TREND MICRO

10.0 Worry-Free™ Business Security Standard и Advanced

пакет обновления 1

Руководство администратора

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Trend Micro Incorporated оставляет за собой право вносить изменения в данный документ и содержащееся в нем описание продукт без предварительного уведомления. Перед установкой и использованием продукт прочтите файлы Readme, примечания к выпуску и последнюю версию соответствующей документации, которые доступны на веб-сайте компании Trend Micro по адресу:

http://docs.trendmicro.com/ru-ru/smb/worry-free-business-security.aspx

Trend Micro, логотип Trend Micro t-ball, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan и ScanMail являются товарными знаками или зарегистрированными товарными знаками Trend Micro Incorporated. Все прочие наименования продуктов или компаний могут быть товарными знаками или зарегистрированными товарными знаками их владельцев.

© 2019. Trend Micro Incorporated. Все права защищены.

Номер части документа: WFEM108677/190617

Дата выпуска: Июнь 2019 г.

Защищено патентами США №: 5 951 698 и 7 188 369

В этом руководстве описаны основные функции продукт и/или инструкции по установке для рабочей среды. Прочтите это руководство перед установкой или использованием продукт.

Подробные сведения об использовании конкретных функций продукт можно получить в интерактивном справочном центре Trend Micro и/или в базе знаний Trend Micro.

Компания Trend Micro постоянно совершенствует свою документацию. Если у вас есть вопросы, замечания или предложения относительно этого или любого другого документа компании Trend Micro, отправьте их по адресу docs@trendmicro.com.

Оцените эту документацию на следующем веб-сайте:

https://www.trendmicro.com/download/documentation/rating.asp

Содержание

Введение

Введение xiii

Документация решения Worry-Free Business Security xiv

Аудитория xiv

Условные обозначения в документах xv

Глава 1: Введение в Worry-Free Business Security Standard и Advanced

Обзор программы Trend Micro Worry-Free Business Security 1-2

Новые возможности, предусмотренные в данном выпуске 1-2

Основные возможности и преимущества 1-3

- Trend Micro Smart Protection Network 1-3
- Служба репутации файлов 1-4
- Службы Web Reputation 1-4
- Email Reputation (только Advanced) 1-5
- Smart Feedback 1-6
- Фильтрация URL-адресов 1-7

Преимущества защиты 1-8

Сведения об угрозах 1-9

- Вирусы/вредоносные программы 1-9
- Шпионские и нежелательные программы 1-11
- Спам 1-12
- Проникновения 1-13
- Вредоносные действия 1-13
- Фальшивые точки доступа 1-13
- Фишинг 1-13
- Массовые почтовые атаки 1-14
- Веб-угрозы 1-15

Глава 2: Начало работы

Сеть Worry-Free Business Security 2-2

Security Server 2-2
Scan Server 2-2

Агенты 2-4

Веб-консоль 2-4
Открытие веб-консоли 2-5
Навигация по веб-консоли 2-9
Значки веб-консоли 2-11

Глава 3: Установка агентов

Установка Security Agent 3-2
Требования к установке Security Agent 3-2
Условия установки Security Agent 3-2
Доступные функции Security Agent 3-3
Установка Security Agent и поддержка адреса IPv6 3-5

Способы установки Security Agent 3-7
Установка с внутренней веб-страницы 3-10
Установка с использованием программы настройки сценариев входа 3-12
Установка с использованием Client Packager 3-15
Удаленная установка 3-19
Установка с использованием сканера уязвимостей .. 3-22
Установка с уведомлением по электронной почте ... 3-34
Переход на Security Agent 3-35
Выполнение задач после установки для агентов Security Agent 3-36

Установка Messaging Security Agent 3-39
Требования к установке Messaging Security Agent 3-39
Установка агентов Messaging Security Agent (только Advanced) 3-39

Удаление агентов 3-41
Удаление агентов из веб-консоли 3-43
Удаление агентов из веб-консоли 3-43

Удаление Security Agent с локального компьютера ... 3-45
Удаление агента Messaging Security Agent с сервера Microsoft Exchange (только Advanced) 3-45

Глава 4: Управление устройствами

Использование дерева устройств 4-2
Использование команд устройств 4-5
Добавление агентов в группы 4-7
Добавление групп 4-9
Настройка столбцов списка устройств 4-10
Перемещение агентов 4-12
Перемещение агентов Security Agent между группами 4-14
Перемещение агентов между серверами Security Server с помощью веб-консоли 4-15
Перемещение агента Security Agent между серверами Security Server с помощью инструмента переназначения клиентов 4-16
Дублирование параметров 4-18
Дублирование параметров группы Security Agent 4-18
Дублирование параметров Messaging Security Agent (только Advanced) 4-19
+Импорт и экспорт параметров групп Security Agent 4-20
Экспорт параметров 4-22
Импорт параметров 4-22

Глава 5: Управление основными параметрами безопасности агентов Security Agent

Краткий обзор основных параметров безопасности для Security Agent 5-2
Методы сканирования 5-3
Настройка способов сканирования 5-6

Сканирование в режиме реального времени для агентов Security Agent 5-8
Настройка сканирования в режиме реального времени для агентов Security Agent 5-9
Прогнозное машинное самообучение 5-9
Настроить прогнозное машинное самообучение 5-11
Контроль действий 5-13
Настройка контроля действий 5-13
Надежные программы 5-18
Конфигурирование надежных программ 5-19
Папка карантина 5-20
Настройка папки карантина 5-23
Web Reputation 5-23
Настройка службы Web Reputation для агентов Messaging Security Agent 5-25
Фильтрация URL-адресов 5-27
Настройка фильтрации URL-адресов 5-27
Разрешенные/заблокированные URL-адреса 5-28
Настройка разрешенных/заблокированных URL-адресов 5-29
Брандмауэр 5-30
Настройка брандмауэра 5-33
Работа с исключениями брандмауэра 5-35
Отключение брандмауэра для группы агентов 5-37
Отключение брандмауэра для всех агентов 5-38
Контроль устройств 5-38
Настройка контроля устройств 5-39
Инструменты пользователя 5-41
Настройка инструментов пользователя 5-41
Права агента 5-42
Настройка прав агента 5-42

Глава 6: Управление основными параметрами безопасности агентов Messaging Security Agent (только Advanced)

Агентов Messaging Security Agent 6-2
Сканирование электронной почты агентом Messaging Security Agent 6-3
Параметры Messaging Security Agent по умолчанию ... 6-4

Сканирование в режиме реального времени для агентов Messaging Security Agent 6-6
Настройка сканирования в режиме реального времени для агентов Messaging Security 6-6

Защита от спама 6-7
Email Reputation 6-8
Сканирование содержимого 6-10

Фильтрация содержимого 6-17
Управление правилами фильтрации содержимого .. 6-18
Типы правил фильтрации содержимого 6-22
Добавление правила фильтрации при совпадении всех условий 6-23
Добавление правила фильтрации при совпадении любого условия 6-26
Добавление правила мониторинга фильтрации содержимого 6-30
Создание исключений в правилах фильтрации содержимого 6-33

Предотвращение потери данных 6-34
Подготовительная работа 6-35
Управление правилами предотвращения потери данных 6-36
Правила предотвращения потери данных по умолчанию 6-43
Добавление правил предотвращения потери данных 6-44

Блокирование вложений 6-50
Настройка блокирования вложений 6-51

Web Reputation 6-54
Настройка службы Web Reputation для агентов Messaging Security Agent 6-56
Mobile Security 6-58
Поддержка безопасности мобильных устройств 6-59
Настройка управления доступом к устройствам 6-61
Отмена отложенной очистки устройства 6-62
Очистка устройств вручную 6-62
Настройка политик безопасности 6-63
Карантин для агентов Messaging Security Agent 6-69
Запрос папок карантина 6-70
Просмотр результатов запроса и выполнение действий 6-72
Обслуживание папок карантина 6-74
Настройка папок карантина 6-75
Параметры уведомлений для Messaging Security Agent ... 6-76
Настройка параметров уведомлений для агентов Messaging Security Agent 6-78
Настройка обслуживания базы спама 6-79
Управление пользовательским карантином 6-80
Служба технической поддержки компании Trend Micro / Отладчик 6-82
Создание отчетов системного отладчика 6-83
Контроль режима реального времени 6-84
Работа с программой контроля в режиме реального времени 6-85
Добавление предупреждения к исходящим электронным сообщениям 6-85

Глава 7: Управление сканированием

Сведения о сканировании 7-2
Сканирование в режиме реального времени 7-3
Сканирование вручную 7-3
Запуск сканирования вручную 7-4

Сканирование по расписанию 7-7
Настройка сканирования по расписанию 7-7

Сканирование объектов и действий для Security Agent .. 7-11

Сканирование объектов и действия для агентов Messaging Security Agent 7-20

Глава 8: Управление обновлениями

Обзор обновлений 8-2

Обновляемые компоненты 8-4
Критические обновления, пакеты исправлений и пакеты обновлений 8-12

Обновления сервера Security Server 8-13
Настройка источника обновлений Security Server 8-15
Обновление сервера Security Server вручную 8-17
Настройка запланированных обновлений Security Server 8-17
Откат компонентов 8-19

Обновления агентов Security Agent и Messaging Security Agent 8-20
Автоматические обновления 8-20
Запуск обновления вручную 8-20
Напоминания и подсказки для обновления агентов 8-21

Агенты обновлений 8-22
Настройка агентов обновлений 8-25

Глава 9: Использование раздела «Текущее состояние»

Текущее состояние 9-2
Центр событий 9-3
Обнаружения угроз безопасности за определенный период времени 9-9
Сводка по ПО для вымогательства 9-18
Статус лицензии 9-23
Сводка по серверам Exchange 9-23
Состояние агента 9-23

Глава 10: Управление уведомлениями

Использование уведомлений 10-2
Настройка событий для уведомлений 10-5
Символы переменных 10-6

Глава 11: Управление глобальными параметрами

Глобальные параметры 11-2
Настройка параметров прокси-сервера сети Интернет . 11-3
Настройка параметров SMTP-сервера 11-4
Настройка параметров рабочей станции или сервера ... 11-5
Настройка системных параметров 11-11
Настройка параметров списка исключений 11-15

Глава 12: Использование журналов и отчетов

Журналы 12-2
Запрос журнала 12-4
Отчеты 12-5
Работа с однократными отчетами 12-6
Работа с запланированными отчетами 12-7
Анализ отчетов 12-12
Выполнение задач обслуживания для отчетов и журналов 12-15

Глава 13: Выполнение административных задач

Изменение пароля веб-консоли 13-2
Работа с Plug-in Manager 13-2
Управление лицензией продукта 13-3
Настройка параметров обновления продукта 13-5
Настройка уведомлений об обновлениях продукта 13-6

Участие в программе обратной связи Smart Feedback Program 13-7
Изменение языка интерфейса агента 13-8
Сохранение и восстановление параметров программы . 13-8
Удаление сервера Security Server 13-10

Глава 14: Использование инструментов управления

Типы инструментов 14-2
Агент Trend Micro Remote Manager 14-4
Установка агента Trend Micro Remote Manager (для пользователей портала Customer Licensing Portal) 14-4
Установка агента Trend Micro Remote Manager (для пользователей Licensing Management Platform) 14-6
Управление агентами на управляемом сервере 14-8
Резервное копирование и восстановление параметров агента 14-13
Сохранение дискового пространства 14-15
Запуск средства очистки на Security Server 14-15
Запуск средства очистки диска на Security Server с помощью интерфейса командной строки 14-16
Сохранение дискового пространства на клиентских компьютерах 14-17
Перенос базы данных сервера Scan Server 14-18
Восстановление зашифрованных файлов 14-19
Расшифровка и восстановление файлов на Security Agent 14-20
Расшифровка и восстановление файлов на сервере Security Server, в пользовательской папке карантина или в агенте Messaging Security Agent 14-21
Восстановление почтовых сообщений в формате Transport Neutral Encapsulation 14-23
Использование инструмента ReGenID 14-24
Управление дополнениями SBS и EBS 14-25
Установка дополнений SBS и EBS вручную 14-25

Использование дополнений SBS или EBS 14-26

Приложение A: Значки Security Agent

Проверка состояния Security Agent A-2

Просмотр значков агентов Security Agent на панели задач Windows A-4

Доступ к консоли Flyover A-5

Приложение B: Поддержка IPv6 в Worry-Free Business Security

Поддержка IPv6 в Worry-Free Business Security и Агенты безопасности B-2
- Требования к серверу Security Server IPv6 ..... B-2
- Требования к агентам Messaging Security Agent B-3
- Ограничения сервера только с адресом IPv6 ..... B-3
- Ограничения для Security Agent, использующих исключительно адреса IPv6 ..... B-4

Настройка адресов IPv6 ..... B-5

Окна, отображающие IP-адреса B-7

Приложение C: Техническая поддержка

Ресурсы для поиска и устранения неисправностей C-2
- Использование портала поддержки C-2
- Энциклопедия угроз C-3

Как связаться с Trend Micro C-3
- Ускорение обработки запроса о поддержке C-4

Отправка подозрительного содержимого в компанию Trend Micro C-5
- Email Reputation Services C-5
- Службы File Reputation C-5
- Службы Web Reputation C-5

Другие ресурсы C-6
- Центр загрузок C-6

Отзывы и предложения по документации C-6

Приложение D: Использование терминов и понятий о продукте

Критически важное исправление D-2
Оперативное исправление D-2
IntelliScan D-2
IntelliTrap D-3
Система обнаружения вторжения D-4
Ключевые слова D-5
Исправление D-10
Регулярные выражения D-11
Списки исключений из сканирования D-20
Пакет обновления D-27
Порт, используемый «троянскими конями» D-27
Неизлечимые файлы D-28

Индекс

Индекс IN-1

Введение

Введение

Добро пожаловать в *руководство администратора* Trend Micro™ Worry-Free™ Business Security. В этом документе содержится информация о начале работе, процедурах установки агентов и управлении сервером Security Server и агентами.

Документация решения Worry-Free Business Security

Документация Worry-Free Business Security включает следующее:

Таблица 1. Документация решения Worry-Free Business Security

Документация	Описание
Руководство по установке и обновлению	документ PDF, в котором описаны требования и процедуры установки Security Server, а также обновления сервера и агентов
Руководство администратора	документ PDF, в котором содержится информация о начале работе, процедурах установки клиентов и управлении Security Server и агентами.
Справка	Файлы HTML, скомпилированные в формате WebHelp или CHM, содержащие инструкции, советы по использованию и сведения, касающиеся того или иного параметра.
Файл Readme	содержит список известных проблем и основных этапов установки. В нем также может содержаться последняя информация по продукту, не включенная в справку и печатную документацию.
База знаний	интерактивная база информации по решению проблем, поиску и устранению неисправностей. Здесь можно найти последнюю информацию об известных проблемах продукта. Для доступа к базе знаний посетите следующий веб-сайт: http://esupport.trendmicro.com

Последнюю версию PDF-документов и файла Readme можно найти на следующем сайте:

http://docs.trendmicro.com/ru-ru/smb/worry-free-business-security.aspx

Аудитория

Документация Worry-Free Business Security адресована следующим пользователям.

- **Администраторы безопасности**: отвечают за управление Worry-Free Business Security, включая установку сервера Security Server и агентов и управление ими. Эти пользователи должны обладать глубокими знаниями о сетях и управлении серверами.
- **Конечные пользователи**: пользователи, на чьих компьютерах установлены агенты Security Agent. Сюда входят как новички в работе с компьютером, так и опытные пользователи.

Условные обозначения в документах

Для облегчения поиска и восприятия информации в документации Worry-Free Business Security используются следующие условные обозначения.

Таблица 2. Условные обозначения в документах

Обозначение	Описание
ВСЕ ПРОПИСНЫЕ	Сокращения, аббревиатуры и названия некоторых команд и клавиш на клавиатуре
Полужирный	Меню и команды меню, командные кнопки, вкладки, параметры и действия
Курсив	Ссылки на другие документы или новые технологические компоненты
<Текст>	Показывает, что текст в угловых скобках нужно заменить соответствующими данными. Например, `C:\Program Files\<имя_файла>` может означать `C:\Program Files\sample.jpg`.
Примечание	Примечания или рекомендации по настройке
Совет	Советы и рекомендации Trend Micro

Обозначение	Описание
ПРЕДУПРЕЖДЕНИЕ!	Предупреждения о действиях, которые могут повредить компьютеры в сети

Глава 1

Введение в Worry-Free™ Business Security Standard и Advanced

В этой главе содержится общий обзор программы Trend Micro Worry-Free Business Security (Worry-Free Business Security).

Обзор программы Trend Micro Worry-Free Business Security

Решение Trend Micro Worry-Free Business Security (Worry-Free Business Security) защищает пользователей и активы малых предприятий от хищения данных, кражи личных сведений, посещения опасных веб-сайтов и спама (только версия Advanced).

Информация, содержащаяся в настоящем документе, касается версий Worry-Free Business Security Standard и Advanced. Разделы и главы, относящиеся только к версии Advanced, обозначены как «(только Advanced)».

Разработанное на основе Trend Micro Smart Protection Network, решение Worry-Free Business Security является:

- **Более надежным**: предотвращает проникновение вирусов, шпионских программ, спама (только Advanced) и веб-угроз на компьютеры. Фильтрация URL-адресов блокирует доступ к опасным сайтам и позволяет увеличить продуктивность пользователей.
- **Более интеллектуальным**: быстрое сканирование и непрерывное обновление предотвращают появление новых угроз, при этом минимально воздействуя на клиентские системы.
- **Более простым**: Простая в развертывании и не требующая администрирования, программа Worry-Free Business Security обнаруживает угрозы более эффективно, что позволяет сосредоточиться на бизнесе и не думать о безопасности.

Новые возможности, предусмотренные в данном выпуске

В следующей таблице описаны новые функции и улучшения, включенные в этот выпуск Worry-Free Business Security.

Функция/улучшение	Описание
Глубокое сканирование	В Worry-Free Business Security доступна функция глубокого сканирования для углубленного сканирования и зачистки зараженных локальных компьютеров. Для получения дополнительной информации см. *Использование дерева устройств на странице 4-2* и *Использование команд устройств на странице 4-5*.
Улучшенная защита от бесфайловых вредоносных программ	Worry-Free Business Security теперь использует новейшие технологии защиты от бесфайловых вредоносных программ для защиты конечных точек от бесфайловых атак.
Поддержка операционных систем	Worry-Free Business Security теперь поддерживает установку сервера Security Server и агента Security Agent на следующие операционные системы: • Обновление Windows 10 за май 2019 г. • Windows Server 2019

Основные возможности и преимущества

Worry-Free Business Security предоставляет указанные ниже возможности и преимущества.

Trend Micro™ Smart Protection Network™

Решение Trend Micro™ Smart Protection Network™ является следующим поколением клиент-серверной инфраструктуры безопасности содержимого, разработанной для защиты пользователей от различных угроз. Оно совмещает в себе локальные и размещенные в компании Trend Micro решения для защиты пользователей, работающих в сети, дома или в дороге. Сеть Smart Protection Network использует «облегченные» агенты для доступа к системе уникальных технологий защиты электронной почты, Web Reputation, File Reputation и баз данных угроз, взаимодействующих в удаленной среде. Степень защиты

пользователей автоматически усиливается по мере доступа к сети большего количества продуктов, служб и пользователей, что позволяет создать службу защиты в реальном времени.

Для получения дополнительных сведений о программе Smart Protection Network посетите веб-сайт:

http://www.trendmicro.com.ru/technology-innovation/our-tech/smart-protection-network/index.html

Служба репутации файлов

Служба репутации файлов проверяет репутацию каждого файла в обширной облачной базе данных. Поскольку информация о вредоносном ПО хранится удаленно, она моментально доступна всем пользователям. Высокопроизводительные сети для доставки содержимого и локальные серверы кэширования обеспечивают минимальное время задержки во время проверки. Клиент-серверная архитектура обеспечивает мгновенную защиту и позволяет устранить необходимость развертывания вирусной базы данных, в то же время сокращая объем клиента.

Для использования службы репутации файлов агенты Security Agent должны работать в режиме интеллектуального сканирования Smart Scan. Такие агенты в этом руководстве называются **агентами Smart Scan**. Агенты, не работающие в режиме smart scan, не используют службы File Reputation и называются **агентами обычного сканирования**. Администраторы Worry-Free Business Security могут настроить режим smart scan для всех или нескольких агентов.

Службы Web Reputation

Технология Web Reputation Trend Micro, в основе которой используется одна из крупнейших в мире баз данных со сведениями о репутации доменов, отслеживает надежность доменов, присваивая им баллы на основании таких факторов, как возраст веб-сайта, изменение расположения сайта на протяжении его существования и сведения о

подозрительных действиях, обнаруженных в ходе анализа вредоносного поведения. Служба Web Reputation сканирует сайты и блокирует доступ пользователей к зараженным страницам. Служба Web Reputation помогает убедиться в том, что посещаемые пользователями страницы безопасны и не содержат таких веб-угроз, как вредоносные, шпионские программы и фишинг, предназначенные для получения от пользователей личной информации обманным путем. Для достижения большей точности и сокращения количества ложных тревог она позволяет оценивать репутацию определенных страниц или ссылок на сайтах вместо классифицирования или блокировки всего сайта, так как часто доверенные сайты взламываются частично, вследствие чего репутация со временем может меняться.

Агенты, к которым применяется политика репутации веб-сайтов, используют службы Web Reputation. Администраторы Worry-Free Business Security могут применить политики Web Reputation ко всем или нескольким агентам.

Email Reputation (только Advanced)

Технология Email Reputation компании Trend Micro проверяет IP-адреса по базе данных репутации, содержащей сведения об известных источниках спама, и с помощью динамической службы оценивает репутацию отправителя в режиме реального времени. Уровни репутации определяются путем последовательного анализа поведения IP-адресов, набора действий и предшествующей истории. Вредоносные сообщения электронной почты блокируются на удаленном сервере на основании данных об IP-адресе отправителя, что предотвращает их попадание в сеть или на компьютер пользователя.

Технология Email Reputation позволяет распознавать спам на основе данных о репутации исходного транспортного агента электронной почты (MTA). Это приводит к выгрузке задания с сервера Security Server. При использовании технологии Email Reputation весь входящий трафик SMTP проверяется по базам данных IP-адресов; при этом выясняется, чист ли исходный IP-адрес и не помещен ли он в список известных источников спама.

Существует два режима работы службы Email Reputation:

- **Стандартный**:Стандартный уровень использует базу данных, отслеживающую репутацию около 2 млрд. IP-адресов. IP-адреса, которые несколько раз оказались связаны с рассылкой нежелательной почты, вносятся в эту базу данных и редко из нее удаляются.
- **Расширенный**: Расширенный уровень службы — служба на основе запросов DNS наподобие стандартной службы. Ядром этой службы является стандартная база данных репутации, используемая совместно с динамически определяемой репутацией — базой данных реального времени, которая блокирует сообщения из известных и подозреваемых источников спама.

При обнаружении сообщения с заблокированного или подозрительного IP-адреса Email Reputation Services (ERS) блокируют это сообщение до того, как оно достигнет шлюза. Если Email Reputation блокирует сообщения с IP-адреса, который вы считаете безопасным, добавьте этот IP-адрес в список разрешенных IP-адресов.

Smart Feedback

Модуль Trend Micro Smart Feedback обеспечивает ежедневный круглосуточный обмен данными между продуктами Trend Micro, а также центрами и технологиями исследования угроз. Каждая новая угроза, найденная на пользовательском компьютере во время обычной проверки, обновляет все базы данных угроз Trend Micro, защищая других пользователей от этой угрозы в дальнейшем.

Постоянно обрабатывая угрозы, собранные с помощью обширной глобальной сети клиентов и партнеров, Trend Micro в режиме реального времени предоставляет автоматическую защиту от самых последних угроз безопасности и обеспечивает совместную защиту. Это своего рода аналог программы взаимопомощи, когда членов коллектива защищает весь коллектив. Конфиденциальность личных или коммерческих данных клиентов постоянно защищена благодаря тому, что собираемая информация об угрозах учитывает репутацию

источника подключения, а не только содержимое определенного сообщения.

Вот несколько примеров данных, отправляемых в Trend Micro:

- контрольные суммы файлов;
- веб-сайты, к которым был осуществлен доступ;
- сведения о файле, включая размеры и пути;
- имена исполняемых файлов.

Участие в программе можно остановить в любой момент с помощью веб-консоли.

Для получения дополнительных сведений см. *Участие в программе обратной связи Smart Feedback Program на странице 13-7*.

Совет

Для защиты локальных компьютеров необязательно участвовать в программе Smart Feedback. Участие исключительно добровольное и может быть прервано в любое время. Компания Trend Micro рекомендует участвовать в программе Smart Feedback, чтобы помочь обеспечить комплексную защиту всем клиентам Trend Micro.

Для получения дополнительных сведений о программе Smart Protection Network посетите веб-сайт:

http://www.trendmicro.com.ru/technology-innovation/our-tech/smart-protection-network/index.html

Фильтрация URL-адресов

Фильтрация URL-адресов помогает контролировать доступ к веб-сайтам, тем самым сокращая непродуктивное время сотрудников, уменьшая использование полосы пропускания и создавая более безопасную рабочую Интернет-среду. Можно выбрать уровень защиты фильтрацией URL-адресов или задать нужные типы файлов.

Преимущества защиты

В приведенной ниже таблице перечислены различные компоненты Worry-Free Business Security и выполняемые ими функции по защите компьютеров от угроз.

Таблица 1-1. Преимущества защиты

Угроза	Защита
Вирусы/Вредоносные программы. Вирусы, «троянские кони», черви, «черные ходы» и руткиты **Шпионские и нежелательные программы**. «Шпионские» программы, программы набора номера, хакерские инструменты, приложения для взлома паролей, рекламные программы, программы-шутки и программы перехвата нажатий клавиш	Сканирование файлов («Сканирование в режиме реального времени», «Сканирование вручную», «Сканирование по расписанию»)
Угрозы безопасности, передаваемые через сообщения электронной почты	**Сканирование почты POP3** в Security Agent
Сетевые черви/вирусы и проникновения	Брандмауэр в Security Agent
Предположительно вредоносные веб-сайты и фишинг-сайты	Служба Web Reputation и фильтрация URL-адресов в Security Agent
Угрозы, распространяющиеся через USB-устройства и другие внешние устройства	Управление устройствами в Security Agent
Вредоносные действия	Контроль действий в Security Agent
ПО для вымогательства, которое направлено на документы, запущенные на оконечных устройствах	Контроль действий и Прогнозное машинное самообучение в агенте Security Agent

Сведения об угрозах

Организации без выделенных сотрудников службы безопасности и с мягкими политиками безопасности все чаще подвергаются угрозам, даже если они имеют базовую инфраструктуру безопасности. Даже если угрозы были обнаружены, они, возможно, уже распространились на многие вычислительные ресурсы, и требуют значительного количества времени и усилий для полного устранения. Непредвиденные расходы, связанные с устранением угроз, также могут быть очень большими.

Служба безопасности сети и облачные серверы Trend Micro, которые являются частью сети Trend Micro Smart Protection Network, выявляют следующее поколение угроз и помогают их устранить.

Вирусы/вредоносные программы

На данный момент существуют десятки тысяч вирусов/вредоносных программ, и каждый день создаются новые. Когда-то наиболее распространенные в DOS или Windows, в настоящее время компьютерные вирусы могут нанести серьезный урон корпоративным сетям, системам электронной почты и веб-сайтам, используя различного рода уязвимости.

- **Программа-шутка**: вирусоподобная программа, перехватывающая управление над некоторыми элементами оформления рабочего стола.
- **Вероятный вирус/ вредоносная программа**: подозрительные файлы, которые по своим характеристикам похожи на вирусы или вредоносные программы. Для получения подробных сведений см. энциклопедию угроз Trend Micro.

  http://about-threats.trendmicro.com/threatencyclopedia.aspx
- **Руткиты**: Программа (или набор программ), которая устанавливает и запускает код в системе незаметно для пользователя. Чтобы поддерживать постоянное и необнаруженное

присутствие на компьютере, она использует различные уловки. Руткиты не заражают машины, а, скорее, стремятся обеспечить необнаруженную среду для выполнения вредоносного кода. Руткиты устанавливаются на системы с помощью социального инжиниринга, после выполнения вредоносной программы или просто во время просмотра вредоносного веб-сайта. После установки программа может виртуально выполнять любую функцию в системе, чтобы включить удаленный доступ и подслушивание, а также скрывать процессы, файлы, ключи реестра и каналы связи.

- **«Троянский конь»**: Этот тип угроз часто использует порт, чтобы получить доступ к компьютерам или исполняемым программам. «Троянские кони» не копируют себя, но вместо этого постоянно находятся в системе для выполнения потенциально опасных действий, таких как открытие портов для доступа хакеров. Традиционные антивирусные решения могут обнаруживать и удалять вирусы, но не «троянские кони», особенно если те уже работают в системе.
- **Вирус**: программа, способная самовоспроизводиться. Для этого нужно, чтобы вирус был прикреплен к какой-либо программе. В результате он будет автоматически выполняться во время запуска этой программы, включая:
  - **Вредоносный код ActiveX**: Код, находящийся на веб-странице, содержащей элементы управления ActiveX™.
  - **Загрузочный вирус**: Вирус, заражающий загрузочный сектор раздела или диска.
  - **Вирусы файлов .com и .exe**: Исполняемая программа с расширением `.com` или `.exe`.
  - **Вредоносный код Java**: Не зависящий от операционной системы вирусный код, написанный на Java™ или встроенный в Java-приложения.
  - **Макровирус**: Разновидность вируса, написанного как макрос для определенного приложения и зачастую встроенного в документ.

- **Упаковщик**: Сжатая и/или зашифрованная исполняемая программа под Windows или Linux™, часто являющаяся «троянским конем». Сжатие исполняемого кода затрудняет определение упаковщика антивирусными программами.
- **Тестовый вирус**: Инертный файл, ведущий себя как настоящий вирус и обнаруживаемый при проверке на вирусы. Правильность работы установленного антивируса можно проверить с помощью тестовых вирусов (например EICAR).
- **Вирусы HTML**, **VBScript** или **JavaScript**: Вирус, находящийся на веб-страницах и загружаемый через браузер.
- **Червь**: Автономная программа (или группа программ), заражающая своими копиями или фрагментами другие компьютеры. Зачастую заражение происходит через сообщение электронной почты.
- **Другие**: Вирусы/вредоносные программы, которые невозможно отнести ни к одному из существующих типов.

Шпионские и нежелательные программы

Безопасность Локальные компьютеры может пострадать не только от вирусов и вредоносного ПО, но и от других потенциальных угроз. Шпионские и нежелательные программы относятся к приложениям или файлам, которые не расцениваются как вирусы или троянские программы, однако могут отрицательно сказаться на производительности клиенты в сети, а также повлечь за собой потерю конфиденциальной информации компании и юридические проблемы. Шпионские и нежелательные программы часто выполняют действия, ставящие под угрозу безопасность и мешающие работать пользователю, такие как отображение раздражающих всплывающих окон, запись нажатых клавиш, а также делают клиент уязвимым для различных атак.

Если вы считаете, что какой-либо файл является нежелательной программой, но Worry-Free Business Security не обнаруживает в нем

ничего подозрительного, отправьте его для анализа в компанию Trend Micro:

https://success.trendmicro.com/solution/1059565

Тип	Описание
Шпионские программы	Собирают данные, например, имена пользователей и пароли, и передают их третьим лицам.
Рекламные программы	отображают рекламные сообщения, а также собирают различную информацию, например, данные по часто посещаемым веб-сайтам. Как правило, затем эта информация используется в рекламных целях.
Программа дозвона	изменяет клиентские параметры соединения клиент с Интернетом и может принудительно настроить клиент на набор предварительно заданных телефонных номеров через модем. Как правило, такие программы используют номера, вызовы по которым оплачиваются, или международные номера, что может привести к дополнительным затратам организации.
Программа-шутка	вызывает нештатное поведение системы клиент, например, открытие и закрытие дисковода CD-ROM и выведение на экран множества окон с сообщениями.
Хакерский инструмент	используются хакерами для проникновения в систему.
Программы для удаленного доступа	используются хакерами для проникновения и удаленного управления компьютером.
Приложения для взлома паролей	используются хакерами для расшифровки имени пользователя и пароля к учетной записи.
Прочие	другие типы потенциально вредоносных программ.

Спам

Спам — нежелательные сообщения электронной почты, как правило, коммерческого характера, массово отправляемые по спискам рассылки, в группы новостей или конечным адресатам. Различают два

вида спама: нежелательные коммерческие электронные сообщения и массовые рассылки.

Проникновения

Проникновением называется вход в сеть или на клиенты с применением силы или без разрешения. Оно подразумевает обход механизма защиты сети или клиент.

Вредоносные действия

Злонамеренными действиями называются несанкционированные изменения, вносимые программой в операционную систему, системный реестр, в другие программы, а также файлы и папки.

Фальшивые точки доступа

Фальшивые точки доступа, известные также под названием Evil Twin («злой двойник») — мошеннические точки доступа, выдаваемые за законные, но предназначенные для подслушивания беспроводных подключений.

Фишинг

Фишинг — быстро распространяющаяся форма мошенничества, суть которого сводится к выведыванию персональных данных у доверчивых пользователей путем имитации легального сайта.

Согласно стандартному сценарию доверчивый пользователь получает срочное сообщение о проблемах с его учетной записью, которую необходимо немедленно исправить, иначе она будет закрыта. В сообщении содержится URL-адрес веб-сайта, вид которого не вызывает сомнений. Не составляет труда скопировать настоящее письмо и настоящий сайт, а затем изменить небольшой фрагмент, который и определяет реального получателя данных

В сообщении пользователю рекомендуется зайти на сайт и подтвердить некоторые данные учетной записи. В результате в распоряжении хакера оказывается информация, введенная пользователем: имя пользователя, пароль, номер кредитной карты или номер социального страхования.

Фишинг — быстрый, дешевый и легкий, а потому распространенный способ мошенничества. Кроме того, он может оказаться весьма прибыльным. Распознать фишинг очень сложно даже грамотным пользователям. Так же сложно отыскать следы мошенничества органам правопорядка, более того, это почти невозможно.

Сообщайте компании Trend Micro обо всех сайтах, которые вызывают подозрения в фишинге. Дополнительную информацию см. в разделе *Отправка подозрительного содержимого в компанию Trend Micro на странице C-5*.

Массовые почтовые атаки

Почтовые вирусы и вредоносное ПО имеют способность распространяться по электронной почте, используя в автоматическом режиме клиент электронной почты на зараженном компьютере или путем самостоятельного распространения вируса/вредоносного ПО. В случае массовых почтовых рассылок инфекция быстро распространяется между клиентскими компьютерами и серверами в среде Microsoft Exchange. Компанией Trend Micro разработан модуль сканирования, который обнаруживает действия, обычно проявляющиеся при массовых почтовых атаках. Эти действия содержатся в файле вирусной базы данных, который обновляется с помощью серверов Trend Micro ActiveUpdate.

Можно настроить агент Messaging Security Agent (только Advanced) таким образом, чтобы всякий раз при выявлении признаков массовой почтовой рассылки принимались специальные меры по борьбе с атаками типа «массовая почтовая рассылка». Действия по массовым почтовым атакам имеют приоритет над всеми остальными действиями. Действием по умолчанию против массовых почтовых атак является удаление всего сообщения.

Это может произойти в следующих случаях. настройте Messaging Security Agent для перемещения сообщений в папку карантина в случае, если они инфицированы червем или «троянским конем». Также можно включить распознавание массовых почтовых атак и настроить агент на удаление всех сообщений, демонстрирующих поведение, характерное для этих атак. Агент получает сообщение, содержащее червя, например, модификацию червя MyDoom. Этот червь использует собственный модуль SMTP для рассылки своей копии по адресам электронной почты, собранным на зараженном компьютере. Когда агент обнаруживает червя MyDoom и его массовую почтовую рассылку, он удаляет все сообщения электронной почты, содержащие червя. Для червей, не рассылающих массовых писем, применяется действие «Поместить на карантин».

Веб-угрозы

К веб-угрозам относится широкий ряд угроз, которые происходят из Интернета. Принцип работы веб-угроз довольно сложен. В них используются комбинации различных файлов и технологий, а не какой-либо один файл или метод. Например, создатели веб-угроз постоянно изменяют используемую версию или вариант угрозы. Поскольку веб-угроза находится в определенном расположении на веб-сайте, а не на зараженном компьютере клиент, создатель веб-угрозы постоянно изменяет ее код, чтобы избежать обнаружения.

Для обозначения лиц, ранее называвшихся хакерами, создателями вирусов, спамерами и разработчиками шпионских программ, в последние годы используется термин «киберпреступники». При помощи веб-угроз такие лица преследуют одну из двух целей. Первой целью является похищение информации для последующей продажи. Следствием таких действий является утечка конфиденциальной информации в форме потери идентификации. Кроме того, зараженный компьютер клиент может становиться направлением для проведения фишинг-атаки или других действий по захвату информации. Среди прочих воздействий эта угроза обладает потенциалом к снижению уверенности в сфере веб-коммерции, что приводит к подрыву доверия, необходимого для проведения операций

в Интернете. Вторая цель — это превращение мощности ЦП пользовательского компьютера в инструмент для выполнения действий, приносящих прибыль. К таким видам деятельности относятся спам, вымогательство в форме распространения атак типа «отказ в обслуживании» или деятельность в сфере «оплаты за щелчок мышью» (pay-per-click).

Глава 2

Начало работы

В этой главе рассказывается, как начать работу с Worry-Free Business Security.

Сеть Worry-Free Business Security

Worry-Free Business Security включает следующее:

- *Security Server на странице 2-2*
- *Агенты на странице 2-4*
- *Веб-консоль на странице 2-4*

Security Server

В основе решения Worry-Free Business Security находится сервер Security Server. На сервере Security Server находится веб-консоль для централизованного управления Worry-Free Business Security. Сервер Security Server устанавливает агенты на клиенты сети и формирует с ними отношения «агент-сервер». Сервер Security Server позволяет просматривать агентов и информацию о состоянии безопасности сети, настраивать системную безопасность и централизованно загружать компоненты. Кроме этого, Security Server содержит базу данных, в которой хранятся журналы обнаруженных Интернет-угроз, о которых сообщают агенты.

Security Server выполняет следующие важные функции:

- устанавливает, контролирует и управляет агентами в сети;
- загружает необходимые клиентам компоненты. По умолчанию сервер Security Server загружает компоненты с сервера Trend Micro ActiveUpdate, а затем распространяет их для агентов.

Scan Server

Сервер Security Server включает в себя службу под названием Scan Server, которая автоматически устанавливается во время установки Security Server. Таким образом, нет необходимости устанавливать ее отдельно. В консоли управления (MMC) Scan Server выполняется как

процесс `iCRCService.exe` и отображается как служба **Trend Micro Smart Scan Service**.

Когда агенты Security Agent используют метод сканирования под названием **Smart Scan**, Scan Server помогает этим агентам выполнять сканирование более эффективно. Процесс Smart Scan можно описать следующим образом.

- Агент Security Agent сканирует клиентскую систему на наличие угроз безопасности, используя **базу данных агента Smart Scan**, которая является облегченной версией традиционной вирусной базы данных. База данных агента Smart Scan включает большую часть сигнатур угроз, содержащихся в вирусной базе данных.
- Агент Security Agent, который не может определить степень опасности файла во время сканирования, проверяет ее, отправляя запрос сканирования на сервер Scan Server. Scan Server подтверждает опасность, используя **вирусную базу данных Smart Scan**, которая содержит сигнатуры угроз, недоступные в базе данных агента Smart Scan.
- Security Agent «кэширует» результат запроса сканирования, таким образом позволяя Scan Server улучшить производительность сканирования.

Размещение некоторых сигнатур угроз на сервере Scan Server позволяет увеличить пропускную способность агентов Security Agent для загрузки компонентов. Вместо загрузки вирусной базы данных агенты Security Agent загружают базу данных агента Smart Scan, которая значительно меньше по размеру.

Если агентам Security Agent не удается подключиться к Scan Server, они отправляют запросы сканирования в систему Trend Micro Smart Protection Network, которая имеет те же функции, что и Scan Server.

Удаление Scan Server отдельно от Security Server невозможно. Если вы не хотите использовать Scan Server, выполните следующие действия.

1. Откройте консоль управления (MMC) на компьютере с установленным сервером Security Server и отключите службу **Trend Micro Smart Scan Service**.

2. На веб-консоли переключите агент Security Agent на обычное сканирование, перейдя на вкладку **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер** и выбрав параметр **Отключить службу Smart Scan**.

Агенты

Агенты защищают клиентские системы от угроз безопасности. К клиентским системам относятся рабочие станции, серверы и серверы Microsoft Exchange. Агентами Worry-Free Business Security являются:

Таблица 2-1. Агенты Worry-Free Business Security

Агент	Описание
Security Agent	Защищает рабочие станции и серверы от угроз безопасности и вторжений
Агент Messaging Security Agent (только Advanced)	Защищает серверы Microsoft Exchange от угроз, связанных с электронной почтой

Агент отправляет отчеты на сервер Security Server, с которого он был установлен. Для предоставления серверу Security Server актуальной информации о клиентской системе агент отправляет серверу данные о событиях в режиме реального времени. Агент сообщает о событиях, например об обнаружении угрозы, загрузке и выключении, начале сканирования и завершении обновления.

Веб-консоль

Веб-консоль является центральной точкой контроля агентов Security Agent в корпоративной сети. Эта консоль содержит набор параметров и значений по умолчанию, которые можно изменять в зависимости от требований безопасности и спецификаций. Веб-консоль использует стандартные интернет-технологии, такие как Java, CGI, HTML и HTTP.

Используйте веб-консоль для:

- Развертывания агентов на локальные компьютеры;
- Объединения агентов в логические группы для одновременной настройки и управления;
- Настройки параметров продукта и запуска сканирования вручную на локальных компьютерах;
- Получения уведомлений и просмотр сообщений журнала о представляющей потенциальную угрозу активности;
- Получения уведомлений и отправки предупреждений об эпидемиях по электронной почте при обнаружении угроз на локальных компьютерах.

Открытие веб-консоли

Веб-консоль можно открыть с помощью поддерживаемого веб-браузера на любом локальном компьютере в сети. Подробные сведения о требованиях к браузеру см. в документе *Требования к системе*.

Процедура

1. Выберите один из следующих вариантов открытия веб-консоли.
   - На локальном компьютере, на котором размещен сервер Security Server, перейдите к рабочему столу и щелкните ярлык Worry-Free Business Security.
   - На локальном компьютере, на котором размещен сервер Security Server, откройте **меню Windows «Пуск»** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.
   - На подключенном к сети локальном компьютере запустите веб-браузер и введите в адресной строке:

     `https://{имя_сервера_безопасности или IP-адрес}:{номер порта}/SMB`

     Это может произойти в следующих случаях.

`https://my-test-server:4343/SMB`

`https://192.168.0.10:4343/SMB`

`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

Совет

Если не используется SSL, введите `http` вместо `https`. При подключении по протоколу HTTP по умолчанию используется порт 8059, а при подключении по протоколу HTTPS — 4343.

Если в среде не поддерживается разрешение имен DNS, вместо IP-адреса используйте имя сервера.

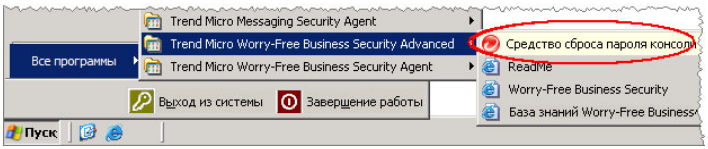
В браузере откроется окно входа в Worry-Free Business Security.

2. Введите пароль и нажмите кнопку **Вход в систему**.

   В браузере откроется окно **Текущее состояние**.

После выполнения

Если вы не можете получить доступ к веб-консоли, проверьте следующие параметры.

Элемент для проверки	Подробнее
Пароль	Если вы забыли свой пароль, можно воспользоваться средством сброса пароля консоли. Для этого на сервере Security Server выберите соответствующий пункт в папке Trend Micro Worry-Free Business Security в меню Windows «Пуск». 

Элемент для проверки	Подробнее
Кэш браузера	Если обновление было выполнено с предыдущей версии Worry-Free Business Security, кэш-файлы веб-браузера и прокси-сервера могут препятствовать загрузке веб-консоли. Очистите кэш-память браузера и всех прокси-серверов, находящихся между сервером Trend Micro Security Server и локальным компьютером, который вы используете для доступа к веб-консоли.
Сертификат SSL	Проверьте, правильно ли функционирует веб-сервер. При использовании SSL убедитесь в том, что сертификат все еще действует. Дополнительную информацию см. в документации по веб-серверу.

Элемент для проверки	Подробнее

Параметры виртуального каталога	При запуске веб-консоли на сервере IIS может произойти ошибка параметров виртуального каталога.
	
	`Появится следующее сообщение:`
	
	`Невозможно отобразить страницу Ошибка HTTP 403.1 — Запрещено:выполнение запрещено.`
	
	`Информационные службы Интернет (IIS)`
	
	Это сообщение может появиться при попытке доступа к консоли с одного из следующих адресов:
	
	`http://{имя сервера}/SMB/`
	
	`http://{имя сервера}/SMB/default.htm`
	
	При этом консоль может без каких-либо проблем открываться с адреса:
	
	`http://{имя сервера}/SMB/console/html/cgi/cgichkmasterpwd.exe`
	
	Для устранения проблемы проверьте права на исполнение для виртуального каталога SMB.
	
