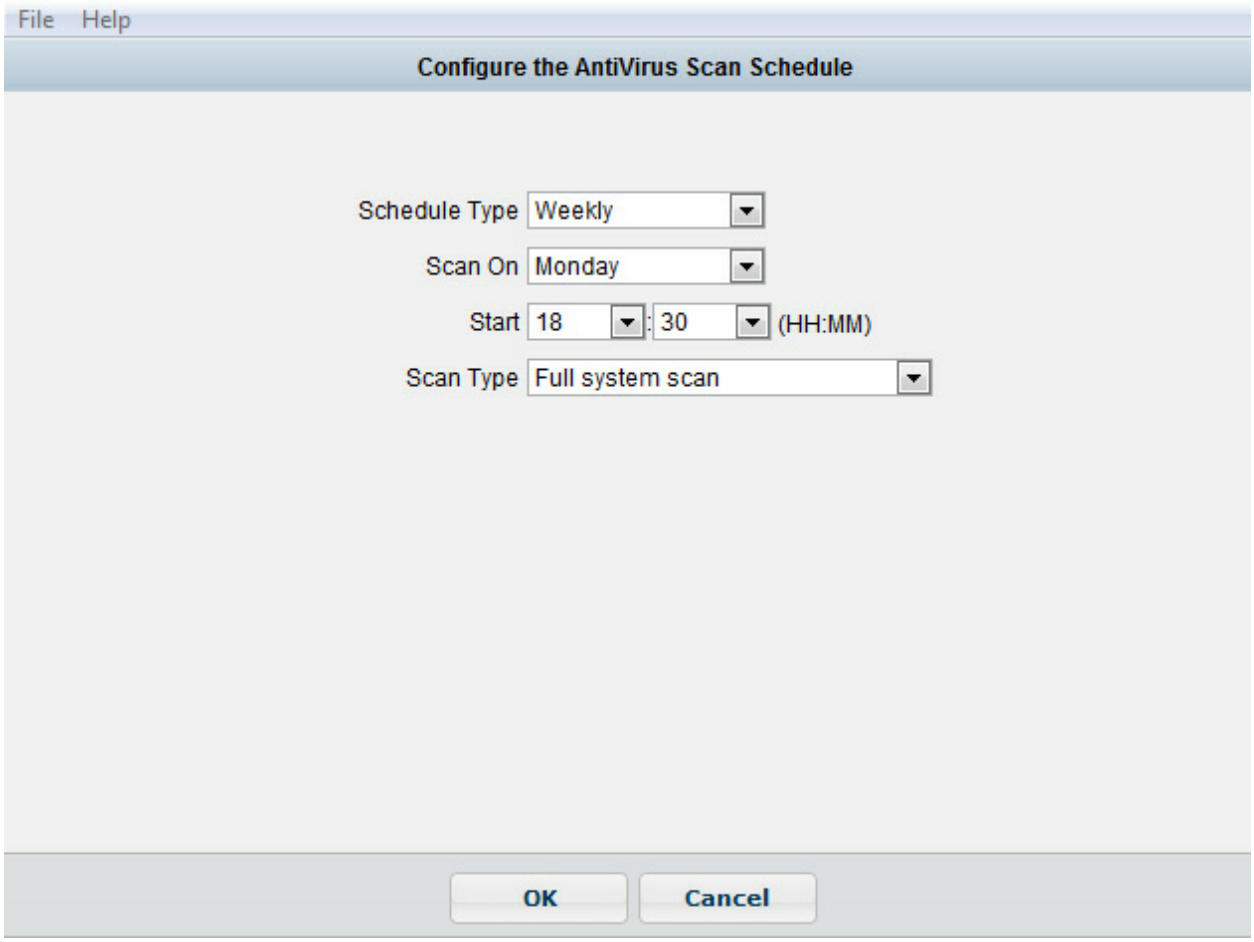
Рисунок 43: FortiClient страницы.



Расписание Антивирусная проверка

Чтобы запланировать антивирусное сканирование, выберите еженедельного осмотра на панели содержимого. В этом меню вы можете настроить параметры, описанные в

следующих рисунков и таблиц.
Рисунок 44: Antivirus планирования.



Тип расписания

Выберите ежедневно, еженедельно или ежемесячно в выпадающем меню.

Сканирование.

Для еженедельного сканирования по расписанию, выберите день недели на раскрывающегося меню. Ежемесячные проверки по расписанию, день месяца, на раскрывающегося меню.

Начало

Выберите время начала на выпадающее меню. Формат времени:
представлены в часах и минутах, 24-часовом формате.

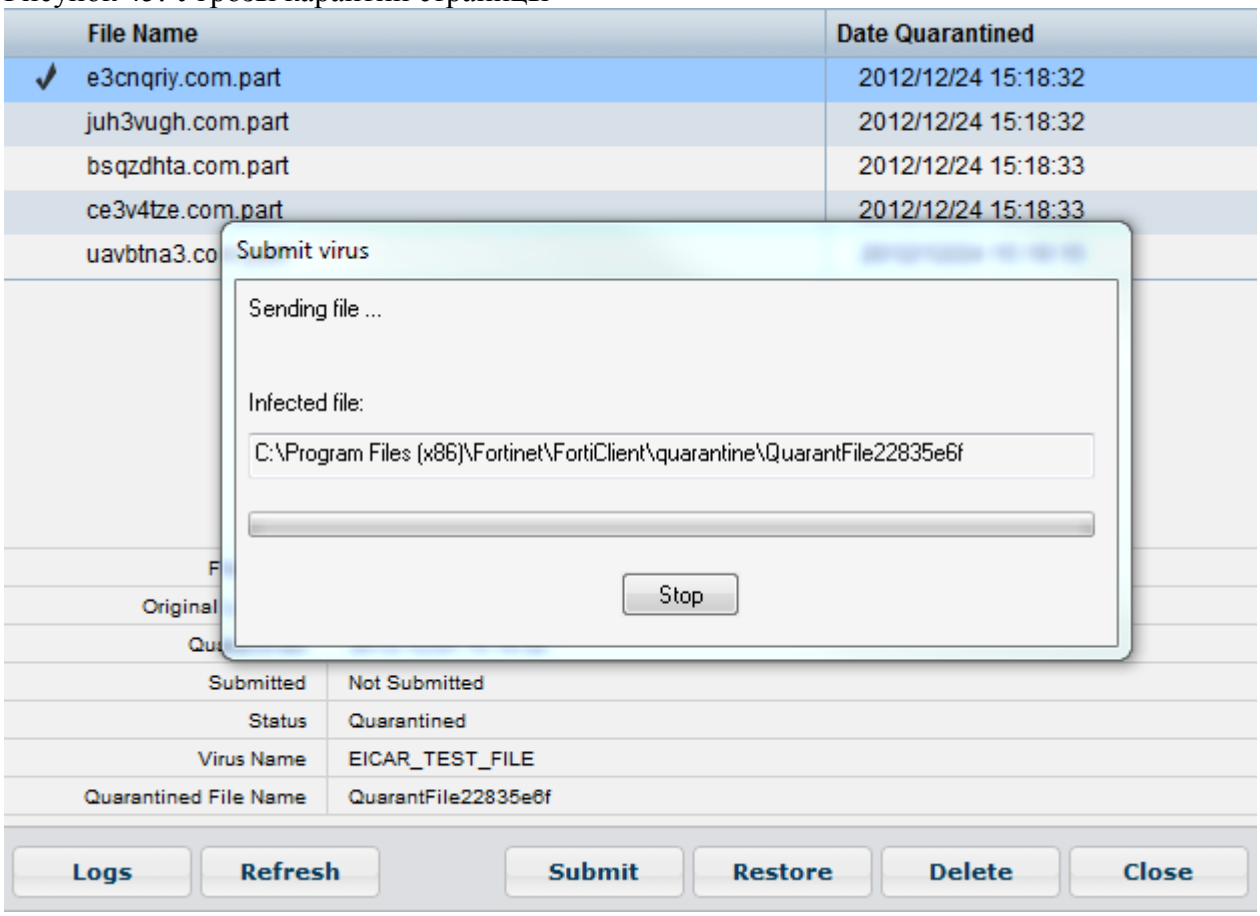
Тип сканирования

Выберите тип сканирования:
Выборочное сканирование работает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Выборочная проверка позволяет выбрать определенную папку файл на вашем локальном жестком диске (HDD) для сканирования на наличие угроз.
Полная проверка запускается двигатель обнаружения руткитов для обнаружения и удаления руткитов. Полная проверка выполняет полное сканирование системы, включая все файлы, исполняемые файлы, DLL, и драйверами для угроз.
Быстрое сканирование системы запускает двигатель обнаружения руткитов для обнаружения и удаления руткитов. Быстрое сканирование системы только проверяет исполняемые файлы, DLL, драйверы, которые в настоящее время работают на наличие угроз.