	Для включения сценариев выполните следующие действия.
	
	1. Откройте диспетчер Internet Information Services (IIS).
	
	2. В виртуальном каталоге SMB выберите пункт **«Свойства»**.
	
	3. Откройте вкладку «Виртуальный каталог» и установите права на исполнение Сценарии вместо нет. Кроме того, измените права на исполнение для виртуального каталога установки клиента.

Навигация по веб-консоли

Веб-консоль состоит из следующих основных разделов:

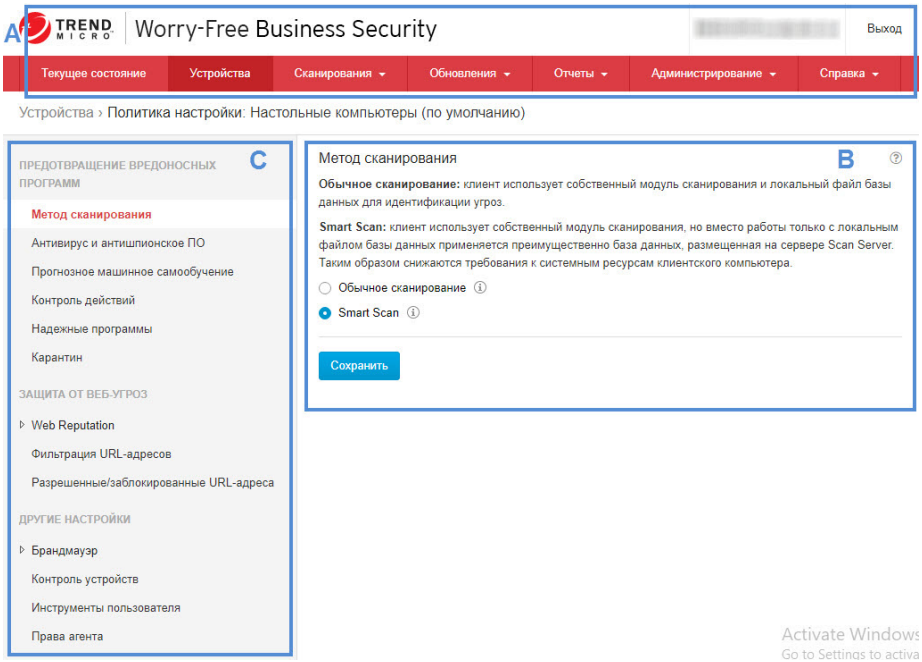


Таблица 2-2. Основные разделы веб-консоли

Раздел	Описание
A. Главное меню	В верхней части веб-консоли находится главное меню. Также отображается ссылка **Выход**, позволяющая завершить текущую сессию.
B. Область настройки	Под главным меню располагается область настройки. Здесь можно настроить параметры и задать значения для выбранного пункта меню.

Раздел	Описание
C. Боковое меню (доступно не во всех окнах)	Если выбрать группу агента Security Agent в окне **Устройства** и нажать кнопку **Политика настройки**, отобразится боковое меню. Оно позволяет настроить параметры безопасности и режимов сканирования для настольных ПК и серверов, которые принадлежат к этой группе. Если в окне **Устройства** выбрать Messaging Security Agent (только Advanced), в боковом меню можно настроить параметры безопасности и режимы сканирования для серверов Microsoft Exchange Server.

Таблица 2-3. Раздел главного меню

Пункт меню	Описание
Текущее состояние	Контроль общего состояния функций защиты агентов Security Agent, а также рабочего состояния сервера Security Server.
Устройства	• Можно настраивать параметры защиты для агентов • Дублировать параметры для групп
Сканирование	• Сканирование локальных компьютеров на предмет угроз. • Расписание сканирования для клиентских компьютеров можно настраивать.
Обновления	• Можно проверять сервер Trend Micro ActiveUpdate (или настроенный источник обновлений) на наличие последних обновлений, включая обновления вирусной базы данных, модуля сканирования, компонентов лечения и программы агента. • Источник обновлений можно выбирать. • Можно назначать агенты Security Agent агентами обновления.
Отчеты	Создание отчетов для отслеживания угроз и других событий, связанных с безопасностью

Пункт меню	Описание
Администрирование	• Можно настроить программу так, чтобы она рассылала уведомления о нештатных событиях, связанных с вирусными угрозами. • Для упрощения работы можно создавать глобальные параметры. • Инструменты управления позволяют управлять безопасностью в сети и на клиентских компьютерах. • Ознакомьтесь со сведениями о лицензии, сохраните пароль администратора и помогите поддерживать безопасность обмена электронной информацией — присоединитесь к программе Smart Feedback. • Настройте автоматическое обновление продукта и уведомление пользователей о выпуске нового пакета обновления.
Справка	• Воспользуйтесь возможностью поиска определенных данных и тем • Просмотрите руководство администратора • Получите последнюю информацию из базы знаний • Просмотрите данные о безопасности, продажах, поддержке и версии программы

Значки веб-консоли

В следующей таблице описаны значки веб-консоли.

Таблица 2-4. Значки веб-консоли

Значок	Описание
	Значок «Справка». При нажатии открывается интерактивная справка.
	Значок «Обновить». При нажатии выполняется обновление текущей страницы.

Значок	Описание
	Значок «Развернуть или свернуть раздел». При нажатии отображаются или скрываются разделы. Разделы можно разворачивать только по одному.
	Значок «Информация». При нажатии отображаются сведения об определенном элементе.
	Значок «Настройка уведомлений». Отображает различные параметры уведомлений.

Глава 3

Установка агентов

В этой главе описаны шаги, необходимые для установки агентов Security Agent и Messaging Security Agent (только Advanced). В ней также рассказывается о способах удаления этих агентов.

Установка Security Agent

Выполните новую установку агента Security Agent на клиентские системы Windows (рабочие станции и серверы). Используйте наиболее подходящий для вас тип установки.

Перед началом установки Security Agent закройте все запущенные на клиентах программы. Процесс может затянуться, если во время установки будут запущены другие приложения.

Примечание

Для получения сведений об обновлении агентов Security Agent до данной версии, см. *Руководство по установке и обновлению*.

Требования к установке Security Agent

Чтобы просмотреть полный список требований к установке и совместимых сторонних продуктов, посетите следующий веб-сайт:

http://docs.trendmicro.com/ru-ru/smb/worry-free-business-security.aspx

Условия установки Security Agent

Перед установкой Security Agent примите во внимание следующее.

- **Функции агента.** Некоторые функции Security Agent не доступны в некоторых системах Windows. Для получения дополнительных сведений см. *Доступные функции Security Agent на странице 3-3*.
- **64-разрядные системы**:Существует упрощенная версия Security Agent для 64-разрядных систем. Однако поддержка для платформ IA-64 в настоящее время не предоставляется.
- **Поддержка IPv6**. Security Agent может быть установлен на клиенты с двойным стеком или локальные компьютеры, имеющие только адрес IPv6. Однако для некоторых способов установки могут быть конкретные требования.

Для получения дополнительных сведений см. *Установка Security Agent и поддержка адреса IPv6 на странице 3-5*.

- **Списки исключений**: Убедитесь, что списки исключений для следующих функций были настроены должным образом.
  - **Контроль действий**:добавьте критически важные приложения клиентов в список одобренных программ, чтобы запретить агенту Security Agent блокировать эти приложения. Дополнительные сведения см. в разделе *Настройка контроля действий на странице 5-13*.
  - **Web Reputation**: добавьте сайты, которые вы считаете безопасными, в список одобренных URL-адресов, чтобы запретить агенту Security Agent блокировать доступ к этим сайтам. Дополнительные сведения см. в разделе *Настройка службы Web Reputation для агентов Messaging Security Agent на странице 5-25*.
- **Папка установки агента**: во время установки сервера Security Server программа установки предложит вам указать папку установки агента, которой по умолчанию является `$ProgramFiles\Trend Micro\Security Agent`. Если вы хотите установить Security Agent в другую папку, укажите ее в разделе **Администрирование** > **Глобальные параметры** > **Система** > **Установка Security Agent**.

Доступные функции Security Agent

Функции агента Security Agent, доступные на клиентском компьютере, зависят от операционной системы. Учитывайте неподдерживаемые функции при установке агента на конкретную операционную систему.

Таблица 3-1. Функции Security Agent

Объект	Операционная система Windows		
	10	Протокол SBS 2011	Server 2012/2012 R2/2016/2019
Сканирование вручную (стандартное и глубокое), сканирование в режиме реального времени и сканирование по расписанию	Да	Да	Да
Брандмауэр	Да	Да	Да
Web Reputation	Да	Да	Да
Фильтрация URL-адресов	Да	Да	Да
Контроль действий	Да	Да	Да
Контроль устройств	Да	Да	Да
Службы Damage Cleanup Services	Да	Да	Да
Сканирование почты (POP3)	Да	Да	Да
Обновления вручную и по расписанию	Да	Да	Да
Агент обновления	Да	Да	Да
Plug-in Manager для агентов	Да	Да	Да
Smart Feedback	Да	Да	Да

Объект	Операционная система Windows		
	10	Протокол SBS 2011	Server 2012/2012 R2/2016/2019
панель инструментов защиты от спама Trend Micro;	Да Поддерживаемые почтовые клиенты (32- и 64-разрядные версии): • Outlook 2010 • Outlook 2013 • Outlook 2016	Нет	Нет
HouseCall	Да	Да	Да
Инструмент Case Diagnostic Tool	Да	Да	Да
Мастер Wi-Fi	Да	Нет	Нет

Установка Security Agent и поддержка адреса IPv6

В этом разделе рассматриваются условия установки Security Agent на клиентские компьютеры с двойным стеком или только с адресом IPv6.

Операционная система

Security Agent может быть установлен только на следующие операционные системы, поддерживающие адреса IPv6:

- Windows SBS 2011
- Windows 10 (все версии)
- Windows Server 2012/2012 R2 (все версии)
- Windows Server 2016 (Standard, Datacenter, Essentials)

- Windows Server 2019 (Standard, Datacenter, Essentials)

Для получения полного списка системных требований посетите следующий веб-сайт:

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

Поддерживаемые способы установки

Для установки агента Security Agent на клиентские компьютеры с двойным стеком или только с адресом IPv6 можно использовать любые доступные способы. Для некоторых способов установки существуют специальные требования для успешной установки агента Security Agent.

Таблица 3-2. Способы установки и поддержка IPv6

Способ установки	Требования/условия
Установка с внутренней веб-страницы и установка с помощью почтового уведомления	При установке на клиент, имеющий только адрес IPv6, сервер Security Server должен иметь двойной стек или только адрес IPv6, а его имя или адресаIPv6 должны быть частью URL-адреса. В случае клиентов с двойным стеком адреса IPv6, которые отображаются в окне состояния установки, зависят от выбора параметра в разделе **Предпочтительный IP-адрес** на вкладке **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер**.
Сканер уязвимостей и удаленная установка	Сервер Security Server, не имеющий адреса IPv6, не может установить агент Security Agent на клиентские компьютеры, имеющие только адрес IPv4. Аналогичным образом, Security Server с адресом IPv4 не может установить агент Security Agent на клиентские компьютеры с адресом IPv6.

IP-адреса агентов Security Agent

Security Server, установленный в среде, которая поддерживает адресацию IPv6, может управлять следующими агентами Security Agent.

- Security Server, установленный на клиент с адресом IPv6, может управлять агентами Security Agent с адресом IPv6.

- Security Server, установленный на клиент с двойным стеком, которому были назначены как IPv4, так и IPv6-адреса, может управлять агентами Security Agent с двойным стеком или с адресами IPv6 и IPv4.

После установки или обновления агенты Security Agent регистрируются на Security Server, используя IP-адрес.

- Агенты Security Agent, имеющие только адрес IPv6, регистрируются, используя свой адрес IPv6.
- Агенты Security Agent, имеющие только адрес IPv4, регистрируются, используя свой адрес IPv4.
- Агенты Security Agent с двойным стеком регистрируются, используя свой адрес IPv4 или IPv6. Вы можете выбрать IP-адрес, который будут использовать эти агенты, в разделе **Предпочтительный IP-адрес** на вкладке **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер**.

Способы установки Security Agent

В данном разделе приводится обзор различных способов новой установки Security Agent. Все способы установки предполагают обладание локальными правами администратора на целевых локальных компьютерах.

Если при установке Security Agent вы хотите включить поддержку IPv6, см. *Установка Security Agent и поддержка адреса IPv6 на странице 3-5*.

Таблица 3-3. Способы установки

Способ установки/ Поддержка операционной системы	Условия развертывания					
	Развертывание WAN	С централизованным управлением	Требующее вмешательства пользователя	Использующее ИТ-ресурсы	Массовое развертывание	Загрузка линий связи
Внутренняя веб-страница Поддерживается на всех ОС	Да	Да	Да	Нет	Нет	Низкая, если действие запланировано
Уведомление по электронной почте Поддерживается на всех ОС	Да	Да	Да	Нет	Нет	Высокая, если процессы установки запускаются одновременно
Удаленная установка Поддерживается на всех ОС	Нет	Да	Нет	Да	Да	Низкая, если действие запланировано
Настройка сценария входа в сеть Поддерживается на всех ОС	Нет	Да	Нет	Да	Да	Высокая, если процессы установки запускаются одновременно

Способ установки/ Поддержка операционной системы	Условия развертывания					
	Развертывание WAN	С централизованным управлением	Требующее вмешательства пользователя	Использующее ИТ-ресурсы	Массовое развертывание	Загрузка линий связи
Client Packager Поддерживается на всех ОС	Да	Нет	Да	Да	Нет	Низкая, если действие запланировано
Trend Micro Vulnerability Scanner (TMVS) Поддерживается на всех ОС, за исключением Windows 10	Нет	Да	Нет	Да	Да	Низкая, если действие запланировано

В случае единичного развертывания и в организациях со строгими ИТ-политиками ИТ-администраторы могут выбрать развертывание с помощью **удаленной установки** или утилиты **настройки сценариев входа в сеть**.

В организациях, где политики ИТ-безопасности выполняются не так строго, компания Trend Micro рекомендует устанавливать Security Agent с помощью **внутренней веб-страницы**. Использование этого метода требует предоставления конечным пользователям, устанавливающим Security Agent, прав администратора.

Применение **удаленной установки** эффективно в сетях с поддержкой Active Directory. Если в сети не используется служба каталогов Active Directory, следует остановиться на установке с использованием внутренней веб-страницы.

Установка с внутренней веб-страницы

Перед выполнением

Для установки с внутренней веб-страницы требуется следующее.

Элемент для проверки	Требование
Security Server	Security Server должен быть установлен в системах: • Windows 7, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 или SBS 2008, 2011 • с сервером Internet Information Server (IIS) 7.0, 7.5, 8.0, 8.5, 10 или Apache 2.4
Целевой локальный компьютер	• Целевой локальный компьютер должен быть установлен в Windows 10, Server 2012, 2012 R2, 2016, 2019 или SBS 2011. • На целевом локальном компьютере должен быть установлен Internet Explorer 9.0 или более поздней версии. • При входе в систему локального компьютера пользователи должны использовать учетную запись с правами администратора. **Примечание** Если целевой локальный компьютер работает под управлением настольной операционной системы, сначала включите встроенную учетную запись администратора. Для получения дополнительной информации посетите сайт поддержки Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Элемент для проверки	Требование
Настройки безопасности Internet Explorer	Пользователи должны выполнить следующие действия. 1. Запустите Internet Explorer и добавьте URL-адрес Security Server (например, `https://<имя сервера безопасности>:4343/SMB/console/html/client`) в список надежных узлов. Чтобы открыть список, перейдите на вкладку **Сервис** > **Свойства обозревателя** > **Безопасность**, выберите значок **Надежные узлы** и нажмите **Узлы**. 2. Измените настройки безопасности Internet Explorer и включите параметр **Автоматические запросы элементов управления ActiveX**. Перейдите на вкладку **Сервис** > **Свойства обозревателя** > **Безопасность** и выберите элемент **Другой уровень**.
IPv6	Если у вас смешанная среда, состоящая из локальных компьютеров только с адресом IPv4 или IPv6 и локальных компьютеров с двойным стеком, Security Server должен иметь как IPv4-, так и IPv6-адреса, чтобы все локальные компьютеры могли подключаться к внутренней веб-странице на сервере Security Server.

В сообщении электронной почты отправьте пользователям приведенные ниже инструкции по установке Security Agent с внутренней веб-страницы. Сведения о том, как отправить уведомление об установке по электронной почте, см. *Установка с уведомлением по электронной почте на странице 3-34*.

Процедура

1. Войдите в систему локального компьютера с правами администратора.
2. Откройте Internet Explorer и в адресной строке введите следующее:
   - Security Server с SSL:

     ```
     https://<имя или IP-адрес Security Server>:4343/SMB/
     console/html/client
     ```

   - Security Server без SSL:

```
http://<имя или IP-адрес Security Server>:8059/SMB/
console/html/client
```

3. Нажмите кнопку **Начать установку**, чтобы начать установку Security Agent.

   Начнется процесс установки. При запросе разрешите установку элементов управления ActiveX. После установки на панели задач Windows появится значок Security Agent.

Примечание

Список значков, которые отображаются на панели задач Windows, см. в *Проверка состояния Security Agent на странице A-2*.

После выполнения

Если пользователи сообщают, что они не могут выполнить установку с внутренней веб-страницы, попробуйте сделать следующее.

- Используя программы ping и telnet, проверьте связь между локальным компьютером и сервером.
- Проверьте настройку и работу протокола TCP/IP на локальном компьютере.
- При использовании прокси-сервера между локальным компьютером и сервером проверьте параметры прокси-сервера.
- В веб-браузере удалите надстройки Trend Micro и журнал браузера.

Установка с использованием программы настройки сценариев входа

Настройка сценария входа в сеть позволяет автоматически выполнять установку агента Security Agent на незащищенные компьютеры при их входе в сеть. Утилита настройки сценариев входа добавляет в сценарий входа на сервер программу `AutoPcc.exe`.

AutoPcc.exe устанавливает агент Security Agent на незащищенные клиентские компьютеры и обновляет программные файлы и компоненты. Чтобы использовать AutoPcc через сценарий входа, клиентские системы должны быть частью домена.

Если у вас уже есть существующий сценарий входа, программа настройки сценариев входа добавляет команду, которая выполняет AutoPcc.exe. В противном случае она создает командный файл ofcscan.bat, содержащий команду запуска AutoPcc.exe.

Утилита настройки сценариев входа добавляет следующие строки к концу сценария:

```
\\<Server_name>\ofcscan\autopcc
```

Где:

- <Server_name> — это имя или IP-адрес компьютера, на который производится установка Security Server.
- «ofcscan» — имя общей папки на сервере Security Server.
- «autopcc» является ссылкой на исполняемый файл autopcc, который устанавливает агент Security Agent.

Местоположение программы сценариев входа на всех версиях Windows Server (через общую папку входа в сеть):

```
\\Windows server\system drive\windir\sysvol\domain\scripts
\ofcscan.bat
```

Процедура

1. На компьютере, с которого была произведена установка сервера, откройте <папку установки Security Server>\PCCSRV\Admin.
2. Запустите файл SetupUsr.exe.

   Произойдет загрузка **настройки сценариев входа в сеть**. В консоли отобразится дерево, содержащее все домены в сети.
3. Выберите сервер, чей сценарий входа в сеть необходимо изменить, выделите его и нажмите **Выбрать**. Убедитесь, что сервер является

первичным контроллером домена и что у вас есть права администратора для доступа к серверу.

Программа настройки сценариев входа в сеть предложит ввести имя пользователя и пароль.

4. Введите имя пользователя и пароль. Для продолжения нажмите кнопку **OK**.

   Откроется окно **Выбор пользователей**. В списке **Пользователи** показаны профили пользователей, которые подключаются к серверу. В списке **Выбранные пользователи** показаны профили пользователей, чей сценарий входа в сеть будет изменен.

5. Для изменения сценария входа в сеть для профиля пользователя выберите профиль пользователя в списке «Пользователи» и нажмите кнопку **Добавить**.

6. Для изменения сценария входа всех пользователей нажмите кнопку **Добавить всех**.

7. Для того чтобы исключить из списка профиль пользователя, чей сценарий входа был изменен ранее, выберите его имя в списке **Выбранные пользователи** и нажмите кнопку **Удалить**.

8. Для отмены выбора пользователей нажмите кнопку **Удалить все**.

9. Когда все целевые пользователи появятся в списке **Выбранные пользователи**, нажмите кнопку **Применить**.

   Отобразится сообщение о том, что изменение сценария доступа к серверу прошло успешно.

10. Нажмите кнопку **OK**.

    Утилита настройки сценариев входа вернется к исходному окну.

11. Для того, чтобы закрыть программу настройки сценариев входа, нажмите кнопку **Выход**.

Установка с использованием Client Packager

Client Packager создает установочный пакет, который можно отправить пользователям на обычных носителях, таких как CD-ROM. Пользователи могут запустить пакет на клиентских компьютерах, чтобы установить Security Agent или обновить его версию и компоненты.

Client Packager наиболее полезен в следующих случаях.

- При установке Security Agent или компонентов на клиентские компьютеры, расположенные в удаленных офисах с низкой пропускной способностью соединения.
- При ограничениях среды на доступ в Интернет, например, в случае закрытия ЛВС или отсутствии подключения к Интернету.

Агенты Security Agent, устанавливаемые с помощью Client Packager, уведомляют сервер о месте создания пакета установки.

Процедура

1. На компьютере с сервером Security Server перейдите к `<папке установки сервера>PCCSRV\Admin\Utility\ClientPackager`.
2. Дважды щелкните по файлу `ClnPack.exe`.

   Откроется консоль клиентского инструмента упаковки файлов Client Packager.
3. Выберите операционную систему, для которой будет создан пакет. Устанавливайте пакет только на клиентские компьютеры, работающие под управлением операционной системы данного типа. Для другого типа операционной системы создайте другой пакет.
4. Выберите метод сканирования для этого пакета.

   Для получения дополнительных сведений о методах сканирования см. *Методы сканирования на странице 5-3*.

Включаемые в пакет компоненты зависят от выбранного метода сканирования. Для сканирования Smart Scan будут включены все компоненты за исключением вирусной базы данных. Для обычного сканирования будут включены все компоненты, за исключением вирусной базы данных агента Smart Scan.

5. Выберите тип создаваемого пакета.

Таблица 3-4. Типы пакетов клиента

Тип пакета	Описание
Установка	Выберите **Установка**, чтобы создать пакет в виде файла MSI, соответствующего формату пакета установщика Microsoft. Пакет устанавливает программу Security Agent и ее компоненты, доступные в данный момент на сервере Security Server. Если на целевом клиенте установлена более ранняя версия агента Security Agent, и вы хотите его обновить, создайте файл MSI с помощью Security Server, который управляет агентом. В противном случае агент не будет обновлен.
Обновление	Выберите **Обновить** для создания пакета, в который будут включены компоненты, доступные в данный момент на сервере Security Server. Пакет будет создан в формате исполняемого файла. Используйте этот пакет при возникновении проблем обновления компонентов на клиентских компьютерах, где установлен Security Agent.

6. Выберите **Автоматический режим** для создания пакета, который устанавливается на клиентский компьютер в фоновом режиме — незаметно для пользователя и без отображения окна состояния установки. Используйте этот параметр, если собираетесь устанавливать пакет на клиентский компьютер удаленно.

7. Нажмите **Отключить предварительное сканирование (только для установки в новую систему)**, если не хотите выполнять сканирование клиентской системы для обнаружения угроз перед установкой Security Agent. Используйте данную функцию только в том случае, если вы уверены, что клиентская система не содержит вредоносного ПО.

Если предварительное сканирование включено, программа установки запускает поиск вирусов/вредоносных программ в наиболее уязвимых областях компьютера, к которым относятся следующие разделы:

- загрузочная область и каталог загрузки (для поиска загрузочных вирусов);
- папка Windows;
- папка Program Files.

8. Необходимо убедиться в том, что в поле **Источник** правильно указано местоположение файла `ofcscan.ini`. Для изменения пути нажмите () и укажите местоположение файла `ofcscan.ini`. По умолчанию этот файл находится в `<папке установки сервера>\PCCSRV`.

9. В поле «Выходной файл» нажмите ( ), чтобы указать папку создания пакета и ввести имя файла пакета (например, `ClientSetup.exe`).

10. Нажмите **Создать**.

    После завершения работы клиентского инструмента упаковки файлов появится сообщение «Создание пакета завершено». Найдите пакет в каталоге, который вы указали в предыдущем шаге.

После выполнения

Установите пакет на клиентские компьютеры.

Требования для клиента:

- Дисковое пространство
  - Обычное сканирование: минимум 1,5 ГБ (рекомендуется 2 ГБ)
  - Smart Scan: 500 МБ

  1 ГБ свободного места на диске, если для пакета выбран метод обычного сканирования, 500 МБ при выборе Smart Scan

- Установщик Windows версии 4.5 или более поздней (для запуска пакета MSI)

Инструкции по установке пакета:

- Отправьте пакет пользователям и попросите их запустить его, дважды щелкнув по файлу (`.msi` или `.exe`).

Примечание

Пакет можно отправлять только тем пользователям, чьи агенты Security Agent передают отчеты на сервер, на котором был создан пакет.

- Попросите пользователей щелкнуть пакет правой кнопкой мыши и выбрать пункт **Запуск от имени администратора**.
- При использовании Active Directory вы можете автоматически выполнить установку агентов Security Agent на всех клиентских компьютерах одновременно с помощью файла `.msi`. При этом у пользователей отпадает необходимость устанавливать Security Agent самостоятельно. Используйте **Конфигурацию компьютера** вместо **Конфигурации пользователя**, чтобы Security Agent можно было установить независимо от того, какой пользователь входит в клиентскую систему.
- Если вновь установленный агент Security Agent не может подключиться к серверу Security Server, он сохранит настройки по умолчанию. Когда Security Agent подключится к Security Server, он получит настройки для своей группы в веб-консоли.
- При возникновении проблем с обновлением Security Agent с помощью программы Client Packager компания Trend Micro рекомендует сначала удалить предыдущую версию Security Agent, а затем установить новую. Инструкции по удалению см. *Удаление агентов на странице 3-41*.

Удаленная установка

Перед выполнением

Установите Security Agent удаленно на один или несколько локальных компьютеров, подключенных к сети.

Для удаленной установки требуется следующее.

Элемент для проверки	Требование
Целевой локальный компьютер	• Используйте учетную запись администратора для входа на каждом из целевых локальных компьютеров. **Примечание** • Если целевой локальный компьютер работает под управлением настольной операционной системы, сначала включите встроенную учетную запись администратора. Для получения дополнительной информации посетите сайт поддержки Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account). • При выполнении удаленной установки в ОС Windows 10 для входа в нужный клиент нельзя использовать учетную запись Microsoft • На целевом локальном компьютере не должен быть установлен Security Server. При удаленной установке агент Security Agent не устанавливается на локальный компьютер с уже запущенным Security Server.
Общий доступ к файлам и принтерам	Временно включите на локальном компьютере общий доступ к файлам и принтерам.

Элемент для проверки	Требование
	Примечание Если брандмауэр Windows отключен согласно политике безопасности компании, пропустите раздел «Удаленный реестр». 1. В панели управления откройте брандмауэр Windows. 2. Выберите команду **«Разрешение запуска программы через брандмауэр Windows»**. При запросе пароля администратора или подтверждения введите пароль или подтверждение. Появится окно параметров брандмауэра Windows. 3. Убедитесь в том, что на вкладке **«Исключения»** в разделе **«Программа или порт:»** установлен флажок **File and Printer Sharing** («Общий доступ к файлам и принтерам»). 4. Нажмите кнопку **OK**. 5. Если необходимо, после установки агентов Security Agent вернитесь к исходным настройкам.
Управление учетными записями пользователей	Отключите функцию управления учетными записями пользователей. **Примечание** Чтобы отключить функцию управления учетными записями пользователей, измените следующий ключ: `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies \System] “EnableLUA”=dword:00000000`. Если необходимо, после установки агентов Security Agent вернитесь к исходным настройкам.
Удаленный реестр	Временно запустите службу удаленного реестра. 1. **Примечание** В окне «Выполнить» введите команду `services.msc`, чтобы запустить консоль управления (MMC).

Элемент для проверки	Требование
	2. Правой кнопкой мыши щелкните пункт **Remote Registry** («Удаленный реестр») и выберите команду **Пуск»**. 3. Если необходимо, после установки агентов Security Agent вернитесь к исходным настройкам.
IPv6	Security Server с двойным стеком может установить Security Agent на любой локальный компьютер. Сервер Security Server с адресом IPv6 может установить Security Agent только на локальные компьютеры с адресом IPv6 или с двойным стеком.

Процедура

1. Перейдите к **Устройства**.
2. Щелкните пункт **Добавить устройства**.
3. Выберите **Настольный ПК или сервер** из меню **Тип компьютера**.
4. В разделе **«Способ»** выберите **«Удаленная установка»**.
5. Нажмите кнопку **Далее**.

   Появится новое окно.
6. Из списка компьютеров в поле **Группы и компьютеры** выберите клиента, затем нажмите кнопку **Добавить**. Появится запрос имени пользователя и пароля для клиента.
7. Введите имя пользователя и пароль и нажмите **Войти**. Клиент отобразится в списке **Выбранные компьютеры**.
8. Повторяйте эти шаги до тех пор, пока все компьютеры не появятся в списке **Выбранные компьютеры**.
9. Нажмите кнопку **Установить**.

   Появится окно подтверждения.
10. Для подтверждения установки агента на клиентской системе необходимо нажать **Да**.

Откроется окно, показывающее ход копирования файлов агента Security Agent на каждый клиент.

Когда Security Server завершит установку на клиентском устройстве, в поле **Состояние** списка **Выбранные компьютеры** отобразится состояние установки, а рядом с именем компьютера появится зеленая отметка.

После выполнения

Если удаленная установка не удалась, выполните следующие действия.

- Используя программы ping и telnet, проверьте связь между клиентом и сервером.
- Проверьте настройку и работу протокола TCP/IP на клиентском компьютере.
- При использовании прокси-сервера между клиентом и сервером проверьте параметры прокси-сервера.
- В веб-браузере удалите надстройки Trend Micro и журнал браузера.

Установка с использованием сканера уязвимостей

Перед выполнением

Сканер уязвимостей используется для обнаружения установленных антивирусных решений, поиска незащищенных компьютеров в сети и установки на них агентов Security Agent.

Для установки сканера уязвимостей требуется сделать следующее.

Элемент для проверки	Требование
Где запускать сканер уязвимостей	Вы можете запустить сканер уязвимостей на сервере Security Server или на любом клиенте в сети. На клиенте не должен быть запущен Terminal Server.

Элемент для проверки	Требование
Конечный клиент	• На конечном клиенте не должен быть установлен Security Server. Сканер уязвимостей не позволяет устанавливать агенты Security Agent на клиенты, на которых запущен Security Server. • При входе в клиентскую систему пользователи должны использовать учетную запись с правами администратора. **Примечание** Если конечный клиент работает под управлением настольной операционной системы, сначала включите встроенную учетную запись администратора. Для получения дополнительной информации посетите сайт поддержки Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Существует несколько способов сканирования уязвимостей.

- *Запуск сканирования уязвимостей вручную на странице 3-23*
- *Запуск сканирования DHCP на странице 3-25*
- *Настройка регулярной проверки уязвимостей на странице 3-28*

Запуск сканирования уязвимостей вручную

Запуск сканирования уязвимостей по требованию.

Процедура

1. Запустите сканер уязвимостей.

Запуск сканера уязвимостей:	Шаги
Security Server	a. Откройте <папку установки сервера>\PCCSRV\Admin\Utility\TMVS. b. Запустите файл TMVS.exe.
Клиент в сети	a. На компьютере с сервером Security Server откройте <папку установки сервера>\PCCSRV\Admin\Utility. b. Скопируйте на другой клиент всю папкуTMVS. c. Откройте на другом клиенте папку TMVS и запустите файл TMVS.exe.

2. Перейдите в раздел **Сканирование вручную**.
3. Введите диапазон IP-адресов компьютеров, которые необходимо проверить.
   a. Введите диапазон адресов IPv4.

   Примечание

   Сканер уязвимостей может запросить диапазон IPv4-адресов только в том случае, если он работает на клиентском компьютере только с адресом IPv4 или с двойным стеком. Сканер уязвимостей поддерживает только диапазон IP-адресов класса B (например, от 168.212.1.1 до 168.212.254.254.)

   b. Чтобы задать диапазон IPv6-адресов, введите префикс и длину IPv6-адреса.

   Примечание

   Сканер уязвимостей может запросить диапазон IPv6-адресов только в том случае, если он работает на клиентском компьютере только с адресом IPv6 или с двойным стеком.
4. Нажмите кнопку **Параметры**.

   Откроется окно **Параметры**.

5. Настройте параметры сканирования уязвимостей. Для получения дополнительных сведений см. *Настройки сканирования уязвимостей на странице 3-30*.

6. Нажмите кнопку **ОК**.

   Окно «Параметры» закроется.

7. Нажмите **Пуск**.

   Результаты сканирования уязвимостей выводятся в таблице **Результаты** на вкладке **Сканирование вручную**.

   Примечание

   Если компьютер работает под управлением Windows Server 2008, информация о MAC-адресах не отображается в таблице **Результаты**.

8. Чтобы сохранить результаты в файл CSV, нажмите **Экспорт**, укажите папку, куда вы хотите сохранить файл, введите имя файла и нажмите кнопку **Сохранить**.

Запуск сканирования DHCP

Запускает сканер уязвимостей на компьютерах, получающих IP-адрес от сервера DHCP.

Сканер уязвимостей прослушивает порт 67, который является портом прослушивания сервера DHCP для запросов DHCP. При обнаружении запроса DHCP от клиентского компьютере на нем выполняется поиск уязвимостей.

Примечание

Сканер уязвимостей не может обнаружить DHCP-запросы при запуске в системах Windows Server 2008 или Windows 7.

Процедура

1. Настройте параметры DHCP в файле `TMVS.ini`, расположенном в следующей папке: `<папка установки сервера>\PCCSRV\Admin\Utility\TMVS`.

Таблица 3-5. Параметры DHCP в файле `TMVS.ini`

Параметр	Описание
DhcpThreadNum=x	Укажите номер потока в режиме DHCP. Минимум 3, максимум 100. Значение по умолчанию — 3.
DhcpDelayScan=x	Это время задержки в секундах перед проверкой запрашивающего компьютера на наличие установленных антивирусных программ. Минимум 0 (без ожидания), максимум 600. Значение по умолчанию — 60.
LogReport=x	0 — отключить ведение журнала, 1 — включить Сканер уязвимостей отправляет результаты сканирования на сервер Worry-Free Business Security. Журналы отображаются в окне **Журналы системных событий** на веб-консоли.
OsceServer=x	Это IP-адрес сервера Worry-Free Business Security или имя DNS-сервера.
OsceServerPort=x	Это порт веб-сервера на сервере Worry-Free Business Security.

2. Запустите сканер уязвимостей.

Запуск сканера уязвимостей:	Шаги
Security Server	a. Откройте `<папку установки сервера>\PCCSRV\Admin\Utility\TMVS`. b. Запустите файл `TMVS.exe`.

Запуск сканера уязвимостей:	Шаги
Клиент в сети	a. На компьютере с сервером Security Server откройте `<папку установки сервера>\PCCSRV\Admin\Utility`. b. Скопируйте на другой клиент всю папку `TMVS`. c. Откройте на другом клиенте папку `TMVS` и запустите файл `TMVS.exe`.

3. Рядом с разделом **Сканирование вручную** нажмите **Параметры**.

   Откроется окно **Параметры**.

4. Настройте параметры сканирования уязвимостей. Для получения дополнительных сведений см. *Настройки сканирования уязвимостей на странице 3-30*.

5. Нажмите кнопку **OK**.

   Окно «Параметры» закроется.

6. Перейдите на вкладку **Сканирование DHCP** в окне **Результаты**.

   Примечание

   Вкладка **Сканирование DHCP** недоступна на компьютерах под управлением Windows Server 2008 и Windows 7.

7. Нажмите кнопку **Запуск DHCP**.

   Сканер уязвимостей начнет прослушивание запросов DHCP и проверку уязвимостей на клиентах в сети.

8. Чтобы сохранить результаты в файл CSV, нажмите **Экспорт**, укажите папку, куда вы хотите сохранить файл, введите имя файла и нажмите кнопку **Сохранить**.

Настройка регулярной проверки уязвимостей

Сканирование уязвимостей запускается автоматически в соответствии с расписанием.

Процедура

1. Запустите сканер уязвимостей.

Запуск сканера уязвимостей:	Шаги
Security Server	a. Откройте `<папку установки сервера>\PCCSRV\Admin\Utility\TMVS`. b. Запустите файл `TMVS.exe`.
Клиент в сети	a. На компьютере с сервером Security Server откройте `<папку установки сервера>\PCCSRV\Admin\Utility`. b. Скопируйте на другой клиент всю папку`TMVS`. c. Откройте на другом клиенте папку `TMVS` и запустите файл `TMVS.exe`.

2. Перейдите в раздел **Сканирование по расписанию**.
3. Нажмите кнопку **Добавить/Изменить**.

   Откроется окно **Сканирование по расписанию**.
4. Введите имя для сканирования уязвимостей по расписанию.
5. Введите диапазон IP-адресов компьютеров, которые необходимо проверить.

   a. Введите диапазон адресов IPv4.

Примечание

Сканер уязвимостей может запросить диапазон IPv4-адресов только в том случае, если он работает на компьютере только с адресом IPv4 или с двойным стеком, который имеет доступный IPv4-адрес. Сканер уязвимостей поддерживает только диапазон IP-адресов класса B (например, от 168.212.1.1 до 168.212.254.254.)

b. Чтобы задать диапазон IPv6-адресов, введите префикс и длину IPv6-адреса.

Примечание

Сканер уязвимостей может запросить диапазон IPv6-адресов только в том случае, если он работает на компьютере только с адресом IPv6 или с двойным стеком, который имеет доступный IPv6-адрес.

6. Укажите время начала сканирования в 24-часовом формате, а затем определите, как часто будет выполняться сканирование. Укажите «Ежедневно», «Еженедельно» или «Ежемесячно».

7. Выберите **Использовать текущие параметры**, если вы выполнили конфигурацию и хотите использовать параметры сканирования уязвимостей вручную. Более подробную информацию о параметрах сканирования уязвимостей вручную см. *Запуск сканирования уязвимостей вручную на странице 3-23*.

   Если вы не задали параметры сканирования уязвимостей вручную или хотите использовать другой набор параметров, выберите **Изменить параметры**, а затем нажмите **Параметры**. Откроется окно **Параметры**. Настройте параметры сканирования и нажмите кнопку **OK**. Для получения дополнительных сведений см. *Настройки сканирования уязвимостей на странице 3-30*.

8. Нажмите кнопку **OK**.

   Окно **Сканирование по расписанию** будет закрыто. Созданное запланированное сканирование уязвимостей появится в разделе **Сканирование по расписанию**. Если вы включили уведомления,

сканер уязвимостей будет отправлять вам результаты запланированного сканирования уязвимостей.

9. Для выполнения запланированного сканирования уязвимостей немедленно, нажмите кнопку **Запустить сейчас**.

   Результаты сканирования уязвимостей выводятся в таблице **Результаты** на вкладке **Сканирование по расписанию**.

   Примечание

   Если компьютер работает под управлением Windows Server 2008, информация о MAC-адресах не отображается в **таблице «Результаты»**.

10. Чтобы сохранить результаты в файл `CSV`, нажмите **Экспорт**, укажите папку, куда вы хотите сохранить файл, введите имя файла и нажмите кнопку **Сохранить**.

11. Чтобы остановить выполнение запланированных сканирований уязвимостей, перейдите в раздел **Сканирование по расписанию**, выберите сканирование и нажмите кнопку **Удалить**.

Настройки сканирования уязвимостей

При запуске сканирования уязвимостей настройте следующие параметры. Для получения дополнительной информации о различных типах сканирования уязвимостей см. *Установка с использованием сканера уязвимостей на странице 3-22*.

Настройки	Описание и инструкции
Запрос продукта	Сканер уязвимостей может выполнять проверку на наличие программного обеспечения защиты на целевых клиентских компьютерах. 1. Выберите защитное программное обеспечение для проверки. 2. Для проверки программного обеспечения сканер уязвимостей использует порты по умолчанию, отображаемые в окне. Если администратор изменил порты по умолчанию, внесите необходимые изменения, иначе сканер уязвимостей не сможет обнаружить программное обеспечение. 3. Для решения Norton Antivirus Corporate Edition можно изменить параметры времени ожидания, нажав **Параметры**.
	Другие настройки запроса продуктов Чтобы установить количество клиентов, на которых сканер уязвимостей будет одновременно проверять наличие антивирусного программного обеспечения, сделайте следующее. 1. Перейдите в папку `<папка установки сервера>\PCCSRV\Admin\Utility\TMVS` и откройте файл `TMVS.ini` в текстовом редакторе, например в Блокноте. 2. Чтобы установить количество проверяемых клиентов, сделайте следующее. • Для сканирования уязвимостей вручную измените значение для `ThreadNumManual`. Укажите значение от 8 до 64. Например, введите `ThreadNumManual=60`, если необходимо, чтобы сканер уязвимостей одновременно проверял 60 компьютеров. • Для сканирования уязвимостей по расписанию измените значение для `ThreadNumSchedule`. Укажите значение от 8 до 64. Например, введите `ThreadNumSchedule=50`, если необходимо, чтобы сканер уязвимостей одновременно проверял 50 клиентов. 3. Сохраните файл `TMVS.ini`.

Настройки	Описание и инструкции
Параметры получения описания	Если сканер уязвимостей имеет возможность отправлять клиентам запрос ping, он может получать дополнительную информацию о клиентах. Существует три метода получения информации. • **Обычный метод**: извлекает информацию о домене и компьютере. • **Быстрый метод**: Извлекает только имя компьютера.
Параметры сигналов тревоги	Для автоматической отправки результатов сканирования уязвимостей администраторам вашей организации, сделайте следующее. 1. Выберите **Отправлять результаты системному администратору по электронной почте**. 2. Выберите **Настройка** и введите параметры сообщения электронной почты. 3. В поле **Кому** укажите адрес электронной почты получателя. 4. В поле **От** укажите адрес электронной почты отправителя. 5. В поле **SMTP-сервер** введите адрес сервера SMTP. Например, `smtp.company.com`. Информация о сервере SMTP является обязательной для заполнения. 6. В поле **Тема** укажите новую тему сообщения или оставьте тему, установленную по умолчанию. 7. Нажмите кнопку **OK**. Чтобы сообщить пользователям, что на их компьютерах не установлено антивирусное программное обеспечение, сделайте следующее. 1. Выберите **Выводить уведомления на незащищенных компьютерах**. 2. Нажмите **Настроить** для настройки уведомлений. 3. В окне **Уведомления** введите новое сообщение или оставьте сообщение по умолчанию. 4. Нажмите кнопку **OK**.

Настройки	Описание и инструкции
Сохраните как файл CSV	Сохраните результаты сканирования уязвимостей в файл CSV. Файл будет сохранен на клиентском компьютере, где был запущен сканер уязвимостей. Используйте путь по умолчанию или измените его в соответствии с вашими предпочтениями.
Параметры пакетов	Используйте параметры пакетов для проверки существования клиента и определения его операционной системы. Если эти параметры отключены, сканер уязвимостей проверяет все IP-адреса в указанном диапазоне IP-адресов (даже те, которые не используются на клиентах), тем самым без необходимости увеличивая длительность сканирования. 1. Примите значения по умолчанию или укажите новые в полях **Размер пакета** и **Время ожидания**. 2. Выберите **Определять тип операционной системы с помощью экспертизы ICMP OS**. При выборе этой функции сканер уязвимостей определяет, работает клиент под управлением Windows или другой операционной системы. Для клиентов, использующих Windows, сканер уязвимостей может определить версию Windows.
	Другие параметры пакетов Для установки количества компьютеров, для которых сканер уязвимостей будет одновременно выполнять проверку связи, сделайте следующее. 1. Перейдите в папку `<папка установки сервера>\PCCSRV\Admin\Utility\TMVS` и откройте файл `TMVS.ini` в текстовом редакторе, например в Блокноте. 2. Введите значение для параметра `EchoNum`. Укажите значение от 1 до 64. Например, укажите `EchoNum=60`, чтобы сканер уязвимостей выполнял проверку связи на 60 компьютерах одновременно. 3. Сохраните файл `TMVS.ini`.

Настройки	Описание и инструкции
параметры Security Server;	1. Выберите **Автоматическая установка Security Agent на незащищенные компьютеры** для установки Security Agent на клиентские компьютеры, которые будут проверяться сканером уязвимостей. 2. Введите имя или IPv4/IPv6-адрес Security Server, а также номер порта. Агенты Security Agent, установленные сканером уязвимостей, будут отправлять отчеты этому серверу. 3. Настройте данные учетной записи администратора, используемые при входе в клиентские системы, нажав **Установить учетную запись**. В окне **Учетная запись** введите имя пользователя и пароль и нажмите кнопку **OK**.

Установка с уведомлением по электронной почте

Используйте этот метод установки для того, чтобы отправить письмо со ссылкой на программу установки.

Процедура

1. Перейдите к **Устройства**.
2. Щелкните пункт **Добавить устройства**.
3. Выберите **Настольный ПК или сервер** из меню **Тип компьютера**.
4. В разделе **Метод** выберите пункт **Установка с помощью почтового уведомления**.
5. Нажмите кнопку **Далее**.