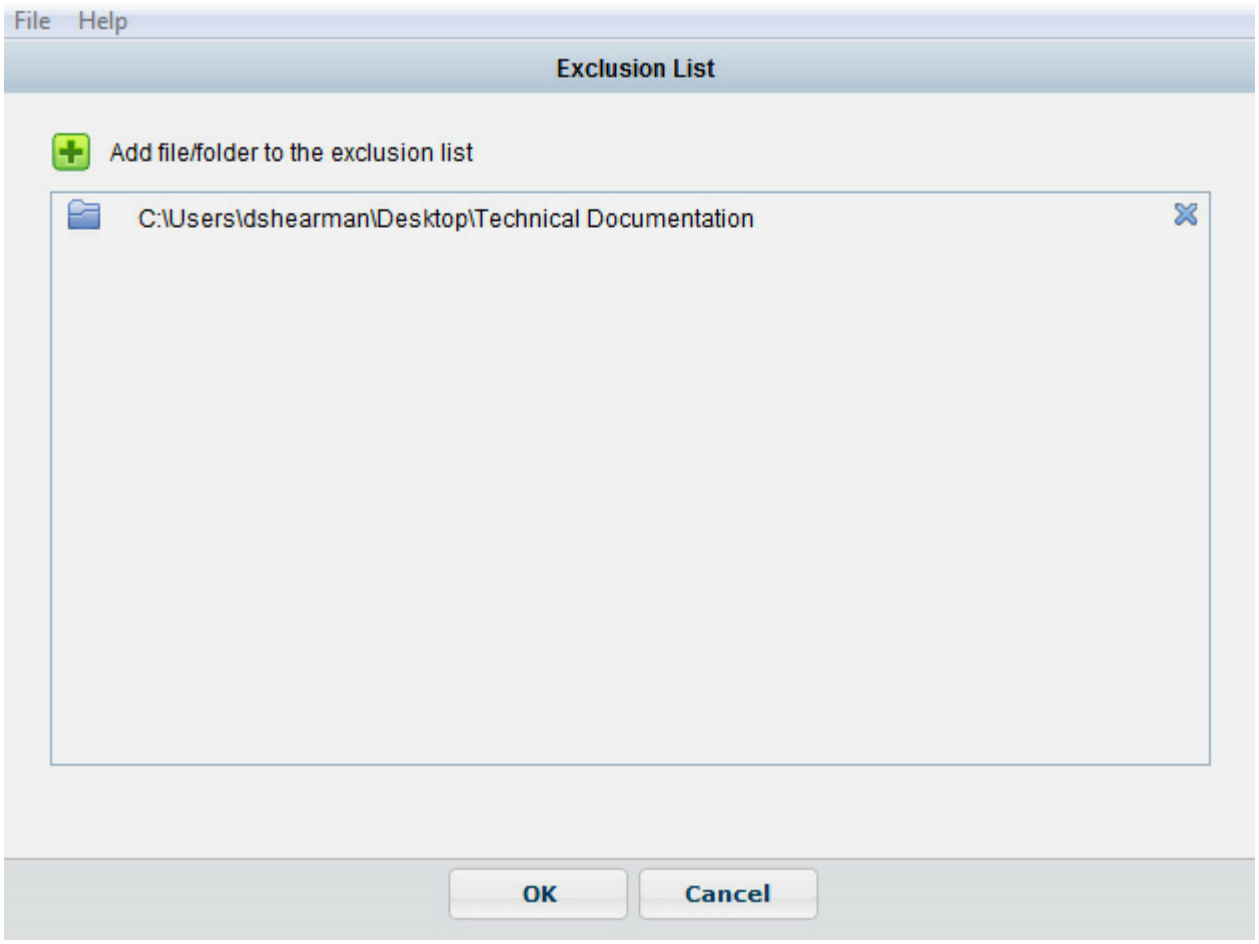
Посмотреть карантин угрозы

Для просмотра карантин угроз, выберите раздел Угрозы карантине на FortiClient приборной панели. На этой странице вы можете просмотреть, восстановить или удалить

файл из карантина. Вы также можете отправить файл в FortiGuard.
Рисунок 45: Угрозы карантин страницы



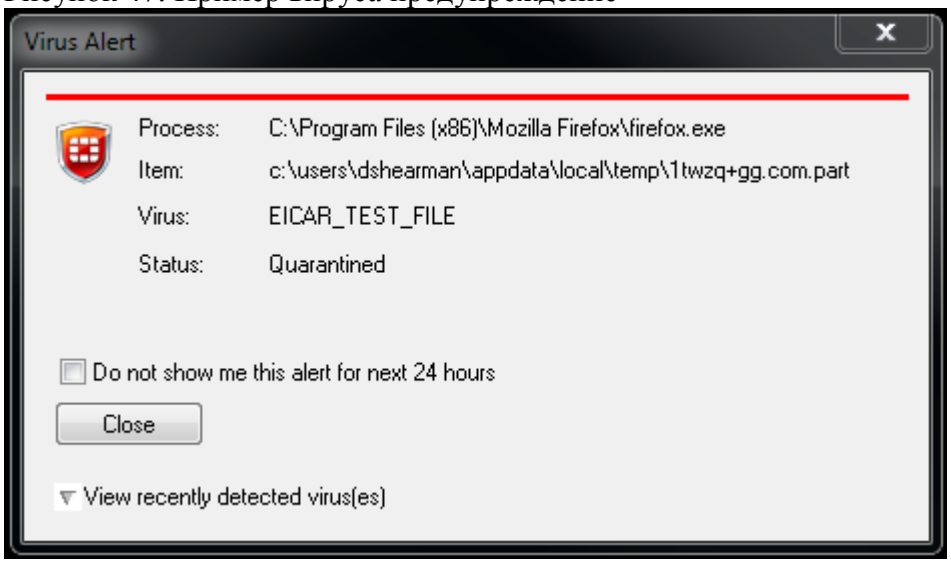
Имя файла.
Дату и время, когда файл был помещен на карантин FortiClient.
Информация о файле. Выберите файл из списка, чтобы просмотреть подробную информацию, включая карантин, статус, имя вируса и помещенных в карантин имя файла.
Журналы. Выберите для просмотра FortiClient данных журнала.
Обновление. Выберите, чтобы обновить список.
Представлять. Выберите представить файл на карантине FortiGuard.
Восстановление. Выберите, чтобы добавить выбранный файл / папку в список исключений.
Удалять. Выберите для удаления файла в карантине.
Близко. Выберите, чтобы закрыть страницу и вернуться к FortiClient приборной панели.
Для добавления файлов / папок в список исключений антивируса, выберите Список исключений на панели содержимого. На следующие страницы конфигурации, выберите символ '+', чтобы добавить файлы или папки в список. Любые файлы
или папки на этом список исключений не будет проверяться.
Рисунок 46: Список исключений антивируса



Antivirus предупреждение

Когда FortiClient антивирус обнаруживает вирус при попытке скачать файл через веб-браузер, Вы получите сообщение предупреждающий диалог как на рисунке 47. Перейдите в карантин угрозы на приборной панели, чтобы просмотреть сведения об обнаружении угрозы.

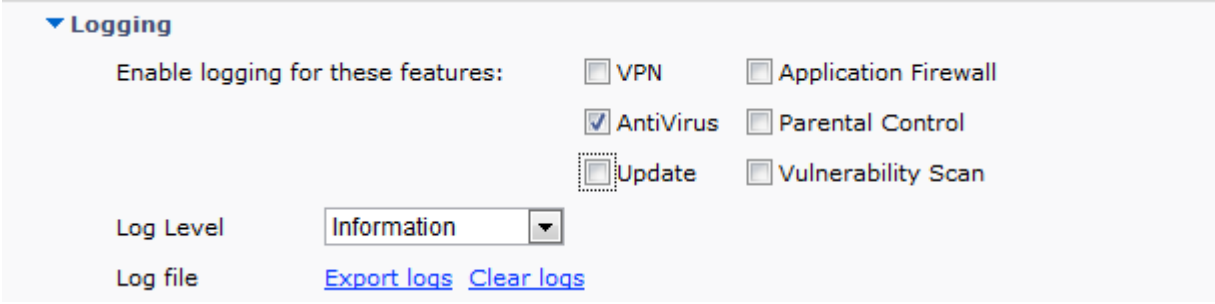
Рисунок 47: Пример вируса предупреждение



Antivirus регистрации

Чтобы настроить антивирусную лесозаготовки, выберите Файл на панели инструментов и настройки на выпадающее меню. Выберите вход, чтобы посмотреть в выпадающем меню.

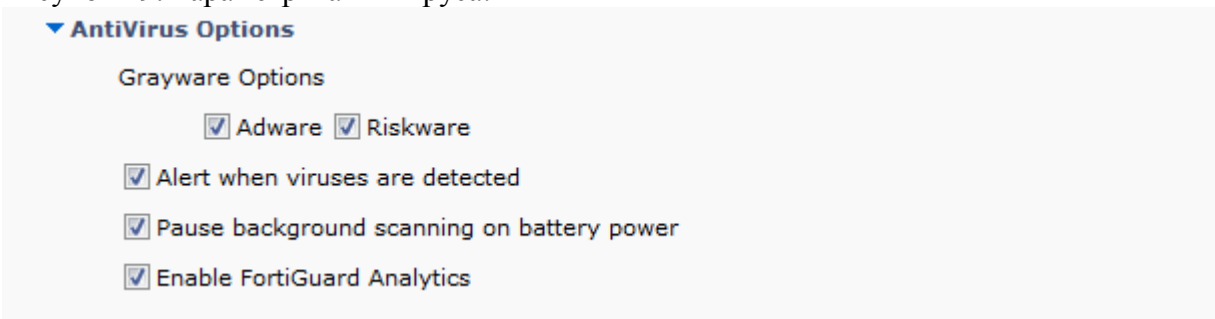
В этом меню вы можете настроить вариантов, изложенных на следующем рисунке.
Рисунок 48: Вход варианты.



Активируйте функцию ведения эти функции
Выберите антивирусную включить ведение журнала для этой функции.
Уровень Журнала
Выберите уровень регистрации:
Авария: система становится нестабильной.
Alert: требуются незамедлительные действия.
Критические: Функциональность влияет.
Ошибка: ошибка существует и функциональность может быть затронуто.
Предупреждение: функциональность может быть затронуто.
Примечание: Информация о нормальных событий.
Информация: Общие сведения о системе операций.
Debug: Debug FortiClient.
Лог-файл
Экспорт журналов. Выберите для экспорта журналов на локальном жестком диске (HDD)
Журнал формат.
Очистить журналы. Выберите, чтобы очистить все журналы. Вы увидите окно подтверждения, выберите Да, чтобы продолжить.

Параметры антивируса

Чтобы настроить параметры антивируса, выберите Файл на панели инструментов, и настройки на выпадающее меню. Выберите параметры антивируса, чтобы посмотреть в выпадающем меню. В этом меню вы можете настроить параметры изложенным в следующих рисунков и таблиц.
Рисунок 49: параметры антивируса.



Параметры антивируса

Опции нежелательных программ
Нежелательных программ это зонтичный термин применяется к широкому кругу Вредоносные программы, такие как шпионское, рекламное ПО и ключевые лесорубов, которые часто тайно установленных на компьютере пользователя, чтобы отслеживать и / или сообщать определенную информацию обратно на внешнее источника без разрешения пользователя или знаний.
Выберите, чтобы включить обнаружение рекламного и карантина в течение антивирусное сканирование.

Потенциально опасные программы. Выберите, чтобы включить обнаружение потенциально опасных программ в течение антивирусное сканирование.
Сигнал тревога когда вирусы обнаружены.
Выберите для FortiClient направлять уведомление, когда
обнаружении угрозы на вашем персональном компьютере.

Пауза фоне сканирования от батареи.

Выберите, чтобы приостановить фоновое сканирование, когда ваши личные компьютер работает от батареи.
Включить FortiGuard Analytics Выберите для автоматической отправки подозрительных файлов в FortiGuard

FortiClient Родительский контроль / веб-фильтрации

Родительский контроль / Веб-фильтрация позволяет блокировать, позволяют, предупреждают и мониторинга веб-трафика на основе URL на категорию. URL категоризации обрабатывается FortiGuard Сети.
Включить / отключить Родительский контроль / веб-фильтрации
Чтобы включить или отключить Родительский контроль FortiClient / Веб-фильтрация, переключите [Enable / Disable]
кнопки на приборной панели FortiClient. Родительский контроль включен по умолчанию.
Рисунок 50: модуль Родительский контроль.

Когда FortiClient зарегистрирован в FortiGate, модуль Родительский контроль будет отражать веб- фильтрация. Вы можете отключить веб-фильтрации на FortiClient от FortiGate. Устройство находится за FortiGate, клиентское устройство будет использовать Web Filter профиль на FortiGate.

Включить / Выключить

Переключите для включения или отключения функции родительского контроля.

Настройки.

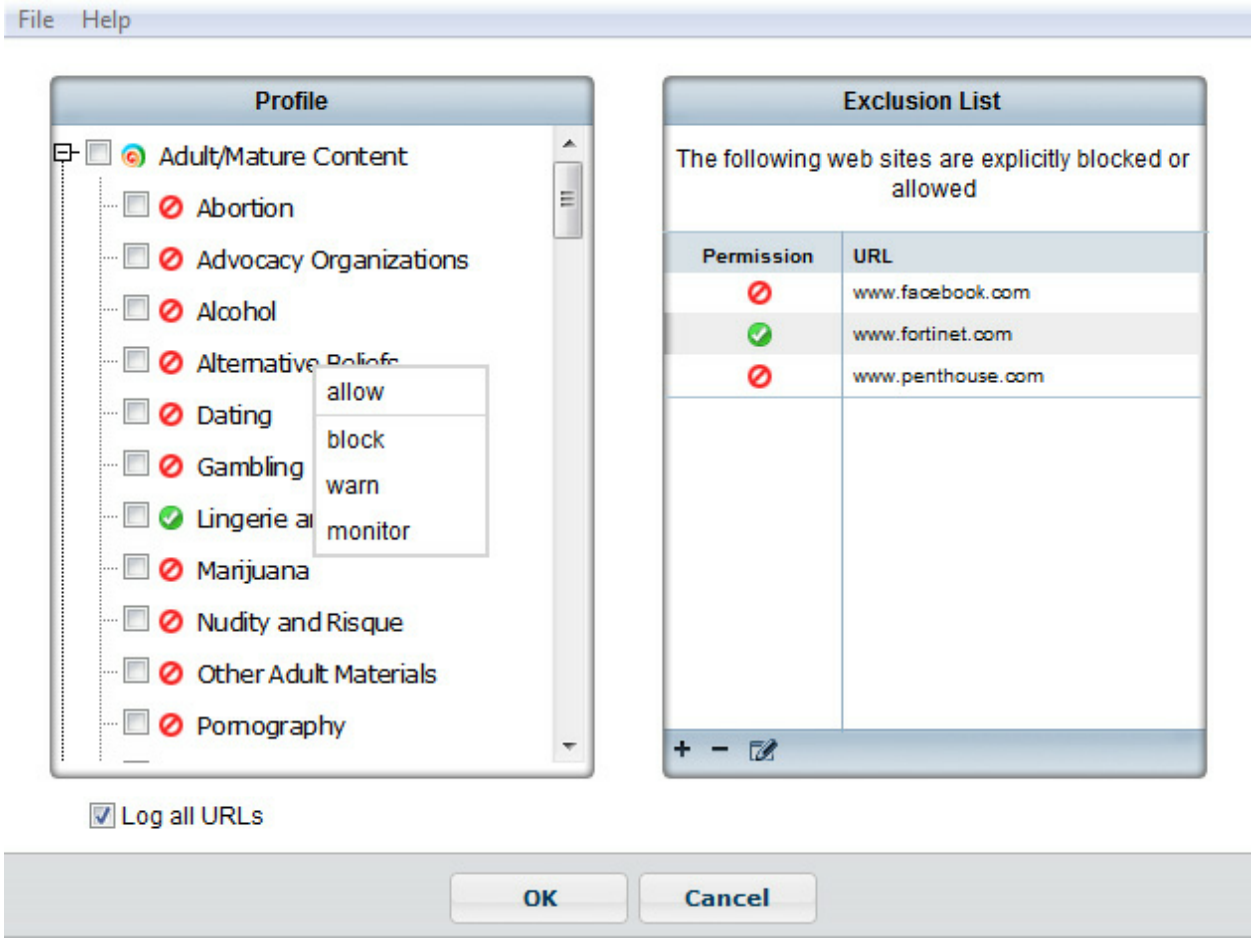
Выберите вариант настройки профиля Родительского контроля.

Родительский контроль / Web параметров фильтрации

Вы можете настроить профиль разрешать, блокировать, предупредить или мониторинга веб-трафика на основе категории Профиль. Используйте меню правой кнопкой мыши, чтобы установить меры для полного категорию или подкатегорию.

Вы можете добавлять сайты в список исключений и установить разрешение, разрешить или запретить. Если сайт является частью заблокированного категории, позволяющие разрешение в списке исключений позволит
пользователю получить доступ к конкретным URL.

Рисунок 51: Профиль и список исключений.



Посмотреть профиль нарушений

Для просмотра профиля нарушений, выберите правонарушениях (в течение последних 7 дней) на FortiClient приборной панели.

Рисунок 52: Нарушения правил дорожного движения.

Website	Category	Time	User
ffupdate.conduit-services.com	Malicious Websites	25/10/2012 9:53:37 AM	dshearman

Application Firewall

FortiClient Применение межсетевого экрана

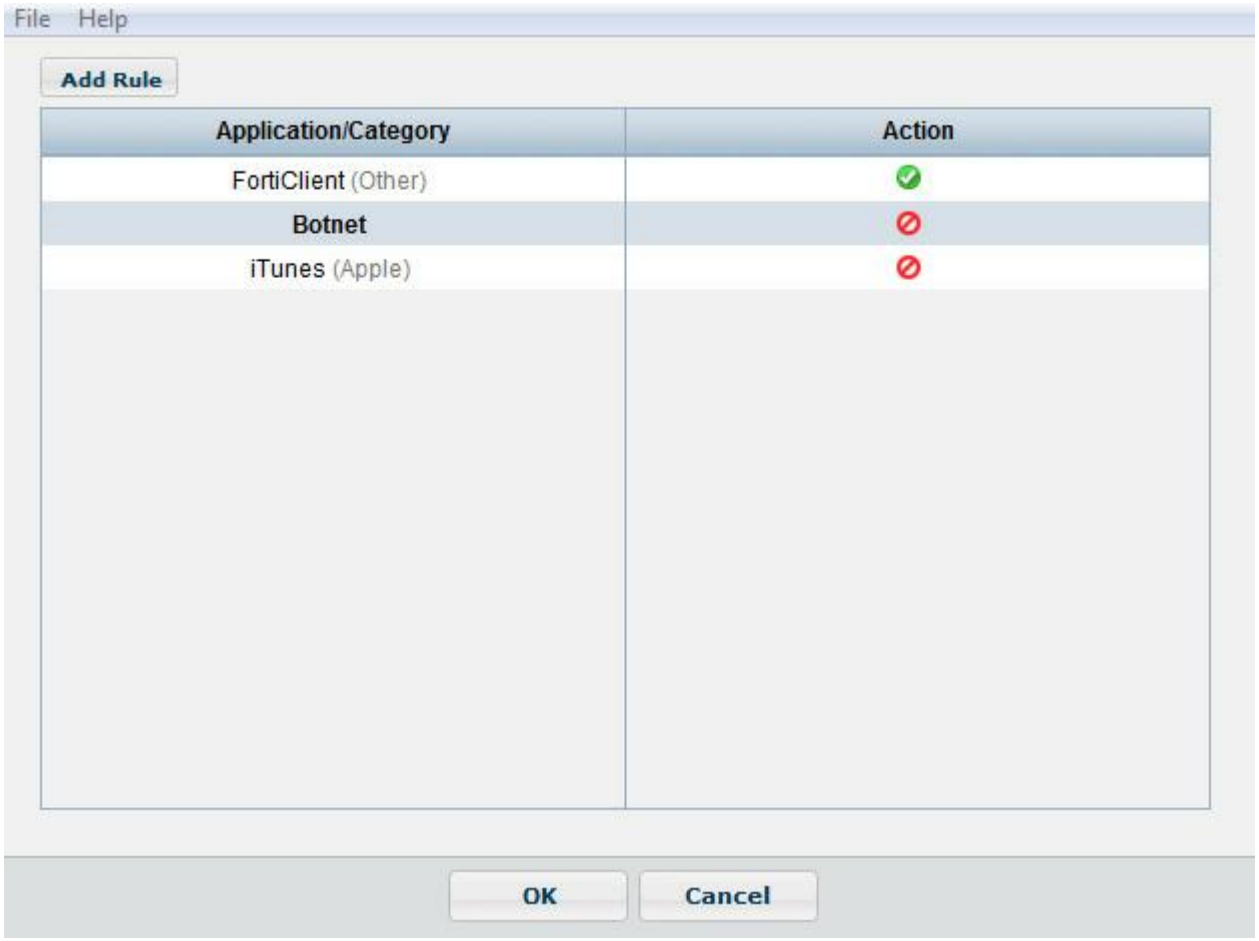
FortiClient v5.0 может распознавать трафик, генерируемый большое количество приложений. Вы можете создавать правила для блокировки или разрешения этого трафика в каждой категории, или приложение.
В этом разделе описывается, как включить настройки Application Firewall.
Включение / выключение Application Firewall
Чтобы включить или отключить FortiClient защита в реальном времени, выберите [Enable / Disable] на пульте FortiClient приборной панели.
Рисунок 53: Модуль Application Firewall.

Посмотреть Блокировка приложений

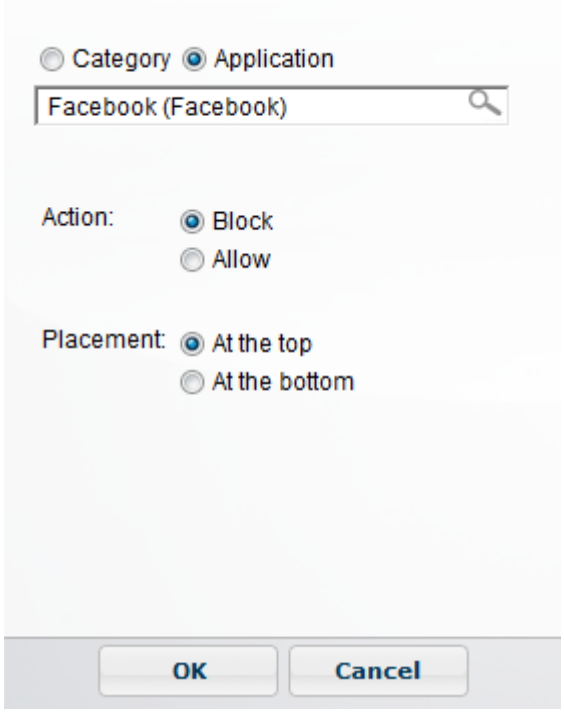
Для просмотра блокированных приложений, выберите Блокировка приложений на приборной панели FortiClient странице перечислены все приложения заблокированы в последние семь дней, в том числе количество и время последнего запуска.

Правила Application Firewall

Для просмотра правил Application Firewall, выберите Настройки на FortiClient приборной панели.
Рисунок 54: Правила Application Firewall.