   Появится новое окно.
6. Введите тему сообщения и получателя.
7. Нажмите кнопку **Применить**. Почтовый клиент по умолчанию открывается с получателем, темой и ссылкой на мастера установки.

Переход на Security Agent

При установке агента Security Agent программа установки проверяет наличие программного обеспечения Trend Micro или стороннего программного обеспечения для защиты конечных пользователей, установленного на клиентском компьютере.

Программа установки позволяет выполнять следующие действия:

- удалять другие программы для защиты конечных пользователей, установленные на клиентском компьютере, а затем заменять их на Security Agent;
- обнаруживать другое программное обеспечение для защиты конечных пользователей, но не удалять его.

Для получения списка программного обеспечения для защиты конечных пользователей посетите следующий веб-сайт:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Если программное обеспечение на клиентском компьютере не может быть удалено автоматически или может быть только обнаружено, но не удалено, удалите его вручную. В зависимости от процесса удаления программного обеспечения, после удаления может потребоваться перезагрузка клиентского компьютера.

Проблемы перехода и возможные решения

Автоматическое удаление программного обеспечения сторонних производителей для защиты конечных пользователей может быть неудачным по следующим причинам:

- неправильный ключ продукта или номер версии приложения стороннего производителя;
- неполадка программы удаления приложения стороннего производителя;
- некоторые файлы приложения стороннего производителя отсутствуют или повреждены;

- невозможно удалить ключ реестра приложения стороннего производителя;
- программа удаления приложения стороннего производителя отсутствует.

Возможные решения этих проблем:

- Удалите приложение стороннего производителя вручную.
- Остановите службы, запущенные приложением сторонних производителей.
- Выгрузите службы или процессы, относящиеся к приложению сторонних производителей.

Выполнение задач после установки для агентов Security Agent

Процедура

1. Убедитесь в следующем.
   - Ярлыки агента Security Agent отображаются в меню Windows «Пуск» на локальном компьютере.
   - **Trend Micro Worry-Free Business Security Agent** отображается в списке «Установка и удаление программ» в панели управления локального компьютера.
   - Агент Security Agent отображается в окне **Устройства** на веб-консоли. Он отнесен к группе **Настольные компьютеры (по умолчанию)** или **Серверы (по умолчанию)**, в зависимости от операционной системы локального компьютера.

Примечание

Если вы не видите Security Agent, запустите задачу проверки соединения из меню **Администрирование** > **Глобальные параметры** > **Система (вкладка)** > **Проверка соединения агента**.

- На **консоли управления Microsoft** отображаются следующие службы Security Agent:
  - Trend Micro Security Agent Listener (`tmlisten.exe`)
  - Служба сканирования в режиме реального времени Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`)
  - Брандмауэр Trend Micro Security Agent (`TmPfw.exe`), если брандмауэр был включен во время установки.
  - Служба предотвращения несанкционированных изменений Trend Micro (`TMBMSRV.exe`), если во время установки был включен контроль действий или контроль устройств.
  - Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. Если Security Agent не появляется на веб-консоли, возможно, что он не смог отправить свой статус серверу. Выполните любое из указанных ниже действий.
   - Откройте браузер на клиентском компьютере, введите в адресной строке `https://{имя_Trend Micro Security Server}:{номер порта}/SMB/cgi/cgionstart.exe` и нажмите клавишу ENTER.

     Если в следующем окне будет отображено «-2», то соединение между агентом и сервером работает. Это также указывает на ошибку в базе данных сервера, связанную с отсутствием в ней записи об агенте.
   - Используя программы ping и telnet, проверьте связь между клиентом и сервером.

- При подключении по низкоскоростному соединению убедитесь в отсутствии превышения времени ожидания между сервером и клиентом.
- Проверьте наличие прав общего доступа к папке `\PCCSRV`. Все пользователи должны обладать правами полного доступа.
- Проверьте параметры прокси-сервера Trend Micro Security Server.

3. Проверьте Security Agent с помощью тестового скрипта EICAR.

Европейский институт исследования антивирусных программ (EICAR) разработал тестовый вирус для тестирования антивирусного программного обеспечения. Тестовая программа представляет собой инертный текстовый файл, бинарный код которого встречается в базах данных вирусов большинства поставщиков антивирусного программного обеспечения. Тем не менее, файл не является вирусом и не содержит никакого программного кода.

Загрузите файл по одной из ссылок (URL):

http://www.eicar.org/anti_virus_test_file.htm

Кроме того, тестовый вирусный файл EICAR можно создать самостоятельно, создав файл, содержащий следующую строку, и назвав файл «eicar.com»:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Примечание

Перед тестированием необходимо очистить кэш на сервере и локальном браузере.

Установка Messaging Security Agent

Агенты Messaging Security Agents можно установить только на решения Worry-Free Business Security Advanced.

Выполните новую установку Messaging Security Agent на серверы Microsoft Exchange.

Примечание

Для получения сведений об обновлении агентов Messaging Security Agent до данной версии, см. «Руководство по установке и обновлению».

Требования к установке Messaging Security Agent

Чтобы просмотреть полный список требований к установке, посетите следующий веб-сайт:

http://docs.trendmicro.com/ru-ru/smb/worry-free-business-security.aspx

Установка агентов Messaging Security Agent (только Advanced)

Перед выполнением

Примечания и напоминания по установке.

- Перед установкой или после нее останавливать или запускать службы Microsoft Exchange не требуется.
- При наличии на локальном компьютере сведений о предыдущей установке агента Messaging Security Agent установка будет невозможна. Чтобы полностью удалить предыдущую версию, воспользуйтесь панелью управления Windows.

  Дополнительную информацию см. в разделе *Удаление агента Messaging Security Agent с сервера Microsoft Exchange (только Advanced) на странице 3-45*.

- В случае установки Messaging Security Agent на сервер, на котором запущены средства блокировки, удалите средство блокировки. После удаления оно не заблокирует службу ISS и не приведет к сбою процесса установки.
- Установка агента Messaging Security Agent также может быть выполнена во время установки сервера Security Server. Более подробную информацию см. в руководстве по установке и обновлению.
- В Messaging Security Agent не поддерживаются некоторые функции Microsoft Exchange Server Enterprise, такие как Data Availability Group (DAG).

Процедура

1. Перейдите к **Устройства**.
2. Щелкните пункт **Добавить устройства**.
3. Выберите **Сервер Exchange**.
4. В разделе **Сведения об Exchange Server** введите следующие данные.
   - **Имя сервера**: имя сервера Microsoft Exchange Server, на который необходимо установить агент.
   - **Учетная запись** Имя пользователя встроенной учетной записи администратора домена.
   - **Пароль**: пароль встроенной учетной записи администратора домена.
5. Нажмите кнопку **Далее**.

   Мастер установки отобразит экран, зависящий от выбранного типа установки.

   - **Новая установка**: агент не существует на сервере Microsoft Exchange Server и будет установлен.

- **Обновить**: на сервере Microsoft Exchange Server существует предыдущая версия агента, которая будет обновлена до текущей версии.
- **Установка не требуется**: на сервере Microsoft Exchange Server существует текущая версия агента. Если в настоящее время агент не отображается в дереве групп безопасности, он будет автоматически добавлен.
- **Недопустимо**: проблема с установкой агента.

Примечание

В качестве **типа управления спама** будет использовано значение **Карантин конечного пользователя**.

6. На вкладке **Папки** выберите целевые и общие папки по умолчанию для установки агента Messaging Security Agent или измените их. Целевые и общие каталоги по умолчанию находятся по путям `C:\Program Files\Trend Micro\Messaging Security Agent` и `C$` соответственно.
7. Нажмите кнопку **Далее**.

   Откроется новое окно.
8. Проверьте правильность параметров сервера Microsoft Exchange, заданных в предыдущих окнах, и нажмите кнопку **Далее**, чтобы начать установку.
9. Для просмотра хода установки откройте вкладку **Текущее состояние**.

Удаление агентов

Команда **Удалить агент** дает возможность удалять агенты Security Agent и Messaging Security Agent (только Advanced) указанными далее способами.

- *Удаление агентов из веб-консоли на странице 3-43*

  Используйте этот способ для неактивных агентов. Неактивный агент все время отображается на веб-консоли в автономном режиме. Это может быть следствием того, что клиентский компьютер, на котором установлен агент, был выключен в течение длительного времени или переформатирован перед тем, как агент был удален.

  При удалении агентов с веб-консоли:

  - агент, если он все еще существует на клиенте, не будет удален;
  - сервер остановит управление агентом.
  - При повторном возобновлении взаимодействия агента с сервером (например, после включения клиентского компьютера), агент вновь добавляется в веб-консоль. Агент Security Agent использует настройки своей исходной группы. Если группа больше не существует, агент будет прикреплен к группе **Настольные компьютеры (по умолчанию)** или **Серверы (по умолчанию)**, в зависимости от операционной системы клиента, и будет использовать настройки этой группы.

Совет

WFBS предлагает еще одну функцию, которая находит и удаляет неактивные агенты из веб-консоли. Используйте эту функцию, чтобы автоматизировать задачу удаления агента. Чтобы использовать функцию, перейдите на вкладку **Администрирование** > **Глобальные параметры** > **Система** и откройте раздел «Удаление неактивного агента Security Agent».

- *Удаление агентов из веб-консоли на странице 3-43*

  Вы можете удалить агент с клиентского компьютера (и, следовательно, удалить его из веб-консоли), если у вас возникли проблемы с программой агента. Trend Micro рекомендует

немедленную переустановку агента для того, чтобы клиент был защищен от угроз.

Удаление агентов из веб-консоли

Процедура

1. Перейдите к **Устройства**.
2. Для удаления агентов Security Agent выберите группу, а затем выберите агенты. Для удаления агента Messaging Security Agent выберите его.

Совет

Для выбора нескольких смежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу SHIFT, — по последнему. Для выбора нескольких несмежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу CTRL, — по тем агентам, которые требуется выбрать.

3. Выберите **Дополнительно** > **Удалить агент**.

   Появится новое окно.

4. Выберите **Удалить выбранные агенты**.
5. Нажмите кнопку **Применить**.

Удаление агентов из веб-консоли

При удалении агента Messaging Security Agent административные службы IIS/сервер Apache и все связанные с ними службы будут автоматически остановлены и перезапущены.

Процедура

1. Перейдите к **Устройства**.
2. Для удаления агентов Security Agent выберите группу, а затем выберите агенты. Для удаления агента Messaging Security Agent выберите его.

   Совет

   Для выбора нескольких смежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу SHIFT, — по последнему. Для выбора нескольких несмежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу CTRL, — по тем агентам, которые требуется выбрать.

3. Выберите **Дополнительно** > **Удалить агент**.

   Появится новое окно.

4. Выберите **Удалить выбранные агенты**.
5. Нажмите кнопку **Применить**.

   Появится всплывающее окно, в котором отображается количество уведомлений об удалении, отправленных сервером, и число агентов, которые получили уведомление.

   Примечание

   Для агента Messaging Security Agent введите соответствующие имя учетной записи и пароль для сервера Microsoft Exchange Server.

6. Нажмите кнопку **ОК**.
7. Чтобы убедиться в том, что агент удален, обновите окно «Параметры безопасности». Агент не должен больше присутствовать в дереве групп безопасности.

Удаление Security Agent с локального компьютера

В зависимости от конфигурации процесс удаления может запросить пароль. Если требуется пароль, убедитесь, что вы сообщаете пароль только тем пользователям, которые будут запускать программу удаления. Если он был разглашен другим пользователям, сразу же измените его.

Пароль может быть установлен или отключен в окне **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер** > **Пароль для удаления Security Agent**.

Процедура

1. Выберите **Панель управления** > **Установка и удаление программ**.
2. Выберите **Trend Micro Worry-Free Business Security Agent** и нажмите кнопку **Изменить** или **Удалить**, в зависимости от доступности.
3. Следуйте инструкциям на экране.
4. Если потребуется, введите пароль удаления.

   Security Server уведомляет пользователя о ходе удаления и его завершении. Пользователю не нужно перезапускать клиент, чтобы завершить удаление.

Удаление агента Messaging Security Agent с сервера Microsoft Exchange (только Advanced)

При удалении агента Messaging Security Agent административные службы IIS/сервер Apache и все связанные с ними службы будут автоматически остановлены и перезапущены.

Процедура

1. Выполните вход на сервер Microsoft Exchange с правами администратора.
2. Нажмите **Панель управления** > **Удаление программы**.
3. Найдите **Trend Micro Messaging Security Agent** и нажмите кнопку **Изменить**.
4. Следуйте инструкциям на экране.

Глава 4

Управление устройствами

Worry-Free Business Security разделяет экран **Устройства** на два основных раздела.

- Дерево устройств

  Дерево устройств представляет собой раскрываемый список логических групп. Можно управлять группами на основе типа оконечного устройства или вручную установить группы и организовать агенты Security Agent в соответствии со своими требованиям.

  Дополнительную информацию см. в разделе *Использование дерева устройств на странице 4-2*.

- Таблица сведений о группах

  При выборе группы из дерева устройств справа появляется список агентов Security Agent в данной группе.

  Дополнительную информацию см. в разделе *Использование команд устройств на странице 4-5*.

Использование дерева устройств

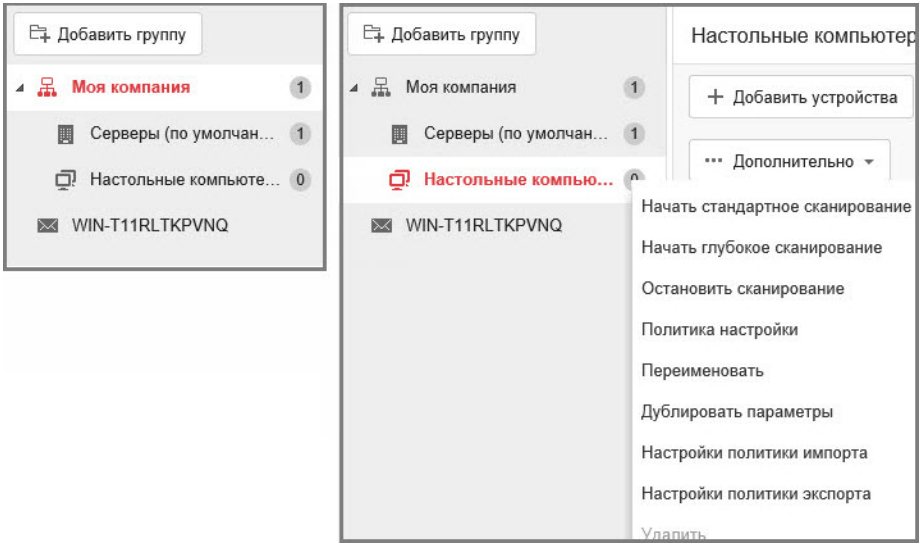


Иллюстрация 4-1. Использование меню команд для дерева устройств

Чтобы открыть меню дерева устройств, выполните следующее.

- Выберите группу в дереве устройств и щелкните значок шестеренки рядом с именем группы.
- Выберите агент Messaging Security Agent и щелкните значок шестеренки рядом с именем агента.

Некоторые команды могут быть неактивными или недоступными для выбранного типа группы.

Таблица 4-1. Команды для дерева устройств

Команда	Описание
Добавить группу	Добавление новой группы к дереву устройств. Дополнительную информацию см. в разделе *Добавление групп на странице 4-9*.
Начать стандартное сканирование	• Начинает сканирование всех оконечных устройств в выбранной группе • Запуск сканирования сервера Exchange Server.
Начать глубокое сканирование	Запуск расширенного сканирования на всех конечных точках в выбранной группе, анализирующего и вычищающего угрозы, которые не могут быть удалены стандартным сканированием. **Примечание** Выполнение глубокого сканирования может повлиять на производительность конечной точки и привести к увеличению числа ложных срабатываний.
Остановить сканирование	• Оканчивает сканирование всех оконечных устройств в выбранной группе • Прекращение сканирования сервера Exchange Server.
Настройка глобальных параметров	Настройка общих параметров агента Security Agent для сканирования, списков разрешенных/заблокированных объектов, управления агентом Security Agent и устройствами Дополнительную информацию см. в разделе *Глобальные параметры на странице 11-2*.

Команда	Описание
Политика настройки	• Настраивает параметры безопасности для всех агентов Security Agent в выбранной группе Дополнительную информацию см. в разделе *Краткий обзор основных параметров безопасности для Security Agent на странице 5-2*. • Настройка параметров безопасности для выбранного агента Messaging Security Agent. Дополнительную информацию см. в разделе *Управление основными параметрами безопасности агентов Messaging Security Agent (только Advanced) на странице 6-1*.
Переименовать	Изменение имени выбранной группы.
Дублировать параметры	Копирование настроек из одной группы в другую. В результате к агентам Security Agent в целевой группе будут применены те же настройки, что и в исходной группе. Дополнительную информацию см. в разделе *Дублирование параметров на странице 4-18*.
Настройки политики импорта	Импорт настроек из другой группы. Дополнительную информацию см. в разделе *+Импорт и экспорт параметров групп Security Agent на странице 4-20*.
Настройки политики экспорта	Экспорт настроек выбранной группы. Дополнительную информацию см. в разделе *+Импорт и экспорт параметров групп Security Agent на странице 4-20*.
Удалить	Удаление группы из дерева устройств.

Использование команд устройств

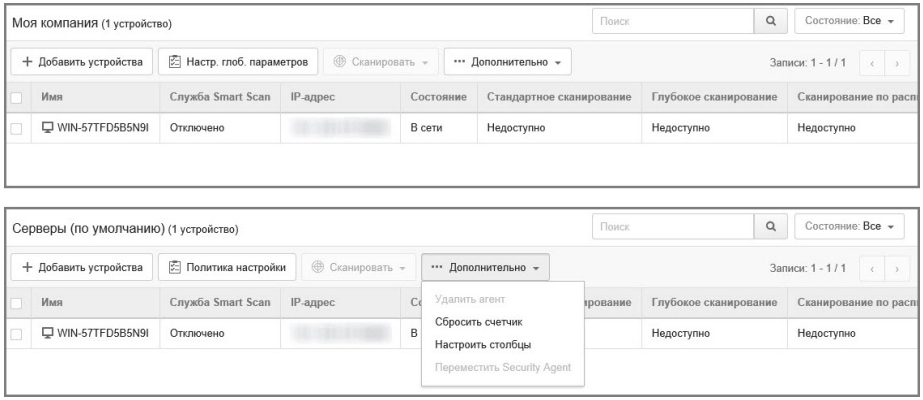


Иллюстрация 4-2. Использование меню команд для устройств

После того как вы выберете в дереве устройств группу, справа в таблице отобразится перечень агентов Security Agent в этой группе. В строке меню над таблицей собраны команды для управления агентами Security Agent. Некоторые команды могут быть неактивными или недоступными для выбранного типа группы.

С помощью поля поиска над экраном **Устройства** можно искать локальные компьютеры по именам, меткам или IP-адресам.

Совет

Чтобы найти локальный компьютер внутри сети, можно ввести часть IP-адреса. Например, если ввести «192», будут показаны все IP-адреса, содержащие «192», а если ввести «192.», то будут показаны только IP-адреса, содержащие в начале «192.». При поиске локальных компьютером по имени нельзя использовать подстановочные символы и специальные знаки (*, +, (,), -, &).

Таблица 4-2. Команды для устройств

Команда	Описание
Добавить устройства	Выполните одно из следующих действий. • Установите **Security Agent** на локальном компьютере (настольный ПК или сервер) • Установите **Messaging Security Agent** на сервер Microsoft Exchange (только Advanced) Дополнительную информацию см. в разделе *Добавление агентов в группы на странице 4-7*.
Политика настройки	Настраивает параметры безопасности для всех агентов Security Agent в выбранной группе Дополнительную информацию см. в разделе *Краткий обзор основных параметров безопасности для Security Agent на странице 5-2*.
Начать стандартное сканирование	Начинает сканирование выбранных оконечных устройств
Начать глубокое сканирование	Запуск расширенного сканирования на всех конечных точках в выбранной группе, анализирующего и вычищающего угрозы, которые не могут быть удалены стандартным сканированием. **Примечание** Выполнение глубокого сканирования может повлиять на производительность конечной точки и привести к увеличению числа ложных срабатываний.
Остановить сканирование	Оканчивает сканирование выбранных оконечных устройств
Удалить агент	Удаление Security Agent с выбранных локальных компьютеров Дополнительную информацию см. в разделе *Удаление агентов на странице 3-41*.

Команда	Описание
Сбросить счетчик	Сбрасываются счетчики обнаруженных угроз безопасности для всех агентов Security Agent в данной сети. Связанную с ними информацию журнала отчетов по-прежнему можно получить посредством запроса журнала.
Настроить столбцы	Выбор столбцов для отображения в таблице. Дополнительную информацию см. в разделе *Настройка столбцов списка устройств на странице 4-10*.
Переместить Security Agent	Переместите выбранные агенты Security Agent в другую группу или на другой сервер Security Server. Дополнительную информацию см. в разделе *Перемещение агентов на странице 4-12*.

Добавление агентов в группы

После установки агента и оповещения Security Server сервер добавляет его в группу.

- Агенты Security Agent, установленные на серверных платформах, добавляются в группу **Серверы (по умолчанию)**.
- Агенты Security Agent, установленные на платформах настольного компьютера, добавляются в группу **Настольные компьютеры (по умолчанию)**.

  Примечание

  Вы можете назначить агентов Security Agent другим группам, переместив их. Для получения дополнительных сведений см. *Перемещение агентов на странице 4-12*.

- Каждый агент Messaging Security Agent (только Advanced) является группой. Невозможно объединить несколько агентов Messaging Security Agent в одну группу.

Если количество агентов, отображаемое в дереве групп безопасности, неверно, возможно, что агенты были удалены без уведомления сервера

(например, если соединение клиент-сервер при удалении агента было прервано). В этом случае сервер сохраняет информацию об агенте в своей базе данных и на веб-консоли отображает агент, как работающий в автономном режиме. При переустановке агента сервер создает новую запись в базе данных и рассматривает агент как новый, что приводит к появлению в дереве групп безопасности агентов-дубликатов. Для выявления дублированных записей агентов используйте функцию проверки соединения агента в разделе **Администрирование** > **Глобальные параметры** > **Система**.

Установка агентов Security Agent

См. следующие темы:

- *Требования к установке Security Agent на странице 3-2*
- *Условия установки Security Agent на странице 3-2*
- *Способы установки Security Agent на странице 3-7*
  - *Установка с внутренней веб-страницы на странице 3-10*
  - *Установка с использованием программы настройки сценариев входа на странице 3-12*
  - *Установка с использованием Client Packager на странице 3-15*
  - *Удаленная установка на странице 3-19*
  - *Установка с использованием сканера уязвимостей на странице 3-22*
  - *Установка с уведомлением по электронной почте на странице 3-34*
- *Выполнение задач после установки для агентов Security Agent на странице 3-36*

Установка агентов Messaging Security Agent (только Advanced)

См. следующие темы:

- *Требования к установке Messaging Security Agent на странице 3-39*

- *Установка агентов Messaging Security Agent (только Advanced) на странице 3-39*

Добавление групп

Добавьте группу серверов или группу рабочих станций, которая может содержать один или несколько агентов Security Agent.

Невозможно добавить группу, содержащую агенты Messaging Security Agent. После того, как Messaging Security Agent установлен и сервер Security Server получил уведомление об этом, он автоматически становится своей собственной группой в **Дереве групп безопасности**.

Процедура

1. Перейдите к **Устройства**.
2. Нажмите кнопку **Добавить группу**.

   Появится новое окно.
3. Выберите тип группы.
   - **Настольные ПК**
   - **Серверы**
4. Введите имя группы.
5. Чтобы применить настройки существующей группы к добавляемой группе, нажмите **Импортировать параметры из группы**, а затем выберите группу. Будут показаны только группы для выбранного типа групп.
6. Нажмите кнопку **Сохранить**.

Настройка столбцов списка устройств

Вы можете выбрать столбцы, которые должны отображаться. Для этого выберите пункты **Дополнительно** > **Настроить столбцы** над списком устройств.

Столбец	Отображаемая информация
Для агентов Security Agent	
Клиент	
IP-адрес	IP-адрес клиентского компьютера, на котором установлен агент
Состояние	• **Подключен**: агент подключен к серверу Security Server • **Отключен**: агент отключен от сервера Security Server
Версия агента	Версия агента
Операционная система	Операционная система клиентского компьютера, на котором установлен агент
Архитектура	• **x64**: 64-разрядная операционная система • **x86**: 32-разрядная операционная система
Версия Exchange	Версия сервера Microsoft Exchange
Сканировать	

Столбец	Отображаемая информация
Служба Smart Scan **Примечание** Этот столбец отображается только при выборе метода Smart Scan.	• **Подключен**: агент подключен к службе Smart Scan • **Отключен**: агент отключен от службы Smart Scan **Примечание** Служба Smart Scan размещена на сервере Security Server. Если агент отключен, это означает, что он не может подключиться к серверу Security Server или что служба Smart Scan не работает (например, если она была остановлена). • **Отключено**: агент использует обычное сканирование
База данных агента Smart Scan / Вирусная база данных	Версия базы данных агента Smart Scan или вирусной базы данных
Сканирование по расписанию	Дата и время последнего сканирования по расписанию
Глубокое сканирование	Дата и время последнего глубокого сканирования
Сканирование почты POP3	• **Включено** • **Отключено**
Метод сканирования	• **Smart**: локальное сканирование и сканирование в облаке • **Обычное**: только локальное сканирование Для получения дополнительных сведений см. *Методы сканирования на странице 5-3*.
Стандартное сканирование	Дата и время последнего стандартного сканирования
Угроза	
Обнаружено вирусов	Количество найденных вирусов/вредоносных программ

Столбец	Отображаемая информация
Обнаружено шпионских программ	Количество обнаруженных шпионских и нежелательных программ
Обнаруженный спам	Количество нежелательных сообщений электронной почты
Доступ к запрещенным URL-адресам	Количество обращений к запрещенным URL-адресам
Модуль вирусного сканирования	Версия модуля вирусного сканирования
Для агентов Messaging Security Agent (только Advanced)	
Имя	Имя клиентского компьютера, на котором установлен агент
IP-адрес	IP-адрес клиентского компьютера, на котором установлен агент
Подключен/Отключен	• **Подключен**: агент подключен к серверу Security Server • **Отключен**: агент отключен от сервера Security Server
Платформа	Операционная система клиентского компьютера, на котором установлен агент
Архитектура	• **x64**: 64-разрядная операционная система • **x86**: 32-разрядная операционная система
Версия Exchange	Версия сервера Microsoft Exchange
Вирусная база данных	Версия вирусной базы данных
Модуль вирусного сканирования	Версия модуля вирусного сканирования
Версия агента	Версия агента

Перемещение агентов

Существует несколько способов перемещения агентов.

Агент для перемещения	Подробнее	Перемещение агентов
Security Agent	Перемещение агентов Security Agent между группами. После перемещения агент получает параметры новой группы.	Для перемещения одного или нескольких агентов используйте веб-консоль. См. *Перемещение агентов Security Agent между группами на странице 4-14*.
	Если у вас есть не менее двух серверов Security Server, переместите агенты Security Agent между серверами. После перемещения агент будет прикреплен к группе **Настольные компьютеры (по умолчанию)** или **Серверы (по умолчанию)** другого сервера Security Server, в зависимости от операционной системы клиентского компьютера. После перемещения агент получает параметры новой группы.	• Для перемещения одного или нескольких агентов используйте веб-консоль. См. *Перемещение агентов между серверами Security Server с помощью веб-консоли на странице 4-15*. • Запустите инструмент переназначения клиентов на клиентском компьютере для перемещения агента, установленного на этом клиенте. См. *Перемещение агента Security Agent между серверами Security Server с помощью инструмента переназначения клиентов на странице 4-16*.

Агент для перемещения	Подробнее	Перемещение агентов
Агент Messaging Security Agent (только Advanced)	Если у вас есть не менее двух серверов Security Server, переместите агенты Messaging Security Agent между серверами. После перемещения агент образует свою собственную группу на другом сервере Security Server и сохранит свои настройки.	Для перемещения одного агента за один раз используйте веб-консоль. См. *Перемещение агентов между серверами Security Server с помощью веб-консоли на странице 4-15*.

Перемещение агентов Security Agent между группами

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Выберите агенты для перемещения.

   Совет

   Для выбора нескольких смежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу SHIFT, — по последнему. Для выбора нескольких несмежных агентов Security Agent щелкните по первому агенту, а затем, удерживая нажатой клавишу CTRL, — по тем агентам, которые требуется выбрать.

4. Перетащите агенты в новую группу.

Перемещение агентов между серверами Security Server с помощью веб-консоли

Перед выполнением

Перемещение агента между серверами Security Server.

- Если агент, работающий под управлением более ранней версии, переходит на Security Server, работающий под управлением текущей версии, он будет обновлен автоматически.
- Не перемещайте агент, работающий под управлением текущей версии, на Security Server под управлением предыдущей версии, так как им невозможно будет управлять (агент будет удален со своего предыдущего сервера, но не сможет зарегистрироваться на новом сервере, вследствие чего не появится на веб-консоли). Агент сохранит текущую версию и не будет переведен на более раннюю.
- Оба сервера Security Server должны иметь одинаковые языковые настройки.
- Запишите имя и порт прослушивания Security Server, на который будет перемещен агент. Имя и порт прослушивания отображаются в окне параметров защиты Security Server над панелью задач.

Процедура

1. На веб-консоли сервера Security Server, который в настоящее время управляет агентами, откройте **Устройства**.
2. Для перемещения агентов Security Agent, выберите группу, а затем выберите агентов. Для перемещения агента Messaging Security Agent выберите его.
3. Щелкните пункт **Дополнительно** > **Переместить Security Agent**.

   Появится новое окно.
4. Введите имя и порт прослушивания сервера Security Server, на который будут перемещены агенты.

5. Нажмите кнопку **Переместить**.

6. Для проверки назначения агентов Security Agent другому серверу Security Server откройте веб-консоль сервера и найдите агент в дереве групп безопасности.

Примечание

Если Security Agent не отображается в дереве групп безопасности, перезапустите Trend Micro Security Server Master Service.

Перемещение агента Security Agent между серверами Security Server с помощью инструмента переназначения клиентов

Перед выполнением

Перемещение агента между серверами Security Server.

- Если агент, работающий под управлением более ранней версии, переходит на Security Server, работающий под управлением текущей версии, он будет обновлен автоматически.
- Не перемещайте агент, работающий под управлением текущей версии, на Security Server под управлением предыдущей версии, так как им невозможно будет управлять (агент будет удален со своего предыдущего сервера, но не сможет зарегистрироваться на новом сервере, вследствие чего не появится на веб-консоли). Агент сохранит текущую версию и не будет переведен на более раннюю.
- Оба сервера Security Server должны иметь одинаковые языковые настройки.
- Запишите имя и порт прослушивания Security Server, на который будет перемещен агент. Имя и порт прослушивания отображаются в окне параметров защиты Security Server над панелью задач.
- Войдите в систему клиента с правами администратора.

Процедура

1. Откройте на клиентском компьютере окно командной строки.

   Примечание

   Необходимо открыть командную строку с правами администратора.

2. Введите `cd` и путь к папке установки Security Agent. Например: `cd C:\Program Files\Trend Micro\Security Agent`

3. Запустите инструмент переназначения клиентов, используя следующий синтаксис:

   ```
   <имя исполняемого файла> -s <имя сервера> -p
   <прослушивающий порт сервера> -c <прослушивающий порт
   клиента> -pwd <пароль с правами на выгрузку и разблокировку
   агента>
   ```

Таблица 4-3. Параметры инструмента переназначения клиентов

Параметр	Объяснение
`<имя исполняемого файла>`	`IpXfer.exe` (32-разрядная версия) `IpXfer_x64.exe` (64-разрядная версия)
`<Имя сервера>`	Имя целевого сервера Worry-Free Business Security (сервер, на который будет перемещаться агент)
`<прослушивающий порт сервера>`	Прослушиваемый (или доверенный порт) сервера назначения Security Server.
`<прослушивающий порт клиента>`	Номер порта, используемого Security Agent для связи с сервером
`<Пароль с правами на выгрузку и разблокировку агента>`	Пароль для выгрузки и разблокировки агента Security Agent