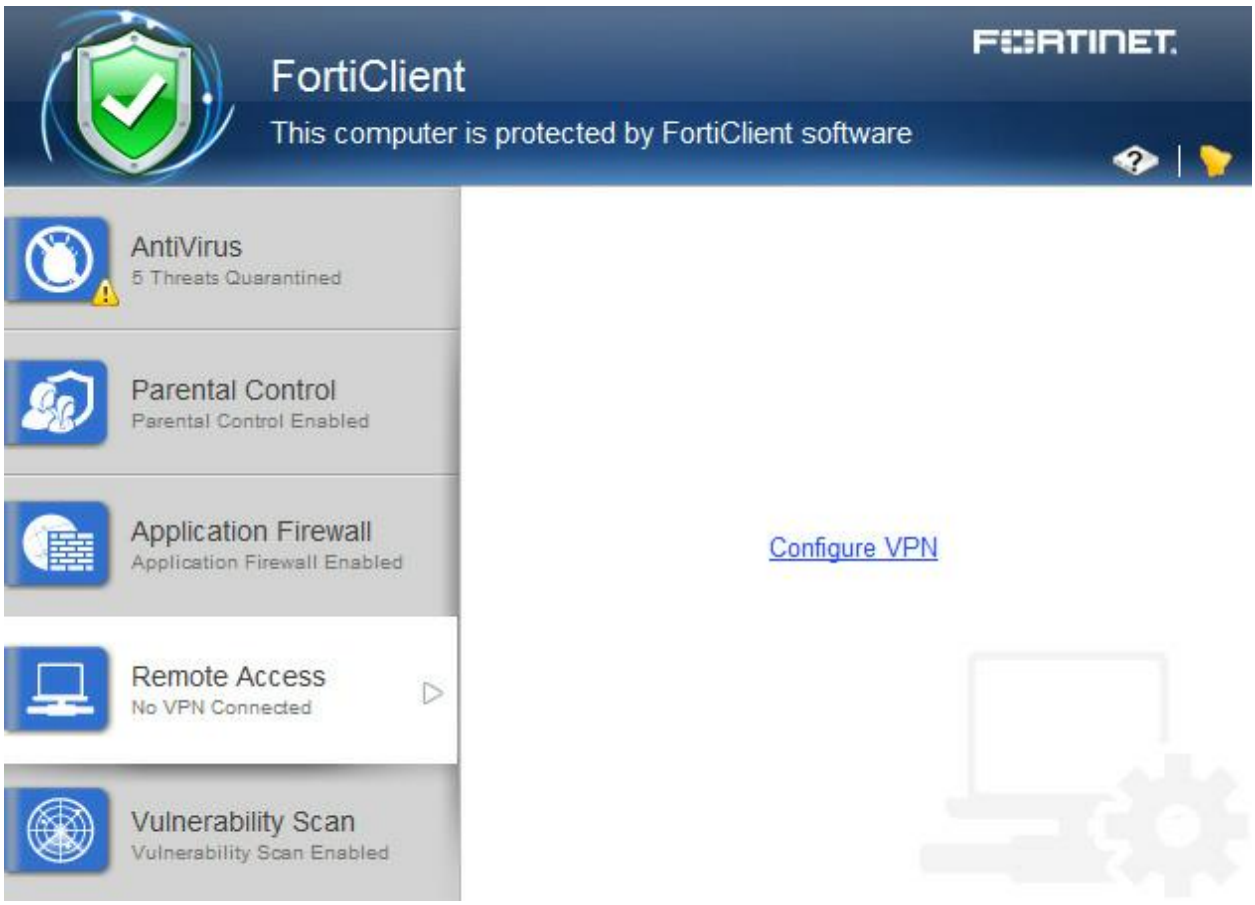


Чтобы добавить новое правило
1. Нажмите кнопку Добавить правило.
Рисунок 55: Окно добавления правила.



2. Выберите любой из этих категорий или приложения. Для категории, используйте выпадающий список для выбора категории. Для приложений, типа поставьте полное имя

приложения или первую букву для поиска.
Все приложения, начиная с выбранного письма.
3. Выберите действие, блокировать или разрешать категорию или приложения.
4. Выберите размещение правило в верхней или в нижней части.
5. Нажмите OK, чтобы сохранить настройки.
Чтобы изменить правило
1. На странице настроек, при наведении курсора мыши на правило, скрытое меню значок доступны.
2. Выберите значок редактирования, чтобы изменить действие для правила.
3. Выберите значок удаления, чтобы удалить правило.
4. Выберите значок перемещения и перетащите и падение правило в новое положение в списке.
5. Нажмите OK для сохранения настроек и возврата в FortiClient приборной панели.
Logging Application Firewall
Для настройки ведения журнала Application Firewall, выберите Файл на панели инструментов, и настройки на раскрывающегося меню. Выберите вход, чтобы посмотреть в выпадающем меню. Выберите Application Firewall вход меню позволяет включить ведение журнала для этого модуля.
FortiClient Firewall приложение может блокировать приложения, для которых имеет FortiGuard
Приложение подпись. Вы можете отправить запрос на добавление приложений на подпись FortiGuard сайта.
IPsec VPN и SSL-VPN
FortiClient удаленного доступа (VPN)
FortiClient v5.0 поддерживает как IPsec и SSL VPN-подключения к сети для удаленного доступа.
В этом разделе описывается, как настроить удаленный доступ.
Добавить новое подключение
Выберите пункт Настройка VPN на приборной панели, чтобы FortiClient добавления новой конфигурации VPN.
Рисунок 56: Настройка нового подключения VPN.



Создайте новый SSL-VPN соединение

Для создания нового SSL-VPN соединение, выберите Настройка VPN или использовать выпадающее меню на приборной панели. В этом меню вы можете настроить параметры, описанные в следующих рисунков и таблиц.

Рисунок 57: SSL-VPN параметры конфигурации.

Имя соединения
Введите имя для соединения.
Тип
Выберите SSL-VPN.
Описание
Введите описание для соединения. (Опционально)
Шлюз удаленных
Введите IP адрес / имя хоста удаленного шлюза. Несколько удаленных
Шлюзы могут быть настроены, разделяя записи точкой с запятой.
Если шлюз не доступен, VPN будут подключаться к следующему
настроить шлюз.
Порт
Выберите для изменения порта. По умолчанию используется порт 443.
Идентификация
Выберите для ввода при входе в систему, или запомнить.
Имя пользователя
Если вы выбрали для сохранения входа, введите имя пользователя в диалоговом окне.
Сертификат клиента
Выберите, чтобы включить клиентские сертификаты.
Сертификат
Выберите сертификат опцию выпадающего меню.
Не предупреждать Неверный
Сертификат сервера
Выберите, если вы не хотите, чтобы предупредил, что если сервер представляет
недействительным
сертификат.

Создайте новый IPsec VPN соединения
Для создания нового IPsec VPN соединение, выберите Настройка VPN или использовать выпадающее меню на GUI. В этом меню вы можете настроить параметры, описанные в следующих рисунков и таблиц.
Рисунок 58: IPsec VPN параметров конфигурации.

Имя соединения
Введите имя для соединения.
Тип
Выберите IPsec VPN.
Описание
Введите описание для соединения. (Опционально)
Шлюз удаленных
Введите IP адрес / имя хоста удаленного шлюза. Несколько удаленных
Шлюзы могут быть настроены, разделяя записи точкой с запятой.
Если шлюз не доступен, VPN будут подключаться к следующему
настроить шлюз.
Идентификация
Метод
Выберите либо сертификатов X.509 или общий ключ на раскрывающийся меню.
Сертификат X.509,
Предварительный ключ
Выберите Сертификат X.509 на выпадающее меню, или введите предварительный ключ в диалоговом окне. См. сертификат управления для информация о настройке Параметры сертификата.
Идентификация
(XAuth)

Выберите для ввода при входе в систему, запомнить, или отключить.
Имя пользователя
Если вы выбрали Сохранить логин, введите имя пользователя в диалоговом окне.
Подключение к VPN
Для подключения к VPN, выберите имя VPN из выпадающего меню. Введите имя пользователя, пароль и выберите кнопку Подключить.
Рисунок 59: Варианты подключения.

Вы можете также выбрать параметры для существующего соединения VPN и удалить существующее соединение VPN с помощью выпадающего меню.
При подключении, приборная панель будет отображать состояние подключения, продолжительность и другие соответствующие информации. Теперь вы можете просматривать ваши отдаленные сети. Выберите кнопку Отключить, когда вы готовы завершить сеанс VPN.
Рисунок 60: SSL-VPN соединение, установленное.

Расширенные функции (Windows)
Соединение VPN перед входом в систему (AD средах)
VPN <options> тег содержит глобальную информацию управления VPN государств. VPN будет подключения, а затем вход в систему к AD / домен.
<forticlient_configuration>
<vpn>
<options>
<show_vpn_before_logon> 1 </ show_vpn_before_logon>
<use_windows_credentials> 1 </ use_windows_credentials>
</ Функции>
</ VPN>
</ Forticlient_configuration>
Статус
Состояние соединения VPN.
Продолжительность
Продолжительность соединения VPN.
Получено байт
Байт получено через соединение VPN.
Отправлено байт
Байты, посланные через соединение VPN.
Fortinet Технологии Инк
Создания избыточного IPsec VPN
Для использования VPN отказоустойчивости / резервирования, вы будете настроить список серверов FortiGate IP / FQDN,
вместо одного:
<forticlient_configuration>
<vpn>

<ipsecvpn>
<options>
...
</ Функции>
<connections>
<connection>
<name> psk_90_1 </ Name>
<type> руководства </ Type>
<ike_settings>
<prompt_certificate> 0 </ prompt_certificate>
<server> 10.10.90.1; ipsecdemo.fortinet.com; 172.17.61
0,143 </ сервер>
<redundantsortmethod> 1 </ redundantsortmethod>
...
</ Ike_settings>
</ Связь>
</ Подключения>
</ Ipsecvpn>
</ VPN>
</ Forticlient_configuration>

Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги включены, но некоторые важные элементы для завершения конфигурации IPsec VPN, опущены.

RedundantSortMethod = 1

Этот тег XML устанавливает соединение IPsec VPN, как пинг-ответ, основанный. VPN будут подключаться к FortiGate который отвечает самым быстрым.

RedundantSortMethod = 0

По умолчанию RedundantSortMethod = 0, и соединение IPsec VPN является приоритет, основанный. Приоритет конфигурации на основе будет пытаться подключиться к FortiGate начиная с первой в списке.

Приоритет, основанный SSL-VPN соединений

SSL-VPN поддерживает конфигурации на основе приоритета для избыточности.