Пример:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -pwd Password
```

4. Для проверки назначения агента Security Agent другому серверу Security Server откройте веб-консольь сервера и найдите агент в дереве групп безопасности.

Примечание

Если Security Agent не отображается в дереве групп безопасности, перезапустите Trend Micro Security Server Master Service.

Дублирование параметров

Дублирование параметров между группами Security Agent или между агентами Messaging Security Agent (только Advanced).

Дублирование параметров группы Security Agent

Используйте эту функцию, чтобы применить настройки определенной группы рабочих станций или серверов к другой группе того же типа. Дублирование параметров группы серверов для группы рабочих станций невозможно, и наоборот.

Если к определенному типу группы относится только одна группа, эта функция будет отключена.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите на значок шестерни рядом с названием группы.
4. Нажмите **Дублировать параметры**.

   Появится новое окно.
5. Выберите целевую группу, которой будут переданы настройки.

6. Нажмите кнопку **Применить**.

Дублирование параметров Messaging Security Agent (только Advanced)

Вы можете копировать параметры и переносить их между агентами Messaging Security Agent, если они используют один и тот же домен.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите на значок шестерни рядом с Messaging Security Agent.
4. Нажмите **Дублировать параметры**.

   Появится новое окно.
5. Выберите агент Messaging Security Agent, которому будут переданы параметры.
6. Нажмите кнопку **Применить**.
7. Если дублирование оказалось неудачным, сделайте следующее.
   a. откройте редактор реестра (regedit).
   b. Перейдите к `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
   c. В контекстном меню выберите **winreg** > **Разрешения**.
   d. Добавьте группу **Smex Admin Group** целевого домена и разрешите **доступ на чтение**.

+Импорт и экспорт параметров групп Security Agent

Экспорт параметров группы рабочих станций или группы серверов в файл `.dat` для резервного копирования настроек. Вы также можете использовать файл `.dat`, чтобы импортировать настройки в другую группу.

Примечание

Можно импортировать и экспортировать параметры из групп настольных ПК в группы серверов и наоборот. Тип группы не влияет на выбор параметров. Вы можете также использовать функцию **Дублировать параметры**, хотя эта функция зависит от типа группы. Для получения дополнительной информации о функции **Дублировать параметры** см. *Дублирование параметров на странице 4-18*.

Таблица 4-4. Параметры, которые могут быть импортированы и экспортированы

Выбор	Окно, содержащее параметры	Параметры, которые могут быть экспортированы/ импортированы
Группа рабочих станций ( ) или группа серверов ( )	Устройства (**Устройства** > **Политика настройки**)	• Антивирус и антишпионское ПО (сканирование в режиме реального времени) • Прогнозное машинное самообучение • Контроль действий • Надежные программы • Поместить в карантин • Web Reputation • Фильтрация URL-адресов • Брандмауэр • Контроль устройств • Инструменты пользователя (только для групп рабочих станций) • Права агента
	Сканирование вручную (**Сканирование** > **Сканирование вручную**)	Все параметры
	Сканирование по расписанию (**Сканирование** > **Сканирование по расписанию**)	Все параметры

Экспорт параметров

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу компьютеров или серверов.
3. Нажмите на значок шестерни рядом с названием группы.
4. Нажмите **Настройки политики экспорта**.

   Появится новое окно.
5. Нажмите **Экспорт**.

   Появится диалоговое окно.
6. Нажмите **Сохранить**, выберите нужное местоположение, а затем опять нажмите **Сохранить**.

Импорт параметров

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу компьютеров или серверов.
3. Нажмите **Настройки политики импорта**.

   Появится новое окно.
4. Нажмите **Обзор**, выберите файл и нажмите кнопку **Импортировать**.

Глава 5

Управление основными параметрами безопасности агентов Security Agent

В этой главе объясняется порядок настройки основных параметров безопасности для агентов Security Agent.

Краткий обзор основных параметров безопасности для Security Agent

Таблица 5-1. Краткий обзор основных параметров безопасности для Security Agent

Параметр	Описание	По умолчанию
Метод сканирования	Укажите, включено или отключено сканирование Smart Scan.	Параметр «Включено» или «Отключено» выбирается при установке.
Антивирус и антишпионское ПО	Настройка параметров сканирования в режиме реального времени, антивируса и защиты от «шпионских» программ	Включено (сканирование в реальном масштабе времени)
Прогнозное машинное самообучение	Настроить параметры предиктивного машинного самообучения	Выкл.
Контроль действий	Настройка параметров контроля действий	Включено для групп компьютеров Отключено для групп серверов
Надежные программы	Укажите, какие программы не нужно контролировать на предмет подозрительного поведения	---
Карантин	Указание папки карантина	http://<имя или IP-адрес Security Server>
Web Reputation	Настройка параметров службы Web Reputation «В офисе» и «Вне офиса»	В офисе: включено, низкий уровень Вне офиса: включено, средний уровень

Параметр	Описание	По умолчанию
Фильтрация URL-адресов	Фильтрация URL-адресов блокирует веб-сайты, нарушающие настроенные политики.	включено, низкий уровень
Разрешенные/ заблокированные URL-адреса	Настройка глобальных списков разрешенных и заблокированных объектов.	Отключено
Брандмауэр	Настройка параметров брандмауэра	Отключено.
Контроль устройств	Настройка автозапуска и доступа к USB-устройствам и сетевым ресурсам	Отключено.
Инструменты пользователя	Настройка мастера Wi-Fi и панели инструментов защиты от спама Trend Micro	Отключено: Мастер Wi-Fi Отключено: Панель инструментов защиты от спама Trend Micro в поддерживаемых почтовых клиентах
Права агента	Настройка доступа к параметрам из консоли агента Отключить развертывание обновлений и исправлений для агента Security Agent.	---

Методы сканирования

Агенты безопасности используют один из двух методов при сканировании угроз безопасности.

- **Интеллектуальное сканирование Smart Scan**: Агенты безопасности, использующие сканирование smart scan, в данном

документе называются **агенты smart scan**. Агенты Smart Scan используют преимущества локального сканирования и сканирования в облаке, предоставляемых службой File Reputation.

- **Обычное сканирование**: Агенты безопасности, которые не используют сканирование smart scan, называются **агентами обычного сканирования**. Агент обычного сканирования хранит все компоненты на клиент и выполняет локальное сканирование файлов.

В следующей таблице приводится сравнение этих двух методов сканирования.

Таблица 5-2. Сравнение обычного сканирования и интеллектуального сканирования Smart Scan

Основа сравнения	Обычное сканирование	Smart Scan
Выполнение сканирования	Security Agent обычного сканирования выполняет проверку на клиент.	• Агент smart scan выполняет проверку на клиент. • Если агент Security Agent не может определить степень опасности файла во время сканирования, Security Agent проверяет ее с помощью отправки запроса сканирования на сервер Scan Server (для агентов Агенты безопасности, подключенных к серверу Smart Scan) или на Trend Micro Smart Protection Network (для агентов Агенты безопасности, отключенных от сервера Smart Scan Server). **Примечание** Scan Server — это служба, размещенная на сервере Smart Scan Server. • Security Agent «кэширует» результат запроса сканирования, таким образом улучшая производительность сканирования.
Используемые и обновляемые компоненты	Все компоненты Security Agent доступны для источника обновления, кроме базы данных агента Smart Scan.	Для источника обновления доступны все компоненты, кроме вирусной базы данных

Основа сравнения	Обычное сканирование	Smart Scan
Стандартный источник обновлений	Сервер ActiveUpdate	Сервер ActiveUpdate

Настройка способов сканирования

Перед выполнением

При установке Security Server вам предлагается возможность включить Smart Scan. При выборе этого параметра по умолчанию будет использоваться метод Smart Scan, что означает, что все агенты Security Agent будут использовать Smart Scan. В противном случае по умолчанию будет использоваться обычное сканирование. Вы можете переключаться между этими методами сканирования в соответствии с текущими потребностями. Это может произойти в следующих случаях.

- Если агенты в настоящее время используют обычный метод сканирования и сканирование занимает значительное количество времени, вы можете переключиться на более быстрое и эффективное интеллектуальное сканирование Smart Scan. Вы также можете переключаться на метод Smart Scan при нехватке свободного места на диске агента, так как агенты Smart Scan используют вирусные базы меньшего размера и, следовательно, занимают меньше места на диске.

  Перед переключением на Smart Scan откройте **Администрирование** > **Глобальные параметры**, выберите вкладку **Настольный ПК или сервер** и перейдите в раздел **Общие параметры сканирования**. Убедитесь, что функция **Отключить службу Smart Scan** выключена.

- Переключите агенты на обычный метод сканирования в случае падения производительности Security Server, так как это может указывать на то, что он не в состоянии своевременно обрабатывать все запросы сканирования от агентов.

В следующей таблице приведены советы по переключению методов сканирования.

Таблица 5-3. Советы по переключению методов сканирования

Совет	Подробнее
Соединение с Security Server	Убедитесь, что агенты Security Agent могут подключиться к серверу Security Server. О переключении на другой метод сканирования будут уведомлены только подключенные агенты. Агенты, работающие в автономном режиме, получат уведомление при подключении. Также убедитесь, что компоненты Security Server обновлены, так как агенты загружают с него новые компоненты, а именно: базы данных агента Smart Scan для агентов, использующих интеллектуальное сканирование, и вирусные базы данных для агентов, работающих в режиме обычного сканирования.
Число переключаемых агентов Security Agent	Одновременное переключение относительно небольшого числа агентов Security Agent позволяет более эффективно использовать ресурсы Security Server. Во время изменения метода сканирования агентов Security Server может выполнять другие важные задачи.
Выбор времени	При переключении агентов Security Agent в первый раз они должны загрузить **полную версию** базы данных агента Smart Scan (для агентов, переключаемых на интеллектуальное сканирование) и вирусной базы данных (для агентов, переключаемых в режим обычного сканирования). Используйте для переключения часы меньшей загрузки для завершения процесса загрузки за короткий период времени. Также временно отключите на агентах функцию «Обновить сейчас», чтобы предотвратить обновления, инициируемые пользователями, и повторно включите ее после того, как методы сканирования агентов будут переключены. **Примечание** Впоследствии, если агенты часто обновляются, они будут загружать **небольшие, инкрементные** версии базы данных агента Smart Scan или вирусной базы данных.

Совет	Подробнее
Поддержка IPv6	Агенты Smart Scan IPv6, которые находятся в автономном режиме, не могут отправлять запросы непосредственно в систему Trend Micro Smart Protection Network. Для разрешения отправки запросов этим агентам Smart Scan требуется прокси-сервер с двойным стеком, который может преобразовать IP-адреса, например DeleGate.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Откройте **Метод сканирования**.
5. Выберите предпочтительный метод сканирования.
6. Нажмите кнопку **Сохранить**.

Сканирование в режиме реального времени для агентов Security Agent

Сканирование в режиме реального времени обеспечивает непрерывную защиту компьютера. Каждый раз при открытии, загрузке, копировании или изменении файла функция сканирования в режиме реального времени агента **Security Agent** сканирует файл на наличие угроз.

Настройка сканирования в режиме реального времени для агентов Security Agent

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **«Антивирус и антишпионское ПО»**.

   Появится новое окно.
5. Выберите **Включить антивирус и антишпионское ПО в режиме реального времени**.
6. Настройте параметры сканирования. Для получения дополнительных сведений см. *Сканирование объектов и действий для Security Agent на странице 7-11*.

   Примечание

   Если вы предоставите пользователям права настройки пользовательских параметров сканирования, во время сканирования будут использоваться настроенные пользователем параметры.
7. Нажмите кнопку **Сохранить**.

Прогнозное машинное самообучение

Модуль прогнозного машинного самообучения компании Trend Micro использует передовые технологии машинного обучения для сопоставления информации об угрозах и для выполнения углубленного анализа файлов в целях выявления возникающих неизвестных угроз

безопасности с помощью цифровых отпечатков, сопоставления API-интерфейсов и других свойств файлов. Модуль прогнозного машинного самообучения также выполняет анализ поведения неизвестных или малораспространенных процессов для того, чтобы определить попытки вновь появившейся или неизвестной угроз заразить вашу сеть.

Прогнозное машинное самообучение является мощным инструментом, который помогает защитить окружение от неопознанных угроз и атак нулевого дня.

Тип обнаружения	Описание
Файл	После обнаружения неизвестного или малораспространенного файла, программа Security Agent производит его сканирование с использованием расширенного модуля сканирования нежелательных программ (ATSE) для извлечения характеристик этого файла и отправляет отчет в модуль прогнозного машинного самообучения, расположенный в сети Trend Micro Smart Protection Network. Благодаря использованию моделирования вредоносных программ, прогнозное машинное самообучение сравнивает образец с моделью вредоносной программы, присваивает рейтинг вероятности и определяет вероятный тип вредоносной программы, которая содержится в файле. В зависимости от настройки функции прогнозного машинного самообучения программы Security Agent может попытаться поместить поврежденный файл в «карантин» в целях предотвращения распространения угрозы по сети.

Тип обнаружения	Описание
Обработка	После обнаружения неизвестного или малораспространенного процесса, программа Security Agent отслеживает этот процесс с помощью модуля контекстного сбора информации и отправляет отчет о действиях в модуль прогнозного машинного самообучения. Благодаря использованию поведенческого моделирования вредоносных программ, прогнозное машинное самообучение сравнивает поведение процесса с моделью, присваивает рейтинг вероятности и определяет вероятный тип вредоносной программы, которая выполняется в процессе. В зависимости от настройки функции прогнозного машинного самообучения, программа Security Agent может «завершить» пострадавший процесс или сценарий и предпринять попытку очистки файла, запустившего этот процесс или сценарий.

Настроить прогнозное машинное самообучение

Примечание

Для прогнозного машинного самообучения требуется следующее:

- включить контроль действий в меню **Политика настройки** > **Контроль действий**;
- Действующее подключение к Интернету для подключения к Smart Protection Network

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.

4. Нажмите **Прогнозное машинное самообучение**.

5. Выберите **Включить прогнозное машинное самообучение**.

6. Выберите тип обнаружения и соответствующее действие, которое будет выполняться в ходе прогнозного машинного самообучения.

Тип обнаружения	Действия
Файл	• **«Поместить на карантин»**: Автоматическое помещение в карантин файлов, демонстрирующих возможности, которые анализ прогнозного машинного самообучения отнес к характерным для вредоносных программ. • **Только журнал**: Сканирование неизвестных файлов и запись в журнал анализа прогнозного машинного самообучения для дальнейшего исследования угрозы.
Обработка	• **Прервать**: автоматическое завершение процессов или сценариев, выполняющих действия, которые анализ прогнозного машинного самообучения отнес к характерным для вредоносных программ. **Важно** Функция прогнозного машинного самообучения попытается очистить файлы, запустившие вредоносные процессы или сценарии. Если очистка завершится неудачно, то функция прогнозного машинного самообучения поместит пораженные файлы в карантин. • **Только журнал**: сканирование неизвестных процессов или сценариев и запись в журнал анализа прогнозного машинного самообучения для дальнейшего исследования угрозы.

7. Нажмите кнопку **Сохранить**.

Контроль действий

Агенты Security Agent осуществляют постоянный контроль над клиентскими системами для предотвращения необычных изменений в операционной системе и установленных программах. Администраторы или пользователи могут создавать списки исключений для того, чтобы позволить определенным программам работать при включенном контроле и полностью блокировать другие. Кроме того, программы, обладающие действительной цифровой подписью, можно запускать всегда.

Другой функцией контроля действий является защита файлов EXE и DLL от удаления или изменений. Когда функция контроля действий включена, пользователи могут создавать исключения для разрешения или блокировки определенных программ. Кроме того, пользователи могут установить защиту всех программ Intuit QuickBooks.

Настройка контроля действий

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Выберите **Контроль действий**.
5. Настройте следующие параметры необходимым образом:
   - **Включить контроль действий**

Примечание

Чтобы разрешить пользователям устанавливать собственные параметры контроля действий, выберите пункт **Устройства** > **{группа}** > **Политика настройки** > **Права агента** > **Контроль действий** и установите флажок **Разрешить пользователям изменять параметры контроля действий**.

- **Включить блокирование вредоносных программ для известных и потенциальных угроз**: блокирование вредоносных программ осуществляется с помощью набора внутренних правил, определяемых в **файлах вирусной базы**. Эти правила позволяют выявить типичную и подозрительную активность, характерную для вредоносных программ. Примерами такой активности могут служить внезапный и необъяснимый запуск новых служб, изменения брандмауэра, модификация системных файлов.

  Функция контроля действия вредоносного ПО предоставляет следующие параметры сканирования уровня угроз.

  - **Известных угроз**: блокировка действий, связанных с известными угрозами.
  - **Известные и потенциальные угрозы**: блокировка действий, связанных с известными угрозами, и принятие мер в отношении потенциально вредоносной активности.

- **Выводить запрос перед выполнением новых обнаруженных программ, загруженных по протоколу HTTP (кроме серверных платформ)**: контроль действий осуществляется совместно с Web Reputation с целью проверки распространенности файлов, загруженных через HTTP или с помощью приложений электронной почты. Администраторы могут настроить вывод запроса перед запуском для каждого «нового обнаруженного» файла. Trend Micro классифицирует программу как «новую обнаруженную» на основании количества случаев обнаружения файлов или возраста файла в зависимости от настроек, заданных Smart Protection Network.

Примечание

Каналы HTTP: сканируются исполняемые файлы (EXE). Приложения электронной почты (только Outlook и Почта Windows Live): сканируются исполняемые файлы (EXE) в файлах архива, не защищенных паролем.

- **Включить защиту Intuit QuickBooks**: позволяет защитить все файлы и папки Intuit QuickBooks от несанкционированного изменения другими программами. Эта функция не влияет на изменения, вносимые с помощью программ Intuit QuickBooks, предотвращая только изменение файлов другими несанкционированными приложениями.

  Поддерживаются следующие продукты:

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

  Примечание

  Все исполняемые файлы Intuit обладают цифровыми подписями и обновления для этих файлов не блокируются. При попытке другой программы изменить двоичный файл Intuit агент выводит сообщение с названием этой программы. Можно разрешить другим программам обновлять файлы Intuit. Для этого необходимо добавить нужную программу в «Список исключений контроля действий» агента. Выполнив обновление, не забудьте удалить программу из этого списка.

- **Защита от ПО для вымогательства**: Предотвращает несанкционированное изменение и шифрование файлов на компьютерах, выполняемые в следствие угроз «ПО для вымогательства». ПО для вымогательства — это тип вредоносных программ, которые ограничивают доступ к файлам и требуют оплату за восстановление зараженных файлов.

- **Включить защиту документов от несанкционированного шифрования или изменения**: позволяет защитить документы от несанкционированных изменений.
    - **Автоматическое резервное копирование файлов, измененных подозрительной программой**: при включенной защите документов автоматически создаются резервные копии файлов, измененных подозрительными программами.
- **Включить блокировку процессов, обычно связанных с ПО для вымогательства**: позволяет защитить локальные компьютеры от атак ПО для вымогательства благодаря блокированию процессов, как правило, связанных с попытками захвата контроля.
- (Только для групп рабочих станций) **Включить проверку программ с целью обнаружения и блокировки скомпрометированных исполняемых файлов**: вероятность обнаружения повышается благодаря отслеживанию действий, схожих с действиями ПО для вымогательства.
- **Прерывание программ, демонстрирующих нештатные признаки, ассоциирующиеся с хакерскими атаками**: Защита от хакерских атак работает вместе с проверкой программ с целью отслеживания действий программ и выявления нештатных признаков, которые могут указывать на то, что источник атаки использовал уязвимость программы. После обнаружения «Контроль действий» прерывает процессы программы.

Примечание

Для защиты от эксплуатации уязвимостей необходимо выбрать настройку **Включение проверки программ для обнаружения и блокирования исполняемых файлов, представляющих потенциальную угрозу**.

Примечание

Чтобы уменьшить вероятность того, что Worry-Free Business Security посчитает безопасный процесс вредоносным, убедитесь в наличии у компьютера доступа в Интернет для выполнения дополнительных процессов проверки с помощью серверов Trend Micro.

- **Исключения**: исключения включают в себя «Список разрешенных программ» и «Список заблокированных программ». Запуск программ, внесенных в «Список разрешенных программ», разрешен даже в том случае, если они нарушают политику контроля действий, а запуск программ, внесенных в «Список заблокированных программ», запрещен.

  - **Введите полный путь к программе**: введите полный путь Windows или путь UNC к программе. Разделяйте записи точкой с запятой. Нажмите кнопку **Добавить в список разрешенных** или **Добавить в список заблокированных**. При необходимости используйте переменные среды для указания путей.

  - **Список разрешенных программ**: программы из этого списка могут быть запущены. Для удаления программы из списка нажмите на соответствующий ей значок.

    В списке разрешенных программ поддерживаются подстановочные символы и переменные среды.

    Список поддерживаемых переменных среды см. в разделе *Поддерживаемые переменные среды на странице 5-18*.

  - **Список заблокированных программ**: программы из этого списка не могут быть запущены. Для удаления программы из списка нажмите на соответствующий ей значок.

    В списке заблокированных программ поддерживаются только подстановочные символы.

6. Нажмите кнопку **Сохранить**.

Поддерживаемые переменные среды

В следующей таблице перечислены переменные среды, которые можно использовать при добавлении в список пути к файлу или папке.

Переменная окружения	Пример	Эквивалентный путь
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

Надежные программы

Программы, указанные в списке разрешенных программ, не будут контролироваться на предмет подозрительных действий с файлами.

Конфигурирование надежных программ

Примечание

Программы в списке надежных программ не поддерживают подстановочные символы и переменные окружения.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Надежные программы**.

   Появится новое окно.
5. Чтобы исключить программу из числа контролируемых, укажите полный путь к файлу программы и нажмите кнопку **Добавить в список разрешенных программ**.

   `<drive_name>:/<path>/<file_name>`

   Пример 1 `C:\Windows\system32\regedit.exe`

   Пример 2 `D:\backup\tool.exe`

   Это исключит возможность использования злоумышленниками программ, внесенных в список исключений, но размещенных в другом месте.
6. Нажмите кнопку **Сохранить**.

Папка карантина

Если для зараженного файла выбрано действие «Карантин», Security Agent шифрует файл и **временно** перемещает его в папку карантина:

- `<папка установки Security Agent>\quarantine` для агентов, обновленных с версии 6.x или более ранней
- `<папка установки Security Agent>\SUSPECT\Backup` для вновь установленных агентов или обновленных с версии 7.x или более поздней

Security Agent отправляет зараженный файл в центральную папку карантина, которую можно настроить с помощью веб-консоли, выбрав **Устройства** > **{Group}** > **Политика настройки** > **Карантин**.

Центральная папка карантина по умолчанию

Центральная папка карантина по умолчанию расположена на сервере Security Server. Папка создана в формате URL и содержит имя или IP-адрес сервера Security Server, например `http://server`. Эквивалентный полный путь: `<папка установки Security Server>\PCCSRV\Virus`.

- Если сервер управляет агентами IPv4 и IPv6, используйте имя хоста для того, чтобы все агенты могли отправлять находящиеся на карантине файлы на сервер.
- Если у сервера есть только адрес IPv4 или он идентифицируется только по нему, только агенты IPv4 или агенты с двумя стеками могут отправлять находящиеся на карантине файлы на сервер.
- Если у сервера есть только адрес IPv6 или он идентифицируется только по нему, только агенты IPv6 или агенты с двумя стеками могут отправлять находящиеся на карантине файлы на сервер.

Альтернативная центральная папка карантина

Вы можете указать альтернативную центральную папку карантина, введя местоположение в виде URL-адреса, пути UNC либо полного пути к файлу. Агенты Security Agent должны иметь возможность подключаться к этой папке. Например, если в папку будут

отправляться находящиеся на карантине файлы от агентов с двумя стеками или только с адресом IPv6, то у нее должен быть адрес IPv6. Trend Micro рекомендует назначить папку с двойным стеком, определив ее по имени хоста и используя при вводе путь UNC.

Инструкции по определению центральной папки карантина

В таблице ниже приведены рекомендации, когда использовать URL-адрес, путь UNC или полный путь к файлу:

Таблица 5-4. Папка карантина

Папка карантина	Приемлемый формат	Пример	Примечания
Папка по умолчанию на сервере Security Server	URL-адрес	`http:// <имя хоста-сервера или IP-адрес>`	Если используется папка по умолчанию, настройте для нее параметры обслуживания (например, размер папки карантина) в разделе **Администрирование** > **Глобальные параметры** > **Вкладка «Система»** > **Обслуживание карантина**.
	Путь UNC	`\\<имя хоста сервера или IP-адрес>\ ofcscan \Virus`	
Другая папка на сервере Security Server	Путь UNC	`\\<имя хоста сервера или IP-адрес>\ D$ \Quarantined Files`	Если вы не хотите использовать папку по умолчанию (например, если недостаточно места на диске), укажите путь UNC к другой папке. В этом случае введите эквивалентный полный путь в разделе **Администрирование** > **Глобальные параметры** > **Вкладка «Система»** > **Обслуживание карантина**, чтобы настройки обслуживания вступили в силу.

<table>
<tr><th>Папка карантина</th><th>Приемлемый формат</th><th>Пример</th><th>Примечания</th></tr>
<tr><td rowspan="2">Папка на другом компьютере под управлением Security Server (если в вашей сети есть другие компьютеры, на которых установлен сервер Security Server)</td><td>URL-адрес</td><td>http:// <имя хоста сервера 2 или IP-адрес></td><td rowspan="3">Убедитесь, что агенты могут подключиться к этой папке. Если вы укажете неправильную папку, находящиеся на карантине файлы будут храниться в агенте, пока не будет указана верная папка карантина. В журнале вирусов/вредоносных программ сервера результат сканирования будет следующим: «Не удается отправить помещенный на карантин файл в назначенную папку карантина».

В случае использования пути UNC убедитесь, что папка карантина является общей для группы «Все» и вы установили для этой группы разрешение на чтение и запись.</td></tr>
<tr><td>Путь UNC</td><td>\\<имя хоста сервера 2 или IP-адрес>\ofcscan\Virus</td></tr>
<tr><td>Другой компьютер в сети</td><td>Путь UNC</td><td>\\<computer_name>\temp</td></tr>
<tr><td>Другая папка на клиентском компьютере</td><td>Полный путь</td><td>C:\temp</td><td>Укажите полный путь, если:

• вы хотите, чтобы находящиеся на карантине файлы находились только на клиентском компьютере;

• вы не хотите, чтобы агенты сохраняли файлы на клиентском компьютере в папке по умолчанию.

Если путь не существует, Security Agent создаст его автоматически.</td></tr>
</table>

Настройка папки карантина

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Поместить на карантин»**.

   Появится новое окно.
5. Настройте папку карантина. Для получения дополнительных сведений см. *Папка карантина на странице 5-20*.
6. Нажмите кнопку **Сохранить**.

Web Reputation

Служба Web Reputation помогает предотвратить доступ к URL-адресам в Интернете или URL-адресам, встроенным в сообщения электронной почты, которые представляют угрозу безопасности. Служба Web Reputation проверяет репутацию URL-адреса на серверах веб-репутации Trend Micro, а затем сопоставляет эту репутацию с политикой веб-репутации, используемой на клиенте. В зависимости от используемой политики:

- Security Agent будет блокировать или разрешать доступ к сайту.
- Messaging Security Agent (только Advanced) будет помещать на карантин, удалять или отмечать сообщение электронной почты, содержащее вредоносный URL-адрес, или разрешать отправку сообщения, если URL-адрес является безопасным.

Служба Web Reputation способна отправлять уведомления администратору по электронной почте, а также пользователям по сети об обнаруженных угрозах.

Для агентов Security Agent устанавливайте уровень безопасности в зависимости от месторасположения клиента (в офисе или вне офиса).

В случае, если служба Web Reputation блокирует сайты, которые вы считаете безопасными, добавьте их в список разрешенных URL-адресов.

Совет

Для сохранения пропускной способности сети компания Trend Micro рекомендует добавлять внутренние веб-сайты компании в список разрешенных URL-адресов Web Reputation.

Оценка репутации

«Оценка репутации» URL-адреса определяет, является веб-сайт опасным или нет. Оценка опирается на систему показателей, принадлежащую компании Trend Micro.

Trend Micro считает URL-адрес веб-угрозой, если его оценка находится ниже определенного порога, и безопасным, если его оценка превышает пороговое значение.

Существует три уровня безопасности, на основании которых агенты Security Agent блокируют URL-адрес или разрешают доступ к нему.

- **Высокий**: Блокировать страницы следующих типов.
  - **Опасные**: являющиеся мошенническими или известными источниками угроз.
  - **Чрезвычайно подозрительные**: подозреваемые в мошенничестве или в возможных источниках угроз
  - **Подозрительные**: связанные с рассылкой спама или взломанные

- **Не проверено**. Поскольку компания Trend Micro ведет активную деятельность по проверке безопасности веб-страниц, пользователи могут встречать непроверенные веб-страницы при посещении новых или не очень популярных веб-сайтов. Блокирование доступа в непроверенным страницам может повысить безопасность, но также может заблокировать доступ к безопасным страницам.

- **Средний**: Блокировать страницы следующих типов.
  - **Опасные**: являющиеся мошенническими или известными источниками угроз.
  - **Чрезвычайно подозрительные**: подозреваемые в мошенничестве или в возможных источниках угроз

- **Низкий**: Блокировать страницы следующих типов.
  - **Опасные**: являющиеся мошенническими или известными источниками угроз.

Настройка службы Web Reputation для агентов Messaging Security Agent

Служба Web Reputation оценивает потенциальную угрозу безопасности со стороны любого запрошенного URL-адреса, получая информацию из базы данных веб-безопасности компании Trend Micro при каждом запросе по протоколу HTTP/HTTPS.

Примечание

(только Standard) Настройте параметры Web Reputation для профилей «В офисе» и «Вне офиса». Если служба сведений о местонахождении отключена, настройки для режима «В офисе» могут быть использованы и в соединениях в режиме «Вне офиса». Для получения дополнительных сведений о службе местонахождения см. *Настройка параметров рабочей станции или сервера на странице 11-5*.

Если функция Web Reputation и предотвращение эксплойтов браузера включены, URL-адреса, заблокированные службой Web Reputation, сканируются службой «Предотвращение эксплойтов браузера». Функция «Предотвращение эксплойтов браузера» сканирует встроенные объекты (например, jar, class, pdf, swf, html, js) веб-страниц, связанных с URL-адресом.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Web Reputation** > **в офисе** или**Репутация веб-сайтов** > **вне офиса**.

   Появится новое окно.
5. Настройте следующие параметры необходимым образом:
   - **Включить Web Reputation**
   - Уровень безопасности: **высокий**, **средний** или **низкий**
   - Предотвращение эксплойтов браузера: **Блокирование страниц с вредоносным кодом сценариев**
6. Нажмите кнопку **Сохранить**.

Фильтрация URL-адресов

Фильтрация URL-адресов помогает контролировать доступ к веб-сайтам, тем самым сокращая непродуктивное время сотрудников, уменьшая использование полосы пропускания и создавая более безопасную рабочую Интернет-среду. Можно выбрать уровень защиты фильтрацией URL-адресов или задать нужные типы файлов.

Примечание

Для защиты пользователей Trend Micro автоматически блокирует все страницы с содержимым, считающимся незаконным в большинстве стран.

Настройка фильтрации URL-адресов

Выберите пункт **«Пользовательская»**, чтобы выбрать определенные типы веб-сайтов для блокирования в разное время дня.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Фильтрация URL-адресов**.

   Появится новое окно.
5. Настройте следующие параметры необходимым образом:
   - **Включить фильтрацию URL-адресов**
   - **Уровень эффективности фильтра**

- **Высокий**: Блокировка известных или потенциальных угроз безопасности, неприемлемого или потенциально оскорбительного содержимого, содержимого, способного повлиять на производительность работы или пропускную способность сети, а также неклассифицированных страниц
- **Средний**: Блокировка известных угроз безопасности и неприемлемого содержимого
- **Низкий**: Блокировка известных угроз безопасности
- **Пользовательская**: Выберите собственные категории, а также укажите время для блокировки этих категорий — в рабочее время и время отдыха.

- **Правила фильтрации**: Выберите целые категории или подкатегории, которые необходимо блокировать.
- **Рабочие часы**: Любые дни или часы, не подпадающие под определение рабочего времени, считаются нерабочим временем.

6. Нажмите кнопку **Сохранить**.

Разрешенные/заблокированные URL-адреса

Функция автоматического разрешения и блокировки URL-адресов позволяет управлять доступом к веб-сайтам и обеспечивать более безопасную работу в Интернете. Указать разрешенные или заблокированные URL-адреса можно в разделе «Глобальные параметры».

Также можно создавать пользовательские списки разрешенных и заблокированных URL-адресов для конкретных групп. Если параметр **Настроить список разрешенных/блокированных URL-адресов для этой группы** выбран, то для управления доступом к веб-сайтам в

программе Security Agent используется пользовательский список разрешенных или заблокированных URL-адресов, назначенный группе.

Настройка разрешенных/заблокированных URL-адресов

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите кнопку **Разрешенные/заблокированные URL-адреса**.

   Появится новое окно.
5. Настройте следующие параметры необходимым образом.
   - **Настроить список разрешенных/заблокированных URL-адресов для этой группы**: URL-адреса, указанные в этом списке, имеют приоритет над другими параметрами.
   - Чтобы исключить адреса из списка проверки служб Web Reputation и фильтрации URL-адресов, введите в текстовом поле **Разрешить URL-адреса** URL-адреса нужных веб-сайтов. Если нужно указать несколько URL-адресов, разделите их точками с запятой (;). Нажмите кнопку **Добавить**.

     Совет

     Нажмите **Импортировать из глобальных настроек**, чтобы вставить все записи. Для этой группы возможна настройка URL-адресов.
   - Чтобы заблокировать URL-адреса определенных веб-сайтов с помощью службы фильтрации, введите в текстовом поле **Заблокировать URL-адреса** URL-адреса нужных веб-сайтов.

Если нужно указать несколько URL-адресов, разделите их точками с запятой (;). Нажмите кнопку **Добавить**.

Совет

Нажмите **Импортировать из глобальных настроек**, чтобы вставить все записи. Для этой группы возможна настройка URL-адресов.

6. Нажмите кнопку **Сохранить**.

Брандмауэр

Брандмауэр может блокировать или разрешать определенные типы сетевого трафика, выполняя роль барьера между клиентом и сетью. Кроме того, брандмауэр определяет шаблоны в сетевых пакетах, которые могут свидетельствовать об атаке на клиенты.

Программа Worry-Free Business Security предлагает на выбор два варианта при настройке брандмауэра: простой режим и расширенный режим. В простом режиме брандмауэр работает с параметрами по умолчанию, рекомендованными компанией Trend Micro. Расширенный режим используется для изменения параметров брандмауэра.

Совет

Компания Trend Micro рекомендует удалить другие программные брандмауэры перед установкой и включением брандмауэра Trend Micro.

Настройки по умолчанию простого режима брандмауэра

Брандмауэр предлагает параметры по умолчанию в качестве основы для создания собственной стратегии защиты клиента. Настройки по умолчанию учитывают обычные требования к клиентским системам, такие как необходимость доступа в Интернет и передачи файлов по протоколу FTP.

Примечание

По умолчанию Worry-Free Business Security отключает брандмауэр на всех новых группах и агентах Security Agent.

Таблица 5-5. Параметры брандмауэра по умолчанию

Настройки	Состояние
Уровень безопасности	Низкий Входящий и исходящий трафик разрешен, блокируются только сетевые вирусы.
Система обнаружения вторжения	Отключено.
Предупреждение (отправить)	Отключено.

Таблица 5-6. Исключения брандмауэра по умолчанию

Имя исключения	Действие	Направление	Протокол	Порт
DNS	Разрешить	Входящие и исходящие	TCP/UDP	53
NetBIOS	Разрешить	Входящие и исходящие	TCP/UDP	137, 138, 139, 445
HTTPS	Разрешить	Входящие и исходящие	TCP	443
HTTP	Разрешить	Входящие и исходящие	TCP	80
Telnet	Разрешить	Входящие и исходящие	TCP	23
SMTP	Разрешить	Входящие и исходящие	TCP	25
FTP	Разрешить	Входящие и исходящие	TCP	21

Имя исключения	Действие	Направление	Протокол	Порт
POP3	Разрешить	Входящие и исходящие	TCP	110
MSA	Разрешить	Входящие и исходящие	TCP	16372, 16373
LDAP	Разрешить	Входящие и исходящие	TCP/UDP	389

Таблица 5-7. Параметры брандмауэра по умолчанию в зависимости от местоположения

Местоположение	Параметры брандмауэра
В офисе	Выкл.
Вне офиса	Выкл.

Фильтрация трафика

Брандмауэр может контролировать как входящий, так и исходящий трафик, а также блокировать трафик определенного типа в зависимости от следующих условий:

- направление (входящий/исходящий);
- протокол (TCP/UDP/ICMP/ICMPv6);
- порты назначения;
- компьютер назначения.

Сканирование на наличие сетевых вирусов

Кроме того, брандмауэр проверяет каждый пакет на наличие сетевых вирусов.

Потоковая проверка трафика

Брандмауэр позволяет выполнять потоковую проверку трафика. Он контролирует все подключения к клиентскому компьютеру и

запоминает состояния соединений. С помощью брандмауэра потоковой проверки трафика можно определить условия любого соединения, последующую транзакцию, а также нарушение стандартных условий соединения. Таким образом, эффективное использование брандмауэра включает в себя не только создание профилей и политик, но и анализ подключений и фильтрацию пакетов, которые проходят через брандмауэр.

Общий драйвер брандмауэра

Общий драйвер брандмауэра вместе с параметрами, определенными пользователем брандмауэра, блокирует порты во время вирусной эпидемии. Общий драйвер брандмауэра использует также файл сетевой вирусной базы данных для определения сетевых вирусов.

Настройка брандмауэра

Настройка брандмауэра для офисного режима и для режима вне офиса. Если служба сведений о местонахождении отключена, настройки для режима «В офисе» могут быть использованы и в соединениях в режиме «Вне офиса».

Для получения дополнительных сведений о службе местонахождения см. *Настройка параметров рабочей станции или сервера на странице 11-5*.

Trend Micro по умолчанию отключает брандмауэр.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Брандмауэр** > **В офисе** или **Вне офиса**.

5. Выберите **Включить брандмауэр**.

6. Выберите один из следующих параметров.

   - **Простой режим**. Включает настройки брандмауэра по умолчанию.

     Для получения дополнительных сведений см. *Брандмауэр на странице 5-30*.

   - **Расширенный режим**. Включает брандмауэр с возможностью выбора пользовательских настроек.

7. Если вы выбрали **Расширенный режим**, при необходимости настройте следующие параметры:

   - **Уровень безопасности**: Уровень безопасности определяет применение правил для портов, не внесенных в список исключений.

     - **Высокий**: блокирование всего входящего и исходящего трафика, за исключением трафика, указанного в списке исключений.

     - **Средний**: блокирование всего входящего трафика и разрешение всего исходящего трафика, за исключением трафика, разрешенного и заблокированного в списке исключений.

     - **Низкий**: разрешение всего входящего и исходящего трафика, за исключением заблокированного трафика, указанного в списке исключений. Это настройка по умолчанию для простого режима.

   - **Настройки**

     - **Включить систему обнаружения проникновения**: Система обнаружения проникновений распознает шаблоны в потоке сетевых пакетов, которые могут указывать на наличие атаки.

       Подробную информацию см. в разделе *Система обнаружения вторжения на странице D-4*.

- **Включить предупреждения**: Если Worry-Free Business Security обнаружит нарушение, клиент будет уведомлен об этом.

- **Исключения**. Порты в списке исключений не будут блокированы.

  Подробную информацию см. в разделе *Работа с исключениями брандмауэра на странице 5-35*

8. Нажмите кнопку **Сохранить**.

Работа с исключениями брандмауэра

Записи в списке исключений брандмауэра клиента можно настраивать, разрешая или запрещая различные типы сетевого трафика с учетом номеров портов клиента и IP-адресов. Во время вирусной эпидемии Security Server применяет исключения для политики Trend Micro, которая автоматически развертывается для защиты сети.

Во время вирусной эпидемии можно запретить весь трафик клиентского компьютера, включая HTTP-порт (порт 80). Однако чтобы предоставить заблокированным компьютерам доступ в Интернет, можно добавить в список исключений прокси-сервер.

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Брандмауэр** > **В офисе** или **Брандмауэр** > **Вне офиса**.

   Появится новое окно.

5. Выберите **Включить брандмауэр**.
6. Выберите **Расширенный режим**.
7. Добавление исключения
   a. Нажмите кнопку **Добавить**.

      Появится новое окно.

   b. Введите имя исключения.
   c. В разделе **«Действие»** выберите один из следующих вариантов:
      - **Разрешить передачу всего сетевого трафика**
      - **Запретить передачу всего сетевого трафика**
   d. В разделе **«Направление»** выберите **«Входящий»** или **«Исходящий»**, указав тип трафика, к которому будут применены настройки исключений.
   e. Выберите тип сетевого протокола из списка «Протокол»:
      - **Все**
      - **TCP/UDP** (по умолчанию);
      - **TCP**
      - **UDP**
      - **ICMP**
      - **ICMPv6**
   f. Укажите порт клиента, выбрав один из следующих вариантов:
      - **Все порты** (по умолчанию)
      - **«Диапазон»**: введите диапазон портов.
      - **Указанные порты**: укажите конкретные порты. Номера портов должны быть разделены запятой (,).

g. В разделе **Компьютеры** выберите IP-адреса клиентов, которые необходимо включить в список исключений. Например, если выбрать **Запретить весь сетевой трафик (входящий и исходящий)**) и ввести IP-адрес одного компьютера в сети, то любой клиент, в политике которого есть это исключение, не сможет обмениваться информацией с этим IP-адресом. Выберите один из следующих вариантов:

- **Все IP-адреса** (по умолчанию)
- **Один IP-адрес**: введите адрес IPv4 или IPv6 либо имя хоста. Для преобразования имени компьютера клиента в IP-адрес нажмите кнопку **«Преобразовать»**.
- **Диапазон IP-адресов (IPv4 или IPv6)** введите два адреса IPv4 или два адреса IPv6 в полях **С** и **По**. Невозможно ввести в одно поле адрес IPv6, а в другое адрес IPv4.
- **Диапазон IP-адресов (IPv6)**: введите префикс адреса IPv6 и длину.

h. Нажмите кнопку **Сохранить**.

8. Чтобы изменить исключения, нажмите **Правка**, а затем в появившемся окне измените параметры.

9. Для перемещения исключения вверх или вниз по списку выберите исключение, а затем нажимайте **Вверх** или **Вниз**, пока оно не окажется в необходимой позиции.

10. Для удаления исключения выберите его и нажмите кнопку **Удалить**.

Отключение брандмауэра для группы агентов

Процедура

1. Перейдите к **Устройства**.

2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Брандмауэр** > **В офисе** или **Брандмауэр** > **Вне офиса**.

   Появится новое окно.
5. Выберите пункт **Отключить брандмауэр**.
6. Нажмите кнопку **Сохранить**.

Отключение брандмауэра для всех агентов

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. Нажмите **Настольный ПК или сервер**.
3. В окне **Параметры брандмауэра** выберите **Отключить брандмауэр и удалить драйверы**.
4. Нажмите кнопку **Сохранить**.

Контроль устройств

Служба контроля устройств управляет доступом к внешним устройствам хранения, подключенным к локальным компьютерам. В частности, служба контроля устройств ограничивает доступ ко всем видам запоминающих устройств, которые подключаются через интерфейс USB, за исключением мобильных устройств и цифровых камер.

Настройка контроля устройств

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Контроль устройств**.
5. Настройте следующие параметры необходимым образом:
   - **Включить контроль устройств**
   - **Включить предотвращение автозапуска USB-устройств**
   - **Разрешения**:Устанавливаются для USB-устройств и сетевых ресурсов.

     Таблица 5-8. Разрешения контроля устройств

Разрешения	Файлы на устройстве	Входящие файлы
Полный доступ	Разрешенные действия: копирование, перемещение, открывание, сохранение, удаление, исполнение	Разрешенные действия: сохранение, перемещение, копирование Это означает, что файл может быть сохранен, перемещен и скопирован на устройство.
Нет доступа	Запрещенные действия: все операции Устройство и содержащиеся в нем файлы видны пользователю (например, из Windows Explorer).	Запрещенные действия: сохранение, перемещение, копирование

Разрешения	Файлы на устройстве	Входящие файлы
чтение	Разрешенные действия: копирование, открывание Запрещенные действия: сохранение, перемещение, удаление, исполнение	Запрещенные действия: сохранение, перемещение, копирование
Модификация	Разрешенные действия: копирование, перемещение, открывание, сохранение, удаление Запрещенные действия: исполнение	Разрешенные действия: сохранение, перемещение, копирование
Чтение и исполнение	Разрешенные действия: копирование, открывание, исполнение Запрещенные действия: сохранение, перемещение, удаление	Запрещенные действия: сохранение, перемещение, копирование

- **Исключения**. Если пользователю не предоставлено разрешение на чтение с определенного устройства, он все же может запускать или открывать любой файл или программу из списка разрешенных.

  Однако, если включена функция предотвращения автозапуска, то даже файл, включенный в список разрешенных, не может быть запущен.

  Чтобы добавить исключение в список разрешенных, введите имя файла, включая путь или цифровую подпись, и нажмите кнопку **Добавить в список разрешенных**.

6. Нажмите кнопку **Сохранить**.

Инструменты пользователя

- **Панель инструментов защиты от спама**: Фильтрует спам в Microsoft Outlook, отображает статистику и позволяет изменять отдельные настройки.
- **HouseCall**: Определяет безопасность беспроводного соединения путем проверки подлинности точек доступа на основе действительности их SSID, методов аутентификации и требований шифрования. В случае небезопасного соединения отображается всплывающее предупреждение.
- **Инструмент Case Diagnostic Tool**. Инструмент Case Diagnostic Tool Trend Micro (CDT) собирает необходимую отладочную информацию с продукта клиента всякий раз, когда возникают проблемы. Он автоматически включает и выключает статус отладки продукта и собирает необходимые файлы согласно категориям проблем. Trend Micro использует эти данные для устранения неполадок, связанных с продуктом.

  Данный инструмент доступен только на консоли агента Security Agent.
- **Инструмент переназначения клиентов**: Этот инструмент можно использовать для назначения клиентских систем одного сервера другому. Типы и языковые версии серверов должны совпадать.
- **Средство связи клиента с сервером**: используйте этот инструмент для устранения неполадок, связанных с взаимодействием между клиентом и сервером.

Настройка инструментов пользователя

Процедура

1. Перейдите к **Устройства**.
2. Выберите группу рабочих станций или серверов.

3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.

4. Нажмите **Инструменты пользователя**.

   Появится новое окно.

5. Настройте следующие параметры необходимым образом:

   - **Мастер Wi-Fi**: Выполняет проверку безопасности беспроводных сетей на основе действительности их SSID, методов аутентификации и требований шифрования.
   - **Панель инструментов защиты от спама**: Выполняет фильтрацию спама в приложении Microsoft Outlook.

6. Нажмите кнопку **Сохранить**.

Права агента

Для того чтобы пользователи имели возможность изменять параметры агента Security Agent в клиенте, они должны обладать правами агента.

Совет

Для обеспечения упорядоченной политики безопасности во всей организации Trend Micro рекомендует предоставлять пользователям ограниченные права. Таким можно гарантировать, что пользователи не смогут изменить параметры сканирования или выгрузить Security Agent.

Настройка прав агента

Процедура

1. Перейдите к **Устройства**.

2. Выберите группу рабочих станций или серверов.
3. Нажмите **Политика настройки**.

   Политика настройки: появится экран <название группы>.
4. Нажмите **Права агента**.
5. Настройте следующие параметры необходимым образом:

Раздел	Права
Антивирус и антишпионское ПО	• Настройки сканирования в режиме реального времени • Настройки сканирования вручную • Настройки сканирования по расписанию • Пропустить сканирование по расписанию
Брандмауэр	Параметры брандмауэра
Web Reputation — продолжить поиск	Отображение ссылки, которая позволяет пользователям продолжить просмотр определенного вредоносного URL-адреса до перезагрузки компьютера. При открытии других вредоносных URL-адресов будут по-прежнему отображаться предупреждения.
Фильтрация URL-адресов — продолжить поиск	Отображение ссылки, которая позволяет пользователям продолжить просмотр определенного запрещенного URL-адреса до перезагрузки компьютера. При открытии других запрещенных URL-адресов будут по-прежнему отображаться предупреждения.
Контроль действий	Пользователи могут изменять параметры контроля действий.
Надежные программы	Пользователи могут изменять параметры списка доверенных программ.

Раздел	Права
Параметры прокси-сервера	Пользователи могут настраивать параметры прокси-сервера. **Примечание** При отключении этой функции будут восстановлены параметры прокси-сервера по умолчанию.
Права обновления	• Пользователи могут выполнять обновления вручную. • Использовать Trend Micro ActiveUpdate в качестве второстепенного источника обновлений • Отключить развертывание оперативного исправления **Примечание** Одновременное развертывание оперативных, критических исправлений, обновлений, исправлений безопасности и пакетов обновления для большого числа агентов может значительно увеличить сетевой трафик. Этот параметр можно включить для некоторых групп с целью разнесения развертывания. Кроме того, этот параметр позволяет отключить автоматическое **обновление сборок** агентов (например, обновление бета-версии до сборки выпуска текущей версии продукта), но НЕ автоматическое **обновление версий** (например, обновление версии 7.x до текущей версии). Чтобы отключить автоматическое обновление версий, запустите пакет установки Security Server и выберите вариант отсрочки обновлений.
Безопасность клиента	Предотвращение изменения программных файлов, регистров и процессов Trend Micro пользователями или другими процессами.

6. Нажмите кнопку **Сохранить**.

Глава 6

Управление основными параметрами безопасности агентов Messaging Security Agent (только Advanced)

В данной главе описана программа Messaging Security Agent и рассмотрен процесс установки настроек сканирования в реальном времени, защиты от спама, фильтрации содержимого, блокирования вложений, а также настроек карантина для агентов.

Агентов Messaging Security Agent

Агенты Messaging Security Agent предназначены для защиты серверов Microsoft Exchange. Эти агенты предотвращают атаки с использованием электронной почты путем сканирования входящих и исходящих сообщений почтового ящика Microsoft Exchange и сообщений между Microsoft Exchange Server и внешними источниками. Кроме того, Messaging Security Agent позволяет:

- уменьшить количество спама;
- блокировать сообщения в зависимости от содержания;
- блокировать или ограничивать сообщения с вложениями.
- обнаруживать вредоносные URL-адреса в электронной почте;
- предотвращать утечки конфиденциальной информации.

Важная информация об агентах Messaging Security Agent

- Агенты Messaging Security Agent могут быть установлены только на сервере Microsoft Exchange.
- В Messaging Security Agent не поддерживаются некоторые функции Microsoft Exchange Server Enterprise, такие как Data Availability Group (DAG).
- В дереве групп безопасности в веб-консоли отображаются все агенты Messaging Security Agent. Несколько агентов Messaging Security Agent нельзя объединить в группу; каждым агентом Messaging Security Agent необходимо управлять отдельно.
- Программа Worry-Free Business Security использует агенты Messaging Security Agent для сбора связанной с безопасностью информации с серверов Microsoft Exchange. Например, Messaging Security Agent сообщает о случаях обнаружения спама или обновлениях компонентов серверу Security Server. Эта информация отображается в веб-консоли. Сервер Security Server также использует эту информацию для создания записей и отчетов о состоянии безопасности серверов Microsoft Exchange.

При каждом обнаружении угрозы создается одна журнальная запись или уведомление. Это означает, что если в одном сообщении электронной почты агент Messaging Security Agent обнаруживает несколько угроз, для каждой из них будет создана своя запись в журнале и уведомления. Бывают случаи множественного обнаружения одной и той же угрозы, особенно при работе в режиме кэширования в программе Outlook 2003. Когда включен режим кэширования, одна и та же угроза может быть обнаружена в очереди отправки, в папке «Отправленные» или «Исходящие».

- На компьютерах под управлением Microsoft Exchange Server 2007 агент Messaging Security Agent использует базу данных сервера SQL Server. Для предотвращения возникновения проблем службы Messaging Security Agent разработаны зависимыми от экземпляра службы `MSSQL$SCANMAIL`. При остановке или повторном запуске этого экземпляра следующие службы Messaging Security Agent также останавливаются:
  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  Если экземпляр `MSSQL$SCANMAIL` остановлен или повторно запущен, перезапустите эти службы вручную. Различные события, включая обновление SQL-сервера, могут вызвать повторный запуск или останов `MSSQL$SCANMAIL`.

Сканирование электронной почты агентом Messaging Security Agent

При сканировании сообщений электронной почты агент Messaging Security Agent выполняет следующие действия:

1. сканирование на наличие спама (антиспам);
   a. сравнение адреса отправителя сообщения электронной почты с адресами из списка разрешенных или заблокированных администратором отправителей;

b. проверка на наличие случаев фишинга;

c. сравнение электронной почты со списком исключений, который предоставляет компания Trend Micro;

d. сравнение электронной почты с базой сигнатур спама;

e. применение эвристических правил сканирования;

2. сканирование на наличие нарушений правил фильтрации содержимого;

3. сканирование на наличие вложений, выходящих за пределы заданных пользователем параметров;

4. сканирование на вирусы/вредоносные программы (антивирус);

5. сканирование на наличие вредоносных URL-адресов.

Параметры Messaging Security Agent по умолчанию

Обратите внимание на параметры в таблице, помогающие оптимизировать настройки Messaging Security Agent.

Таблица 6-1. Действия Trend Micro по умолчанию для агента Messaging Security Agent

Параметр сканирования	Сканирование в режиме реального времени	Сканирование вручную и по расписанию
Защита от спама		
Спам	Поместить сообщение на карантин в пользовательскую папку спама (по умолчанию, при установленном пользовательском карантине или папке Junk Email программы Outlook)	Информация отсутствует
Фишинг	Удалить сообщение целиком	Неприменимо.

Параметр сканирования	Сканирование в режиме реального времени	Сканирование вручную и по расписанию
Фильтрация содержимого		
Фильтровать сообщения, отвечающие любому из заданных условий	Поместить в карантин сообщение целиком	Заменить
Фильтровать сообщения, удовлетворяющие всем заданным условиям	Поместить в карантин сообщение целиком	Неприменимо.
Контролировать содержимое сообщений определенных учетных записей электронной почты	Поместить в карантин сообщение целиком	Заменить
Создать исключение для определенных почтовых ящиков	Пропустить	Пропустить
Блокирование вложений		
Действие	Заменить вложение текстом или файлом	Заменить вложение текстом или файлом
Прочее		
Зашифрованные и защищенные паролем файлы	Пропустить (При выборе действия «Пропустить» зашифрованные и защищенные паролем файлы игнорируются, и событие не фиксируется в журнале.)	Пропустить (При выборе действия «Пропустить» зашифрованные и защищенные паролем файлы игнорируются, и событие не фиксируется в журнале.)

Параметр сканирования	Сканирование в режиме реального времени	Сканирование вручную и по расписанию
Исключения (файлы, сканирование которых не производится)	Пропустить (При выборе действия «Пропустить» игнорируются файлы и тела сообщений, не удовлетворяющие установленным параметрам сканирования, и событие не фиксируется в журнале.)	Пропустить (При выборе действия «Пропустить» игнорируются файлы и тела сообщений, не удовлетворяющие установленным параметрам сканирования, и событие не фиксируется в журнале.)

Сканирование в режиме реального времени для агентов Messaging Security Agent

Сканирование в режиме реального времени обеспечивает непрерывную защиту компьютера. Сканирование в режиме реального времени с использованием **Messaging Security Agent** (только Advanced) защищает все известные точки проникновения вирусов путем проверки всех входящих сообщений, SMTP-сообщений, документов, размещаемых в публичных папках, и файлов, копируемых с других серверов Microsoft Exchange.

Настройка сканирования в режиме реального времени для агентов Messaging Security

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Нажмите **Антивирусная защита**.

   Появится новое окно.

5. Выберите **Включить антивирусное сканирование в режиме реального времени**.

6. Настройте параметры сканирования. Для получения дополнительных сведений см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*.

7. Нажмите кнопку **Сохранить**.

   Укажите получателя уведомлений при наступлении событий. См. *Настройка событий для уведомлений на странице 10-5*.

Защита от спама

Worry-Free Business Security предоставляет два способа борьбы со спамом: **службу Email Reputation** и **сканирование содержимого**.

Messaging Security Agent пользуется следующими компонентами для обнаружения спама и фишинга в почтовых сообщениях:

- Модуль защиты от спама компании Trend Micro
- Шаблоны спама компании Trend Micro

Trend Micro регулярно обновляет модуль и файл базы данных и делает их доступными для загрузки. Security Server может загружать эти компоненты посредством обновления по расписанию или обновления вручную.

Модуль защиты от спама использует сигнатуры спама и эвристические правила фильтрации писем. Все электронные сообщения сканируются, и каждому из них присваиваются баллы спама в зависимости от степени совпадения сообщения с правилами и шаблоном письма-спама. Messaging Security Agent сравнивает балл спама с заданным пользователем уровнем обнаружения спам-сообщений. Если оценка

спама превышает уровень диагностики, то агент выполняет действие по защите от спама.

Это может произойти в следующих случаях. спамеры часто используют восклицательные знаки, в том числе несколько восклицательных знаков подряд (!!!!), в своих электронных сообщениях. Когда Messaging Security Agent обнаруживает сообщение с большим количеством восклицательных знаков, он начисляет ему определенное количество баллов спама.

Совет

В дополнение к использованию модуля защиты от спама можно настроить функцию фильтрации содержимого. Она сканирует заголовок, тему и тело сообщения, а также вложение на предмет спама и нежелательного содержания.

Пользователь не может изменить метод, используемый модулем защиты от спама для присвоения баллов спама, но он может настраивать уровни обнаружения, которые Messaging Security Agent использует для причисления письма к спаму.

Примечание

Программа Microsoft Outlook может автоматически фильтровать сообщения, помеченные Messaging Security Agent как спам, и отправлять их в папку «Нежелательная почта».

Email Reputation

Технология Email Reputation позволяет распознать спам, основываясь на данных о репутации исходного транспортного агента электронной почты (MTA). Это приводит к выгрузке задания с сервера Security Server. При использовании технологии Email Reputation весь трафик, входящий по протоколу SMTP, проверяется по базам данных IP-адресов, чтобы убедиться в том, что исходный IP-адрес чист и не был помещен в черный список как известный источник спама.

Существует два режима работы службы Email Reputation. К ним относятся следующие:

- **Стандартный**: Стандартный уровень использует базу данных, отслеживающую репутацию около 2 млрд. IP-адресов. IP-адреса, которые несколько раз оказались связаны с рассылкой нежелательной почты, вносятся в эту базу данных и редко из нее удаляются.
- **Расширенный**: Расширенный уровень службы — служба на основе запросов DNS наподобие стандартной службы. Ядром этой службы является стандартная база данных репутации, используемая совместно с динамически определяемой репутацией — базой данных реального времени, которая блокирует сообщения из известных и подозреваемых источников спама.

При обнаружении сообщения с заблокированного или подозрительного IP-адреса служба Email Reputation блокирует это сообщение прежде чем оно достигнет шлюза.

Настройка службы Email Reputation

Email Reputation можно настроить для блокирования сообщений от известных или подозреваемых источников спама. Кроме этого, можно создать исключения для разрешения или блокирования сообщений от других отправителей.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Защита от спама** > **Email Reputation**.

   Появится новое окно.

5. Настройте необходимые параметры на вкладке **Цель**
   - **Включить защиту от спама в режиме реального времени (Email Reputation)**
   - **Уровень службы**:
     - **Стандартный**
     - **Расширенный**
   - **Разрешенные IP-адреса**: Сообщения с этих IP-адресов никогда не блокируются. Введите IP-адрес, который следует разрешить, и нажмите кнопку **Добавить**. Список IP-адресов можно загрузить из текстового файла. Для того чтобы удалить IP-адрес, выберите его и нажмите кнопку **Удалить**.
   - **Заблокированные IP-адреса**: Сообщения с этих IP-адресов блокируются всегда. Введите IP-адрес, который следует заблокировать, и нажмите кнопку **Добавить**. Список IP-адресов можно загрузить из текстового файла. Для того чтобы удалить IP-адрес, выберите его и нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить**.
7. Откройте веб-страницу http://ers.trendmicro.com/ для просмотра отчетов.

Примечание

Email Reputation является веб-службой. Администратор может настроить уровень службы только с веб-консоли.

Сканирование содержимого

Сканирование содержимого обнаруживает спам, исходя из содержимого сообщения, а не на основании IP-адреса отправителя. Messaging Security Agent использует модуль защиты от спама компании Trend Micro и шаблон спам-сообщений для фильтрации всех

электронных сообщений и проверки на спам перед доставкой их в Information Store. Сервер Microsoft Exchange Server не будет обрабатывать почту, определенную как спам, и она не будет доставлена в почтовые ящики конечных пользователей.

Примечание

Не путайте сканирование содержимого (защита от спама на основании сигнатур и эвристических данных) с фильтрацией содержимого (сканирование и блокирование электронной почты на основании категоризированных ключевых слов). См. *Фильтрация содержимого на странице 6-17*.

Настройка сканирования содержимого

Messaging Security Agent **в режиме реального времени** отсеивает спам-сообщения и принимает меры по защите серверов Microsoft Exchange.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Защита от спама** > **Сканирование содержимого**.

   Появится новое окно.
5. Выберите **Включить защиту от спама в режиме реального времени**.
6. Откройте вкладку **Цель** для выбора метода и уровня обнаружения спама, которыми будет пользоваться Messaging Security Agent для обнаружения спама.

   a. Выберите уровень обнаружения (**низкий**, **средний** или **высокий**) в списке уровней обнаружения спама. Messaging

Security Agent использует этот уровень при проверке всех сообщений.