<forticlient_configuration>
<vpn>
<sslvpn>
<options>
<enabled> 1 </ включен>
...
</ Функции>
<connections>
<connection>

<name> ssl_90_1 </ Name>
<server> 10.10.90.1; ssldemo.fortinet.com; 172.17.61.143:44
3 </ сервер>
...
</ Связь>
</ Подключения>
</ SSLVPN>
</ VPN>

</ Forticlient_configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги включены, но некоторые важные элементы для завершения SSL VPN конфигурации, опущены. Для SSL-VPN, все FortiGates должны использовать тот же порт TCP.
Включение VPN автосоединения
VPN Auto Connect использует следующие XML тег:
<autoconnect_tunnel> ipsecdemo.fortinet.com </ autoconnect_tunnel>
Внутри:
<vpn>
<options>
Запомнить пароль также необходимо, потому что это автосоединения:
<save_password> 1 </ save_password>
Включение VPN всегда VPN всегда используются следующие XML тег:
<keep_running> 1 </ keep_running>
Внутри:
<vpn>
<connection>
Расширенные функции (Mac OS X)
Создания избыточного IPsec VPN
Для использования VPN отказоустойчивости / резервирования, вы будете настроить список серверов FortiGate IP / FQDN, вместо одного:
<forticlient_configuration>
<vpn>
<ipsecvpn>
<options>
...
</ Функции>
<connections>
<connection>
<name> psk_90_1 </ Name>
<type> руководства </ Type>
<ike_settings>
<prompt_certificate> 0 </ prompt_certificate>
<server> 10.10.90.1; ipsecdemo.fortinet.com; 172.17.61
0,143 </ сервер>
<redundantsortmethod> 1 </ redundantsortmethod>
...
</ Ike_settings>
</ Связь>
</ Подключения>
</ Ipsecvpn>
</ VPN>
</ Forticlient_configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги включены, но некоторые важные элементы для завершения конфигурации IPsec VPN, опущены.
RedundantSortMethod = 1
Этот тег XML устанавливает соединение IPsec VPN, как пинг-ответ, основанный. VPN будут подключаться к FortiGate который отвечает самым быстрым.
RedundantSortMethod = 0
По умолчанию RedundantSortMethod = 0, и соединение IPsec VPN является приоритет, основанный. Приоритет конфигурации на основе будет пытаться подключиться к

FortiGate начиная с первой в списке.
Приоритет, основанный SSL-VPN соединений
SSL-VPN поддерживает конфигурации на основе приоритета для избыточности.
<forticlient_configuration>
<vpn>
<sslvpn>
<options>
<enabled> 1 </ включен>
...
</ Функции>
<connections>
<connection>
<name> ssl_90_1 </ Name>
<server> 10.10.90.1; ssldemo.fortinet.com; 172.17.61.143:44
3 </ сервер>
...
</ Связь>
</ Подключения>
</ SSLVPN>
</ VPN>
</ Forticlient_configuration>
Это сбалансированная, но неполное XML фрагмент конфигурации. Все закрывающие теги включены, но некоторые важные элементы для завершения SSL VPN конфигурации, опущены.
Для SSL-VPN, все FortiGates должны использовать тот же порт TCP.
Включение VPN автосоединения
VPN Auto Connect использует следующие XML тег:
<autoconnect_tunnel> SSL 198 не CERT </ autoconnect_tunnel>
Включение VPN всегда
VPN всегда используются следующие XML тег:
<keep_running> 1 </ keep_running>
VPN туннеля и сценарий (Windows)
Обзор функций
Эта функция поддерживает автоматический запуск пользовательского сценария после настроено VPN туннель подключены или отключены. Сценарии пакетных сценариев в окнах и скрипты в Mac
OS X. Они будут определены как часть конфигурации VPN туннелей на XML формат FortiGate автора Endpoint профиля. Профиль будет толкнул вниз, чтобы FortiClient от FortiGate. Когда VPN туннеля FortiClient в подключении или отключении, соответствующие сценарию, что определено в
Туннель будет выполнен. VPN перед входом в настоящее время не поддерживается в FortiClient v5.0 Патч Release 1 (Mac OS X).
Подключить сетевой диск после туннельное соединение
Сценарий будет подключить сетевой диск и скопировать некоторые файлы после туннеля связано.
<on_connect>
<script>
<OS> окна </ OS>
<script>
<script>
<! [CDATA [
NET USE X: \ \ 192.168.10.3 \ ftpshare / пользователь: Мед Бу-Бу

MD C: \ Test
Копия X: \ PDF \ * * C:. \ Test
]]>
</ SCRIPT>
</ SCRIPT>
</ SCRIPT>
</ On_connect>
Удаление сетевого диска после туннеля отключен
Сценарий будет удалить сетевой диск после туннеля отключен.
<on_disconnect>
<script>
<OS> окна </ OS>
<script>
<script>
<! [CDATA [
Чистая x использования: / DELETE
]]>
</ SCRIPT>
</ SCRIPT>
</ SCRIPT>
</ On_disconnect>
VPN туннеля и сценарий (Mac OS X)
Подключить сетевой диск после туннельное соединение
Сценарий будет подключить сетевой диск и скопировать некоторые файлы после туннеля связано.
<on_connect>
<script>
<OS> Mac </ OS>
<script>
/ BIN / MkDir / Volumes / инсталляторов
/ Sbin / пинг-C 4 192.168.1.147>
/ Users / Admin / Desktop / Dropbox / p.txt
/ Sbin / Mount-T SMBFS
/ / Kimberly: RigUpTown@ssldemo.fortinet.com / установки

S / Volumes / строителей />
/ Users / Admin / Desktop / Dropbox / m.txt
/ BIN / MkDir / Users / Admin / Desktop / Dropbox / каталог
/ BIN / CP / Volumes / строителей / *. Журнал
/ Users / Admin / Desktop / Dropbox / каталог /.
</ SCRIPT>
</ SCRIPT>
</ On_connect>
Удаление сетевого диска после туннеля отключен
Сценарий будет удалить сетевой диск после туннеля отключен.
<on_disconnect>
<script>
<OS> Mac </ OS>
<script>
/ Sbin / размонтирование / Volumes / инсталляторов

/ BIN / RM-FR / Users / Admin / Desktop / Dropbox / *
</ SCRIPT>
</ SCRIPT>
</ On_disconnect>
Для получения дополнительной информации см. FortiClient v5.0 Справочник по XML в Fortinet Технические Документация сайт, http://docs.fortinet.com.

Поиски уязвимости
FortiClient v5.0 включает в себя модуль поиска уязвимостей и проверить персональный компьютер для известные уязвимости системы.
В этом разделе описывается, как включить поиск уязвимостей, и параметры конфигурации.
Scan Now
Для выполнения поиска уязвимостей, выберите кнопку Scan Now на FortiClient приборной панели.
FortiClient будет сканировать ваш персональный компьютер на наличие известных уязвимостей. Приборная панель отмечает дату последнего сканирования выше кнопки.
Рисунок 61: Поиск уязвимостей в прогрессе.

Обновить сейчас

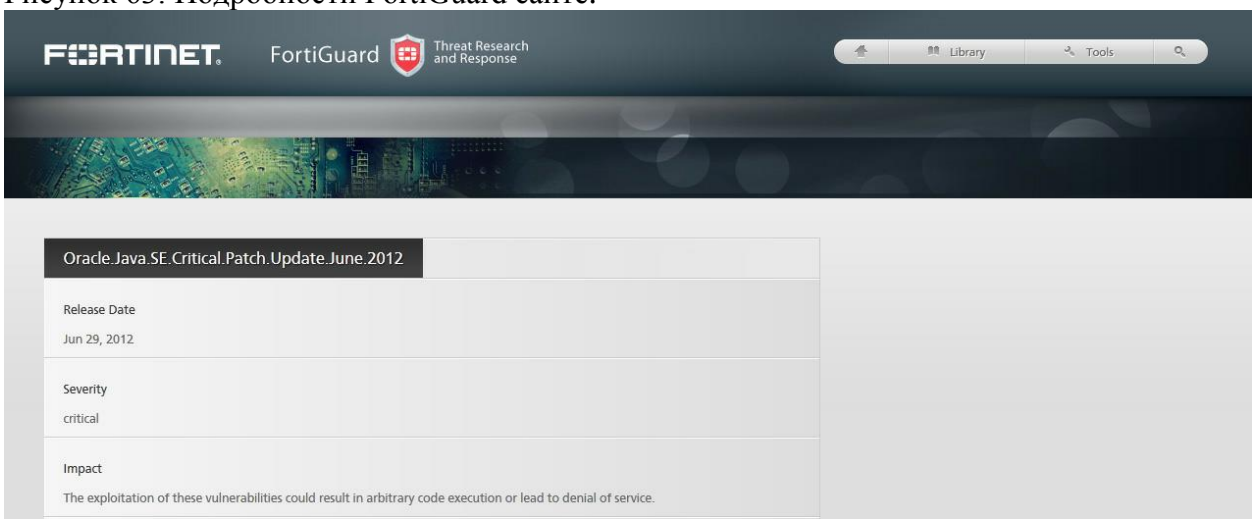
Выберите кнопку Обновить на панели FortiClient для обновления.
Когда проверка завершится, FortiClient будет отображать количество уязвимостей, обнаруженных на приборной панели. Выберите найдена ссылка на просмотр списка уязвимостей, обнаруженных в вашей системе.
Рисунок 62: Уязвимости, обнаруженные страницы.

Vulnerabilities Detected in the Last 30 Days

Vulnerability Name	Severity	Details	Time
Most Recent Scan			
1 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-24	Critical	33877	24/12/2012 2:35:21 PM
2 MS.VS.Active.Template.Library.Remote.Code.Execution	Critical	20531	24/12/2012 2:35:21 PM
3 Oracle.Java.SE.Critical.Patch.Update.October.2012	Critical	33716	24/12/2012 2:35:21 PM
4 Oracle.Java.SE.Critical.Patch.Update.Advisory.February.2012	Critical	32669	24/12/2012 2:35:21 PM
5 Oracle.Java.SE.Critical.Patch.Update.February.2011	Critical	27928	24/12/2012 2:35:21 PM
6 Oracle.Java.SE.Critical.Patch.Update.June.2011	Critical	30899	24/12/2012 2:35:21 PM
7 Oracle.Java.Runtime.True.Type.Font.IDEF.Opcode.Buffer.Ove...	Critical	31444	24/12/2012 2:35:21 PM
8 Oracle.Java.Runtime.Environment.Memory.Corruption.Vulnera...	Critical	33599	24/12/2012 2:35:21 PM
9 Oracle.Java.MixerSequence.Array.Index.Remote.Code.Execut...	Critical	30551	24/12/2012 2:35:21 PM
10 Oracle.Java.FileDialog.Show.Buffer.Overflow	Critical	28761	24/12/2012 2:35:21 PM
11 Oracle.Java.SE.Critical.Patch.Update.June.2012	Critical	32430	24/12/2012 2:35:21 PM
12 Microsoft.XML.Core.Services.Remote.Code.Execution.Vulner...	Critical	32958	24/12/2012 2:35:21 PM
13 MS.Windows.Unauthorized.Digital.Certificates.Spoofing.KB2...	Critical	32685	24/12/2012 2:35:21 PM
14 Apple.Safari.Multiple.Vulnerabilities.APPLE-SA-2012-11-01-2	Critical	33927	24/12/2012 2:35:21 PM
15 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-14	Critical	32255	24/12/2012 2:35:21 PM
16 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-19	Critical	33028	24/12/2012 2:35:21 PM
17 Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB12-22	Critical	33582	24/12/2012 2:35:21 PM

Close Clear

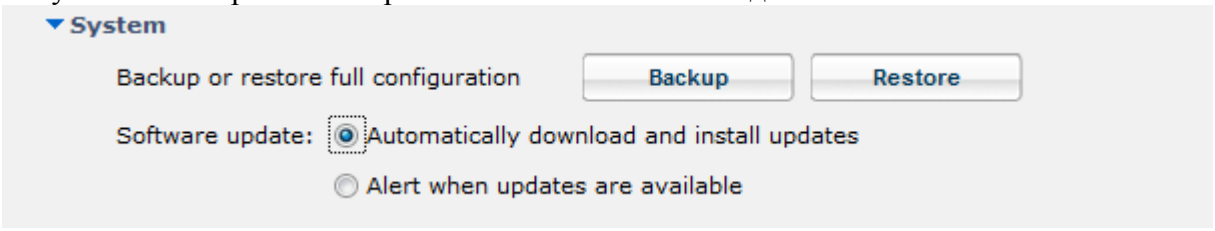
Выберите номер Details ID из списка, чтобы просмотреть информацию о выбранном уязвимость FortiGuard сайта. На сайте подробно дате выпуска, степень тяжести,, описание, пострадавшим продуктов, и рекомендуемые действия.
Уязвимость Имя уязвимости
Суровость. Степень серьезности назначен на уязвимости, критические, высокий, средний, Низкий, информация.
Детали. FortiClient поиска уязвимостей перечисляет Bugtraq (BID) номер, под подробнее колонки. Вы можете выбрать BID для просмотра сведений о уязвимости FortiGuard на сайте, или искать в Интернете с помощью этой ставки числа.
Время. Дата и время, что уязвимость была обнаружена.
Близко. Закрыть окно и вернуться к FortiClient приборной панели.
Очистить. Очистить результаты поиска уязвимостей.
Рисунок 63: Подробности FortiGuard сайте.



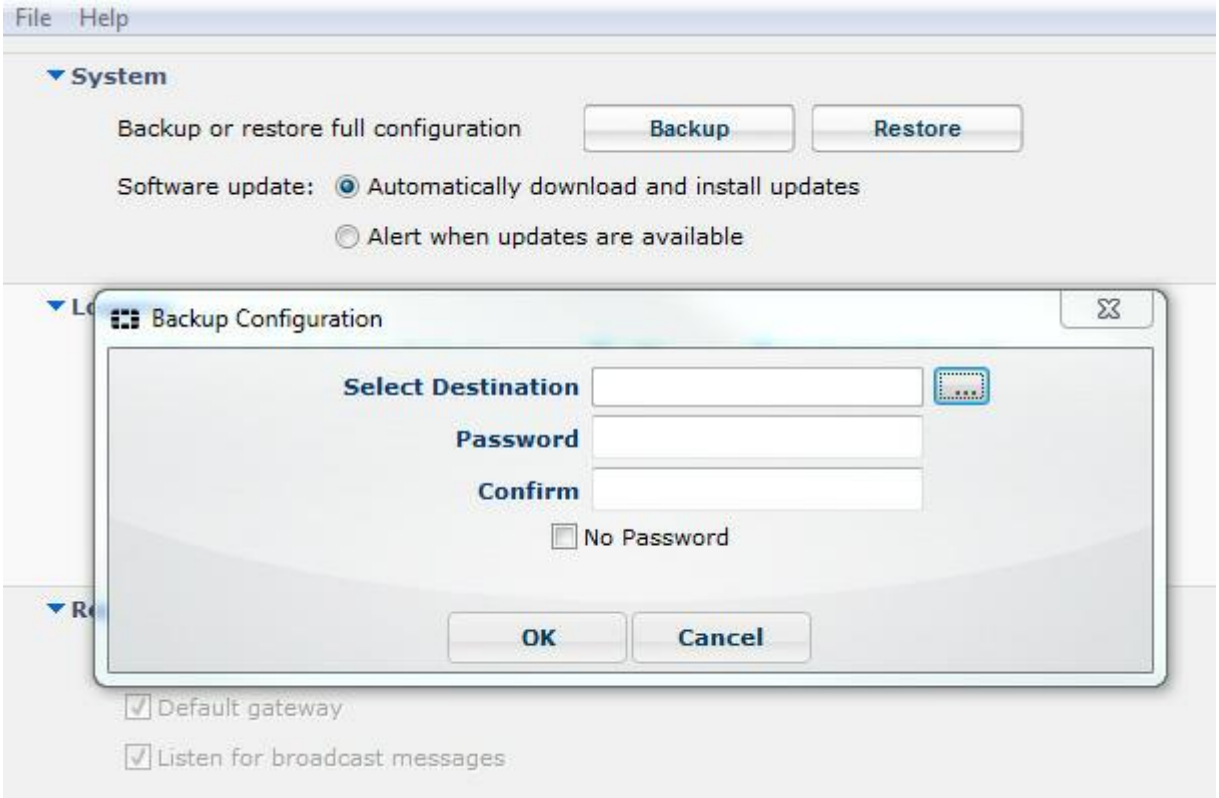
Поиск уязвимостей регистрации.
Для настройки ведения журнала поиска уязвимостей, выберите Файл на панели инструментов, и настройки на раскрывающемся меню. Выберите вход, чтобы посмотреть в выпадающем меню. Выберите поиск уязвимостей на вход меню позволяет включить ведение журнала для этого модуля.

Резервного копирования или восстановления полной конфигурации

Для резервного копирования или восстановления полного файла конфигурации Файл выберите на панели инструментов и настройки на раскрывающемся меню. Выберите Система, чтобы посмотреть в выпадающем меню. В этом меню вы можете выполнить резервного копирования или восстановления файла конфигурации.
Рисунок 64: Резервное копирование и восстановления данных.



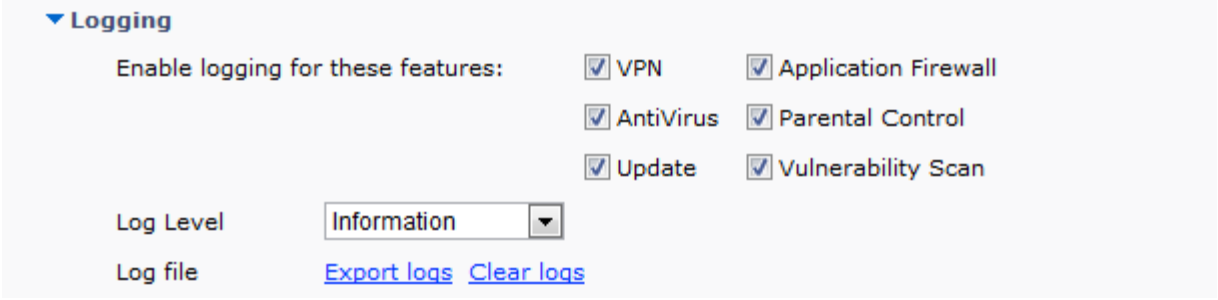
При выполнении резервного копирования можно выбрать конечный файл и сохранить файл в незашифрованном или зашифрованном виде.
Рисунок 65: Параметры резервного копирования файлов.



Чтобы настроить ведение журнала, выберите Файл на панели инструментов и настройки на выпадающее меню. Вход для просмотра выпадающего меню. В этом меню вы можете настроить ведение журнала для следующих

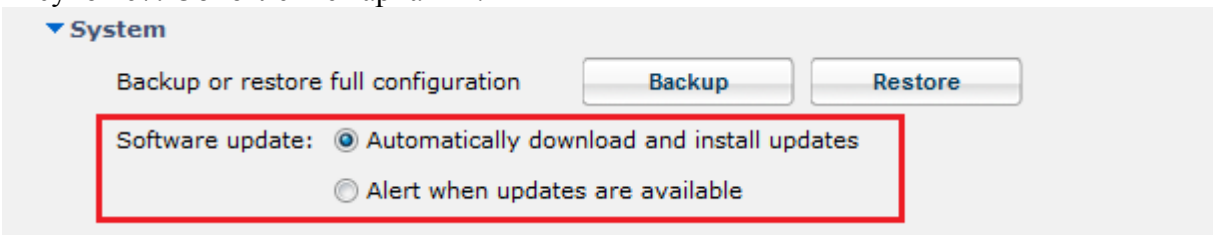
Особенности:
VPN
Антивирус
Обновление

Application Firewall
Родительский контроль
Поиск уязвимостей.
Вы можете задать уровень ведения журнала и выберите для экспорта бревен или Очистить журналы.
Рисунок 66: Вход варианты.



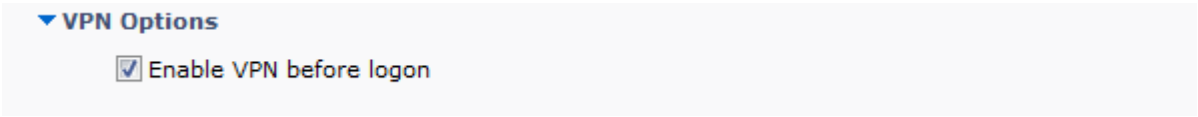
Обновления

Для настройки обновлений, выберите Файл на панели инструментов и настройки на выпадающее меню. Выбрать в системе, чтобы посмотреть в раскрывающемся меню. В этом меню вы можете настроить поведение FortiClient, когда новая версия программного обеспечения доступна на серверах FortiGuard Распределение (FDS).
Уровень регистрации
Описание
Аварийный
Система становится неустойчивой.
Оповещение
Требуются незамедлительные действия.
Критический
Функциональность влияет.
Ошибка
Ошибка существует и функциональность может быть затронуто.
Предупреждение
Функциональность может быть затронуто.
Замечать
Информация о нормальных событий.
Информация
Общая информация о системе операций.
Отлаживать
Отладка FortiClient.
Рисунок 67: Обновление варианты.



VPN варианты

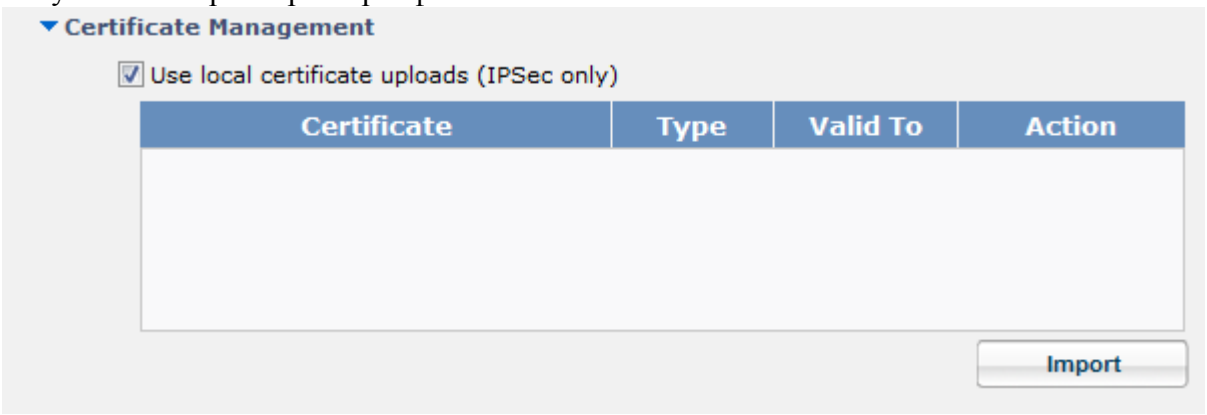
Для настройки VPN параметров выберите Файл на панели инструментов и настройки на выпадающее меню. Выберите VPN функции для просмотра выпадающего меню. В этом меню вы можете настроить для предоставления VPN перед входом в систему.
Рисунок 68: VPN варианты.