- **«Высокий»**: это уровень, на котором процент относимых к спаму сообщений максимален. Messaging Security Agent проверяет все сообщения на наличие подозрительных файлов или текста, но при этом выше вероятность ложной тревоги. Ложные тревоги — это случаи причисления агентом Messaging Security Agent к спаму сообщений, которые таковыми не являются.

- **«Средний»**: это настройка используется по умолчанию и является рекомендуемой. Messaging Security Agent проверяет все сообщения на высоком уровне обнаружения спама, но при этом процент ложных тревог остается средним.

- **Низкий**: Это уровень, на котором процент относимых к спаму сообщений минимален. Messaging Security Agent осуществляет только фильтрацию явно выраженных и общих спам-сообщений. В данном случае вероятность ложных тревог крайне низка. Фильтрация по баллу спама.

b. Выберите пункт **Обнаружение случаев фишинга**, чтобы агент Messaging Security Agent отслеживал случаи фишинга. Для получения дополнительных сведений см. *Фишинг на странице 1-13*.

c. Добавьте адреса в списки разрешенных и заблокированных отправителей. Для получения дополнительных сведений см. *Списки разрешенных и заблокированных отправителей на странице 6-14*.

- **Разрешенные отправители**: электронные сообщения с этих адресов или из доменов с этими именами никогда не блокируются. Введите адреса или доменные имена для их разрешения и нажмите кнопку **Добавить**. При необходимости можно импортировать список адресов или имен доменов из текстового файла. Для того чтобы

удалить адрес или имя домена, выделите их и нажмите кнопку **Удалить**.

- **Заблокированные отправители**: электронные сообщения с этих адресов или из доменов с этими именами всегда блокируются. Введите адреса или имена доменов, которые следует заблокировать, и нажмите кнопку **Добавить**. При необходимости можно импортировать список адресов или имен доменов из текстового файла. Для того чтобы удалить адрес или имя домена, выделите их и нажмите кнопку **Удалить**.

Примечание

Администратор сервера Microsoft Exchange ведет отдельный список разрешенных и заблокированных отправителей на сервере Microsoft Exchange. Если пользователь добавляет адрес разрешенного отправителя, а этот адрес уже занесен администратором в список заблокированных, то Messaging Security Agent будет считать сообщения от этого отправителя спамом и принимать соответствующие меры.

7. Откройте вкладку **Действие**, чтобы задать действия, выполняемые агентом Messaging Security Agent, при обнаружении спам-сообщения или случая фишинга.

Примечание

Для получения дополнительных сведений о действиях см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*.

В зависимости от настройки Messaging Security Agent предпринимает одно из следующий действий:

- **Переместить сообщение на карантин в папку для спама на сервере**
- **Переместить сообщение в карантин в пользовательскую папку для спама**

Примечание

При выборе этого действия настройте карантин конечного пользователя. Для получения дополнительных сведений см. *Настройка обслуживания базы спама на странице 6-79*.

- **Удалить сообщение целиком**
- **Пометить и доставить**

8. Нажмите кнопку **Сохранить**.

Списки разрешенных и заблокированных отправителей

Список разрешенных отправителей — это список адресов электронной почты, заслуживающих доверия. Messaging Security Agent не причисляет к спамерам отправителей, которые занесены в список разрешенных, если не включена настройка **Обнаружение случаев фишинга**. При включенном параметре **Обнаружение случаев фишинга** агент обнаруживает случаи фишинга в электронной почте, после чего электронное сообщение не отправляется, даже если оно находится в списке разрешенных отправителей. Список заблокированных отправителей — это список подозрительных адресов электронной почты. Агент всегда распределяет электронные сообщения от заблокированных отправителей в категорию спама и выполняет соответствующие действия.

Существует два списка разрешенных отправителей: один список для администратора Microsoft Exchange и один — для конечных пользователей.

- Список разрешенных отправителей администратора Microsoft Exchange и список заблокированных отправителей (в окне **Защита от спама**) определяют, каким образом Messaging Security Agent будет сортировать письма, приходящие на сервер Microsoft Exchange.
- Конечный пользователь управляет папкой для спама, которая создается во время установки. Списки конечных пользователей

действуют только для тех сообщений, которые привязаны к хранилищу почты на сервере для каждого отдельно взятого конечного пользователя.

Общие принципы

- Списки разрешенных и заблокированных отправителей на сервере Microsoft Exchange обладают более высоким приоритетом, чем списки на клиентской системе. Допустим, что отправитель user@example.com внесен администратором в список заблокированных, однако пользователь добавил его в свой список разрешенных отправителей. Когда письма от этого отправителя приходят на сервер Microsoft Exchange, Messaging Security Agent расценивает их как спам и принимает соответствующие меры. Если агент, расценив письмо как спам, направляет его на карантин в локальную папку спама в ящике пользователя, то письмо в итоге будет доставлено в папку «Входящие», потому что отправитель занесен пользователем в список разрешенных.

- При использовании программы Outlook существует ограничение на количество и размер адресов в списке. Для предотвращения ошибки системы Messaging Security Agent ограничивает количество адресов, которые пользователь может добавлять в списки разрешенных. Это количество может меняться в зависимости от длины адресов.

Подстановка универсального символа

Messaging Security Agent поддерживает подстановочные символы для списков разрешенных и заблокированных отправителей. При этом в качестве группового символа (подстановочного знака) используется звездочка (*).

Messaging Security Agent не поддерживает подстановочные символы в поле «имя пользователя». Но при вводе шаблона, например «*@trend.com», агент все же интерпретирует этот адрес как «@trend.com».

Подстановочный знак можно использовать только в случае, если он:

- находится рядом только с одной фразой, первым или последним символом в строке;
- находится слева от знака @ и является первым символом в строке;
- выполняет ту же функцию, что и пропущенная часть в начале или конце строки.

Таблица 6-2. Сопоставление электронных адресов по групповым символам

Шаблон	Соответствующие образцы	Несоответствующие образцы
john@example.com	john@example.com	Любой адрес, отличный от шаблона
@example.com *@example.com	john@example.com mary@example.com	john@ms1.example.com john@example.com.us mary@example.com.us
example.com	john@example.com john@ms1.example.com mary@ms1.rd.example.com mary@example.com	john@example.com.us mary@myexample.com.us joe@example.comon
*.example.com	john@ms1.example.com mary@ms1.rd.example.com joe@ms1.example.com	john@example.com john@myexample.com.us mary@ms1.example.comon
example.com.*	john@example.com.us john@ms1.example.com.us john@ms1.rd.example.com.us mary@example.com.us	john@example.com mary@ms1.example.com john@myexample.com.us

Шаблон	Соответствующие образцы	Несоответствующие образцы
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us
..*.example.com *****.example.com	То же, что и *.example.com	
example.com example.com example.*.com @*.example.com	Неверные шаблоны	

Фильтрация содержимого

При фильтрации содержимого оцениваются входящие и исходящие сообщения на основе заданных пользователем правил. Каждое правило содержит список ключевых слов и фраз. При фильтрации содержимого оценивается заголовок и / или содержимое сообщений посредством сравнения сообщений со списком ключевых слов. Если фильтр содержимого находит слово, совпадающее с ключевым, то может быть выполнено действие по предотвращению доставки клиентам Microsoft Exchange нежелательного содержимого. Агент Messaging Security Agent может отправлять уведомления всякий раз при выполнении действиям по защите от нежелательного содержимого.

Примечание

Не путайте сканирование содержимого (защита от спама на основании сигнатур и эвристических данных) с фильтрацией содержимого (сканирование и блокирование электронной почты на основании категоризированных ключевых слов). См. *Сканирование содержимого на странице 6-10*.

Фильтр содержимого предоставляет средства для администратора по оценке и контролю доставки электронной почты, исходя из текста сообщения. Этот фильтр может использоваться для контроля входящих и исходящих сообщений с целью проверки существования надоедливого, агрессивного или по другим причинам нежелательного содержимого сообщений. Фильтр содержимого также предоставляет функцию проверку синонимов, которая позволяет расширить область действия своей политики. Например, можно создать правила для проверки следующих компонентов:

- сексуальные домогательства;
- расистский язык;
- спам, встроенный в тело электронного сообщения.

Примечание

По умолчанию фильтрация содержимого отключена.

Управление правилами фильтрации содержимого

Агент Messaging Security Agent выводит все правила фильтрации содержимого на экране **Фильтрация содержимого**. Чтобы открыть этот экран, выберите следующие пункты.

- Сканирование в режиме реального времени:

  Устройства > **{Messaging Security Agent}** > **Политика настройки** > **Фильтрация содержимого**

- Сканирование вручную:

  Сканирование > **Вручную** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

- Сканирование по расписанию:

  Сканирование > **По расписанию** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

Процедура

1. Ознакомьтесь с краткой информацией о правилах:

   - **Правило**: Worry-Free Business Security поставляется с заданными по умолчанию правилами фильтрации содержимого на основании указанных ниже категорий. **Оскорбительное содержимое**, **расовая дискриминация**, **половая дискриминация**, **мошенничество**, **письма по цепочке**. По умолчанию эти правила отключены. Вы можете изменять эти правила в соответствии с вашими требованиями или удалять их. Если ни одно из этих правил не отвечает вашим требованиям, вы можете добавить свои собственные правила.

   - **Действие**: действие, выполняемое агентом Messaging Security Agent при обнаружении нежелательного содержимого.

   - **Приоритет**: агент Messaging Security Agent последовательно применяет каждый фильтр в порядке, указанном на этой странице.

   - **Включено**: зеленый значок указывает на включенное правило, красный значок – на отключенное.

2. Выполните следующие задачи.

Задача	Шаги
Включить/ отключить фильтрацию содержимого	Установите или снимите флажок **Включить фильтрацию содержимого в режиме реального времени** в верхней части экрана.
Добавить правило	Нажмите кнопку **Добавить**. Откроется новое окно, в котором вы можете выбрать тип добавляемого правила. Подробные сведения см. здесь: *Типы правил фильтрации содержимого на странице 6-22*.

Задача	Шаги
Изменить правило	a. Щелкните по имени правила. Откроется новое окно. b. Доступные параметры зависят от типа правила. Чтобы определить тип правила, используйте второй пункт в навигационном меню в верхней части экрана. Это может произойти в следующих случаях. Фильтрация содержимого > **При соблюдении любого условия** > Изменить правило Подробнее о параметрах правил, которые можно изменять, см. далее. • *Добавление правила фильтрации при совпадении любого условия на странице 6-26* • *Добавление правила фильтрации при совпадении всех условий на странице 6-23* **Примечание** Это правило не распространяется ручные и запланированные сканирования фильтрации содержимого. • *Добавление правила мониторинга фильтрации содержимого на странице 6-30* • *Создание исключений в правилах фильтрации содержимого на странице 6-33*

Задача	Шаги
Изменить порядок правил	Агент Messaging Security Agent применяет к почтовым сообщениям правила фильтрации в том порядке, в каком они перечислены в окне **Фильтрация содержимого**. Установите порядок, в котором должны выполняться правила. Агент фильтрует все сообщения электронной почты в соответствии с каждым правилом до тех пор, пока нарушение правила не приведет к запуску действия, препятствующего дальнейшей проверке (например, удалить или поместить в карантин). Для оптимизации фильтрации содержимого порядок этих правил можно изменять. a. Установите флажок, соответствующий правилу, для которого необходимо изменить порядок. b. Нажмите кнопку **Изменить порядок**. Вокруг порядкового номера правила появится рамка. c. В поле столбца **Приоритет** удалите существующий порядковый номер и введите новый. **Примечание** Убедитесь, что введенное число не превышает общее число правил в списке. В случае ввода числа, превышающего общее число правил, Worry-Free Business Security не учитывает запись и не перемещает правило по порядку. d. Нажмите кнопку **Сохранить порядок**. Правило будет перемещено на введенный уровень приоритета, и порядковые номера всех остальных правил будут изменены соответственно. Например, если выбрано правило с номером 5, который изменен на номер 3, то номера 1 и 2 останутся без изменений, а номера, начиная с 3 и выше, увеличатся на одну позицию.
Включение/ отключение правил	Щелкните по значку под столбцом «Включено».

Задача	Шаги
Удалить правила	При удалении правила Messaging Security Agent обновляет порядок следования остальных правил, чтобы отразить внесенное изменение. **Примечание** Удаление правила является необратимым, но вместо удаления можно прибегнуть к отключению правила. a. Выберите правило. b. Нажмите кнопку **Удалить**.

3. Нажмите кнопку **Сохранить**.

Типы правил фильтрации содержимого

Создание правил фильтрации сообщений электронной почты в соответствии с заданными условиями или в соответствии с адресами электронной почты отправителя или получателя. Правила фильтрации содержат следующие условия: какие поля заголовков необходимо сканировать, сканировать тело сообщения или нет, а также поиск по ключевому слову.

Можно создать правила, которые позволяют осуществлять следующие действия.

- **Фильтровать сообщения, которые соответствуют любому из заданных условий**: С помощью правил этого типа можно фильтровать содержимое любого сообщения в процессе сканирования. Для получения дополнительных сведений см. *Добавление правила фильтрации при совпадении любого условия на странице 6-26*.
- **Фильтровать сообщения, удовлетворяющие всем заданным условиям**: С помощью правил этого типа можно фильтровать содержимое любого сообщения в процессе сканирования. Для

получения дополнительных сведений см. *Добавление правила фильтрации при совпадении всех условий на странице 6-23*.

Примечание

Это правило не распространяется ручные и запланированные сканирования фильтрации содержимого.

- **Отслеживать содержимое сообщений с определенных почтовых ящиков**: С помощью правил этого типа можно контролировать содержимое сообщений, поступающих на определенную учетную запись. Правила контроля аналогичны общим правилам фильтрации содержимого, за исключением того, что они фильтруют содержимое только тех сообщений, которые принадлежат определенной учетной записи. Для получения дополнительных сведений см. *Добавление правила мониторинга фильтрации содержимого на странице 6-30*.
- **Создать исключения для определенных почтовых ящиков**: С помощью правила этого типа можно создавать исключение для отдельных учетных записей. Если учетная запись исключена, она не будет фильтроваться на наличие нарушений правил содержимого. Для получения дополнительных сведений см. *Создание исключений в правилах фильтрации содержимого на странице 6-33*.

После того как правило создано, агент Messaging Security Agent начинает фильтровать все входящие и исходящие сообщения в соответствии с этим правилом. При обнаружении недопустимого содержимого Messaging Security Agent принимает меры по обработке почтового сообщения. При этом действия Security Server также определяются установленным пользователем правилом.

Добавление правила фильтрации при совпадении всех условий

Это правило не распространяется ручные и запланированные сканирования фильтрации содержимого.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Фильтрация содержимого**.

   Появится новое окно.
5. Нажмите кнопку **Добавить**.

   Появится новое окно.
6. Выберите **Фильтровать сообщения, удовлетворяющие всем заданным условиям**.
7. Нажмите кнопку **Далее**.
8. Введите имя правила в поле **Имя правила**.
9. Выберите часть сообщения, из которого требуется удалить нежелательное содержимое. Messaging Security Agent может фильтровать сообщения электронной почты по:
   - заголовку («От», «Кому», «Копия»);
   - Тема
   - размеру тела сообщения или вложения;
   - имени файла вложения.

   Примечание

   Messaging Security Agent поддерживает фильтрацию по заголовку и теме сообщения только при выполнении сканирования в режиме реального времени.
10. Нажмите кнопку **Далее**.

11. Выберите действие, которое Messaging Security Agent будет совершать при обнаружении нежелательного содержимого. Messaging Security Agent может выполнять следующие действия (для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

    - Заменить текстом или файлом

      Примечание

      Замена текста из полей «От», «Кому», «Копия» или «Тема» невозможна.

    - Поместить в карантин сообщение целиком
    - Поместить часть сообщения в карантин
    - Удалить сообщение целиком
    - Архивировать
    - Пропустить сообщение целиком

12. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил законных получателей сообщений о том, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

13. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил отправителей сообщений, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

14. В разделе **Дополнительные параметры** нажмите значок «плюс» (+), чтобы развернуть подраздел **Параметры архивирования**.

a. В поле **Папка карантина** введите путь к папке, в которую функция фильтрации содержимого будет помещать электронную почту на карантин, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\quarantine`

b. В поле **Папка архива** введите путь к папке, в которую функция фильтрации содержимого будет помещать архивированную электронную почту, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\backup for content filter`

15. Щелкните значок «плюс» (+), чтобы развернуть вложенный раздел **Параметры замены**.

a. В поле **Имя файла замены** введите имя файла, которым функция фильтрации содержимого будет заменять сообщение электронной почты при запуске правила с действием «Заменить текстом или файлом», или примите значение по умолчанию.

b. В поле **Текст замены** введите или вставьте содержимое текста замены, который функция фильтрации содержимого будет использовать, когда сообщение электронной почты запускает правило с действием «Заменить текстом или файлом», или примите текст по умолчанию.

16. Нажмите кнопку **Готово**.

Мастер закроется и вновь откроется экран «Фильтрация содержимого».

Добавление правила фильтрации при совпадении любого условия

- Сканирование в режиме реального времени:

  Устройства > **{Messaging Security Agent}** > **Политика настройки** > **Фильтрация содержимого**

- Сканирование вручную:

  Сканирование > **Вручную** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

- Сканирование по расписанию:

  Сканирование > **По расписанию** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

Процедура

1. Нажмите кнопку **Добавить**.

   Появится новое окно.

2. Выберите **Фильтровать сообщения, отвечающие любому из заданных условий**.

3. Нажмите кнопку **Далее**.

4. Введите имя правила в поле **Имя правила**.

5. Выберите часть сообщения, из которого требуется удалить нежелательное содержимое. Messaging Security Agent может фильтровать сообщения электронной почты по:

   - заголовку («От», «Кому», «Копия»);
   - Тема
   - тексту;
   - вложению.

   Примечание

   Messaging Security Agent поддерживает фильтрацию по заголовку и теме сообщения только при выполнении сканирования в режиме реального времени.

   ---

6. Нажмите кнопку **Далее**.

7. Добавьте ключевые слова для части сообщения, фильтруемого на наличие нежелательного содержимого. Для получения подробной информации о работе с ключевыми словами см. *Ключевые слова на странице D-5*.

   a. При необходимости выберите учет регистра при фильтрации.

   b. При необходимости импортируйте новые файлы ключевых слов из файла `.txt`.

   c. Определите список синонимов.

8. Нажмите кнопку **Далее**.

9. Выберите действие, которое Messaging Security Agent будет совершать при обнаружении нежелательного содержимого. Messaging Security Agent может выполнять следующие действия (для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

   - Заменить текстом или файлом

     Примечание

     Замена текста из полей «От», «Кому», «Копия» или «Тема» невозможна.

   - Поместить в карантин сообщение целиком
   - Поместить часть сообщения в карантин
   - Удалить сообщение целиком
   - Архивировать

10. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил законных получателей сообщений о том, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

11. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил отправителей сообщений, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

12. В разделе **Дополнительные параметры** нажмите значок «плюс» (+), чтобы развернуть подраздел **Параметры архивирования**.

    a. В поле **Папка карантина** введите путь к папке, в которую функция фильтрации содержимого будет помещать электронную почту на карантин, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\quarantine`

    b. В поле **Папка архива** введите путь к папке, в которую функция фильтрации содержимого будет помещать архивированную электронную почту, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\backup for content filter`

13. Щелкните значок «плюс» (+), чтобы развернуть вложенный раздел **Параметры замены**.

    a. В поле **Имя файла замены** введите имя файла, которым функция фильтрации содержимого будет заменять сообщение электронной почты при запуске правила с действием «Заменить текстом или файлом», или примите значение по умолчанию.

    b. В поле **Текст замены** введите или вставьте содержимое текста замены, который функция фильтрации содержимого будет использовать, когда сообщение электронной почты запускает правило с действием «Заменить текстом или файлом», или примите текст по умолчанию.

14. Нажмите кнопку **Готово**.

Мастер закроется и вновь откроется экран «Фильтрация содержимого».

Добавление правила мониторинга фильтрации содержимого

- Сканирование в режиме реального времени:

  Устройства > **{Messaging Security Agent}** > **Политика настройки** > **Фильтрация содержимого**

- Сканирование вручную:

  Сканирование > **Вручную** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

- Сканирование по расписанию:

  Сканирование > **По расписанию** > **{развернуть Messaging Security Agent}** > **Фильтрация содержимого**

Процедура

1. Нажмите кнопку **Добавить**.

   Появится новое окно.

2. Выберите **Контролировать содержимое сообщений определенных учетных записей электронной почты**.

3. Нажмите кнопку **Далее**.

4. Введите имя правила в поле **Имя правила**.

5. Укажите учетные записи электронной почты для отслеживания.

6. Нажмите кнопку **Далее**.

7. Выберите часть сообщения, из которого требуется удалить нежелательное содержимое. Messaging Security Agent может фильтровать сообщения электронной почты по:

- Тема
- тексту;
- вложению.

Примечание

Фильтрация по этим полям агентом Messaging Security Agent может осуществляться только во время сканирования в режиме реального времени. В режимах сканирования вручную и сканирования по расписанию содержание заголовка и темы сообщения не фильтруется.

8. Добавьте ключевые слова для части сообщения, фильтруемого на наличие нежелательного содержимого. Для получения подробной информации о работе с ключевыми словами см. *Ключевые слова на странице D-5*.

   a. При необходимости выберите учет регистра при фильтрации.

   b. При необходимости импортируйте новые файлы ключевых слов из файла `.txt`.

   c. Определите список синонимов.

9. Нажмите кнопку **Далее**.

10. Выберите действие, которое Messaging Security Agent будет совершать при обнаружении нежелательного содержимого. Messaging Security Agent может выполнять следующие действия (для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

    - Заменить текстом или файлом

Примечание

Замена текста из полей «От», «Кому», «Копия» или «Тема» невозможна.

    - Поместить в карантин сообщение целиком

- Поместить часть сообщения в карантин
- Удалить сообщение целиком
- Архивировать

11. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил законных получателей сообщений о том, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

12. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил отправителей сообщений, что содержимое было отфильтровано.

    Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

13. В разделе **Дополнительные параметры** нажмите значок «плюс» (+), чтобы развернуть подраздел **Параметры архивирования**.

    a. В поле **Папка карантина** введите путь к папке, в которую функция фильтрации содержимого будет помещать электронную почту на карантин, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\quarantine`

    b. В поле **Папка архива** введите путь к папке, в которую функция фильтрации содержимого будет помещать архивированную электронную почту, или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\backup for content filter`

14. Щелкните значок «плюс» (+), чтобы развернуть вложенный раздел **Параметры замены**.

a. В поле **Имя файла замены** введите имя файла, которым функция фильтрации содержимого будет заменять сообщение электронной почты при запуске правила с действием «Заменить текстом или файлом», или примите значение по умолчанию.

b. В поле **Текст замены** введите или вставьте содержимое текста замены, который функция фильтрации содержимого будет использовать, когда сообщение электронной почты запускает правило с действием «Заменить текстом или файлом», или примите текст по умолчанию.

15. Нажмите кнопку **Готово**.

Мастер закроется и вновь откроется экран «Фильтрация содержимого».

Создание исключений в правилах фильтрации содержимого

- Сканирование в режиме реального времени:

  Устройства > **{Messaging Security Agent}** > **Политика настройки** > **Фильтрация содержимого**

- Сканирование вручную:

  Сканирование > **Вручную** > **{Expand Messaging Security Agent}** > **Фильтрация содержимого**

- Сканирование по расписанию:

  Сканирование > **По расписанию** > **{Expand Messaging Security Agent}** > **Фильтрация содержимого**

Процедура

1. Нажмите кнопку **Добавить**.

Появится новое окно.

2. Выберите **Создать исключение для определенных почтовых ящиков**.
3. Нажмите кнопку **Далее**.
4. Введите имя правила.
5. В имеющееся поле введите учетную запись электронной почты, которую необходимо исключить из фильтрации содержимого и нажмите **«Добавить»**.

   Учетная запись добавляется в список исключенных учетных записей электронной почты. Агент Messaging Security Agent не применяет правила, приоритет которых ниже приоритета данного правила, к учетным записям электронной почты в данном списке.
6. После подготовки списка учетных записей нажмите **Готово**.

   Мастер закроется, и вновь откроется окно **Фильтрация содержимого**.

Предотвращение потери данных

Функция предотвращения потери данных предназначена для защиты от потери данных при передаче электронной почты. Эта функция может защищать такие данные, как номера социального страхования, номера телефона, номера банковских счетов, а также другую конфиденциальную деловую информацию, соответствующую заданной базе данных.

Данная версия поддерживает следующие версии Microsoft Exchange:

Таблица 6-3. Поддерживаемые версии Microsoft Exchange

Поддерживаемые	Неподдерживаемые
2007 x64	2003 x86/x64
2010 x64	2007 x86

Поддерживаемые	Неподдерживаемые
	2010 x86

Подготовительная работа

До начала проверки важных данных на предмет потенциальных потерь следует определить следующее.

- Какие данные нуждаются в защите от несанкционированных пользователей
- Где находятся данные
- Куда и как передаются данные
- Какие пользователи имеют право на доступ к такой информации и ее передачу

Эта важная проверка, как правило, требует ввода данных от нескольких отделов и персонала, которому известна важная информация в организации. Описанные ниже процедуры предусматривают, что была определена важная информация и установлены политики безопасности в отношении обращения с конфиденциальной деловой информацией.

Функция предотвращения потери данных состоит из трех основных элементов.

- **Правила** (базы данных для поиска соответствий).
- **Домены, исключаемые** из фильтрации.
- **Разрешенные отправители** (учетные записи электронной почты, исключаемые из фильтрации).

Для получения дополнительных сведений см. *Управление правилами предотвращения потери данных на странице 6-36*.

Управление правилами предотвращения потери данных

Все правила предотвращения потери данных Messaging Security Agent отображаются в окне **Предотвращение потери данных** (**Устройства** > **{Messaging Security Agent}** > **Политика настройки** > **Предотвращение потери данных**).

Процедура

1. Ознакомьтесь с краткой информацией о правилах:

   - **Правило**: Worry-Free Business Security поставляется с заданными по умолчанию правилами (см. *Правила предотвращения потери данных по умолчанию на странице 6-43*). По умолчанию эти правила отключены. Вы можете изменять эти правила в соответствии с вашими требованиями или удалять их. Если ни одно из этих правил не отвечает вашим требованиям, вы можете добавить свои собственные правила.

     Совет

     Чтобы просмотреть правило, наведите курсор на его имя. Правила, использующие регулярное выражение, помечены значком увеличительного стекла (

).

   - **Действие**: действие, выполняемое агентом Messaging Security Agent, когда правило активировано.

   - **Приоритет**: агент Messaging Security Agent последовательно применяет каждое правило в порядке, указанном на этой странице.

   - **Включено**: зеленый значок указывает на включенное правило, красный значок – на отключенное.

2. Выполните следующие задачи.

Задача	Шаги
Включение/ отключение функции предотвращения потери данных	Установите или снимите флажок **Включить предотвращение потери данных в режиме реального времени** в верхней части экрана.
Добавить правило	Нажмите кнопку **Добавить**. Откроется новое окно, в котором вы можете выбрать тип добавляемого правила. Подробные сведения см. здесь: *Добавление правил предотвращения потери данных на странице 6-44*.
Изменить правило	Щелкните по имени правила. Откроется новое окно. Подробнее о параметрах правил, которые можно изменять, см. *Добавление правил предотвращения потери данных на странице 6-44*.

Импорт и экспорт правил	Импортируйте одно или несколько правил из (или экспортируйте их в) текстовый файл, как показано ниже. При необходимости правила затем можно будет изменять непосредственно с помощью этого файла.
	
	`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`
	
	`RuleName=Bubbly`
	
	`UserExample=`
	
	`Value=Bubbly`
	
	`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`
	
	`RuleName=Master Card No.`
	
	`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b`

Задача	Шаги
	Чтобы экспортировать правила в текстовый файл, выберите одно или несколько правил в списке и нажмите **Экспорт**. **Совет** Можно выбирать только те правила, которые отображаются на экране. Для выбора правил, которые на данный момент отображаются на разных экранах, увеличьте значение «Строк на странице» в верхней части таблицы со списком правил, чтобы отобразить достаточное количество строк со всеми правилами, которые необходимо экспортировать.
	Импорт правил: a. Создайте текстовый файл в указанном выше формате. Вы также можете нажать **Загрузить дополнительные правила по умолчанию** внизу таблицы, а затем сохранить правила. b. Нажмите кнопку **Импортировать**. Откроется новое окно. c. Нажмите кнопку **Обзор**, чтобы указать файл для импорта, а затем нажмите кнопку **Импорт**. Функция предотвращения потери данных импортирует правила из файла и добавляет их в конец текущего списка правил. **Совет** Если список уже содержит более 10 правил, импортированные правила не будут отображаться на первой странице. Для отображения последней страницы списка пользуйтесь значками навигации по страницам в верхней или нижней части списка правил. Вновь импортированные правила должны отображаться здесь.

Задача	Шаги
Изменить порядок правил	Агент Messaging Security Agent применяет к сообщениям электронной почты правила предотвращения потери данных в том порядке, в котором они указаны в окне **Предотвращение потери данных**. Установите порядок, в котором должны выполняться правила. Агент фильтрует все сообщения электронной почты в соответствии с каждым правилом до тех пор, пока нарушение правила не приведет к запуску действия, препятствующего дальнейшей проверке (например, удалить или поместить в карантин). Для оптимизации предотвращения потери данных порядок этих правил можно изменять. a. Установите флажок, соответствующий правилу, для которого необходимо изменить порядок. b. Нажмите кнопку **Изменить порядок**. Вокруг порядкового номера правила появится рамка. c. В поле столбца **Приоритет** удалите существующий порядковый номер и введите новый. **Примечание** Убедитесь, что введенное число не превышает общее число правил в списке. В случае ввода числа, превышающего общее число правил, Worry-Free Business Security не учитывает запись и не перемещает правило по порядку. d. Нажмите кнопку **Сохранить порядок**. Правило будет перемещено на введенный уровень приоритета, и порядковые номера всех остальных правил будут изменены соответственно. Например, если выбрано правило с номером 5, который изменен на номер 3, то номера 1 и 2 останутся без изменений, а номера, начиная с 3 и выше, увеличатся на одну позицию.
Включение/ отключение правил	Щелкните по значку под столбцом «Включено».

Задача	Шаги
Удалить правила	При удалении правила Messaging Security Agent обновляет порядок следования остальных правил, чтобы отразить внесенное изменение. **Примечание** Удаление правила является необратимым, но вместо удаления можно прибегнуть к отключению правила. a. Выберите правило. b. Нажмите кнопку **Удалить**.

Задача	Шаги
Исключение отдельных учетных записей домена	Обмен конфиденциальной коммерческой информацией внутри компании — это неизбежное ежедневное явление. Кроме того, нагрузка на серверы Security Server была бы чрезмерной, если бы функция предотвращения потери данных фильтровала все внутренние сообщения. По этим причинам следует установить один или несколько доменов по умолчанию, которые являются источниками внутреннего почтового трафика компании, чтобы функция предотвращения потери данных не фильтровала сообщения, отправляемые с одной учетной записи электронной почты на другую в пределах домена компании. Этот список позволяет всем внутренним сообщениям электронной почты (в пределах домена компании) обходить правила предотвращения потери данных. Необходим по крайней мере один такой домен. Добавляйте элементы в этот список в случае использования более одного домена. Это может произойти в следующих случаях. `*@example.com` a. Щелкните значок «плюс» (+), чтобы развернуть раздел **Отдельные учетные записи доменов, исключенные из предотвращения потери данных**. b. Разместите курсор в поле **Добавить** и введите домен, используя следующий шаблон: `*@example.com` c. Нажмите кнопку **Добавить**. Этот домен отображается в списке под полем **Добавить**. d. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. **ПРЕДУПРЕЖДЕНИЕ!** Функция предотвращения потери данных не добавит указанный домен, пока не будет нажата кнопка **Сохранить**. Если нажать кнопку **Добавить**, но не нажать кнопку **Сохранить**, домен не будет добавлен.

Задача	Шаги
Добавить учетные записи электронной почты в список разрешенных отправителей	Электронная почта от разрешенных отправителей выходит за пределы вашей сети, не проходя фильтрацию функцией предотвращения потери данных. Функция предотвращения потери данных будет игнорировать содержимое любых сообщений, полученных от учетных записей электронной почты, входящих в список разрешенных. a. Щелкните значок «плюс» (+), чтобы развернуть раздел **Разрешенные отправители**. b. Разместите курсор в поле **Добавить** и введите полный адрес электронной почты, используя следующий шаблон: `example@example.com` c. Нажмите кнопку **Добавить**. Этот адрес электронной почты отображается в списке под полем **Добавить**. d. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. **Примечание** Функция предотвращения потери данных не добавит указанный адрес, пока не будет нажата кнопка **Сохранить**. Если нажать кнопку **Добавить**, но не нажать кнопку **Сохранить**, адрес не будет добавлен.

Задача	Шаги

Импортировать учетные записи электронной почты в список разрешенных отправителей	Можно импортировать список адресов электронной почты из текстового файла в формате по одной учетной записи электронной почты на строку, например:
	`admin@example.com`
	`ceo@example.com`
	`president@example.com`
	a. Щелкните значок «плюс» (+), чтобы развернуть раздел **Разрешенные отправители**.
	b. Нажмите кнопку **Импортировать**.
	Откроется новое окно.
	c. Нажмите кнопку **Обзор**, чтобы указать текстовый файл для импорта, а затем нажмите кнопку **Импорт**.
	Функция предотвращения потери данных импортирует правила из файла и добавляет их в конец текущего списка.

3. Нажмите кнопку **Сохранить**.

Правила предотвращения потери данных по умолчанию

Функция предотвращения потери данных имеет несколько правил по умолчанию, которые приведены в следующей таблице.

Таблица 6-4. Правила предотвращения потери данных по умолчанию

Имя правила	Пример	Регулярное выражение
Номер счета Visa Card	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
Номер счета MasterCard	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b

Имя правила	Пример	Регулярное выражение
Номер счета American Express	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Номер счета Diners Club/Carte Blanche	3111-111111-1111	.REG. [^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
Номер IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w](([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Код SWIFT	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
Дата ISO	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

Примечание

Файл архива, содержащий расширенные правила предотвращения потери данных, можно загрузить загружен с веб-консоли. Перейдите в раздел **Параметры защиты** > **{Messaging Security Agent}** > **Настроить параметры** > **Предотвращение потери данных** и нажмите кнопку **Загрузить дополнительные правила по умолчанию**.

Добавление правил предотвращения потери данных

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Нажмите **Предотвращение потери данных**.

   Появится новое окно.

5. Нажмите кнопку **Добавить**.

   Появится новое окно.

6. Выберите часть сообщения, которую необходимо оценить. Messaging Security Agent может фильтровать сообщения электронной почты по:

   - заголовку («От», «Кому», «Копия»);
   - Тема
   - тексту;
   - вложению.

7. Добавить правило.

   Чтобы добавить правило, основанное на ключевом слове, выполните следующее.

   a. Выберите **Ключевое слово**.

   b. Введите ключевое слово в появившееся поле. Длина такого ключевого слова должна составлять от 1 до 64 буквенно-цифровых символов.

   c. Нажмите кнопку **Далее**.

   Чтобы добавить правило, основанное на автоматически создаваемых выражениях, выполните следующее.

   a. См. *Регулярные выражения на странице D-11* для описания определения регулярных выражений.

   b. Выберите **Регулярное выражение (создано автоматически)**.

   c. В соответствующем поле введите **Имя правила**. Это поле обязательно для заполнения.

d. В поле **Пример** введите или вставьте пример типа строки (длиной до 40 символов), с которым должно совпадать регулярное выражение. Буквенно-цифровые символы отображаются в верхнем регистре в выделенной области с рядами ячеек под полем **Пример**.

e. Если в выражении имеются константы, выделите их, нажимая на ячейки, в которых отображаются символы.

   После щелчка по ячейке ее рамка становится красной, указывая на то, что это константа, а средство автоматического создания изменяет регулярное выражение, отображаемое под выделенной областью.

Примечание

Символы, которые не являются буквенно-цифровыми (например, пробелы, точки с запятой и другие знаки препинания), автоматически принимаются за константы и не могут быть переменными.

f. Для проверки того, что созданное регулярное выражение соответствует заданному шаблону, выберите пункт **Указать еще один пример для проверки правила (необязательно)**.

   Под этим параметром будет отображаться тестовое поле.

g. Введите другой пример введенного только что шаблона.

   Так, если это выражение должно совпадать с серией номеров счетов по шаблону «01-EX????? 20??», введите еще один соответствующий пример, такой как «01-Extreme 2010», и нажмите кнопку **Проверить**.

   Инструмент проверит новый образец по существующему регулярному выражению, и, если новый образец совпадает, напротив данного поля будет отображаться зеленая галочка. Если регулярное выражение не соответствует новому образцу, напротив поля будет отображаться красный символ X.

ПРЕДУПРЕЖДЕНИЕ!

В регулярных выражениях, создаваемых этим инструментом, учитывается регистр. Эти выражения могут совпасть только с шаблонами с точно таким же количеством символов, как и в образце. Оценка шаблонов с «одним и более» из указанных символов невозможна.

h. Нажмите кнопку **Далее**.

Чтобы добавить правило, основанное на определяемых пользователем выражениях, выполните следующее.

ПРЕДУПРЕЖДЕНИЕ!

Регулярные выражения являются высокоэффективным инструментом поиска совпадений строк. Перед их использованием обязательно хорошо освойте синтаксис регулярных выражений. Плохо составленные регулярные выражения могут иметь сильное отрицательное влияние на производительность. Компания Trend Micro рекомендует начинать с простых регулярных выражений. При создании нового правила используйте «архивирование» и проследите, как функция предотвращения потери данных работает с сообщениями с использованием данного правила. Если вы уверены, что у правила нет непредсказуемых последствий, действие можно изменить.

a. См. *Регулярные выражения на странице D-11* для описания определения регулярных выражений.

b. Выберите **Регулярное выражение (задано пользователем)**.

Отобразятся поля **Имя правила** и **Регулярное выражение**.

c. В соответствующем поле введите **Имя правила**. Это поле обязательно для заполнения.

d. В поле **Регулярное выражение** введите регулярное выражение, начинающееся с префикса `.REG.`, длиной до 255 символов, включая префикс.

ПРЕДУПРЕЖДЕНИЕ!

Будьте очень внимательны, копируя текст в это поле. Если в содержимое буфера обмена внесены какие-либо лишние символы, например «перевод строки» для определенной ОС или тег HTML, вставляемое выражение будет неточным. Поэтому компания Trend Micro рекомендует вводить выражения вручную.

e. Для проверки того, что регулярное выражение соответствует заданному шаблону, выберите пункт **Указать еще один пример для проверки правила (необязательно)**.

Под этим параметром будет отображаться тестовое поле.

f. Введите другой пример введенного только что шаблона (не более 40 символов).

Так, если это выражение должно совпадать с серией номеров счетов по шаблону «ACC-????? 20??», введите еще один соответствующий пример, такой как «Acc-65432 2012», и нажмите кнопку **Тест**.

Инструмент проверит новый образец по существующему регулярному выражению, и, если новый образец совпадает, напротив данного поля будет отображаться зеленая галочка. Если регулярное выражение не соответствует новому образцу, напротив поля будет отображаться красный символ X.

g. Нажмите кнопку **Далее**.

8. Выберите действие, которое агент Messaging Security Agent должен выполнять при обнаружении нежелательного содержимого (для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

- Заменить текстом или файлом

Примечание

Замена текста из полей «От», «Кому», «Копия» или «Тема» невозможна.

- Поместить в карантин сообщение целиком
- Поместить часть сообщения в карантин
- Удалить сообщение целиком
- Архивировать
- Пропустить сообщение целиком

9. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил предполагаемых получателей, когда правила предотвращения потери данных фильтруют определенное сообщение электронной почты.

   По различным причинам, может быть необходимо не уведомлять внешних получателей электронной почты о том, что сообщение, содержащее важную информацию, было заблокировано. Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

10. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил предполагаемых отправителей, когда правила предотвращения потери данных отфильтруют определенное сообщение электронной почты.

    По различным причинам может быть необходимо не уведомлять внешних отправителей электронной почты о том, что сообщение, содержащее важную информацию, было заблокировано. Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

11. В разделе **Дополнительные параметры** нажмите значок «плюс» (+), чтобы развернуть подраздел **Параметры архивирования**.

    a. В поле **Папка карантина** введите путь к папке, в которую функция предотвращения потери данных будет помещать электронную почту на карантин или примите значение по

умолчанию: `<папка установки Messaging Security Agent>\storage\quarantine`

b. В поле **Папка архива** введите путь к папке, в которую функция предотвращения потери данных будет помещать архивированную электронную почту или примите значение по умолчанию: `<папка установки Messaging Security Agent>\storage\backup for content filter`

12. Щелкните значок «плюс» (+), чтобы развернуть вложенный раздел **Параметры замены**.

a. В поле **Имя файла замены** введите имя файла, которым функция предотвращения потери данных будет заменять сообщение электронной почты при запуске правила с действием «Заменить текстом или файлом», или примите значение по умолчанию.

b. В поле **Текст замены** введите или вставьте содержимое текста замены, который функция предотвращения потери данных будет использовать, когда сообщение электронной почты запускает правило с действием «Заменить текстом или файлом», или примите текст по умолчанию.

13. Нажмите кнопку **Готово**.

Мастер закроется, и вновь откроется окно «Предотвращение потери данных».

Блокирование вложений

Блокирование вложений запрещает доставку файлов, вложенных в сообщения электронной почты, службе Information Store сервера Microsoft Exchange. Существует возможность настроить Messaging Security Agent на блокирование вложений по типу или имени, с последующей заменой, помещением на карантин или удалением всех сообщений, вложения в которые соответствуют выбранному критерию.

Блокирование может произойти во время сканирования в режиме реального времени, вручную или по расписанию, но действия удаления и помещения на карантин недоступны при сканировании вручную и по расписанию.

Расширение вложения определяет тип файла, например `.txt`, `.exe` или `.dll`. Однако Messaging Security Agent определяет фактический тип файла скорее по его заголовку, нежели по имени файла. Многие вирусы распространяются через файлы определенного типа. С помощью блокирования вложения в соответствии с типом файла снижается риск вирусной атаки на серверы Microsoft Exchange. Точно так же многие виды вирусов часто называют определенными именами.

Совет

Функция блокирования очень эффективна в борьбе с проникновением вирусов. Все файлы с высокой степенью риска и файлы, названия которых похожи на названия известных вирусов/вредоносных программ, можно временно помещать в карантин. Затем, когда появится время, можно проверить папку карантина и предпринять меры по защите от зараженных файлов.

Настройка блокирования вложений

Настройка параметров блокирования вложений для серверов Microsoft Exchange включает указание правила для блокирования сообщений с определенными вложениями.

- Сканирование в режиме реального времени:

  Устройства > **{Messaging Security Agent}** > **Политика настройки** > **Блокирование вложений**

- Сканирование вручную:

  Сканирование > **Вручную** > **{развернуть Messaging Security Agent}** > **Блокирование вложений**

- Сканирование по расписанию:

Сканирование > **По расписанию** > **{развернуть Messaging Security Agent}** > **Блокирование вложений**

Процедура

1. Настройте необходимые параметры на вкладке **Цель**

   - **Все вложения**: агент может блокировать все электронные сообщения с вложениями. Однако этот вариант сканирования требует объемной обработки. Уточните этот тип сканирования, исключив определенные типы или имена вложений.

     - **Исключить вложения следующих типов**

     - **Исключить вложения со следующими именами**

   - **Указанные вложения**: при выборе этого типа сканирования агент проверяет электронные сообщения только с указанными вложениями. Этот тип сканирования может быть сугубо индивидуальным и идеально подходит для обнаружения электронных сообщений с вложениями, подозрительных для вас с точки зрения угроз. Это сканирование выполняется очень быстро при указании относительного небольшого количества имен файлов или типов во вложениях.

     - **Типы вложений**: агент определяет действительный тип файла в первую очередь по заголовку, а не по имени файла.

     - **Имена вложений**: по умолчанию агент определяет действительный тип файла в первую очередь по заголовку, а не по имени файла. Если настроено блокирование вложений со сканированием по определенным именам, агент определяет типы вложений в соответствии с заданными именами.

   - **Блокировать типы или имена файлов внутри zip-архивов**

2. Откройте вкладку **Действие**, чтобы задать действия, выполняемые агентом Messaging Security Agent при обнаружении вложений. Messaging Security Agent может выполнять следующие действия

(для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

- Заменить текстом или файлом
- Поместить в карантин сообщение целиком
- Поместить часть сообщения в карантин
- Удалить сообщение целиком

3. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил предполагаемых получателей сообщений о том, что сообщение имеет вложения.

   Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

4. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил отправителей сообщений, что сообщение имеет вложения.

   Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

5. Щелкните значок «плюс» (+), чтобы развернуть вложенный раздел **Параметры замены**.

   a. В поле **Имя файла замены** введите имя файла, которым функция блокировки вложений будет заменять сообщение электронной почты при запуске правила с действием «Заменить текстом или файлом», или примите значение по умолчанию.

   b. В поле **Текст замены** введите или вставьте содержимое текста замены, который функция блокировки вложений данных будет использовать, когда сообщение электронной почты будет

запускать правило с действием «Заменить текстом или файлом», или примите текст по умолчанию.

6. Нажмите кнопку **Сохранить**.

Web Reputation

Служба Web Reputation помогает предотвратить доступ к URL-адресам в Интернете или URL-адресам, встроенным в сообщения электронной почты, которые представляют угрозу безопасности. Служба Web Reputation проверяет репутацию URL-адреса на серверах веб-репутации Trend Micro, а затем сопоставляет эту репутацию с политикой веб-репутации, используемой на клиенте. В зависимости от используемой политики:

- Security Agent будет блокировать или разрешать доступ к сайту.
- Messaging Security Agent (только Advanced) будет помещать на карантин, удалять или отмечать сообщение электронной почты, содержащее вредоносный URL-адрес, или разрешать отправку сообщения, если URL-адрес является безопасным.

Служба Web Reputation способна отправлять уведомления администратору по электронной почте, а также пользователям по сети об обнаруженных угрозах.

Для агентов Security Agent устанавливайте уровень безопасности в зависимости от месторасположения клиента (в офисе или вне офиса).

В случае, если служба Web Reputation блокирует сайты, которые вы считаете безопасными, добавьте их в список разрешенных URL-адресов.

Совет

Для сохранения пропускной способности сети компания Trend Micro рекомендует добавлять внутренние веб-сайты компании в список разрешенных URL-адресов Web Reputation.

Оценка репутации

«Оценка репутации» URL-адреса определяет, является веб-сайт опасным или нет. Оценка опирается на систему показателей, принадлежащую компании Trend Micro.

Trend Micro считает URL-адрес веб-угрозой, если его оценка находится ниже определенного порога, и безопасным, если его оценка превышает пороговое значение.

Существует три уровня безопасности, на основании которых агенты Security Agent блокируют URL-адрес или разрешают доступ к нему.

- **Высокий**: Блокировать страницы следующих типов.
  - **Опасные**: являющиеся мошенническими или известными источниками угроз.
  - **Чрезвычайно подозрительные**: подозреваемые в мошенничестве или в возможных источниках угроз
  - **Подозрительные**: связанные с рассылкой спама или взломанные
  - **Не проверено**. Поскольку компания Trend Micro ведет активную деятельность по проверке безопасности веб-страниц, пользователи могут встречать непроверенные веб-страницы при посещении новых или не очень популярных веб-сайтов. Блокирование доступа в непроверенным страницам может повысить безопасность, но также может заблокировать доступ к безопасным страницам.
- **Средний**: Блокировать страницы следующих типов.
  - **Опасные**: являющиеся мошенническими или известными источниками угроз.
  - **Чрезвычайно подозрительные**: подозреваемые в мошенничестве или в возможных источниках угроз
- **Низкий**: Блокировать страницы следующих типов.

- **Опасные**: являющиеся мошенническими или известными источниками угроз.

Настройка службы Web Reputation для агентов Messaging Security Agent

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Web Reputation**.

   Появится новое окно.
5. Настройте следующие параметры необходимым образом:
   - **Включить Web Reputation**
   - Уровень безопасности: **высокий**, **средний** или **низкий**
   - Разрешенные URL-адреса
     - **Разрешить URL-адреса**: если нужно указать несколько URL-адресов, разделите их точками с запятой (;). Нажмите кнопку **Добавить**.

Примечание

Разрешение URL-адреса приводит к разрешению всех его поддоменов.

Будьте внимательны при использовании подстановочных символов, поскольку они могут допускать большое количество URL-адресов.

- **Список разрешенных URL-адресов**: URL-адреса из этого списка не будут блокироваться.

6. Откройте вкладку **Действие** и выберите действие, которое агент Messaging Security Agent должен выполнять при обнаружении сайта с нежелательной репутацией (для описания см. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*):

   - Заменить текстом или файлом

     Примечание

     Замена текста из полей «От», «Кому», «Копия» или «Тема» невозможна.

   - Переместить сообщение на карантин в пользовательскую папку для спама
   - Удалить сообщение целиком
   - Пометить и доставить

7. Выберите **Выполнять действие с URL-адресами, которые не были оценены компанией Trend Micro** для определения неклассифицированных URL-адресов как подозрительных. Для сообщений электронной почты, содержащих неклассифицированные URL, также будет выполнено действие, указанное в предыдущем шаге.

8. Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил предполагаемых получателей, когда служба Web Reputation фильтрует определенное сообщение электронной почты.

   По различным причинам, может быть необходимо не уведомлять внешних получателей электронной почты о том, что сообщение, содержащее вредоносные URL-адреса, было заблокировано. Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите

внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

9. Выберите **Уведомлять отправителей**, чтобы агент Messaging Security Agent уведомил предполагаемых отправителей, когда служба Web Reputation фильтрует определенное сообщение электронной почты.

   По различным причинам может быть необходимо не уведомлять внешних отправителей электронной почты о том, что сообщение, содержащее вредоносные URL-адреса, было заблокировано. Выберите **Не уведомлять внешних отправителей**, чтобы отправлять уведомления только внутренним отправителям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

10. Нажмите кнопку **Сохранить**.

Mobile Security

Параметры защиты мобильных устройств позволяют предотвратить доступ посторонних устройств к серверу Microsoft Exchange Server и загрузку сведений с сервера. Администраторы определяют устройства, которым разрешен доступ к серверу Microsoft Exchange Server, а затем то, могут ли пользователи таких устройств загружать или обновлять электронную почту, календарь, контакты или задачи.

Администраторы могут также применять к устройствам политики безопасности. С помощью таких политик осуществляется управление длиной и сложностью пароля, блокировкой устройств после некоторого периода неактивности, использованием шифрования устройствами, а также очисткой данных устройства после серии неудачных попыток входа.

Поддержка безопасности мобильных устройств

Таблица 6-5. Поддержка мобильных устройств

ОС	Версия IIS	Политики защиты данных устройств		Управление доступом		
		Exchange 2007 (или более поздней версии), 64-разрядная версия	Exchange 2003, 32-разрядная версия	Exchange 2010 (и более поздней версии), 64-разрядная версия	Exchange 2007, 64-разрядная версия	Exchange 2003, 32-разрядная версия
• Windows 2008 (64-разрядная версия) • SBS 2008 (64-разрядная версия)	7 +	Да	Несовместимо	Да	Нет	Несовместимо
Windows 2003 (64-разрядная версия)	6.0	Да	Несовместимо	Нет	Нет	Несовместимо

ОС	Версия IIS	Политики защиты данных устройств		Управление доступом		
		Exchange 2007 (или более поздней версии), 64-разрядная версия	Exchange 2003, 32-разрядная версия	Exchange 2010 (и более поздней версии), 64-разрядная версия	Exchange 2007, 64-разрядная версия	Exchange 2003, 32-разрядная версия
• Windows 2003 (32-разрядная версия) • SBS 2003 (32-разрядная версия)	6.0	Несовместимо	Нет	Несовместимо	Несовместимо	Нет

Таблица 6-6. Поддержка ОС мобильных устройств

ОС мобильного устройства	Версия ОС
iOS	3.0 - 6.1 (4.3 - 7.0)
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

Настройка управления доступом к устройствам

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите кнопку **Mobile Security** > **Управление доступом к устройствам**.

   Появится новое окно.
5. Выберите параметр **Включить управление доступом к устройствам**.
6. Нажмите кнопку **Добавить**.
7. Введите имя и содержательное описание политики.
8. Выберите устройства, для которых необходимо разрешить или заблокировать доступ к серверу Microsoft Exchange Server путем определения владельцев устройств:
   - **Любое**
   - **Указать владельцев устройств**
9. Если выбран параметр **Указать владельцев устройств**
   a. Введите имя владельца устройства и нажмите кнопку **Поиск** для обнаружения владельца устройства в глобальном списке адресов сервера Microsoft Exchange Server.
   b. Выберите владельца устройства и нажмите кнопку **Добавить**.
10. Если известно, какая операционная система установлена на устройстве, выберите ее в раскрывающемся списке **Тип**.

11. Если известно, какие версии поддерживаются данной операционной системой, выберите параметр **Указать диапазон номеров версий** и укажите эти версии.
12. Укажите, должен ли агент Messaging Security Agent разрешать или блокировать доступ к электронной почте, календарю, контактам или задачам владельца устройства.
13. Нажмите кнопку **Сохранить**.

Отмена отложенной очистки устройства

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите кнопку **Mobile Security** > **Очистка устройств**.

   Появится новое окно.
5. Выберите устройство в таблице очистки и нажмите **Отменить очистку**.
6. Нажмите кнопку **ОК**.

Очистка устройств вручную

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.

3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Нажмите кнопку **Mobile Security** > **Очистка устройств**.

   Появится новое окно.

5. Нажмите кнопку **Выбрать устройства**.

   Появится новое окно.

6. Введите имя владельца устройства и нажмите кнопку **Поиск** для обнаружения его устройств.

7. Если устройство доступно для очистки, выберите устройство и нажмите кнопку **Очистить**.

   Примечание

   Если после поиска состояние устройства имеет значение **Очистка успешно завершена** или **В очереди на очистку**, устройство нельзя выбрать.

Настройка политик безопасности

Worry-Free Business Security использует политику по умолчанию Microsoft Exchange в качестве политики по умолчанию. Политика по умолчанию отображается в списке политик безопасности.

Worry-Free Business Security не поддерживает другие политики, добавленные с помощью консоли управления Microsoft Exchange или Exchange Cmdlet.

Trend Micro рекомендует администраторам управлять политиками безопасности с консоли управления Worry-Free Business Security или Microsoft Exchange.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите кнопку **Mobile Security** > **Политики безопасности**.

   Появится новое окно.
5. Нажмите кнопку **Добавить**.
6. Введите имя и содержательное описание политики.
7. Введите имя владельца устройства и нажмите кнопку **Поиск** для обнаружения владельца устройства в глобальном списке адресов сервера Microsoft Exchange Server.
8. Выберите владельца устройства и нажмите кнопку **Добавить**.
9. Выберите критерий безопасности, который необходимо применить к устройству.
   - **Минимальная длина пароля**: инструкции по настройке пароля для мобильных устройств см. в *Требования к уровню сложности пароля на странице 6-65*.
   - **Минимальное количество наборов символов**: инструкции по настройке пароля для мобильных устройств см. в *Требования к уровню сложности пароля на странице 6-65*.
   - **Блокировка устройства при неактивности**
   - **Обязательное использование шифрования на устройстве**: мобильное устройство должно поддерживать шифрование.
   - **Очистка устройства после неудачных попыток входа**
10. Нажмите кнопку **Сохранить**.

Требования к уровню сложности пароля

Требования к уровню сложности пароля отличаются в зависимости от типа устройства и используемой операционной системы.

В следующих таблицах описано поведение каждого «варианта» уровня сложности для устройств, протестированных с выходом Worry-Free Business Security 9,0 SP3.

Примечание

Функциональность пароля зависит от типа и операционной системы устройства. Если указанный пароль не соответствует требованиям уровня сложности, пользователь устройства, как правило, получает сообщение с указанием требований, характерных для данного типа устройства.

Таблица 6-7. Устройства Android

Уровень сложности	Требования к уровню сложности	
	Android 4	Android 2
Вариант 1	Комбинация типов символов, представленных ниже: • Как минимум одна прописная (A–Z) или строчная (a–z) буква • Как минимум одна цифра (0–9) или один специальный символ (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Буквенно-цифровые символы
Вариант 2	Комбинация типов символов, представленных ниже: • Как минимум одна прописная (A–Z) или строчная (a–z) буква • Как минимум две цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум две цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Уровень сложности	Требования к уровню сложности	
	Android 4	Android 2
Вариант 3	Комбинация типов символов, представленных ниже: • Как минимум одна прописная (A–Z) или строчная (a–z) буква • Как минимум три цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум три цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Вариант 4	Комбинация типов символов, представленных ниже: • Как минимум одна прописная (A–Z) или строчная (a–z) буква • Как минимум четыре цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум четыре цифры (0–9) или специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Таблица 6-8. Устройства iOS

Уровень сложности	Требования к уровню сложности
Вариант 1	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум один специальный символ (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Вариант 2	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум два специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Уровень сложности	Требования к уровню сложности
Вариант 3	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум три специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Вариант 4	Комбинация типов символов, представленных ниже: • Буквенно-цифровые символы • Как минимум четыре специальных символа (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Таблица 6-9. Устройства Windows Phone

Уровень сложности	Требования к уровню сложности	
	Windows Phone 8	Windows Phone 7
Вариант 1	Как минимум один тип символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)	Комбинация как минимум двух типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)
Вариант 2	Комбинация как минимум двух типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)	Комбинация как минимум двух типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)

Уровень сложности	Требования к уровню сложности	
	Windows Phone 8	Windows Phone 7
Вариант 3	Комбинация как минимум трех типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)	Комбинация как минимум трех типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)
Вариант 4	Комбинация всех типов символов, представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)	Комбинация всех типов символов, представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)

Таблица 6-10. Устройства BlackBerry

Уровень сложности	Требования к уровню сложности
Вариант 1	Как минимум одна прописная (A–Z) или строчная (a–z) буква
Вариант 2	Комбинация как минимум двух типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)

Уровень сложности	Требования к уровню сложности
Вариант 3	Комбинация как минимум трех типов символов из представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)
Вариант 4	Комбинация всех типов символов, представленных ниже: • прописные буквы (A–Z); • строчные буквы (a–z); • цифры (0–9); • специальные символы (!@#$ %^&*()_-=+~`[]{}|;:'"?/&,.)

Карантин для агентов Messaging Security Agent

Когда агент Messaging Security Agent обнаруживает в сообщении электронной почты угрозу, спам, недопустимое вложение или недопустимое содержимое, это сообщение перемещается в папку карантина. Этот процесс является альтернативой удалению сообщения или вложения и предотвращает открытие зараженного сообщения, что может вызвать распространение угрозы.

Папкой карантина по умолчанию на агенте Messaging Security Agent является