Управление сертификатами

Для настройки VPN сертификатов, выберите Файл на панели инструментов и настройки на выпадающее меню. Выбор сертификата, чтобы просматривать выпадающего меню. В этом меню вы можете настроить IPsec VPN использовать локальные сертификаты и сертификаты для импорта FortiClient.

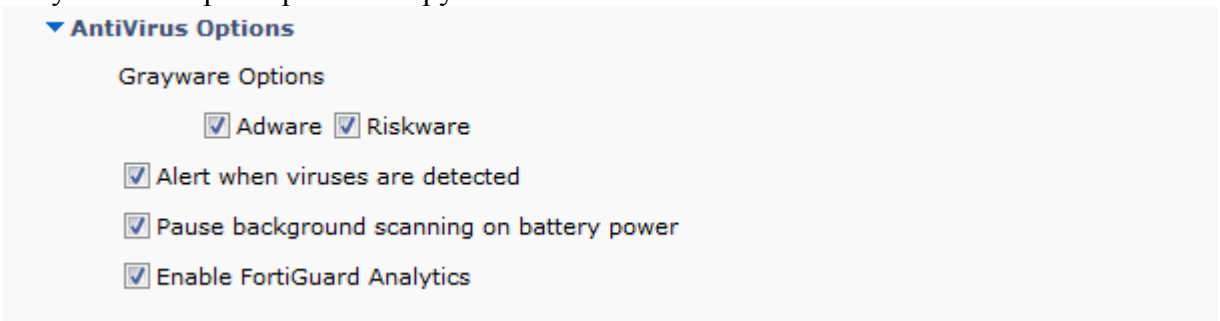
Рисунок 69: Параметры сертификата.



Параметры антивируса

Чтобы настроить параметры антивируса, выберите Файл на панели инструментов, и настройки на выпадающее меню. В этом меню вы можете настроить нежелательные варианты и поведение FortiClient при обнаружении вируса.

Рисунок 70: параметры антивируса.



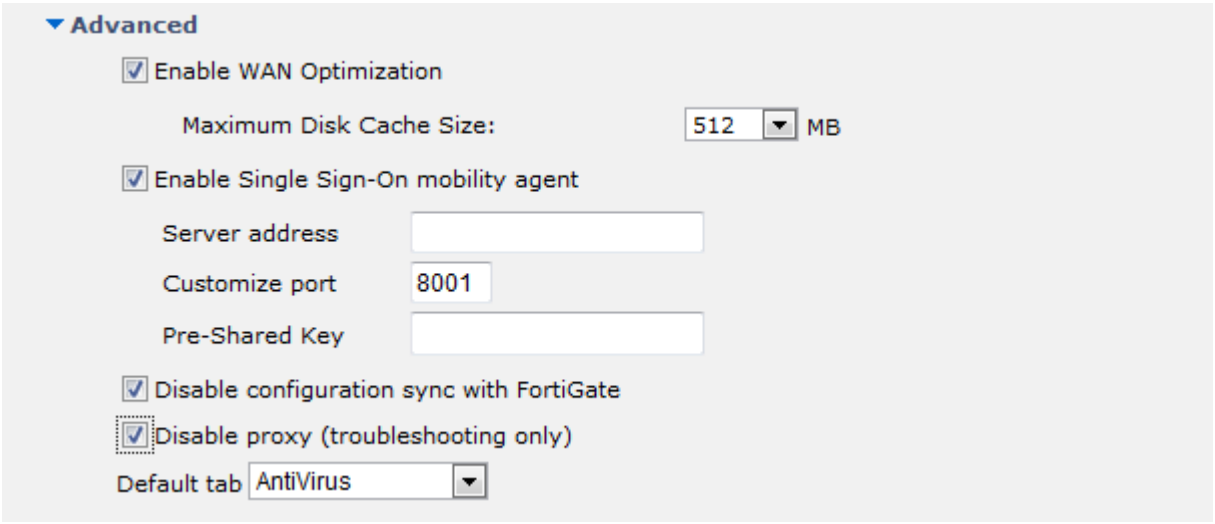
Дополнительные параметры

Чтобы настроить дополнительные параметры, выберите Файл на панели инструментов, и настройки на выпадающее меню.

Выберите Дополнительно, чтобы посмотреть в выпадающем меню. В этом меню вы можете настроить WAN.

Оптимизация, единого входа, настройки синхронизации с FortiGate, отключите прокси, а по умолчанию FortiClient вкладку при запуске.

Рисунок 71: Усовершенствованные функции.



Опции нежелательных программ

Нежелательных программ это зонтичный термин применяется к широкому кругу Вредоносные программы, такие как шпионское, рекламное ПО, которые часто тайно установленных на компьютере пользователя, чтобы отслеживать и сообщать определенную информацию на внешние источники без разрешения пользователя. Выберите, чтобы включить обнаружение сканирование в реальном времени.

Потенциально опасные программы

Выберите, чтобы включить обнаружение потенциально опасных программ и карантина в течение антивирусное сканирование.

Сигнал тревога когда вирусы обнаруженный

Выберите для отображения окна уведомление когда вирус обнаружено.

Пауза фоне сканирования от батареи

Выберите, чтобы приостановить фоновое сканирование при питании от аккумулятора. Включить FortiGuard Analytics Выберите для автоматической отправки подозрительных файлов в FortiGuard.

Сеть для анализа.

Single Sign-On агента мобильности

FortiClient Single Sign-On Мобильность агент выступает в качестве клиента, который с обновлениями FortiAuthenticator с входа пользователя в систему и информационную сеть. FortiAuthenticator прослушивает конфигурируемых порта TCP. FortiClient подключается к FortiAuthenticator использованием TLS / SSL с двусторонней проверки подлинности сертификата. FortiClient посылает вход в систему пакет FortiAuthenticator, которая отвечает с пакет подтверждения.

FortiClient / FortiAuthenticator связи требуется следующее:

IP-адрес должен быть уникальным в пределах всей сети.

FortiAuthenticator должна быть доступна с клиентами во всех регионах.

FortiAuthenticator должны быть доступны для всех FortiGates.

Включить Single Sign-On агента мобильности на FortiClient

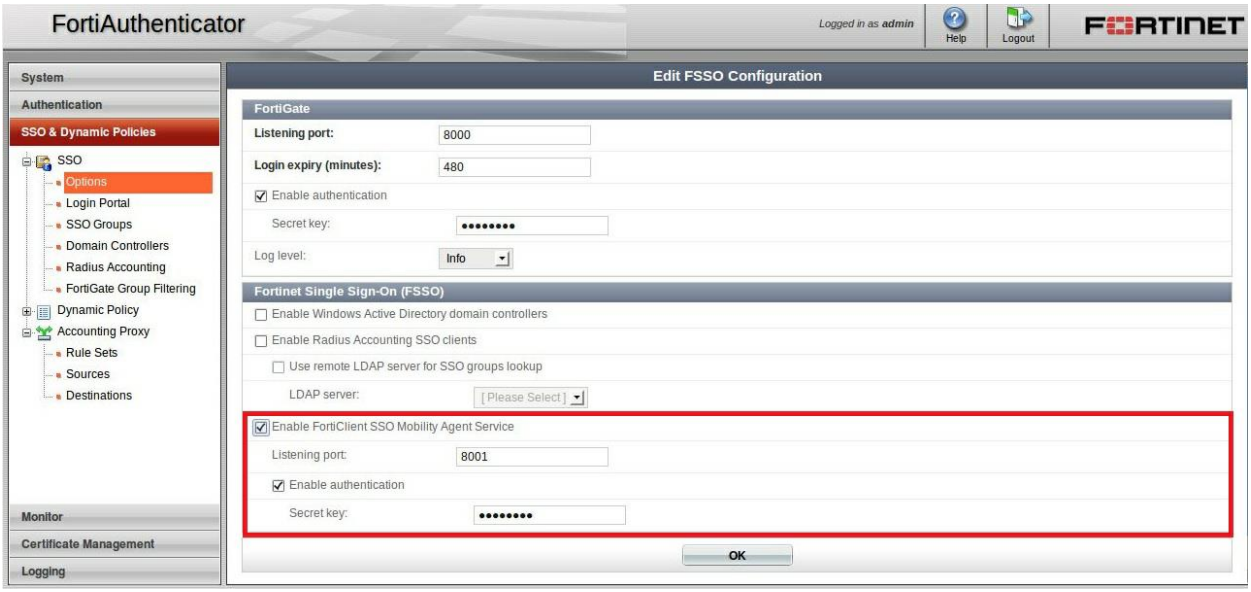
1. Выберите файл на панели инструментов и настройки на выпадающее меню.
2. Выберите Дополнительно, чтобы посмотреть в выпадающем меню.
3. Выберите, чтобы включить Single Sign-On агента мобильности.

Включить WAN Оптимизация

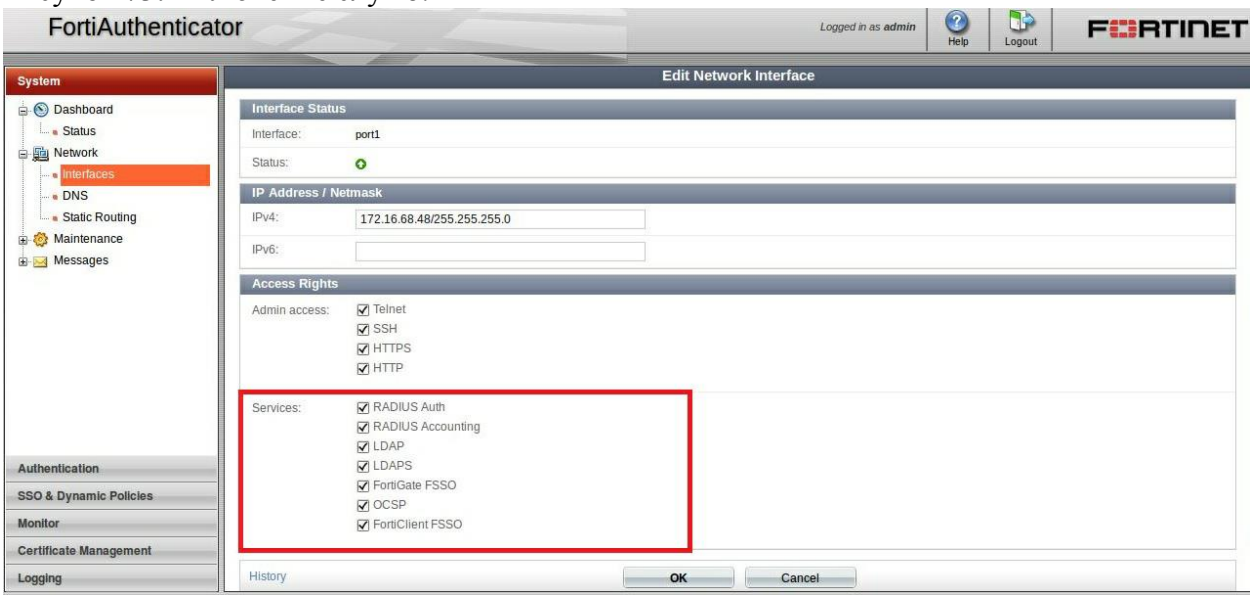
Выберите, чтобы включить оптимизации глобальной сети. Вы должны включить, только если вы FortiGate сконфигурирован для WAN

Оптимизация.

Максимальная диска
Размер кэш-памяти
Выберите, чтобы настроить максимальный размер дискового кэша. Значение по умолчанию 512 Мб.
Включить Single Sign-On агента мобильности
Выберите, чтобы включить Single Sign-On Агент для мобильных FortiAuthenticator. Для использования этой функции необходимо применить FortiClient SSO мобильности лицензии агента FortiAuthenticator вашего устройства.
Адрес сервера
Введите адрес FortiAuthenticator IP.
Настроить порт
Введите номер порта. По умолчанию используется порт 8001.
Pre-Shared Key
Введите общий ключ. Предварительный ключ должен совпадать с ключом настроенный на FortiAuthenticator.
Отключить конфигурацию
синхронизации с FortiGate
Выберите, чтобы отключить синхронизацию с конфигурацией FortiGate.
Отключить прокси
(Диагностика только)
Выберите, чтобы отключить прокси при устранении FortiClient.
Закладку по умолчанию
Выберите закладку по умолчанию, который будет отображаться при открытии FortiClient.
FortiClient Single Sign-On агента мобильности требует FortiAuthenticator работает v2.0.0 GA сборки
0006 или более поздней версии. Введите FortiAuthenticator (сервер) IP-адрес, номер порта, и с предварительным общим
настроен ключ на FortiAuthenticator.
Fortinet Технологии Инк
4. Введите адрес FortiAuthenticator сервера и предварительный ключ.
Включить FortiClient SSO Мобильность Агент службы по FortiAuthenticator
1. Выберите SSO и динамической политики> SSO> Параметры.
2. Выберите Включить FortiClient SSO Мобильность Service Agent и значение TCP порт для прослушивания
порт.
3. Выберите Включить аутентификацию и ввести секретный ключ значение.
Рисунок 72: Конфигурация FortiAuthenticator.



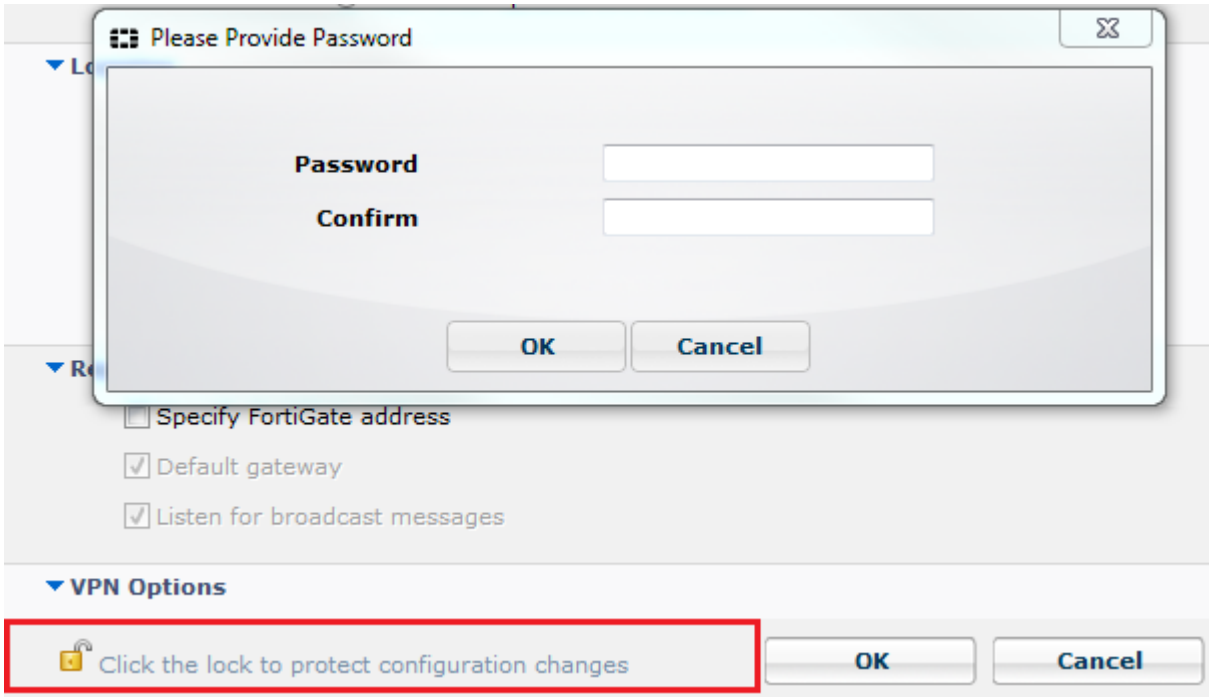
4. Чтобы включить FortiClient FSSO услуг на интерфейсе выберите Система > Сеть > интерфейс.
Выберите Изменить для изменения сетевого интерфейса, выберите FortiClient FSSO включить.
Рисунок 73: Включение служб.



Чтобы включить SSO Мобильность FortiClient Агент службы по FortiAuthenticator, вы должны сначала применяется соответствующая лицензия FortiClient для FortiAuthenticator. Для получения дополнительной информации см. FortiAuthenticator v2.0 Руководство администратора на http://docs.fortinet.com. Для получения информации о приобретение лицензии на FortiClient FortiAuthenticator, пожалуйста, обратитесь к своему уполномоченному Fortinet реселлера.

Конфигурация блокировки

Для предотвращения несанкционированных изменений в FortiClient конфигурации, выберите значок замка расположены в левом нижнем углу страницы настройки. Вам будет предложено ввести и подтвердить пароль.
Когда конфигурация заблокирована, изменения конфигурации ограничен и не может FortiClient быть закрыты или удалены.
Рисунок 74: Настройка блокировки.



Когда конфигурация заблокирована вы можете выполнять следующие действия:
Антивирус
Выполните антивирусное сканирование, вид угроз найден, и просмотр журналов
Выберите Обновить, чтобы обновления сигнатур
Родительский контроль
Посмотреть нарушений
Application Firewall
Посмотреть Блокировка приложений
Удаленный доступ
Настройка, изменение и удаление IPsec VPN или SSL VPN-соединения
Подключение к VPN-соединения
Поиск уязвимостей
Выполните поиск уязвимостей системы
Посмотреть уязвимостей
Регистрации и отмены регистрации FortiClient для контроля конечных точек
Настройки
Экспорт FortiClient журналы
Резервное копирование конфигурации FortiClient
Для выполнения изменений конфигурации или закрыть FortiClient, выберите значок замка и введите Пароль, используемый для блокировки конфигурации.

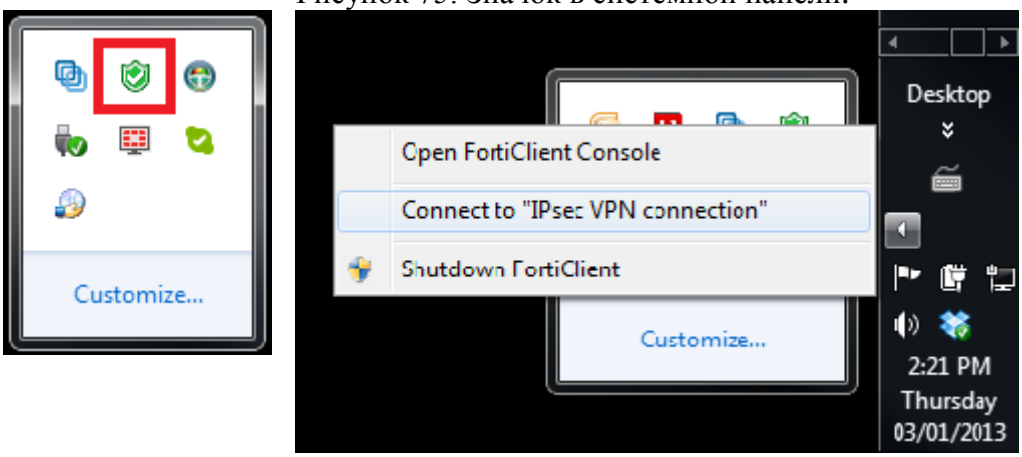
FortiTray

Когда FortiClient работает на вашей системе, вы можете выбрать FortiTray значок на окнах системный трей для выполнения различных действий. Значок FortiTray доступен в системном трее даже, когда панель FortiClient закрыт.

Варианты меню по умолчанию

Открытое FortiClient консоли
Shutdown FortiClient
Динамические параметры меню в зависимости от конфигурации
Подключение к настроено IPsec VPN или SSL VPN-соединени
Откройте окно антивирусной проверки (если проверка по расписанию в данный момент)
Откройте окно поиска уязвимостей (если поиск уязвимостей работает)
При наведении курсора мыши на значок FortiTray, вы будете получать различные уведомления включая версию, A.B. подпись, A. B. двигателя.

Рисунок 75: Значок в системной панели.

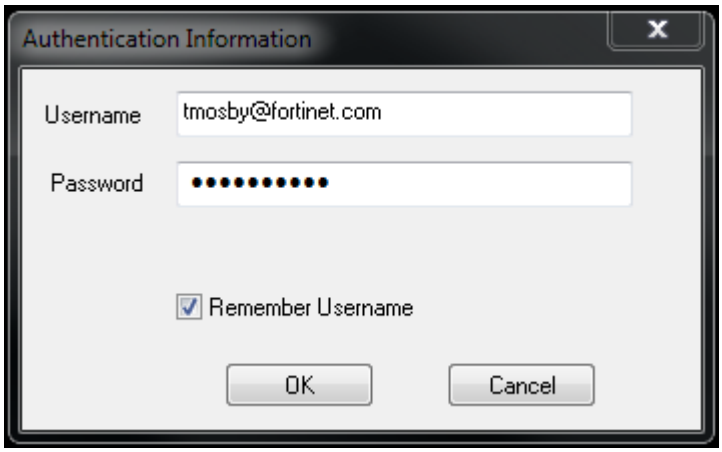


Когда конфигурация заблокирована, опция для закрытия FortiClient от FortiTray неактивна вне.

Подключение к VPN-соединения

Для подключения к VPN-соединения от FortiTray выберите задач Windows и щелкните правой кнопкой на иконку FortiTray. Выберите соединение, которое вы хотите подключиться, введите имя пользователя и пароль в окно аутентификации и выберите OK для подключения.

Рисунок 76: Окно аутентификации.



http://www.fortinet.com