```
<папка установки Messaging Security Agent>\storage\quarantine
```

Файлы, отправленные в карантин, для большей безопасности шифруются. Для открытия зашифрованного файла используйте инструмент восстановления зашифрованных вирусов и шпионских программ (`VSEncode.exe`). См. *Восстановление зашифрованных файлов на странице 14-19*.

Администраторы могут отправлять запросы в базу данных карантина для сбора информации о сообщениях, отправленных на карантин.

Карантин предназначен для

- устранения возможности полного удаления важных сообщений в том случае, если они были ошибочно заблокированы агрессивными фильтрами;
- просмотра сообщений, инициирующих запуск фильтров содержимого, для определения степени опасности нарушения политики;
- сохранения свидетельств возможных злоупотреблений почтовыми ресурсами компании.

Примечание

Не путайте папку карантина с пользовательской папкой для спама. Папка карантина является папкой с файлами. Каждый раз, когда агент Messaging Security Agent помещает сообщение на карантин, он отправляет сообщение в папку карантина. Пользовательская папка для спама находится в хранилище данных каждого пользовательского почтового ящика. В папку спама конечного пользователя попадают только те сообщения, которые были перемещены в пользовательскую папку для спама на карантин, а не отобранные в результате фильтрации содержимого, применения антивирусных, антишпионских политик или политик по блокированию вложений.

Запрос папок карантина

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Нажмите **Запрос** > **карантина**.

   Появится новое окно.

5. Настройте следующие параметры необходимым образом:

   - Диапазон дат и времени
   - Причины помещения в карантин
     - **Все причины**
     - **Указанные типы**: Выберите пункт: «Антивирусное сканирование», «Защита от спама», «Блокирование вложений» и/или «Части сообщений, не допускающие сканирования».
   - Состояние пересылки
     - **Никогда не пересылалось**
     - **Пересылалось как минимум один раз**
     - **И то, и другое**
   - Расширенные критерии
     - **Отправитель**: Сообщения от определенных отправителей. При необходимости можно использовать подстановочные символы.
     - **Получатель**: Сообщения от определенных получателей. При необходимости можно использовать подстановочные символы.
     - **Тема**: Сообщения с определенными темами. При необходимости можно использовать подстановочные символы.
     - **Сортировать по**: Настройка условий сортировки результатов на странице.
     - **Просмотр**: Количество результатов на странице.

6. Нажмите кнопку **Поиск**. См. *Просмотр результатов запроса и выполнение действий на странице 6-72*.

Просмотр результатов запроса и выполнение действий

Окно **«Результаты запроса к карантину»** отображает следующую информацию о сообщениях.

- **Время сканирования**
- **Отправитель**
- **Получатель**
- **Тема**
- **Причина**: Причина, по которой сообщение было отправлено в карантин.
- **Имя файла**: Имя заблокированного файла в сообщении.
- **Путь к папке карантина**: Местонахождение сообщения в карантине. Администраторы могут расшифровать файл при помощи программы VSEncoder.exe (см. раздел*Восстановление зашифрованных файлов на странице 14-19*), а затем изменить его расширение на `.eml` и просмотреть.

  ПРЕДУПРЕЖДЕНИЕ!

  Просмотр зараженных файлов может вызвать распространение заражения.

- **Состояние пересылки**

Процедура

1. Если у вас нет уверенности, что сообщение безопасно, удалите его.

ПРЕДУПРЕЖДЕНИЕ!

Папка карантина содержит электронные сообщения, с большой вероятностью зараженные вирусом. Будьте осторожны при обработке электронных сообщений из папки карантина, чтобы случайно не заразить клиента.

2. Если считаете сообщение безопасным, отправьте его повторно первоначальным получателям ( ).

Примечание

При пересылке из папки карантина сообщения, первоначально отправленного с помощью программы Microsoft Outlook, адресат может получить несколько его копий. Это может происходить из-за того, что модуль антивирусного сканирования разбивает каждое отсканированное сообщение на несколько частей.

3. Если вы не можете переслать сообщение, возможно, что на сервере Microsoft Exchange Server отсутствует учетная запись системного администратора.

   a. На сервере в редакторе реестра Windows откройте следующую запись реестра:

      `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

   b. Отредактируйте запись как указано ниже.

ПРЕДУПРЕЖДЕНИЕ!

Неправильное редактирование реестра может серьезно повредить системе. Перед внесением изменений следует выполнить резервное копирование всех ценных данных на компьютере.

- `ResendMailbox {адрес администратора}`

  Пример: `admin@example.com`

- `ResendMailboxDomain {домен администратора}`

  Пример: `example.com`

- `ResendMailSender {учетная запись электронной почты администратора}`

  Пример: `admin`

c. Закройте редактор реестра.

Обслуживание папок карантина

Эта функция позволяет вручную или автоматически удалять сообщения, помещенные на карантин. Эта функция может удалить все сообщения, сообщения, которые были повторно отправлены и сообщения, которые не были повторно отправлены.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Нажмите **Поместить на карантин** > **Обслуживание**.

   Появится новое окно.

5. Настройте следующие параметры необходимым образом:

   - **Включить автоматическое обслуживание**: Доступно только для автоматического обслуживания.
   - Файлы на удаление
     - **Все файлы из карантина**

- **Файлы из карантина, которые никогда не пересылались**
- **Файлы из карантина, которые пересылались как минимум один раз**

- **Действие**: Количество дней, которое сообщения должны храниться. Например, если текущая дата 21 ноября, а значение, введенное в поле **Удалять выбранные файлы старше**, равняется `10`, то при автоматическом удалении агент Messaging Security Agent удалит все файлы, созданные до 11 ноября.

6. Нажмите кнопку **Сохранить**.

Настройка папок карантина

Укажите папки на сервере Microsoft Exchange, используемые для карантина. Папка карантина исключается из числа сканируемых.

Примечание

Папки карантина являются файловыми и не могут располагаться на Information Store.

Программа Messaging Security Agent помещает в карантин сообщения электронной почты в соответствии с заданными действиями. Ниже приводятся папки карантина:

- **Антивирусная защита**: Помещает в карантин сообщения, содержащие вирусы, вредоносные, шпионские и нежелательные программы, черви, трояны и прочие угрозы.
- **Защита от спама**: Помещает в карантин спам и фишинговые сообщения.
- **Блокирование вложений**: Помещает в карантин сообщения, содержащие запрещенные вложения.

- **Фильтрация содержимого**: Помещает в карантин сообщения, содержащие запрещенное содержимое.

По умолчанию все каталоги имеют одинаковый путь (`<папка установки Messaging Security Agent>\storage\quarantine`). Вы можете изменить пути для одной или всех папок.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Карантин** > **Папка**.

   Появится новое окно.
5. Укажите путь для следующих папок карантина:
   - **Антивирусная защита**
   - **Защита от спама**
   - **Фильтрация содержимого**
   - **Блокирование вложений**
6. Нажмите кнопку **Сохранить**.

Параметры уведомлений для Messaging Security Agent

Программа Worry-Free Business Security может отправлять уведомления о различных тревогах по электронной почте.

Вы можете настроить применение уведомлений только для внутренних сообщений электронной почты с помощью функции

настраиваемых пользователем определений внутренней почты. Это может быть полезно, если в компании используется два или более доменов, и существует необходимость отнести их все к источникам внутренней почты. Например, домены example.com и example.net.

Получатели списка определений внутренней почты получат уведомления, если вы установите флажок **Не уведомлять внешних получателей** в параметрах уведомлений для **Антивирус**, **Фильтрация содержимого** и **Блокирование вложений**. Не путайте список определений внутренней почты со списком разрешенных отправителей.

Чтобы все сообщения электронной почты, отправленные с адресов с внешних доменов, не расценивались как спам, добавьте внешние адреса электронной почты в списки **разрешенных отправителей** для защиты от спама.

Сведения о настраиваемых определениях внутренней почты

Messaging Security Agent разделяет трафик электронной почты на две категории: внутренний и внешний. Агент запрашивает сервер Microsoft Exchange для выяснения способа определения внешних и внутренних адресов. Все внутренние адреса имеют общее доменное имя, а все внешние адреса не принадлежат этому домену.

Например, если внутренним доменным адресом является «@trend_1.com», то агент Messaging Security Agent классифицирует адреса «abc@trend_1.com» и «xyz@trend_1.com» как внутренние. Все остальные адреса, например «abc@trend_2.com» или «jondoe@123.com», классифицируются агентом как внешние.

В качестве внутреннего адреса для программы Messaging Security Agent можно определить только один домен. В случае изменения основного адреса на сервере с помощью Microsoft Exchange System Manager, Messaging Security Agent не распознает новый адрес в качестве внутреннего, так как Messaging Security Agent не может определять изменения политики получателя.

Например, в компании используются адреса из двух доменов: @example_1.com и @example2.com. В качестве основного адреса

устанавливается @example_1.com. Messaging Security Agent считает сообщения электронной почты с основного адреса внутренними (т. е. abc@example_1.com и @example_1.com — внутренние адреса). Через некоторое время с помощью Microsoft Exchange System Manager основной адрес меняется на @example_2.com. Теперь сервер Microsoft Exchange полагает адреса вида abc@example_2.com и xyz@example_2.com внутренними.

Настройка параметров уведомлений для агентов Messaging Security Agent

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Нажмите **Действия** > **Параметры уведомления**.

   Появится новое окно.
5. Настройте следующие параметры необходимым образом:
   - **Адрес электронной почты**: Адрес, с которого программа Worry-Free Business Security будет отсылать уведомления.
   - **Определение внутренней почты**
     - **По умолчанию**: Программа Worry-Free Business Security будет воспринимать сообщения электронной почты с этого домена как внутреннюю почту.
     - **Пользовательская**: Укажите отдельные адреса электронной почты или домены, которые будут считаться внутренними адресами.

6. Нажмите кнопку **Сохранить**.

Настройка обслуживания базы спама

В окне **«Обслуживание базы спама»** можно настраивать параметры пользовательского карантина или карантина на сервере.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.
4. Выберите **Операции** > **Обслуживание базы спама**.

   Появится новое окно.
5. Нажмите **Включить пользовательский карантин**.

   При включении службы карантина на сервере создается папка карантина для каждого клиентского почтового ящика, а в дереве пользовательских папок Outlook создается папка с именем Спам. После включения карантина и создания папки спама, служба карантина будет перемещать в эту папку всю почту, содержащую спам. Для получения дополнительных сведений см. *Управление пользовательским карантином на странице 6-80*.

   Совет

   Если выбрана данная функция, Trend Micro рекомендует отключить панель защиты от спама Trend Micro на агентах для увеличения производительности клиентов.

   Снимите флажок **Включить пользовательский карантин** для отключения пользовательского карантина для всех почтовых

ящиков на сервере Microsoft Exchange. При выключении службы пользовательского карантина почтовые папки спама останутся, но все обнаруженные сообщения не будут в них перемещаться.

6. Нажмите **Создать папку для спама и удалять сообщения, помеченные как спам** для создания (немедленного) почтовых папок спама для всех вновь созданных клиентов, а также для существующих клиентов, у которых данная папка была удалена. Для других существующих клиентов произойдет удаление сообщений спама, у которых истек срок хранения, заданный в параметрах локальной папки для спама.

7. В поле **Удалять спам-сообщения старше {число} дней** измените срок хранения спама агентом Messaging Security Agent. Значение по умолчанию —14 дней, максимум — 30 дней.

8. Чтобы отключить пользовательский карантин для выбранных пользователей, сделайте следующее.

   a. В разделе **Список исключений пользовательского карантина** введите электронный адрес пользователя, для которого карантин должен быть отключен.

   b. Нажмите кнопку **Добавить**.

      Электронный адрес конечного пользователя добавляется в список адресов с отключенным пользовательским карантином.

      Чтобы удалить пользователя из списка и восстановить пользовательский карантин, выберите электронный адрес пользователя из списка и нажмите на **Удалить**.

9. Нажмите кнопку **Сохранить**.

Управление пользовательским карантином

Во время установки программа Messaging Security Agent создает папку «Спам» в почтовом ящике каждого конечного пользователя на сервере.

При поступлении спама система помещает эти сообщения в карантин в эту папку в соответствии с правилами фильтрации спама, предварительно заданными в Messaging Security Agent. Конечные пользователи могут просматривать эту папку со спамом, открывать, читать и удалять подозрительные электронные сообщения. См. *Настройка обслуживания базы спама на странице 6-79*.

В качестве альтернативы администраторы могут создавать папку спама на сервере Microsoft Exchange. После создания администратором учетной записи электронной почты файлы почтового ящика создаются на сервере Exchange не сразу, а при наступлении следующих событий:

- пользователь в первый раз выполняет вход в свой почтовый ящик;
- при поступлении в почтовый ящик первого сообщения.

Для создания папки спама почтовый ящик должен быть уже создан администратором.

Клиентская папка Спам

Конечные пользователи могут открывать электронные сообщения, помещенные на карантин в папку для спама. Когда одно из этих сообщений открывается, появляются две кнопки: **«Разрешенный отправитель»** и **«Просмотреть список разрешенных отправителей»**.

- Когда пользователь открывает сообщение из папки «Спам» и нажимает кнопку **Разрешенный отправитель**, адрес добавляется в список **Разрешенные отправители** для этого пользователя.
- При выборе **Просмотреть список разрешенных отправителей** открывается новое окно, в котором пользователь может просматривать и редактировать список разрешенных адресов или доменов отправителей.

Разрешенные отправители

Когда пользователь открывает сообщение из папки «Спам» и нажимает **Добавить в список разрешенных отправителей**, Messaging Security Agent перемещает сообщение в папку «Входящие» этого пользователя и добавляет адрес во все пользовательские списки разрешенных отправителей. Messaging Security Agent заносит это событие в журнал.

Когда на сервер Microsoft Exchange поступает сообщение от отправителя из списка разрешенных пользователем, оно доставляется в папку «Входящие» вне зависимости от заголовка или содержания письма.

Примечание

Messaging Security Agent может также предоставлять администраторам списки разрешенных и заблокированных отправителей. Для Messaging Security Agent приоритетными являются администраторские списки разрешенных и заблокированных отправителей, а пользовательские стоят следующими по значимости.

Функция обслуживания пользовательского карантина

Служебная функция агента Messaging Security Agent выполняет каждые 24 часа по умолчанию в 02:30 следующие задания:

- автоматическое удаление спам-сообщений с истекшим сроком действия;
- повторное создание папки спама, если она была удалена;
- создание папок для спама для только что созданных учетных записей;
- обслуживание правил для электронных сообщений.

Функция обслуживания является неотъемлемой частью агента Messaging Security Agent и не требует настройки.

Служба технической поддержки компании Trend Micro / Отладчик

Техническая поддержка/Отладчик позволяет выполнять отладку или просто создает отчет о статусе процессов агента Messaging Security Agent. При появлении неожиданных неполадок возможно создание отчетов отладчика и отправка их в службу технической поддержки Trend Micro для анализа.

Каждый агент Messaging Security Agent вставляет сообщения в программу и затем записывает соответствующее действие в файлы журналов после выполнения. Журнал может быть послан в службу технической поддержки Trend Micro для того, чтобы специалисты могли отладить ход выполнения программы в среде пользователя.

Отладчик способен создавать журналы для следующих модулей:

- главная служба Messaging Security Agent
- сервер удаленного конфигурирования Messaging Security Agent
- наблюдатель системы Messaging Security Agent
- программный интерфейс антивирусного сканирования (VSAPI);
- простой протокол электронной почты (SMTP);
- общий шлюзовой интерфейс (CGI).

По умолчанию агент MSA хранит журналы в следующей папке:

```
<папка установки Messaging Security Agent>\Debug
```

Просмотреть их содержимое можно с помощью любого текстового редактора.

Создание отчетов системного отладчика

Отчеты отладчика создаются для оказания помощи службе технической поддержке компании Trend Micro в устранении проблем.

Процедура

1. Перейдите к **Устройства**.
2. Выберите Messaging Security Agent.
3. Нажмите **Политика настройки**.

   Появится новое окно.

4. Выберите **Действия** > **Поддержка / Отладчик**.

   Появится новое окно.

5. Укажите модули для проверки.

   - **главная служба** Messaging Security Agent;
   - **сервер удаленного конфигурирования** Messaging Security Agent;
   - **наблюдатель системы** Messaging Security Agent;
   - **Программный интерфейс антивирусного сканирования (VSAPI)** в среде Exchange Server 2003, 2007 или 2010;
   - **сканирование уровня хранилища** в среде Exchange Server 2013;
   - **простой протокол электронной почты (SMTP)** в среде Exchange Server 2003;
   - **транспортная служба** в среде Exchange Server 2007, 2010 или 2013;
   - **общий шлюзовой интерфейс (CGI)**.

6. Нажмите кнопку **Применить**.

   Отладчик начнет собирать данные об указанных модулях.

Контроль режима реального времени

Контроль в режиме реального времени отображает текущую информацию о выбранном сервере Microsoft Exchange и агенте Messaging Security Agent. Показывается информация о просканированных сообщениях и статистика защиты, включая количество обнаруженных вирусов и спама, заблокированных вложений и недопустимого содержимого. Функция также проверяет, работает ли агент должным образом.

Работа с программой контроля в режиме реального времени

Процедура

1. Процедура входа в программу контроля в режиме реального времени (Real-time Monitor) из веб-консоли.
   a. Перейдите к **Устройства**.
   b. Выберите Messaging Security Agent.
   c. Нажмите **Политика настройки**.

      Появится новое окно.

   d. Нажмите ссылку **Контроль в реальном времени** в правой верхней части экрана.
2. Чтобы открыть программу контроля в режиме реального времени из меню «Пуск» Windows, нажмите **Все программы** > **Trend Micro Messaging Security Agent** > **Контроль режима реального времени**.
3. Для сброса статистики по защите на ноль нажмите **Сброс**.
4. Для удаления устаревшей информации о просканированных сообщениях нажмите **Очистить содержимое**.

Добавление предупреждения к исходящим электронным сообщениям

Вы можете добавить предупреждение только к исходящим сообщениям.

Процедура

1. Создайте текстовый файл и добавьте в него текст предупреждения.

2. Измените следующие ключи в реестре.

   - Первый ключ:

     Путь: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Раздел: `EnableDisclaimer`

     Тип: `REG_DWORD`

     Значение: `0 – отключить, 1 – включить`

   - Второй ключ:

     Путь: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Раздел: `DisclaimerSource`

     Тип: `REG_SZ`

     Значение: Введите полный путь к файлу, содержащему текст предупреждения.

     Например, `C:\Data\Disclaimer.txt`

     Примечание

     По умолчанию Worry-Free Business Security определит, отправлено исходящее сообщение на внутренний или внешний домен, и добавит предупреждение к каждому сообщению, отправленному на внешние домены. Пользователь может изменить настройки по умолчанию и добавлять предупреждение к каждому исходящему сообщению, кроме доменов, включенных в следующий регистрационный ключ.

   - Третий ключ:

     Путь: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Раздел: `InternalDomains`

Тип: `REG_SZ`

Значение: Введите имена доменов, которые следует исключить. Для разделения записей используйте точку с запятой (;).

Это может произойти в следующих случаях.
`domain1.org;domain2.org`

Примечание

Имена доменов здесь являются именами DNS и серверов Exchange.

Глава 7

Управление сканированием

В этой главе описывается, как выполнять сканирование с помощью агентов Security Agent и Messaging Security Agent (только Advanced) для защиты вашей сети от угроз.

Сведения о сканировании

В ходе сканирования модуль сканирования Trend Micro вместе с файлом базы данных выполняет первую стадию обнаружения при помощи сравнения с шаблоном. Поскольку каждая угроза содержит уникальную сигнатуру (строку символов, которые отличают его от любого другого кода), неизменяемые обрывки этого кода фиксируются в файле базы данных. Тогда модуль сравнивает определенные части каждого просканированного файла с образцом в файле базы данных в поисках совпадения.

Когда модуль сканирования находит файл, представляющий угрозу, он может осуществить следующие действия: излечить, поместить в карантин, удалить или заменить текстом или файлом (только Advanced). Эти действия можно настроить при настройке заданий сканирования.

Worry-Free Business Security предоставляет **три метода сканирования**. У каждого сканирования своя цель и использование, но все они настраиваются примерно одинаково.

- Сканирование в реальном времени Для получения дополнительной информации см. *Сканирование в режиме реального времени на странице 7-3*.
- Сканирование вручную Для получения дополнительной информации см. *Сканирование вручную на странице 7-3*.
- Сканирование по расписанию Для получения дополнительной информации см. *Сканирование по расписанию на странице 7-7*.

Агенты Security Agent используют один из двух методов сканирования:

- Smart scan
- обычное сканирование.

Для получения дополнительной информации см. *Методы сканирования на странице 5-3*.

Сканирование в режиме реального времени

Сканирование в режиме реального времени обеспечивает непрерывную защиту компьютера.

Каждый раз при открытии, загрузке, копировании или изменении файла функция сканирования в режиме реального времени агента **Security Agent** сканирует файл на наличие угроз. Для получения дополнительной информации о настройке сканирования в режиме реального времени, см. *Настройка сканирования в режиме реального времени для агентов Security Agent на странице 5-9*.

При проверке сообщений электронной почты сканирование в режиме реального времени с помощью агента **Messaging Security Agent** (только Advanced) защищает все известные точки проникновения вирусов путем проверки всех входящих сообщений, SMTP-сообщений, документов, размещаемых в папках общего доступа, и файлов, копируемых с других серверов Microsoft Exchange. Для получения дополнительной информации о настройке сканирования в режиме реального времени, см. *Настройка сканирования в режиме реального времени для агентов Messaging Security на странице 6-6*.

Сканирование вручную

Сканирование вручную применяется по запросу пользователя.

Сканирование вручную с использованием агентов **Security Agent** устраняет угрозы старых вирусов (если они есть) и уменьшает возможность повторного заражения.

Когда сканирование вручную выполняется на агентах **Messaging Security Agent** (только Advanced), выполняется сканирование всех файлов службы Information Store сервера Microsoft Exchange.

Время, требуемое на сканирование, зависит от системных ресурсов клиента и количества сканируемых файлов. Запущенное сканирование вручную может быть остановлено администратором Security Server,

если проверка была запущена удаленно с веб-консоли, или пользователем, если сканирование выполняется непосредственно на клиенте.

Совет

Компания Trend Micro рекомендует запускать сканирование вручную после вирусной эпидемии.

Запуск сканирования вручную

В этом разделе приведено описание процедуры запуска сканирования вручную администраторами Security Server на агентах **Security Agent** и **Messaging Security Agent** (только Advanced) из веб-консоли.

Примечание

Также можно запустить сканирование вручную непосредственно с клиентских компьютеров, щелкнув правой кнопкой мыши по значку Security Agent на панели задач Windows, а затем выбрав **Начать сканирование**. Запустить сканирование вручную напрямую с серверов Microsoft Exchange невозможно.

Процедура

1. Перейдите к разделу **Сканирование** > **Сканирование вручную**.
2. (Необязательно) Настройте параметры сканирования перед запуском сканирования вручную.

Инструкции и примечания	Рекомендуемые параметры сканирования
Чтобы настроить параметры сканирования для **Security Agent**, откройте группу рабочих станций или группу серверов. См. *Сканирование объектов и действий для Security Agent на странице 7-11*. **Примечание** Параметры сканирования для Security Agent также используются, когда пользователь запускает сканирование вручную непосредственно с клиентского компьютера. Однако, если вы предоставите пользователям права настройки пользовательских параметров сканирования, во время сканирования будут использоваться настроенные пользователем параметры.	Объект • Все, поддающиеся сканированию: Включает все сканируемые файлы. Файлы, не поддающиеся сканированию — это файлы, которые защищены паролем, зашифрованы или не проверяются из-за установленных пользователем ограничений сканирования. • Сканировать сжатые файлы до уровня 1. Сканирует сжатые файлы с одним уровнем сжатия. Параметром по умолчанию для группы серверов является «выключено», а для группы настольных компьютеров по умолчанию — «включено». Исключения • Не сканировать каталоги, в которых установлены приложения Trend Micro Дополнительные настройки • Изменить список разрешенных шпионских и нежелательных программ (только для «антишпионских» программ)

Инструкции и примечания	Рекомендуемые параметры сканирования
Чтобы настроить параметры сканирования для **Messaging Security Agent**, разверните агент и выберите следующее: • **Антивирусная защита**: — выберите этот пункт, чтобы агент проводил сканирование на наличие вирусов и другого вредоносного программного обеспечения. См. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*. • **Фильтрация содержимого**: — выберите этот пункт, чтобы агент сканировал почту на наличие недопустимого содержимого. См. *Управление правилами фильтрации содержимого на странице 6-18*. • **Блокирование вложений**. — выберите этот пункт, чтобы агент сканировал почту на наличие недопустимых вложений. См. *Настройка блокирования вложений на странице 6-51*.	• Агент сканирует все файлы, поддающиеся проверке. Сюда включаются тела проверяемых электронных сообщений. • При обнаружении файла, содержащего вирус или другой вредоносный код, агент лечит файл. Если лечение невозможно, файл заменяется текстом или файлом • При обнаружении файла, содержащего «троянский конь» или червь, агент заменяет такой «троянский конь» или червь текстом или файлом. • При обнаружении файла, содержащего упаковщик, агент заменяет упаковщик текстом или файлом. • Агент не лечит зараженные сжатые файлы. Это позволяет ускорить сканирование в реальном времени.

3. Выберите группы или агенты Messaging Security Agent для сканирования.

4. Нажмите кнопку **Начать сканирование**.

   Security Server отправляет уведомление агентам о запуске сканирования вручную. Появляется окно результатов уведомления о сканировании, которое показывает количество агентов, которые получили и не получили уведомления.

5. Чтобы остановить запущенное сканирование, нажмите **Прекратить сканирование**.

Security Server отправляет агентам другое уведомление об остановке сканирования вручную. Появляется окно результатов уведомления об остановке сканировании, которое показывает количество агентов, которые получили и не получили уведомления. Агенты Security Agent могут не получить уведомление, если во время запуска сканирования они находились в автономном режиме или в случае сетевых сбоев.

Сканирование по расписанию

Сканирование по расписанию сходно со сканированием вручную, но охватывает все файлы и сообщения электронной почты (только Advanced) и производится в определенное время и с установленной периодичностью. Используйте сканирование по расписанию для автоматизации ежедневных сканирований клиентов и для повышения эффективности борьбы с вирусами.

Совет

Запускайте сканирование по расписанию в период наименьшей рабочей нагрузки, чтобы свести к минимуму возможные прерывания соединения с пользователями и сетью.

Настройка сканирования по расписанию

Компания Trend Micro рекомендует не назначать сканирование по расписанию на то же время, на которое назначено обновление по расписанию. Это может привести к преждевременному прерыванию сканирования по расписанию. Точно так же и сканирование вручную, запущенное во время выполнения сканирования по расписанию, приведет к прерыванию сканирования по расписанию, но последнее будет запущено вновь согласно его расписанию.

Процедура

1. Перейдите к разделу **Сканирование** > **Сканирование по расписанию**.
2. Откройте вкладку **«Расписание»**.
   a. Настройте частоту сканирования (ежедневно, еженедельно или ежемесячно) и время его начала. Каждая группа или агент Messaging Security Agent может иметь свое собственное расписание.

      Примечание

      Если для ежемесячных проверок выбраны числа 31, 30 или 29 число, а в месяце меньшее количество дней, в этом месяце проверка не будет запущена.

   b. (Необязательно) Выберите **Выключите компьютер после завершения сканирования по расписанию**.
   c. Нажмите кнопку **Сохранить**.
3. Щелкните вкладку **Параметры** и задайте необходимые настройки сканирования по расписанию.

Инструкции и примечания	Рекомендуемые параметры сканирования
Чтобы настроить параметры сканирования для **Security Agent**, откройте группу рабочих станций или группу серверов. См. *Сканирование объектов и действий для Security Agent на странице 7-11*. **Примечание** Если вы предоставите пользователям права настройки пользовательских параметров сканирования, во время сканирования будут использоваться настроенные пользователем параметры.	Объект • Все, поддающиеся сканированию:Включает все сканируемые файлы. Файлы, не поддающиеся сканированию — это файлы, которые защищены паролем, зашифрованы или не проверяются из-за установленных пользователем ограничений сканирования. • Сканировать сжатые файлы до уровня 2. Сканирует сжатые файлы с двумя уровнями сжатия.
	Исключения • Не сканировать каталоги, в которых установлены приложения Trend Micro
	Дополнительные настройки • Изменить список разрешенных шпионских и нежелательных программ (только для «антишпионских» программ)

Инструкции и примечания	Рекомендуемые параметры сканирования
Чтобы настроить параметры сканирования для **Messaging Security Agent**, разверните агент и выберите следующее: • **Антивирусная защита**: — выберите этот пункт, чтобы агент проводил сканирование на наличие вирусов и другого вредоносного программного обеспечения. См. *Сканирование объектов и действия для агентов Messaging Security Agent на странице 7-20*. • **Фильтрация содержимого**: — выберите этот пункт, чтобы агент сканировал почту на наличие недопустимого содержимого. См. *Управление правилами фильтрации содержимого на странице 6-18*. • **Блокирование вложений** — выберите этот пункт, чтобы агент сканировал почту на наличие недопустимых вложений. См. *Настройка блокирования вложений на странице 6-51*.	• Агент выполняет сканирование каждое воскресенье в 05:00. • Настройте расписание так, чтобы начало сканирования не совпадало со временем пиковой нагрузки на клиентские компьютеры. Агент сканирует все файлы, поддающиеся проверке. Сюда включаются тела проверяемых электронных сообщений. • При обнаружении файла, содержащего вирус или другой вредоносный код, агент лечит файл. Если лечение невозможно, файл заменяется текстом или файлом • При обнаружении файла, содержащего «троянский конь» или червь, агент заменяет такой «троянский конь» или червь текстом или файлом. • При обнаружении файла, содержащего упаковщик, агент заменяет его текстом или файлом. • Агент не лечит зараженные сжатые файлы.

4. Выберите группы или агенты Messaging Security Agent, которые будут использовать параметры сканирования по расписанию.

Примечание

Чтобы отключить сканирование по расписанию, снимите флажок для группы или агента Messaging Security Agent.

5. Нажмите кнопку **Сохранить**.

Сканирование объектов и действий для Security Agent

Настройте следующие параметры для каждого типа сканирования (сканирование вручную, сканирование по расписанию и сканирование в режиме реального времени):

Вкладка «Целевые объекты»

Выберите метод:

- **Все, поддающиеся сканированию**: сканирование всех файлов, поддающихся сканированию. Файлы, не поддающиеся сканированию — это файлы, которые защищены паролем, зашифрованы или не проверяются из-за установленных пользователем ограничений сканирования.

Примечание

Функция обеспечивает максимально возможную защиту. Вместе с тем, сканирование каждого файла занимает много времени и ресурсов и в ряде ситуаций может быть излишним. Поэтому количество файлов для сканирования можно ограничить.

- **IntelliScan использует технологию точного определения типа файла**: сканирование осуществляется на основе истинного типа файла. См. *IntelliScan на странице D-2*.

- **Сканировать файлы со следующими расширениями**: вручную укажите расширения файлов, которые нужно сканировать. Разделяйте записи запятыми.

Выберите активатор сканирования.

- **Чтение**: сканирование файлов, содержимое которых читается; файлы читаются при их открытии, исполнении, копировании и перемещении.
- **Запись**: сканирование файлов, содержимое которых записывается; содержимое файла записывается при изменении, сохранении, загрузке файла или копировании его из другого расположения.
- **Чтение или запись**

Исключения из сканирования

Можно настроить следующие параметры.

- Включить или выключить исключения
- Исключить папки продуктов Trend Micro из сканирования
- Исключить другие папки из сканирования

  Все вложенные папки, расположенные в указанном каталоге, также исключаются
- Исключить из сканирования имена файлов или имена файлов с полным путем
- Исключить расширения файлов

  В расширении файлов нельзя использовать подстановочные знаки, например «*».

Примечание

(Только Advanced) Если на клиентском компьютере установлен сервер Microsoft Exchange, компания Trend Micro рекомендует исключать из сканирования все папки программы Microsoft Exchange Server. Чтобы исключить из сканирования папки сервера Microsoft Exchange на глобальном уровне, перейдите в **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер {вкладка}** > **Общие параметры сканирования** и выберите **Исключить папки сервера Microsoft Exchange, если программа установлена на сервере Microsoft Exchange**.

Дополнительные настройки

Тип сканирования	Параметр
Сканирование в режиме реального времени	**Сканировать сообщения POP3**: по умолчанию программа сканирования почты может сканировать только новые сообщения, отправленные через порт 110, в папках «Входящие» и «Нежелательная почта». Она не поддерживает безопасный протокол POP3 (SSL-POP3). • Microsoft Outlook 2007, 2010 или 2013 • Mozilla Thunderbird 1.5 или более поздней версии Модуль сканирования почты не обеспечивает обнаружение угроз безопасности в сообщениях по протоколу IMAP. Для обнаружения угроз безопасности и спама в сообщениях по протоколу IMAP следует использовать Messaging Security Agent (только Advanced).
Сканирование в режиме реального времени, сканирование вручную	**сканировать отображаемые сетевые диски и общие папки в сети**: выберите эту настройку, чтобы сканировать папки, которые физически находятся на других компьютерах, но отображаются на локальном компьютере.
Сканирование в режиме реального времени	**Сканировать дискеты при выключении системы**
Сканирование в режиме реального времени	**Включить IntelliTrap**: IntelliTrap обнаруживает вредоносный код в сжатых файлах. См. *IntelliTrap на странице D-3*.
Сканирование в режиме реального времени	**Помещать в карантин вредоносные программы, обнаруженные в памяти**: если выбрать этот параметр, когда включены сканирование в режиме реального времени и контроль действий, выполняется сканирование памяти работающего процесса на наличие запакованного вредоносного кода. Любой упакованный вредоносный код, обнаруженный контролем действий, помещается в карантин.

Тип сканирования	Параметр
Сканирование в режиме реального времени, сканирование по расписанию и сканирование вручную	**Сканировать сжатые файлы до уровня __**: сжатый файл имеет имеет столько уровней, сколько раз он был сжат. Если зараженный файл был сжат несколько раз, то для обнаружения заражения необходимо просканировать определенное количество его уровней. Однако сканирование нескольких уровней требует больше времени и ресурсов.
Сканирование в режиме реального времени, сканирование по расписанию и сканирование вручную	**Изменить список разрешенных приложений для шпионских и нежелательных программ**: этот параметр не настраивается с консоли агента.
сканирование вручную, сканирование по расписанию.	**Степень использования ресурсов процессора/скорость сканирования**: Security Agent может делать паузу после сканирования одного файла и перед сканированием следующего. Выберите один из следующих параметров. • **Высокий**: пауза между сканированиями отсутствует. • **Средний**: сканирование файлов приостанавливается, если загрузка процессора превышает 50 %, и не приостанавливается, если этот показатель составляет 50 % и менее. • **Низкий**: сканирование файлов приостанавливается, если загрузка процессора превышает 20 %, и не приостанавливается, если этот показатель составляет 20 % и менее.

Тип сканирования	Параметр
сканирование вручную, сканирование по расписанию.	**Запустить службу усовершенствованной очистки**: Security Agent останавливает деятельность мошеннического антивирусного программного обеспечения, также известного как FakeAV. Агент также использует правила службы расширенной очистки для заблаговременного выявления и остановки приложений, которые демонстрируют FakeAV-поведение. **Примечание** При предоставлении проактивной защиты расширенная очистка также приводит к большему числу ложных срабатываний.

Список разрешенных шпионских и нежелательных программ

Компания Trend Micro классифицирует некоторые приложения как шпионские или нежелательные программы не потому, что они могут повредить систему, в которую устанавливаются, а потому, что они могут спровоцировать атаки хакеров или вредоносных программ на клиент или сеть.

Программа Worry-Free Business Security содержит список потенциально опасных приложений и по умолчанию блокирует их запуск на клиентских компьютерах.

Если на клиентском компьютере или сервере необходимо запустить программу, которую программное обеспечение Trend Micro сочло шпионской или нежелательной, добавьте ее название в список разрешенных.

Вкладка «Действие»

Ниже перечислены действия, которые агенты Security Agent могут выполнять против вирусов/вредоносных программ:

Таблица 7-1. Действия при сканировании вирусов/вредоносных программ

Действие	Описание
Удалить	Удаление зараженного файла.
Поместить на карантин	Переименование и перемещение зараженного файла во временную папку карантина на клиентском компьютере. Агент Security Agent затем отправляет файлы карантина в указанную папку карантина, которая по умолчанию находится на Security Server. Security Agent шифрует файлы карантина, отправляемые в эту папку. Если вам нужно восстановить из карантина любой файл, используйте инструмент VSEncrypt.
Лечить	Лечит зараженный файл, прежде чем разрешить к нему полный доступ. Если файл неизлечимый, Security Agent выполняет над ним одно из следующих действий: помещает в карантин, удаляет, переименовывает или пропускает. Это действие может быть выполнено для всех типов вредоносных программ, кроме вероятных вирусов/вредоносных программ. **Примечание** Некоторые файлы неизлечимы. Для получения дополнительных сведений см. *Неизлечимые файлы на странице D-28*.
Переименовать	Изменение расширения зараженного файла на `vir`. Такой файл невозможно открыть, если не связать его с определенным приложением. При открытии переименованного зараженного файла вирусный или вредоносный код может быть запущен.
Пропустить	Выполняется только во время сканирования вручную и сканирования по расписанию. Security Agent не может использовать это действие во время сканирования в режиме реального времени, потому что отсутствие каких-либо действий при обнаружении попытки открытия или выполнения зараженного файла, разрешит активацию вируса или вредоносной программы. Все остальные действия сканирования во время сканирования в режиме реального времени могут быть использованы.

Действие	Описание
Запретить доступ	Выполняется только во время сканирования в режиме реального времени. Когда Security Agent обнаруживает попытку открытия или выполнения зараженного файла, он немедленно блокирует операцию. Файл можно удалить вручную.

Действие, выполняемое программой Security Agent, зависит от типа сканирования, в ходе которого была обнаружена шпионская или нежелательная программа. Хотя конкретные действия могут быть настроены для каждого типа вирусов/вредоносных программ, для всех типов шпионских или нежелательных программ может быть настроено только одно действие. Например, при обнаружении любого типа шпионских или нежелательных программ в процессе сканирования вручную (тип сканирования) Security Agent лечит зараженные системные ресурсы (действие).

Ниже перечислены действия, которые Security Agent может выполнять против шпионских или нежелательных программ:

Таблица 7-2. Действия при сканировании шпионских или нежелательных программ

Действие	Описание
Лечить	Прерывает процессы или удаляет записи в реестре, файлы, объекты cookie и ярлыки.
Пропустить	Не выполняет никаких действий при обнаружении шпионских или нежелательных компонентов, но записывает обнаружение шпионских/нежелательных программ в журнал. Действие может быть выполнено только во время сканирования вручную и сканирования по расписанию. Во время сканирования в режиме реального времени используется действие «Запретить доступ». Security Agent не будет выполнять никаких действий, если обнаруженная шпионская или нежелательная программа включена в список разрешенных.

Действие	Описание
Запретить доступ	Запрет доступа (копирования и открытия) к обнаруженным компонентам шпионских или нежелательных программ. Действие выполняется только во время сканирования в режиме реального времени. Во время сканирования вручную и сканирования по расписанию применяется действие «Пропустить».

ActiveAction

Различные типы вирусов/вредоносных программ требуют использования различных действий при сканировании. Настройка действий является сложной задачей, требующей высокой квалификации в данной сфере. Для решения этих задач программа Security Agent использует функцию ActiveAction.

ActiveAction — это набор предварительно настроенных действий при сканировании на наличие вирусов/вредоносных программ. Компания Trend Micro рекомендует использовать функцию ActiveAction, если пользователь не обладает достаточными знаниями о действиях при сканировании или не может принять решение о том, какое действие подходит для конкретного типа вирусов/вредоносных программ.

Преимущества использования функции ActiveAction

- Функция ActiveAction использует действия при сканировании, которые рекомендует Trend Micro. Пользователь освобождается от необходимости самостоятельной настройки действий при сканировании.
- Создатели вирусов постоянно меняют методы, с помощью которых вирусы/вредоносные программы атакуют компьютеры. Параметры ActiveAction обновляются для обеспечения защиты от новейших угроз и методов атак вирусов/вредоносных программ.

В следующей таблице показано, как ActiveAction обрабатывает каждый тип вирусов/вредоносных программ:

Таблица 7-3. Рекомендуемые компанией Trend Micro действия против вирусов и вредоносных программ

Тип вируса или вредоносной программы	Сканирование в режиме реального времени		Сканирование вручную/ сканирование по расписанию	
	Первое действие	Второе действие	Первое действие	Второе действие
Программа-шутка	Поместить на карантин	Удалить	Поместить на карантин	Удалить
«Троянские кони» / черви	Поместить на карантин	Удалить	Поместить на карантин	Удалить
Упаковщик	Поместить на карантин	---	Поместить на карантин	---
Вероятный вирус/ вредоносная программа	Пропустить	---	Пропустить или настроенное пользователем действие	---
Вирус	Лечить	Поместить на карантин	Лечить	Поместить на карантин
Тестовый вирус	Запретить доступ	---	---	---
Другие вредоносные программы	Лечить	Поместить на карантин	Лечить	Поместить на карантин

Примечание

- Некоторые файлы неизлечимы. Для получения дополнительных сведений см. *Неизлечимые файлы на странице D-28*.
- Функция ActiveAction недоступна при сканировании на наличие шпионских и нежелательных программ.
- Значения по умолчанию для данных параметров могут меняться, когда становятся доступны новые файлы базы данных.

Дополнительные настройки

Тип сканирования	Параметр
Сканирование в режиме реального времени, сканирование по расписанию	**Показывать на настольном ПК или сервере предупреждение в случае обнаружения вируса или шпионской программы**
Сканирование в режиме реального времени, сканирование по расписанию	**Показывать на настольном ПК или сервере предупреждение в случае обнаружения вероятного вируса или шпионской программы**
Сканирование в режиме реального времени, сканирование по расписанию и сканирование вручную.	**Запускать лечение при обнаружении вероятного вируса или вредоносной программы**: доступно только при выборе ActiveAction и настройке действий для вероятных вирусов и вредоносных программ.

Сканирование объектов и действия для агентов Messaging Security Agent

Настройте следующие параметры для каждого типа сканирования (сканирование вручную, сканирование по расписанию и сканирование в режиме реального времени):

Вкладка **Цель**

- Объекты сканирования
- Параметры сканирования на наличие других угроз
- Исключения из сканирования

Вкладка **Действие**

- Действия при сканировании/ActiveAction
- Уведомления
- Дополнительные настройки

Объекты сканирования

Выберите объекты сканирования.

- **Все файлы вложений**: Будут пропущены только зашифрованные или защищенные паролем файлы.

Примечание

Функция обеспечивает максимально возможную защиту. Вместе с тем, сканирование каждого файла занимает много времени и ресурсов и в ряде ситуаций может быть излишним. Поэтому количество файлов для сканирования можно ограничить.

- **IntelliScan**: Сканирование файлов, основанное на определении истинного содержимого. См. *IntelliScan на странице D-2*.
- **Файлы указанного типа**: Worry-Free Business Security будет сканировать только типы файлов с указанными расширениями. Разделяйте записи точкой с запятой (;).

Выберите другие функции:

- **Включить IntelliTrap**: IntelliTrap обнаруживает вредоносный код в сжатых файлах. См. *IntelliTrap на странице D-3*.
- **Сканировать тело сообщений**: Выполняется сканирование тела сообщения электронной почты, которое может содержать внедренный вредоносный код.

Параметры сканирования на наличие других угроз

Выберите другие угрозы, сканирование которых должен выполнять агент: Для получения информации об этих угрозах см. *Сведения об угрозах на странице 1-9*.

Выберите дополнительные функции:

- **Создавать резервную копию зараженного файла перед его лечением**: Worry-Free Business Security перед очисткой создает резервную копию угрозы. Резервная копия файла шифруется и хранится в папке клиента:

  ```
  <папка установки Messaging Security Agent>\storage\backup
  ```

  Вы можете изменить папку в разделе **Дополнительные параметры**, подразделе **Параметры создания резервных копий**.

  Для получения информации о расшифровке файлов см. *Восстановление зашифрованных файлов на странице 14-19*

- **Отказаться от лечения зараженных сжатых файлов для увеличения производительности**

Исключения из сканирования

На вкладке **Цель** перейдите в раздел **Исключения** и выберите один из следующих критериев, которые агент будет использовать при исключении сообщения электронной почты из сканирования:

- **Размер тела сообщения превышает**: Программа Messaging Security Agent сканирует электронные сообщения, только если размер тела сообщения не превышает указанного значения.
- **Размер вложения превышает**: Программа Messaging Security Agent сканирует электронные сообщения, только если размер вложенного файла не превышает указанного значения.

Совет

Trend Micro рекомендует предельное значение 30 МБ.

- **Количество файлов в архиве превышает**: Если количество файлов в сжатом файле превышает указанное значение, Messaging Security Agent отсканирует только то количество файлов, которое установлено данным параметром.
- **Размер распакованного файла превышает**: Messaging Security Agent отсканирует только те сжатые файлы, размер которых после распаковки не превосходит указанного значения.

- **Количество уровней сжатия превышает**: Messaging Security Agent отсканирует только те сжатые файлы, в которых количество уровней сжатия не превышает указанного значения. Например, если установить ограничение в 5 уровней сжатия, Messaging Security Agent отсканирует первые 5 уровней сжатых файлов, но не будет сканировать файлы, имеющие 6 и более уровней сжатия.

- **Размер распакованного файла превышает размер упакованного файла в «x» раз**: Messaging Security Agent отсканирует только те сжатые файлы, для которых отношение размера распакованного файла к размеру упакованного файла не превышает указанного значения. Эта функция предотвращает сканирование программой Messaging Security Agent таких сжатых файлов, которые могут привести к атаке типа «отказ от обслуживания» (DoS). Атака DoS происходит, если ресурсы почтового сервера переполнены ненужными заданиями. Чтобы исключить такую ситуацию, следует ограничить размер распаковываемых файлов.

  Пример: В указанной ниже таблице в качестве значения x было введено 100.

Размер файла (без сжатия)	Размер файла (без сжатия)	Результат
500 KB	10 КБ (соотношение 50:1)	Просканирован
1000 КБ	10 КБ (соотношение 100:1)	Просканирован
1 001 KB	10 КБ (соотношение превосходит 100:1)	Не сканировался *
2 000 KB	10 КБ (соотношение 200:1)	Не сканировался *

  * Messaging Security Agent предпринимает действия, указанные вами для исключенных файлов.

Действия при сканировании

Messaging Security Agent можно настроить для выполнения действий, определяемых пользователем, в соответствии с типом угроз, таких как вирусы/вредоносные программы, «троянские» программы и черви.

При настройке действий вручную установите действия для угрозы каждого типа.

Таблица 7-4. Настроенные действия Messaging Security Agent

Действие	Описание
Лечить	Удаление вредоносного кода из тел и вложений зараженных сообщений. Оставшийся текст электронного сообщения, все незараженные и вылеченные файлы отправляются получателям. Trend Micro рекомендует использовать действие «лечить» в качестве действия по умолчанию для вирусов/вредоносных программ. При определенных условиях Messaging Security Agent не может вылечить файл. Во время сканирования вручную или сканирования по расписанию Messaging Security Agent обновляет хранилище информации и заменяет файлы на вылеченные.
Заменить текстом или файлом	Удаляет зараженное/отфильтрованное содержимое и заменяет его текстом или файлом. Сообщение отправляется законному получателю, но заменяющий текст информирует о том, что содержимое исходного письма было заражено и поэтому заменено. Для фильтрации содержимого и предотвращения потери данных текст можно заменять только в полях тела или вложения (но не в полях «От», «Кому», «Копия» или «Тема»).
Поместить в карантин сообщение целиком	(Только для сканирования в режиме реального времени) Помещение в папку карантина только инфицированного содержимого, при этом сообщение доставляется получателю без данного содержимого. Для фильтрации содержимого, предотвращения потери данных и блокирования вложений переместите все сообщение в папку карантина.
Поместить часть сообщения в карантин	(Только для сканирования в режиме реального времени) Помещение в папку карантина только инфицированного или отфильтрованного содержимого, при этом сообщение доставляется получателю без данного содержимого.

Действие	Описание
Удалить сообщение целиком	(Только для сканирования в режиме реального времени) Удаляет сообщение целиком. Получатель исходного сообщения его не получит.
Пропустить	Регистрация в журналах заражения файлов вирусами без выполнения какого-либо действия. Исключенные, зашифрованные или защищенные паролем файлы доставляются получателю без добавления обновлений в журналы. Для фильтрации содержимого доставляет сообщение без изменений.
Архивировать	Перемещение сообщения в папку архива и доставка сообщения получателю исходного сообщения.
Переместить сообщение на карантин в папку для спама на сервере	Отправляет сообщение целиком на карантин на сервер Security Server.
Переместить сообщение в карантин в пользовательскую папку для спама	Отправляет сообщение целиком на карантин в пользовательскую папку спама. Папка находится на сервере Information Store.
Пометить и доставить	Добавляет к заголовку сообщения метку, обозначающую сообщение как спам, а затем доставляет сообщение получателю.

В дополнение к этим действиям вы также можете настроить следующие:

- **Включить действие при массовых рассылках**. Выберите действие при массовых рассылках: «Лечить», «Заменить текстом или файлом», «Удалить сообщение целиком», «Пропустить» или «Поместить часть сообщения на карантин».
- **Выполнять при невозможности лечения**: Задайте следующее действие при неудачных попытках лечения. Выберите «Заменить текстом или файлом», «Удалить сообщение целиком», «Пропустить» или «Поместить часть сообщения на карантин».

ActiveAction

В следующей таблице показано, как ActiveAction обрабатывает каждый тип вирусов/вредоносных программ:

Таблица 7-5. Рекомендуемые компанией Trend Micro действия против вирусов и вредоносных программ

Тип вируса или вредоносной программы	Сканирование в режиме реального времени		Сканирование вручную/ сканирование по расписанию	
	Первое действие	Второе действие	Первое действие	Второе действие
Вирус	Лечить	Удалить сообщение целиком	Лечить	Заменить текстом или файлом
«Троянские кони» / черви	Заменить текстом или файлом	---	Заменить текстом или файлом	---
Упаковщик	Поместить часть сообщения в карантин	---	Поместить часть сообщения в карантин	---
Другой вредоносный код	Лечить	Удалить сообщение целиком	Лечить	Заменить текстом или файлом
Прочие угрозы	Поместить часть сообщения в карантин	---	Заменить текстом или файлом	---
Массовая рассылка	Удалить сообщение целиком	---	Заменить текстом или файлом	---

Уведомления о действиях при сканировании

Выберите **Уведомлять получателей**, чтобы агент Messaging Security Agent уведомил предполагаемых получателей при выполнении

действия в отношении сообщения электронной почты. По различным причинам, может быть необходимо не уведомлять внешних получателей электронной почты о том, что сообщение, содержащее важную информацию, было заблокировано. Выберите **Не уведомлять внешних получателей**, чтобы отправлять уведомления только внутренним получателям. Определите внутренние адреса в разделе **Действия** > **Параметры уведомления** > **Определение внутренней почты**.

Также можно отключить отправку уведомлений внешним получателям с подставным адресом.

Дополнительные параметры (действия при сканировании)

Настройки	Подробнее

Макросы	Макровирусы зависят от приложения и заражают макросы в этом приложении. При расширенном сканировании макросов используется эвристический подход, позволяющий обнаруживать вирусы в макросах или удалять все обнаруженные коды макросов. Эвристическое сканирование является оценочным методом обнаружения вирусов, в котором используются технологии распознавания по шаблонам и технологии на основе правил поиска вредоносных макросов. Этот метод отлично подходит для обнаружения неизвестных вирусов и угроз, для которых нет известной сигнатуры вируса.
	
	Агент Messaging Security Agent выполняет действие по защите от вредоносного кода макроса.
	
	• **Уровень эвристики**
	  • Первый уровень использует наиболее специфические критерии, однако обнаруживает минимальное количество кодов макросов.
	  • Четвертый уровень обнаруживает наибольшее количество кодов макросов, но использует наименее специфические критерии и может отнести надежный код макроса к вредоносному.
	
	Совет
	Trend Micro рекомендует устанавливать второй уровень. Он позволяет обнаруживать достаточно много вирусов в макросах, проводить сканирование на высокой скорости и использует только самые необходимые правила для нахождения вирусов в макросах. Кроме того, на втором уровне достаточно низкая степень ошибки при определении вредоносного кода.
	
	• **Удалять все макросы, обнаруженные в ходе расширенного сканирования макросов**: Удалить все коды макросов, обнаруженные в просканированных файлах

Настройки	Подробнее
Части сообщений, не допускающие сканирования	Выберите действие и состояние уведомления для зашифрованных и защищенных паролем файлов. Выберите одно из следующих действий: «Заменить текстом или файлом», «Поместить на карантин сообщение целиком», «Удалить сообщение целиком», «Пропустить» или «Поместить часть сообщения на карантин».
Исключенные части сообщений	Выберите действие и состояние уведомления для частей сообщений, которые были исключены. Выберите одно из следующих действий: «Заменить текстом или файлом», «Поместить на карантин сообщение целиком», «Удалить сообщение целиком», «Пропустить» или «Поместить часть сообщения на карантин».
Параметры создания резервных копий	Папка для сохранения резервных копий зараженных файлов перед их лечением.
Параметры замены	Настройте текст и файл, которыми заменяется вредоносная программа. Если в качестве действия выбрано **Заменить текстом или файлом**, программа Worry-Free Business Security заменит угрозу заданными текстовой строкой и файлом.

Глава 8

Управление обновлениями

В этой главе описываются компоненты Worry-Free Business Security и процедуры обновления.

Обзор обновлений

Все обновления компонентов происходят с сервера Trend Micro ActiveUpdate. При наличии доступных обновлений Security Server загружает обновленные компоненты, а затем распределяет их агентам Security Agent и Messaging Security Agent (только Advanced).

Если Security Server управляет большим количеством агентов Security Agent, процесс обновления может потребовать значительное количество ресурсов сервера, влияя на стабильную работу и производительность сервера. Чтобы решить эту проблему, Worry-Free Business Security предусматривает функцию **Агента обновления**, которая позволяет определенным Security Agent распространять обновления другим агентам Security Agent.

В приведенной ниже таблице описаны параметры обновления различных компонентов Security Server и агентов и даны рекомендации по их использованию.

Таблица 8-1. Параметры обновлений

Последовательность обновления	Описание	Рекомендации
1. ActiveUpdate Server или настроенный источник обновлений 2. Security Server 3. Агенты	Сервер Trend Micro Security Server получает обновленные компоненты с сервера ActiveUpdate (или настроенного источника обновлений) и затем развертывает их непосредственно для агентов (Security Agent и Messaging Security Agent).	Используйте этот метод, если между Security Server и агентами нет участков с низкой пропускной способностью.

Последовательность обновления	Описание	Рекомендации
1. ActiveUpdate Server или настроенный источник обновлений 2. Security Server 3. Агенты обновления, Messaging Security Agent, Security Agent без агентов обновления 4. Все другие Security Agent	Сервер Trend Micro Security Server получает обновленные компоненты с сервера ActiveUpdate (или настроенного источника обновлений) и затем развертывает их непосредственно для: • Агенты обновлений • Агентов Messaging Security Agent • Security Agent без агентов обновления Агентов обновления затем разворачивают компоненты для соответствующих Security Agent. Если эти Security Agent не могут выполнить обновление, они обновляются непосредственно из Security Server.	Если если между Security Server и агентами есть участки с низкой пропускной способностью, используйте этот метод, чтобы сбалансировать нагрузку трафика в сети.
1. Сервер ActiveUpdate 2. Агенты безопасности	Агенты Security Agent, которые не могут выполнить обновление из любого источника обновления, обновляются непосредственно с сервера ActiveUpdate. **Примечание** Агенты Messaging Security Agent никогда не обновляются напрямую с сервера ActiveUpdate. Если все источники обновлений недоступны, агенты Messaging Security Agent выполняют выход из процесса обновления.	Этот механизм предоставляется только в качестве последнего средства. Необходимо выполнить следующее действие. Включите параметр **Использовать Trend Micro ActiveUpdate в качестве вспомогательного источника обновлений** в разделе «Права на выполнение обновлений».

Обновляемые компоненты

Worry-Free Business Security использует свои компоненты для защиты агентов от новейших угроз безопасности. Постоянно обновляйте эти компоненты, запуская обновление вручную или по расписанию.

Список компонентов можно просмотреть, выполнив следующие действия:

- Перейдите в **Обновления** > **Вручную**.
- Перейдите в **Текущее состояние** и нажмите **Проверка состояния компонентов** в мини-приложении Agent Status.

В следующих таблицах перечислены компоненты, загружаемые Security Server с сервера ActiveUpdate:

Таблица 8-2. Компоненты Messaging (только Advanced)

Компонент	Распределяется к	Описание
База данных защиты от спама Messaging Security Agent	Агентов Messaging Security Agent	База данных защиты от спама определяет спам в почтовых сообщениях и вложениях электронной почты.
32- или 64-разрядный модуль защиты от спама Messaging Security Agent	Агентов Messaging Security Agent	Модуль защиты от спама обнаруживает спам в сообщениях и вложениях электронной почты.
32- или 64-разрядный модуль сканирования Messaging Security Agent	Агентов Messaging Security Agent	Модуль сканирования обнаруживает интернет-червей, массовые рассылки, троянские программы, фишинг-сайты, шпионское ПО, сетевые уязвимости и вирусы в сообщениях и вложениях электронной почты.

Компонент	Распределяется к	Описание
32- или 64-разрядный модуль фильтрации URL-адресов Messaging Security Agent	Агентов Messaging Security Agent	Модуль фильтрации URL-адресов обеспечивает связь между Worry-Free Business Security и службой фильтрации URL-адресов Trend Micro. Служба фильтрации URL-адресов — система оценки URL-адресов, которая предоставляет рейтинговую информацию для Worry-Free Business Security.

Таблица 8-3. Антивирусное сканирование и Smart Scan

Компонент	Распространяется на	Описание
Вирусная база данных	Агенты безопасности, использующие функцию обычного сканирования	Вирусная база данных содержит сведения, которые помогают Агенты безопасности определять последние вирусы/вредоносные программы, а также атаки со смешанными типами угроз. Trend Micro создает и выпускает новые версии вирусных баз данных несколько раз в неделю и каждый раз после обнаружения опасного вируса или вредоносной программы.
База данных IntelliTrap	Агенты безопасности	База данных IntelliTrap обнаруживает исполняемые файлы, которые запакованы в режиме реального времени. Для получения дополнительных сведений см. *IntelliTrap на странице D-3*.
База исключений IntelliTrap	Агенты безопасности	База данных исключений IntelliTrap содержит список «разрешенных» сжатых файлов.

Компонент	Распространяется на	Описание
32- или 64-разрядный модуль вирусного сканирования	Агенты безопасности	В основе всех продуктов Trend Micro лежит модуль сканирования, изначально разработанный в ответ на появление первых файловых вирусов. Существующий в настоящее время модуль сканирования является исключительно сложным и способен обнаруживать различные типа вирусов и вредоносных программ. Модуль сканирования также может определить контролируемые вирусы, которые созданы и используются для исследований. В отличие от сканирования каждого байта в каждом файле, модуль сканирования и база данных работают вместе, чтобы определить следующее: • контрольные характеристики вирусного кода; • точное местоположение в файле, в котором скрывается вирус.

Компонент	Распространяется на	Описание
Вирусная база данных Smart Scan	Не установлено на Агенты безопасности. Эта база данных остается наSecurity Server и используется для ответа на запросы сканирования, отправленные Агенты безопасности.	В режиме Smart Scan агенты OfficeScan используют две облегченные базы данных, которые совместно обеспечивают уровень защиты, аналогичный тому, который обеспечивают базы данных защиты от шпионских и вредоносных программ. **Вирусная база данных Smart Scan** содержит большую часть определений БД. **База данных агента Smart Scan** содержит все другие определения БД, не найденные в вирусной базе данных Smart Scan. Security Agent выполняет проверку на наличие угроз безопасности с помощью **базы данных агента Smart Scan**. Агенты безопасности, которые в процессе сканирования не могут определить связанную с файлом потенциальную угрозу, проверяют эту угрозу путем отправки запроса сканирования в службу Scan Server, размещенную на сервере Security Server. Сервер Scan Server оценивает риск, используя **вирусную базу данных Smart Scan**. Чтобы повысить эффективность сканирования, Security Agent кэширует результаты запроса сканирования, переданные службой Scan Server.
База данных агента Smart Scan	Агенты безопасности, использующие функцию smart scan	
Шаблон Устранение повреждений	Агенты безопасности	Шаблон Устранение повреждений используется модулем удаления ущерба для определения троянских программ и процессов, чтобы модуль мог удалить их в дальнейшем.
32- или 64-разрядный Модуль устранения ущерба	Агенты безопасности	Модуль устранения ущерба сканирует и удаляет троянские программы и процессы.

Компонент	Распространяется на	Описание
База данных для проверки памяти	Агенты безопасности	Эта технология обеспечивает улучшенное сканирование на полиморфные и мутирующие вирусы, а также улучшает сканирование на основе вирусной базы данных за счет эмуляции выполнения файла. Результаты сканирования анализируются в контролируемой среде на наличие вредоносных действий без особого ущерба для производительности системы.
Модуль контекстного сбора информации (32/64-разрядная версия)	Агенты безопасности	Модуль контекстного сбора информации отслеживает процессы, запущенные программами с низким приоритетом, и отбирает характерные действия, которые отправляет для анализа в модуль прогнозного машинного самообучения с помощью обработчика запросов контекстного сбора информации.
База данных контекстного сбора информации	Агенты безопасности	В базе данных контекстного сбора информации содержится список «разрешенных» действий программ, не относящихся к каким-либо известным угрозам.
Обработчик запросов контекстного сбора информации (32/64-разрядная версия)	Агенты безопасности	Обработчик запросов контекстного сбора информации обрабатывает действия, определяемые модулем контекстного сбора информации и отправляет отчет в модуль прогнозного машинного самообучения.
Расширенный модуль сканирования нежелательных программ (32/64-разрядная версия)	Агенты безопасности	Расширенный модуль сканирования нежелательных программ извлекает элементы из файлов для программ с низким приоритетом и отправляет информацию в модуль прогнозного машинного самообучения.

Компонент	Распространяется на	Описание
Расширенная база данных сопоставления угроз	Агенты безопасности	В Расширенная база данных сопоставления угроз содержится список элементов файлов, не относящихся к каким-либо известным угрозам.
Early Boot Cleanup Driver (32- и 64-разрядная версия)	Агенты безопасности	Драйвер Trend Micro Early Boot Cleanup загружается до загрузки драйверов операционной системы, что позволяет обнаруживать и блокировать загрузочные руткиты. После загрузки агента Security Agent Early Boot Cleanup Driver Trend Micro вызывает Службы Устранение повреждений для лечения руткитов.

Таблица 8-4. Антишпионское ПО

Компонент	Распространяется на	Описание
Модуль сканирования шпионских и нежелательных программ v.6 (32- или 64-разрядный)	Агенты безопасности	Этот модуль осуществляет сканирование на наличие шпионских и нежелательных программ и выполняет соответствующие действия в отношении них.
База шпионских и нежелательных программ, версия 6	Агенты безопасности	Эта база данных помогает выявлять шпионские и нежелательные программы в файлах, программах, модулях в памяти, реестре Windows и ярлыках для URL-адресов.
База данных шпионских и нежелательных программ	Агенты безопасности	

Таблица 8-5. Сетевые вирусы

Компонент	Распространяется на	Описание
Общая база данных брандмауэра	Агенты безопасности	Как и вирусная база данных, общая база данных брандмауэра помогает выявлять вирусные сигнатуры (уникальные последовательности битов и байтов, указывающие на присутствие сетевого вируса).

Таблица 8-6. Контроль действий и контроль устройств

Компонент	Распространяется на	Описание
База данных обнаружения контроля действий (32/64-разрядная)	Агенты безопасности	Эта база данных содержит правила обнаружения подозрительных действий.
32- или 64-разрядный драйвер контроля действий уровня ядра	Агенты безопасности	Данный драйвер режима ядра контролирует системные события и передает их в службу контроля действий уровня ядра для применения политик.
Служба контроля действий уровня ядра (32- и 64-разрядная версия)	Агенты безопасности	Данная пользовательская служба обладает следующими функциями: • обеспечивает обнаружение руткитов; • регулирует доступ к внешним устройствам; • защищает файлы, разделы реестра и службы.
База данных конфигурации контроля действий	Агенты безопасности	Драйвер контроля действий использует эту базу данных для определения обычных системных событий и исключения их из применения политик.

Компонент	Распространяется на	Описание
Шаблон механизма восстановления	Агенты безопасности	Шаблон механизма восстановления содержит политики, используемые для контроля поведения подозрительных угроз.
База данных цифровых подписей	Агенты безопасности	Эта база данных содержит список действительных цифровых подписей, которые используются службой контроля действий уровня ядра, для определения, является ли программа, ответственная за системное событие, безопасной.
База данных применения политик	Агенты безопасности	Служба контроля действий уровня ядра сравнивает системные события с политиками в этой базе данных.
Шаблон активации сканирования памяти (32-/64-разрядная система)	Агенты безопасности	Служба активации сканирования памяти запускает другие модули сканирования при обнаружении распакованного процесса в памяти.
База данных контроля проверки программ	Агенты безопасности	База данных контроля проверки программ контролирует и хранит контрольные точки, используемые для контроля действий.
База данных отслеживания угроз 32/64-разрядная версия	Агенты безопасности	База данных отслеживания угроз определяет атаки бесфайловых вредоносных программ.

Таблица 8-7. Эксплойты браузера

Компонент	Распространяется на	Описание
База данных предотвращения эксплойтов браузера	Агенты безопасности	Эта база данных позволяет выявлять последние эксплойты веб-браузера и предотвращать их использование для компрометации веб-браузера.

Компонент	Распространяется на	Описание
Унифицированная база данных анализатора сценариев	Агенты безопасности	Эта база данных позволяет анализировать сценарий на веб-страницах и выявить вредоносный код сценариев.

Таблица 8-8. Прогнозное машинное самообучение

Компонент	Распространяется на	Описание
Модель локального файла прогнозного машинного самообучения	Агенты безопасности	Модель локального файла прогнозного машинного самообучения распознает угрозы переносимых исполняемых файлов, когда конечные точки отключены от сети Интернет.

Критические обновления, пакеты исправлений и пакеты обновлений

Часто после официального выпуска продукта компания Trend Micro разрабатывает следующие виды программ для решения проблем, повышения производительности продукта или добавления новых функций.

- *Критически важное исправление на странице D-2*
- *Оперативное исправление на странице D-2*
- *Исправление на странице D-10*
- *Пакет обновления на странице D-27*

Местные поставщики или представители службы поддержки клиентов могут связаться с вами при выпуске обновлений. Информация о новых критических обновлениях, пакетах исправлений и пакетах обновления размещена на веб-сайте компании Trend Micro:

http://downloadcenter.trendmicro.com/index.php?regs=RU

Ко всем обновлениям прилагается файл readme, в котором описано, как устанавливать и настраивать программу. Перед началом установки ознакомьтесь с файлом readme.

Обновления сервера Security Server

Автоматические обновления

Security Server автоматически выполняет следующие обновления:

- Сразу после установки Security Server выполняется обновление с сервера Trend Micro ActiveUpdate.
- При каждом запуске сервера Security Server обновляются его компоненты.
- По умолчанию обновления по расписанию запускаются каждый час (частота обновления может быть изменена с помощью веб-консоли).

Обновления вручную

Вы можете запустить обновление вручную с веб-консоли, если обновление является срочным.

Напоминания и подсказки для обновления серверов

- Если обновление прошло успешно, Security Server выполняет автоматическое распределение обновленных компонентов агентам. Для получения более подробной информации о компонентах, развертываемых для агентов, см. *Обновляемые компоненты на странице 8-4*.
- Сервер Security Server, имеющий только адрес IPv6, не может выполнять следующие задачи:
  - получать обновления непосредственно с сервера Trend Micro ActiveUpdate или пользовательского источника обновлений с адресом IPv4;

- распределять обновления непосредственно для агентов, имеющим только адрес IPv4.

  Аналогичным образом, сервер Security Server, имеющий только адрес IPv4, не может получать обновления непосредственно от пользовательских источников обновления с адресом IPv6 и распространять обновления агентам с адресом IPv6.

  В данных ситуациях, для того, чтобы позволить серверу Security Server получать и распределять обновления, требуется прокси-сервер с двойным стеком, который может преобразовывать IP-адреса, например DeleGate.

- Если для подключения к Интернету используется прокси-сервер, для успешной загрузки обновлений его необходимо правильно настроить на вкладке **Администрирование** > **Глобальные параметры** > **Прокси-сервер**.

Дублирование компонентов

Компания Trend Micro регулярно обновляет базы данных, чтобы обеспечить актуальную защиту клиентов от вирусов. Поскольку обновления файлов базы данных доступны регулярно, Security Server использует механизм под названием **дублирование компонентов**, позволяющий быстрее загружать файлы базы данных.

Когда последняя версия файла полной базы данных доступна для загрузки с сервера Trend Micro ActiveUpdate, также становятся доступными поэтапные обновления. Поэтапные обновления являются уменьшенными версиями файла полной базы данных и представляют собой разницу между последней и предыдущей полной версии базы данных. Например, если последней версией является 175, поэтапные обновления v_173.175 содержит сигнатуры из версии 175, которые не входят в версию 173 (версия 173 является полной предыдущей версией базы данных, поскольку номера версий баз данных выпускаются с шагом 2). Поэтапное обновление v_171.175 содержит сигнатуры из версии 175, не содержащиеся в 171.

Чтобы уменьшить объем сетевого трафика, создаваемого при загрузке последней базы данных, Security Server выполняет дублирование

компонентов — метод обновления компонентов, при котором сервер загружает только поэтапные обновления. Для того, чтобы воспользоваться преимуществами дублирования компонентов, убедитесь, что сервер Security Server обновляется регулярно. В противном случае сервер будет вынужден загрузить файл полной базы данных.

Дублирование компонентов применяется к следующим компонентам:

- Вирусная база данных
- База данных агента Smart Scan
- Шаблон Damage Cleanup
- База исключений IntelliTrap
- База данных «шпионских» программ

Настройка источника обновлений Security Server

Перед выполнением

По умолчанию Security Server получает обновления с сервера Trend Micro ActiveUpdate. Укажите пользовательский источник обновления, если Security Server не может получить доступ к серверу ActiveUpdate напрямую.

- Если выбран сервер **Сервер Trend Micro ActiveUpdate**, убедитесь, что сервер Security Server подключен к Интернету, а в случае использования прокси-сервера, проверьте, что соединение с Интернетом можно установить с помощью указанных параметров прокси-сервера. Для получения дополнительных сведений см. *Настройка параметров прокси-сервера сети Интернет на странице 11-3*.
- Если источником является пользовательский источник обновлений (**Система в интрасети, содержащая копию текущего файла** или **Альтернативный источник обновления**), создайте соответствующую среду и обновляйте ресурсы для этого

источника обновлений. Убедитесь в наличии рабочего соединения между сервером Security Server и данным источником обновлений. Если понадобится помощь при настройке источника обновлений, обратитесь в службу технической поддержки.

- Сервер Security Server, имеющий только адрес IPv6, не может получать обновления непосредственно с сервера Trend Micro ActiveUpdate или любого другого пользовательского источника обновлений с адресом IPv4. Аналогичным образом, сервер Security Server, имеющий только адрес IPv4, не может получать обновления непосредственно от пользовательского источника обновлений с адресом IPv6. Чтобы сервер Security Server мог подключаться к источникам обновлений, требуется прокси-сервер с двойным стеком, который может преобразовать IP-адреса, например DeleGate.

Процедура

1. Перейдите к разделу **Обновления** > **Источник**.
2. На вкладке **Сервер** выберите источник обновлений.
   - **Сервер Trend Micro ActiveUpdate**
   - **Система в интрасети, содержащая копию текущего файла**: Введите UNC-путь в источник, например, `\\Web\ActiveUpdate`. Также укажите учетные данные (имя пользователя и пароль), которые Security Server будет использовать для подключения к этому источнику.
   - **Альтернативный источник обновлений**: Введите URL-адрес источника. Проверьте, что Security Server может получить доступ к целевому виртуальному HTTP-каталогу.
3. Нажмите кнопку **Сохранить**.

Обновление сервера Security Server вручную

Компоненты Security Server следует обновлять вручную после установки или обновления версии сервера, а также при каждом случае эпидемии.

Процедура

1. Обновление вручную можно запустить двумя способами.
   - Откройте **Обновления** > **Вручную**.
   - Выберите **Текущее состояние** и нажмите кнопку **Проверить состояние компонентов** на виджете «Состояние агента».

   Отображается экран **Обновление вручную**.
2. Выберите обновляемые компоненты.

   Для получения дополнительных сведений о компонентах см. *Обновляемые компоненты на странице 8-4*.
3. Нажмите кнопку **Обновить сейчас**.

   Появится новое окно, отображающее состояние обновления. Если обновление прошло успешно, Security Server выполнит автоматическое распределение обновленных компонентов агентам.

Настройка запланированных обновлений Security Server

Настройте Security Server на регулярную проверку источника обновлений и автоматическую загрузку доступных обновлений. Использование обновления по расписанию является простым и эффективным способом обеспечения актуальной защиты от угроз безопасности.

Во время эпидемий вирусов и вредоносного ПО Trend Micro незамедлительно обновляет антивирусные базы данных (обновления

могут выпускаться более одного раза в неделю). Регулярному обновлению подлежит также модуль сканирования и другие компоненты. Компания Trend Micro рекомендует обновлять компоненты ежедневно или даже чаще, особенно во время эпидемий вирусов и вредоносного ПО, для поддержания компонентов агента в актуальном состоянии.

Важно

Не следует запланировать одновременное сканирование и обновление. Это может привести к неожиданному прерыванию сканирования по расписанию.

Процедура

1. Выберите **Обновления** > **По расписанию**.
2. Выберите обновляемые компоненты.

   Для получения дополнительных сведений о компонентах см. *Обновляемые компоненты на странице 8-4*.
3. Откройте вкладку **Расписание** и определите расписание обновлений.
   - **Обновления обычного сканирования** включают в себя все компоненты, за исключением базы данных Smart Scan и вирусной базы данных агента Smart Scan. Выберите период обновления (ежедневно, еженедельно, ежемесячно) и затем укажите значение поля **Обновлять с периодом в** — это количество часов, в течение которых сервер Security Server будет выполнять обновление. Сервер Security Server выполняет обновление в любое заданное время в течение этого периода времени.

     Примечание

     Если для ежемесячных обновлений (не рекомендуется) выбрано 31, 30 или 29 число, а в месяце меньшее количество дней, в этом месяце обновление не будет запущено.

- **Обновления Smart Scan** включают в себя только вирусную базу данных Smart Scan и базу данных агента Smart Scan. Если ни один из ваших агентов не использует Smart Scan, пропустите этот пункт.

4. Нажмите кнопку **Сохранить**.

Откат компонентов

Откат означает возврат к предыдущей версии вирусной базы данных, базы данных агента Smart Scan или модуля вирусного сканирования. Если эти компоненты не работают должным образом, выполните их откат к предыдущим версиям. Сервер Security Server сохраняет текущую и предыдущую версии модуля вирусного сканирования, а также последние три версии вирусной базы данных и базы данных агента Smart Scan.

Примечание

Откат может быть выполнен только для вышеупомянутых компонентов.

Worry-Free Business Security задействует различные модули сканирования для агентов, работающих под управлением 32- и 64-разрядных платформ. Откат этих модулей сканирования необходимо выполнять отдельно. Процедура отката для всех типов модулей сканирования одинакова.

Процедура

1. Выберите **Обновления** > **Откат**.
2. Щелкните **Синхронизировать**, чтобы конкретный компонент уведомлял агентов для синхронизации их версий компонента с версией на сервере.

3. Щелкните **Откат**, чтобы конкретный компонент откатывал указанный компонент на сервере Security Server и агентах.

Обновления агентов Security Agent и Messaging Security Agent

Автоматические обновления

Агенты Security Agent и Messaging Security Agent (только Advanced) автоматически выполняют следующие обновления:

- Сразу же после установки агенты получают обновления с сервера Security Server.
- Каждый раз, когда Security Server завершает обновление, он автоматически посылает обновления агентам.
- Каждый раз, когда агент Update Agent завершает обновление, он автоматически посылает обновления соответствующим агентам Security Agent.
- По умолчанию обновления по расписанию выполняются:
  - Каждые 8 часов на агенты Office Security Agent
  - Каждые 2 часа с агентов Office Security Agent
- По умолчанию агенты Messaging Security Agent запускают обновления по расписанию каждые 24 часа в 00:00.

Запуск обновления вручную

Программа Security Agent автоматически получает обновления от Security Server.

Вы можете выполнить обновление вручную, в случае если вы на некоторое время были отключены от корпоративной сети или если

существует срочная необходимость установить последнюю защиту от угроз (например, после эпидемии).

Если для подключения к Интернету используется прокси-сервер, убедитесь в правильности параметров прокси-сервера.

Процедура

1. Откройте главную консоль и нажмите кнопку **Обновление**.

   Примечание

   Выполнить обновление вручную можно также, щелкнув значок программы Security Agent на панели задач Windows правой кнопкой мыши и выбрав **Обновить сейчас**.

2. После окончания установки обновления нажмите на кнопку **Закрыть**.

Напоминания и подсказки для обновления агентов

- Агенты Security Agent получают обновления с сервера Security Server, агентов Update Agent или сервера Trend Micro ActiveUpdate.

  Агенты Messaging Security Agent получают обновления только с сервера Security Server.

  Для получения подробной информации о процессе обновления см. *Обзор обновлений на странице 8-2*.

- Агент, имеющий только адрес IPv6, не может получать обновления непосредственно с сервера Security Server с адресом IPv4 или от агента обновления Update Agent и сервера Trend Micro ActiveUpdate.

  Аналогичным образом, агент, имеющий только адрес IPv4, не может получать обновления непосредственно с сервера Security Server с адресом IPv6 или от агента обновления Update Agent.

В данных ситуациях для разрешения обновления этим агентам требуется прокси-сервер с двойным стеком, который может преобразовать IP-адреса, например DeleGate.

- Для получения более подробной информации об обновлении компонентов агентов см. *Обновляемые компоненты на странице 8-4*.
- Помимо компонентов, агенты при обновлении получают с сервера Security Server обновленные файлы конфигурации. Они необходимы агентам для применения новых параметров. Каждый раз при изменении параметров агентов из веб-консоли файлы конфигурации тоже изменяются.

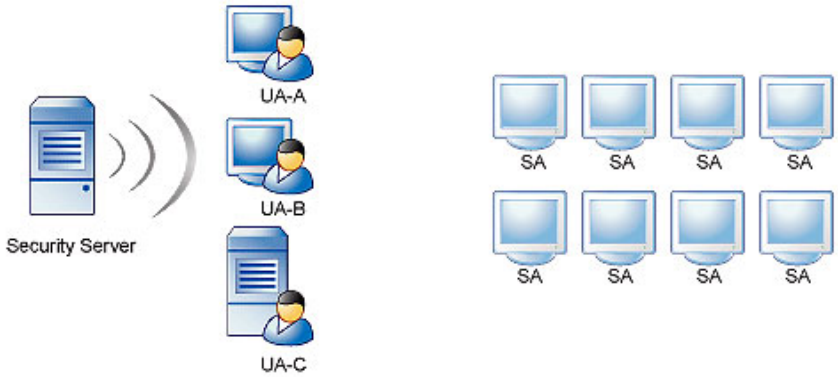
Агенты обновлений

Агенты обновления — это агенты Security Agent, которые могут получать обновленные компоненты от сервера Security Server или сервера ActiveUpdate и выполнять их развертывание на других агентах.

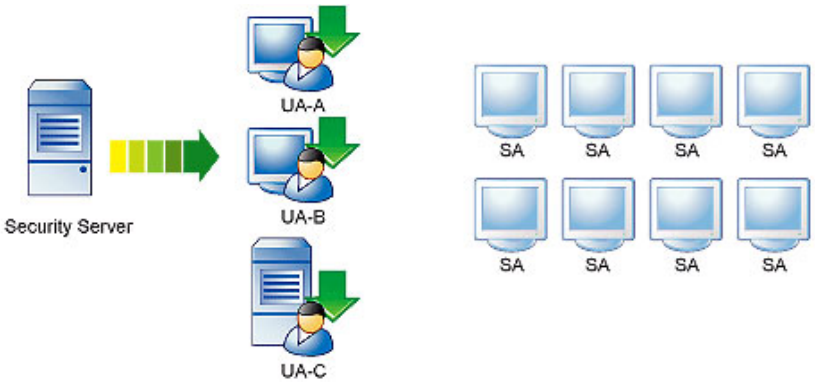
Если сегменты сети между клиентскими компьютерами и сервером Trend Micro Security Server определяются как «узкополосные» или «с интенсивным трафиком», агенты Security Agent могут служить в качестве агентов обновлений. Агенты обновлений позволяют снизить нагрузку на сеть, поскольку всем агентам Security Agent не приходится обращаться к Security Server для получения обновлений компонентов. Если сеть географически распределена, и соединения между сегментами перегружены, компания Trend Micro рекомендует разрешить как минимум одному агенту Security Agent из каждого сегмента выступать в роли агента обновления.

Процесс получения обновлений с помощью агента обновлений может быть описан следующим образом:

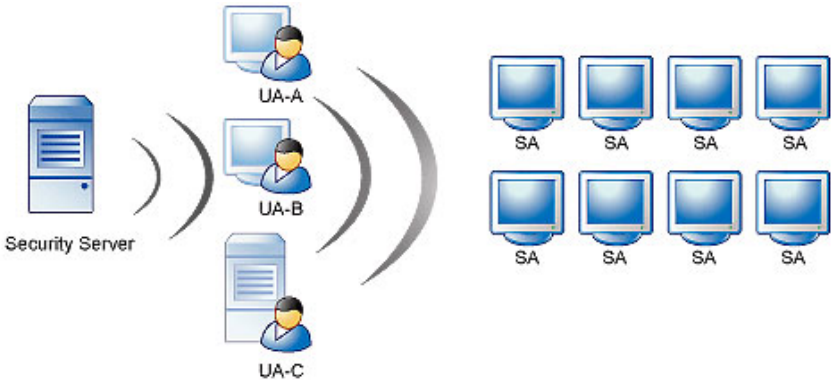
1. Сервер Security Server уведомляет агенты обновления (АО) о наличии новых обновлений.



2. Агенты обновления загружают компоненты обновлений от Security Server.



3. Затем сервер Security Server уведомляет агенты Security Agent о том, что доступны обновленные компоненты.

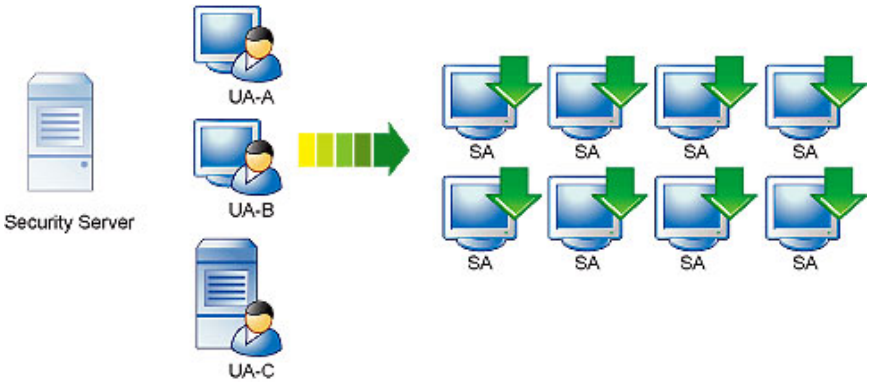


4. Каждый агент Security Agent загружает копию таблицы заказов агента обновления, чтобы определить свой источник обновлений. Заказ агентов обновления в таблице заказов агента обновления изначально определяется заказом, к которому они были добавлены как альтернативные источники обновления на веб-консоли. Каждый агент Security Agent проходит таблицу по одной записи за раз, начиная с первой, пока не обнаружит свой источник обновления.

Таблица последовательности агентов обновления

Диапазон IP-адресов	Агент обновления
10.1.1.1-10.1.1.10	UA-A
10.2.1.1-10.2.1.10	UA-B
10.3.1.1-10.3.1.10	UA-C

5. Затем агенты Security Agent загружают обновленные компоненты из назначенного агента обновлений. Если по какой-либо причине назначенный агент обновлений недоступен, Security Agent попытается загрузить обновленные компоненты из Security Server.



Настройка агентов обновлений

Процедура

1. Перейдите к разделу **Обновления** > **Источник**.
2. Откройте вкладку **Агенты обновления**.
3. Выполните следующие задачи.

Задача	Шаги
Выбор агентов Security Agent в качестве агентов обновлений.	a. В разделе **Выбор агентов обновлений** нажмите кнопку **Добавить**. Откроется новое окно. b. Из списка выберите один или несколько агентов для выполнения функций агентов обновлений. c. Нажмите кнопку **Сохранить**. Окно закроется. d. Вернитесь в раздел **Выбор агентов обновлений** и выберите **Всегда обновлять агенты только непосредственно с сервера Security Server**, если хотите, чтобы агенты обновлений всегда загружали обновленные

Задача	Шаги
	компоненты с сервера Security Server, а не из другого агента обновлений.
Настройка агентов Security Agent для обновления с помощью агентов обновлений	a. В разделе **Альтернативные источники обновлений** выберите **Разрешить альтернативные источники обновлений для агентов Security Agent и агентов обновлений**. **Примечание** Отключение этой функции не позволит агентам Security Agent обновляться с помощью агентов обновлений, устанавливая в качестве источника их обновлений сервер Security Server. b. Нажмите кнопку **Добавить**. Откроется новое окно. c. Введите IP-адреса агентов Security Agent, которые будут обновляться из агента обновлений. • Введите диапазон адресов IPv4. Чтобы указать отдельный агент Security Agent, введите IP-адрес этого агента в поля **от** и **до**. • Для IPv6 введите префикс и длину IP-адреса. d. Выберите агент обновлений из раскрывающегося списка. Если раскрывающийся список недоступен, настроенные агенты обновлений отсутствуют. e. Нажмите кнопку **Сохранить**. Окно закроется. f. При необходимости задайте несколько диапазонов IP-адресов. Если вы определили несколько диапазонов IP-адресов, вы можете использовать функцию **Изменить порядок** для установки приоритета диапазонов IP-адресов. Когда агенты Security Agent получают от Security Server уведомление о наличии обновлений, они сканируют список диапазонов IP-адресов, чтобы определить верный источник обновлений. Security Agent сканирует список,

Задача	Шаги
	начиная с первого элемента, пока не обнаружит верный источник обновлений. **Совет** Задайте несколько агентов обновлений для одного диапазона IP-адресов на случай отказа одного из агентов. Это означает, что если агенты Security Agent не смогут получить обновления от одного агента обновлений, они будут обращаться к другим агентам обновлений. Для этого создайте не менее двух (2) записей с одинаковыми диапазонами IP-адресов и назначьте для них разные агенты обновлений.
Удаление агентов обновлений	Чтобы удалить агент обновлений и запретить связанным с ним агентам Security Agent обращаться к нему, перейдите в раздел **Выбор агентов обновлений**, установите флажок для соответствующего имени компьютера агента обновлений и нажмите кнопку **Удалить**. Это действие не удалит диапазон IP-адресов Security Agent в разделе **Альтернативные источники обновлений**, а только назначит сервер Security Server в качестве источника обновлений для «потерянных» агентов Security Agent. Если у вас есть другой агент обновлений, вы можете назначить его для «потерянных» агентов Security Agent.
Запрет обновления агентов Security Agent с помощью агентов обновлений	Если вы не хотите, чтобы Security Agent, принадлежащие к определенному диапазону IP-адресов, обновлялись с помощью агента обновлений, перейдите в раздел **Альтернативные источники обновлений**, установите флажок для соответствующего диапазона IP-адресов агентов Security Agent и нажмите кнопку **Удалить**.

4. Нажмите кнопку **Сохранить**.

Глава 9

Использование раздела «Текущее состояние»

Текущее состояние

Worry-Free Business Security предоставляет виджеты, которые служат в качестве элементов быстрого получения визуальной информации для облегчения управления агентом Security Agent.

Окно **Текущее состояние** появляется при открытии веб-консоли Worry-Free Business Security или раздела **Текущее состояние** в главном меню.

Таблица 9-1. Элементы интерфейса текущего состояния

Виджет	Описание
Центр действий	Этот виджет отображает события, по которым администраторы должны принять меры для решения проблем.
Обнаружения угроз безопасности за определенный период времени	Этот виджет отображает сводную информацию о локальных компьютерах сети с обнаруженными угрозами и их типами, которые затрагивают сеть в течение заданного интервала времени.
Сводка по ПО для вымогательства	Этот виджет отображает сводную информацию о всех попытках атак ПО для вымогательства в течение заданного интервала времени.
Статус лицензии	Этот виджет отображает сводную информацию о количестве установок программы и истечении срока действия лицензии.
Сводка по серверам Exchange	В этом элементе интерфейса предоставляется обзор состояния подключения агентов Messaging Security Agent и распределения обнаружений угроз на серверах Exchange.
Состояние агента	Этот виджет отображает сводную информацию о подключении и статусе обновления агентов Security Agent в сети.

Частота обновления информации для каждого раздела в окне **Текущее состояние** варьируется от 1 до 10 минут. Чтобы обновить информацию в окне, нажмите в браузере кнопку **Обновить**.

Центр событий

Этот виджет отображает события, по которым администраторы должны принять меры для решения проблем.

Рядом с некоторыми событиями могут отображаться кнопки с рекомендованными действиями. Чтобы попытаться разрешить проблему, можно воспользоваться этими кнопками либо нажать на события для получения подробной информации.

Таблица 9-2. События центра событий

Событие	Рекомендация
Антивирус — неустраненные угрозы	Запустите сканирование с помощью инструмента Trend Micro HouseCall.
Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах	Включите сканирование в режиме реального времени на всех устройствах, чтобы обеспечить защиту.
Антивирус – сканирование в режиме реального времени отключено на серверах Exchange	Включить сканирование в режиме реального времени на всех серверах Exchange, чтобы обеспечить защиту.
Антишпионское ПО — обнаружения, требующие перезагрузки устройства	Перезапустите устройства для полного устранения обнаруженных угроз.
События, связанные с лицензиями	Откройте раздел **Администрирование** > **Лицензия на продукт** и проверьте состояние лицензии.
Недостаток ресурсов – остающееся дисковое пространство менее %threshold%	Запустите инструмент очистки диска, чтобы удалить неиспользуемые файлы резервных копий, журналов и баз данных. Подробную информацию см. в разделе *Сохранение дискового пространства на странице 14-15*.
Службы Smart Protection – служба недоступна	Проверьте состояние сервера Smart Scan Server на консоли Worry-Free Business Security и убедитесь в том, что он работает правильно.

Событие	Рекомендация
Обновление – минимум один устаревший агент Messaging Security Agent через час после выпуска базы данных	Убедитесь в том, что на сервере Security Server включено обновление по расписанию для агентов Messaging Security Agent и что эти агенты могут подключаться к Интернету.
Обновление — степень развертывания менее %threshold% через час после выпуска базы данных	Проверьте подключение Security Agent к Интернету, а затем повторно обновите агенты.
Обновление — компоненты сервера Security Server не обновлялись более %threshold% дн.	Убедитесь в том, что на сервере Security Server включено обновление по расписанию для компонентов и что этот сервер может подключаться к Интернету.
Обновление — вирусная база данных Smart Scan не обновлялась более %threshold% ч.	Убедитесь в том, что на сервере Security Server включено обновление по расписанию для вирусной базы данных Smart Scan и что этот сервер может подключаться к Интернету.

Антивирусная защита: неустраненные угрозы

Эту информацию можно просмотреть, выбрав событие **Антивирусная защита — неустраненные угрозы: %N%** в Центре действий. Worry-Free Business Security создает или обновляет информацию в этом журнале при выполнении сканирования в режиме реального времени, сканирования вручную или по расписанию.

- Для загрузки инструмента Trend Micro HouseCall выберите **Инструмент загрузки**, после чего его можно использовать для сканирования пораженного устройства.
- Нажмите **Удалить из центра событий** для перехода к окну **Текущее состояние** и удаления уведомления из Центра действий. Доступ к журналам, связанным с событиями в этом окне, может осуществляться с помощью запросов к журналу.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время последней неудачной попытки лечения или удаления вируса либо вредоносной программы
Имя устройства	Имя пораженного устройства
Имя вируса/вредоносной программы	Имя обнаруженного вируса или вредоносной программы Перейдите по ссылке в энциклопедию вирусов Trend Micro, чтобы ознакомиться с подробным описанием угрозы, а также инструкциями по устранению атак этой конкретной угрозы вручную.
Имя файла	Имя файла, поврежденного вирусом или вредоносной программой
Путь	Расположение зараженного файла
Тип сканирования	Тип сканирования, используемый для обнаружения вируса или вредоносной программы
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение вируса или вредоносной программы

Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах

Вы можете просмотреть информацию, нажав на событие **Антивирус – сканирование в режиме реального времени отключено на оконечных устройствах: %N%** в Центре событий.

- Нажмите **Включить сканирование в режиме реального времени**, чтобы включить сканирование на всех устройствах.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Имя устройства	Имя устройства со сканированием в режиме реального времени отключено.
Имя группы	Имя группы, к которой принадлежит устройство

Антивирус – сканирование в режиме реального времени отключено на серверах Exchange

Вы можете просмотреть информацию, нажав на событие **Антивирус – сканирование в режиме реального времени отключено на серверах Exchange: %N%** в Центре событий.

- Нажмите **Включить сканирование в режиме реального времени**, чтобы включить сканирование на всех серверах Exchange.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Имя сервера Exchange	Имя сервера Exchange со сканированием в режиме реального времени отключено.

Антишпионское ПО: обнаружения, требующие перезагрузки устройства

Информацию этого журнала можно просмотреть, выбрав событие **Антишпионское ПО: обнаружения, требующие перезагрузки устройства: %N%** в Центре действий.

- Нажмите **Удалить из центра событий** для перехода к окну **Текущее состояние** и удаления уведомления из Центра действий. Доступ к журналам, связанным с событиями в этом окне, может осуществляться с помощью запросов к журналу.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений об обнаружении шпионских или нежелательных программ в Worry-Free Business Security
Имя устройства	Имя пораженного устройства
Имя шпионской или нежелательной программы	Имя обнаруженной шпионской или нежелательной программы Перейдите по ссылке в энциклопедию вирусов Trend Micro, чтобы ознакомиться с подробным описанием угрозы, а также инструкциями по устранению атак этой конкретной угрозы вручную.
Тип сканирования	Тип сканирования, используемый для поиска шпионской или нежелательной программы

Недостаток ресурсов – оставшееся дисковое пространство

Вы можете просмотреть информацию, нажав на событие **Недостаток ресурсов – остающееся дисковое пространство менее %threshold%** в Центре событий.

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Имя сервера	Имя сервера, у которого заканчивается дисковое пространство
Имя группы	Имя группы, к которой принадлежит этот сервер

Обновление: устаревшие агенты

Можно просмотреть эту информацию, нажав на событие **Обновление: степень развертывания менее %threshold% через час после выпуска базы данных** в Центре событий. Агенты Security Agent, приведенные в списке на этом экране, требуют обновления модуля или базы данных.

- Нажмите **Обновить сейчас**, чтобы уведомить устаревшие агенты Security Agent об обновлении до последних версий компонентов.
- Нажмите **Проверить состояние компонентов**, чтобы открылся экран **Обновление вручную**.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Имя устройства	Имя устройства, которому требуются обновления компонентов.
Имя группы	Имя группы, к которой принадлежит устройство
Метод сканирования	• Smart Scan • Обычное сканирование

Обновление – устаревшие агенты Messaging Security Agent

Можно просмотреть эту информацию, нажав на событие **Обновление – минимум один устаревший агент Messaging Security Agent через час после выпуска базы данных** в Центре событий.

- Нажмите **Обновить сейчас**, чтобы уведомить устаревшие агенты Messaging Security Agent об обновлении до последних версий компонентов.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Имя сервера Exchange	Имя сервера Exchange, которому требуются обновления компонентов.

Обнаружения угроз безопасности за определенный период времени

Этот виджет отображает сводную информацию о локальных компьютерах сети с обнаруженными угрозами и их типами, которые затрагивают сеть в течение заданного интервала времени.

- Для переключения между различными видами нажмите или .
- Откройте вкладку **Известных угроз**, **Неизвестные угрозы** или **Нарушения политик** для просмотра сведений об обнаружениях для конкретных угроз.

Просмотр	Описание
График ( )	• Чтобы показать или скрыть информацию об обнаружении на графике, щелкните мышью название типа угрозы в нижней части графика. • Наведите курсор мыши на узел (узлы) за любой конкретный день, чтобы просмотреть общее количество обнаружений для отображаемых типов угрозы. Щелкните узел для перехода в окно журналов для выделенного в списке типа угрозы.
Таблица ( )	• Чтобы открыть экран с журналами, на котором перечислены подробности обнаружения, нажмите на счетчик количества обнаружений.

Обнаружения угроз безопасности: вирус/вредоносная программа

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Известных угроз** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Вирусов/вредоносных программ** в виде таблицы

- Любой узел **Вирусов/вредоносных программ** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время, когда агент Security Agent сообщил информацию об обнаружении вируса или вредоносной программы программе Worry-Free Business Security
Имя устройства	Имя пораженного устройства
Имя вируса/вредоносной программы	Имя обнаруженного вируса или вредоносной программы Перейдите по ссылке в энциклопедию вирусов Trend Micro, чтобы ознакомиться с подробным описанием угрозы, а также инструкциями по устранению атак этой конкретной угрозы вручную.
Имя файла	Имя файла, поврежденного вирусом или вредоносной программой
Путь	Расположение зараженного файла
Тип сканирования	Тип сканирования, используемый для обнаружения вируса или вредоносной программы
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение вируса или вредоносной программы

Обнаружения угроз безопасности: шпионские и нежелательные программы

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Известных угроз** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **шпионских и нежелательных программ** в виде таблицы

- Любой узел **шпионских и нежелательных программ** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений об обнаружении шпионских или нежелательных программ в Worry-Free Business Security
Имя устройства	Имя пораженного устройства Нажмите на имя, чтобы увидеть список отдельных шпионских/нежелательных программ, обнаруженных на этом устройстве.
Имя шпионской или нежелательной программы	Имя обнаруженной шпионской или нежелательной программы
Тип сканирования	Тип сканирования, используемый для поиска шпионской или нежелательной программы
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение шпионских или нежелательных программ

Обнаружения угроз безопасности: Web Reputation

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Известных угроз** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Web Reputation** в виде таблицы
- Любой узел **Web Reputation** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о попытке доступа к запрещенному URL-адресу в Worry-Free Business Security
Имя устройства	Имя устройства, на котором была выполнена попытка получения доступа к запрещенному URL-адресу
URL-адрес	Запрещенный URL-адрес
Уровень риска	Класс заражения в соответствии с классификацией TrendLabs, основанной на тяжести заражения и потенциальном ущербе.

Обнаружения угроз безопасности: сетевые вирусы

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Известных угроз** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Сетевые вирусы** в виде таблицы
- Любой узел **Сетевые вирусы** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время, когда агент Security Agent сообщил информацию об обнаружении сетевого вируса программе Worry-Free Business Security
Имя устройства	Имя пораженного устройства
IP-адрес источника атаки	IP-адрес источника атаки
IP-адрес атакованного компьютера	IP-адрес атакованного компьютера
Направление пакетов	Обнаружение пакета

Столбец	Описание
Имя сетевого вируса	Имя обнаруженного сетевого вируса
Количество	Каждый сетевой вирус учитывается каждый раз, когда он обнаруживается.

Обнаружения угроз безопасности: контроль действий

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Неизвестные угрозы** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Контроля действий** в виде таблицы
- Любой узел **Контроля действий** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о нарушении контроля действий в Worry-Free Business Security
Имя устройства	Имя устройства, нарушившего политику
Угроза безопасности	Тип угрозы безопасности
Тема	Тема действия
Тип события	Соответствующее системное событие
Цель	Цель действия
Операция	Операция, выполненная пользователем, который вызвал нарушение
Результат	Действие, выполненное Worry-Free Business Security в ответ на нарушение контроля действий

Обнаружения угроз безопасности: прогнозное машинное самообучение

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Неизвестные угрозы** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **прогнозного машинного самообучения** в представлении таблицы
- Любой узел **прогнозного машинного самообучения** в представлении графика

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
/	Нажмите значок, чтобы развернуть или закрыть сведения журнала под строкой таблицы.
Дата/время	Дата и время, когда агент Security Agent сообщил информацию об обнаружении Worry-Free Business Security
Имя устройства	Имя пораженного устройства
Имя группы	Имя группы, к которой принадлежит устройство
Неизвестная угроза	Имя вероятной угрозы
Вероятность угрозы	Степень соответствия файла или процесса модели вредоносной программы

Столбец	Описание
Имя файла	Имя объекта файла или программы, выполнившей процесс **Важно** Имя обнаруженного файла для этого обнаружения может не совпадать с именем файла, обнаруженным на других локальных компьютерах. Прогнозное машинное самообучение связывает обнаружения в соответствии с хеш-значением файла, а не конкретными именами файла.
Путь	Путь к объекту файла или путь к программе, выполнившей процесс
Канал заражения	Канал происхождения угрозы
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение

Сведения раздела «Обнаружения угроз безопасности: прогнозное машинное самообучение»

Чтобы просмотреть эти сведения, щелкните любой значок

в первом столбце в окне журналов **Обнаружения угроз безопасности: прогнозное машинное самообучение**.

Раздел информации о журнале состоит из двух вкладок, описанных далее.

- **Неизвестная угроза**: отображаются результаты анализа прогнозного машинного самообучения
- **Имя файла**: отображаются общие сведения, связанные со свойствами файла, и сведения о сертификате для данного журнала обнаружения

Совет

Выберите элемент **Добавить в список исключений**, чтобы быстро добавить значение хэша зараженного файла в глобальный список исключений прогнозного машинного самообучения. Полный список исключений показан в окне **Глобальные параметры**.

Дополнительные сведения см. в разделе *Настройка параметров списка исключений на странице 11-15*.

В таблице ниже описана информация, которая отображается на вкладке **Неизвестная угроза**.

Таблица 9-3. Сведения о вкладке «Неизвестная угроза»

Элемент	Описание
Вероятность угрозы	Степень соответствия файла или процесса модели вредоносной программы
Вероятный тип угрозы	Наиболее вероятный тип угрозы, содержащейся в файле. Для определения типа функция прогнозного машинного самообучения сравнивает результат данного анализа с другими известными угрозами
Идентификаторы угроз	Список функций API, используемых файлом или процессом. Эти функции могут указывать на тип обнаруженной угрозы. **Важно** Определение функций API является лишь одним из факторов определения типа угрозы. Функция прогнозного машинного самообучения использует множество других характеристик файла и методов анализа для вычисления вероятности угрозы и возможного типа угрозы.
Тип обнаружения	Тип объекта, активировавшего обнаружение («Файл» или «Процесс»)
Подобные известные угрозы	Список известных типов угроз, которые обнаруживаются на основе похожих характеристик файлов или процессов

Обнаружения угроз безопасности: URL-фильтрация

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Нарушения политик** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Фильтрации URL-адресов** в виде таблицы
- Любой узел **Фильтрации URL-адресов** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о попытке доступа к запрещенному URL-адресу в Worry-Free Business Security
Имя устройства	Имя устройства, на котором была выполнена попытка получения доступа к запрещенному URL-адресу
URL-адрес	Запрещенный URL-адрес

Обнаружения угроз безопасности: контроль устройств

Данную информацию можно просмотреть, щелкнув одну из следующих ссылок на вкладке **Нарушения политик** виджета **Обнаружения угроз безопасности за определенный период времени**.

- Число обнаружений **Контроля устройств** в виде таблицы
- Любой узел **Контроля устройств** в графическом представлении

Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время, когда агент Security Agent сообщил информацию о нарушении контроля устройств программе Worry-Free Business Security
Имя устройства	Имя устройства, нарушившего политику
Тип	Тип устройства хранения
Разрешение	Разрешение установлено для устройства хранения
Тема	Тема действия
Объект	Объект операции
Операция	Операция выполнена

Сводка по ПО для вымогательства

Этот виджет отображает сводную информацию о всех попытках атак ПО для вымогательства в течение заданного интервала времени.

В представлении по умолчанию отображается сводная информация обо всем обнаруженном ПО для вымогательства, которая затем классифицируется в зависимости от канала заражения.

- Чтобы открыть окно журналов **Сводная информация о ПО для вымогательства**, в котором перечислены подробные сведения об обнаружении ПО для вымогательства, нажмите на количество обнаружений ПО для вымогательства в представлении по умолчанию.
- Для переключения между различными видами используйте раскрывающиеся списки.

Нажмите для отображения информации об обнаружениях в виде графика.

- Наведите курсор мыши на узел (узлы) за любой конкретный день, чтобы просмотреть общее количество обнаружений для

отображаемой категории обнаружения. Щелкните по узлу для перехода в окно журналов **Сводная информация о ПО для вымогательства**, в котором перечислены подробные сведения об обнаружении ПО для вымогательства для этого дня.

Журналы сводок по ПО для вымогательства

Эту информацию можно просмотреть, нажав узел в графике или число обнаружений на виджете **Сводка по ПО для вымогательства**.

- Используйте списки **Канал заражения** и **Период** для изменения просмотра.
- Нажмите **Экспорт** для сохранения журнала событий в файл CSV.

Столбец	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений об обнаружении ПО для вымогательства в Worry-Free Business Security
Угроза безопасности	Тип ПО для вымогательства • Имя вируса/вредоносной программы: отображает имя обнаружения известного файла ПО для вымогательства • Несанкционированное шифрование файлов: отображается, когда Worry-Free Business Security обнаруживает, что подозрительная программа зашифровала файл • <URL>: отображается, когда Worry-Free Business Security обнаруживает известный URL-адрес, связанный с ПО для вымогательства
Source	Тип сканирования, в ходе которого обнаружена угроза
Путь/URL	• Путь к файлу ПО для вымогательства • URL-адрес, зараженный ПО для вымогательства

Столбец	Описание
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение ПО для вымогательства
Имя устройства	Имя пораженного устройства
Канал заражения	Канал обнаружения ПО для вымогательства
Подробнее	Нажмите **Просмотр**, чтобы просмотреть данные журнала.

ПО для вымогательства: данные журналов контроля действий

Эту информацию можно просмотреть, перейдя по ссылке **Просмотр** в столбце **Подробные сведения** окна журналов «Сводная информация о ПО для вымогательства».

Строка	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о нарушении контроля действий в Worry-Free Business Security
Имя устройства	Имя устройства, нарушившего политику
Угроза безопасности	Тип угрозы безопасности
Тема	Тема действия
Тип события	Соответствующее системное событие
Цель	Цель действия
Операция	Операция, выполненная пользователем, который вызвал нарушение
Результат	Действие, выполненное Worry-Free Business Security в ответ на нарушение контроля действий

ПО для вымогательства: сведения журнала фильтрации URL-адресов

Эту информацию можно просмотреть, перейдя по ссылке **Просмотр** в столбце **Подробные сведения** окна журналов «Сводная информация о ПО для вымогательства».

Строка	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о попытке доступа к запрещенному URL-адресу в Worry-Free Business Security
Имя устройства	Имя устройства, на котором была выполнена попытка получения доступа к запрещенному URL-адресу
URL-адрес	Запрещенный URL-адрес
Категория URL-адреса	Категория запрещенного URL-адреса
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на попытку доступа к запрещенным URL-адресам

ПО для вымогательства: сведения журнала вирусов

Эту информацию можно просмотреть, перейдя по ссылке **Просмотр** в столбце **Подробные сведения** окна журналов «Сводная информация о ПО для вымогательства».

Строка	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений об обнаружении ПО для вымогательства в Worry-Free Business Security
Имя устройства	Имя пораженного устройства

Строка	Описание
Имя вируса/вредоносной программы	Имя обнаруженного ПО для вымогательства Перейдите по ссылке в энциклопедию вирусов Trend Micro, чтобы ознакомиться с подробным описанием угрозы, а также инструкциями по устранению атак этой конкретной угрозы вручную.
Имя файла	Имя файла, поврежденного ПО для вымогательства
Путь	Расположение зараженного файла
Канал заражения	Среда, посредством которой ПО для вымогательства получило доступ к локальному компьютеру
Тип сканирования	Тип сканирования, использованный для обнаружения ПО для вымогательства
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на обнаружение ПО для вымогательства

ПО для вымогательства: сведения журнала Web Reputation о программах-вымогателях

Эту информацию можно просмотреть, перейдя по ссылке **Просмотр** в столбце **Подробные сведения** окна журналов «Сводная информация о ПО для вымогательства».

Строка	Описание
Дата/время	Дата и время передачи агентом Security Agent сведений о попытке доступа к запрещенному URL-адресу в Worry-Free Business Security
Имя устройства	Имя устройства, на котором была выполнена попытка получения доступа к запрещенному URL-адресу
URL-адрес	Запрещенный URL-адрес
Уровень риска	Класс заражения в соответствии с классификацией TrendLabs, основанной на тяжести заражения и потенциальном ущербе.

Строка	Описание
Выполненное действие	Действие, выполненное Worry-Free Business Security в ответ на попытку доступа к запрещенным URL-адресам

Статус лицензии

Этот виджет отображает сводную информацию о количестве установок программы и истечении срока действия лицензии.

Сводка по серверам Exchange

В этом элементе интерфейса предоставляется обзор состояния подключения агентов Messaging Security Agent и распределения обнаружений угроз на серверах Exchange.

Нажмите на уровень безопасности, чтобы настроить уровень обнаружения спама для агента Messaging Security Agent.

Столбец	Описание
Сервер	Имя сервера Exchange
Событие	Тип спама электронной почты
Коэффициент	Равняется количеству обнаружений, разделенному на количество сканированных сообщений

Состояние агента

Этот виджет отображает сводную информацию о подключении и статусе обновления агентов Security Agent в сети.

- Нажмите на количество около состояния, чтобы перейти к экрану **Устройства**, на котором приводится список информации об устройстве для данного конкретного состояния.

- Нажмите **Добавить устройства**, чтобы перейти к экрану **Добавить устройства**, где можно установить агент Security Agent на большем количестве устройств.

  Дополнительные сведения см. в разделе *Установка агентов на странице 3-1*.

- Нажмите **Проверить состояние компонентов**, чтобы перейти к экрану **Обновление вручную**, где можно просмотреть последнюю информацию о состоянии компонента.

  Дополнительные сведения см. в разделе *Обновляемые компоненты на странице 8-4*.

Глава 10

Управление уведомлениями

В этой главе описывается использование различных параметров уведомлений.

Использование уведомлений

Настройте на сервере отправку уведомлений об аномальных явлениях в сети. Это позволит администраторам тратить меньше времени на мониторинг Worry-Free Business Security и заблаговременно получать по электронной почте предупреждения о возможных эпидемиях.

По умолчанию выбраны все события, показанные в окне **Уведомления**, и сервер отправляет уведомления обо всех таких событиях администраторам.

Таблица 10-1. Уведомления «Требуется действие»

Тип события	Описание
События, имеющие отношение к угрозам	
Антивирус — неустраненные угрозы	Действия, предпринятые в ответ на угрозы проникновения вируса или вредоносной программы, не привели к успеху. В число выявленных проблем не входит следующее событие сканирования: «Пропущена потенциальная угроза безопасности»
Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах	Сканирование в режиме реального времени отключено на локальных компьютерах.
Антивирус – сканирование в режиме реального времени отключено на серверах Exchange	Сканирование в реальном времени отключено на серверах Exchange.
Антишпионское ПО — обнаружения, требующие перезагрузки устройства	Локальные компьютеры, на которых обнаружены шпионские и нежелательные программы, необходимо перезапустить, чтобы полностью устранить угрозы.
Системные события	
Обновление – устаревшие агенты	Для устаревших агентов Security Agent требуется обновление компонентов.

Тип события	Описание
Обновление – устаревшие агенты Messaging Security Agent	Для устаревших агентов Messaging Security Agent требуется обновление компонентов.
Обновление – устаревшая вирусная база данных Smart Scan	Для устаревшей вирусной базы данных Smart Scan требуется обновление.
Обновление – устаревшие компоненты Security Server	Для устаревшего сервера Security Server требуется обновление компонентов.
Службы Smart Protection – служба недоступна	Агентам Security Agent, настроенным для службы Smart Scan, не удается подключиться к службам Smart Protection, или же служба недоступна.
Недостаток ресурсов – оставшееся дисковое пространство	Остающееся количество свободного дискового пространства на некоторых серверах менее указанного процента.
События, связанные с лицензиями	
Лицензия – срок действия истек	Срок действия лицензии истек.
Лицензия – срок действия лицензии истекает менее чем через 60 дней	Срок действия лицензии скоро истечет.
Лицензия – количество установок программы превысило 110%	Количество установок превысило 110%.
Лицензия – количество установок программы превысило 100%	Количество установок превысило 100%.

Таблица 10-2. Предупреждения

Тип события	Описание
События, имеющие отношение к угрозам	

Тип события	Описание
Антивирус — количество обнаруженных угроз проникновения вируса на локальных компьютерах превышает:	Количество обнаруженных угроз проникновения вируса или вредоносной программы на локальных компьютерах превышает заданное значение для указанного периода времени.
Антивирус — количество обнаруженных угроз проникновения вируса на серверах Exchange превышает:	Количество обнаруженных угроз проникновения вируса или вредоносной программы на серверах Exchange превышает заданное значение для указанного периода времени.
Антишпионское ПО — количество обнаруженных шпионских или нежелательных программ превысило:	Количество обнаруженных угроз проникновения шпионских или нежелательных программ на локальных компьютерах превышает заданное значение для указанного периода времени.
Защита от спама — количество обнаружений спама во всех полученных сообщениях превышает:	Обнаружения спама во всех полученных сообщениях превышают указанный процент.
Web Reputation — количество попыток доступа к запрещенным URL-адресам превысило:	Количество попыток доступа к запрещенным URL-адресам превышает заданное значение для указанного периода времени.
Фильтрация URL-адресов — количество попыток доступа к запрещенным URL-адресам превысило:	Количество попыток доступа к запрещенным URL-адресам превышает заданное значение для указанного периода времени.
Прогнозное машинное самообучение — количество обнаруженных неизвестных угроз превысило:	Количество обнаруженных неизвестных угроз превышает заданное значение для указанного периода времени.
Контроль действий — количество нарушений контроля действий превысило:	Количество нарушений контроля действий превышает заданное значение для указанного периода времени.

Тип события	Описание
Сетевые вирусы — количество обнаруженных сетевых вирусов превысило:	Количество обнаруженных сетевых вирусов превышает заданное значение для указанного периода времени.
Контроль устройств — количество нарушений контроля устройств превысило:	Количество нарушений контроля устройств превышает заданное значение для указанного периода времени.

Настройка событий для уведомлений

Программа Worry-Free Business Security предлагает три метода доставки уведомлений:

- Уведомление по протоколу SNMP
- Журнал событий Windows
- Уведомление по электронной почте

Процедура

1. Выберите пункт **Администрирование** > **Уведомления**.
2. Чтобы получать уведомления по протоколу SNMP, настройте параметры в разделе **Получатель уведомлений по протоколу SNMP**.

   Простой протокол сетевого управления (SNMP) — протокол, используемый для управления сетями. Для просмотра данных прерывания SNMP используйте браузер Management Information Base.

   a. Выберите параметр **Разрешить уведомления SNMP**.

   b. Укажите IP-адрес прерывания SNMP.

   c. Укажите строку SNMP-сообщества.

3. Чтобы получать уведомления в журнал событий Windows, выберите параметр **Сделать запись в журнал событий Windows** в разделе **Запись в журнал**.

4. Чтобы получать уведомления по электронной почте, укажите отправителя и получателей.

Совет

Разделяйте записи точкой с запятой.

5. Нажмите на вкладку **Требуется действие** или **Предупреждения**.

6. В столбце **Уведомление по электронной почте** выберите флажки, соответствующие типам событий, о которых вы хотите получать уведомления.

7. В столбце **Порог угрозы** укажите количество обнаружений или нарушений, вызывающих отправку уведомления в течение каждого периода времени.

8. Чтобы настроить строку темы и тело сообщения для каждого уведомления о событии, нажмите на ссылку уведомления в столбце **Тип**.

   Более подробную информацию о настройке уведомлений см. в *Символы переменных на странице 10-6*.

9. Нажмите кнопку **Сохранить**.

Символы переменных

Используйте символы переменных, чтобы настроить тему и тело сообщений для уведомлений о событиях.

Чтобы сообщения электронной почты с адресов с внешними доменами не определялись как спам, добавьте внешние адреса электронной почты в списки разрешенных отправителей для программ защиты от спама.

Для представления событий, обнаруженных на серверах и настольных ПК, а также серверах Exchange, используются следующие маркеры.

Маркер	Описание	Тип сигнала опасности
%COUNT	Вставляет количество обнаружений	События предупреждения: Все
$CSM_SERVERNAME	Вставляет имя сервера Security Server	Все
%DATE	Вставляет количество дней, оставшихся до окончания срока действия лицензии	Лицензия – срок действия истек Лицензия – срок действия лицензии истекает менее чем через 60 дней

Маркер	Описание	Тип сигнала опасности
%DATE_TIME	Вставляет время и дату события	Антивирус — неустраненные угрозы Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах Антивирус – сканирование в режиме реального времени отключено на серверах Exchange Антишпионское ПО — обнаружения, требующие перезагрузки устройства Обновление – устаревшие агенты Обновление – устаревшие агенты Messaging Security Agent Обновление – устаревшие компоненты Security Server Службы Smart Protection – служба недоступна Недостаток ресурсов – оставшееся дисковое пространство

Маркер	Описание	Тип сигнала опасности
%DEVICE_COUNT	Вставляет количество затронутых устройств	Антивирус — неустраненные угрозы Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах Антивирус – сканирование в режиме реального времени отключено на серверах Exchange Антишпионское ПО — обнаружения, требующие перезагрузки устройства Обновление – устаревшие агенты Обновление – устаревшие агенты Messaging Security Agent Недостаток ресурсов – оставшееся дисковое пространство Все события предупреждения, за исключением следующих: Защита от спама — количество обнаружений спама во всех полученных сообщениях превышает:
%FROM	Вставляет время и дату начала события	Все события предупреждения, за исключением следующих: Защита от спама — количество обнаружений спама во всех полученных сообщениях превышает:

Маркер	Описание	Тип сигнала опасности
%NUMBER	Указывает количество событий	Антивирус — неустраненные угрозы Антивирус – сканирование в режиме реального времени отключено на локальных компьютерах Антивирус – сканирование в режиме реального времени отключено на серверах Exchange Антишпионское ПО — обнаружения, требующие перезагрузки устройства Все события предупреждения, за исключением следующих: Защита от спама — количество обнаружений спама во всех полученных сообщениях превышает:
%SEAT_IN_USE_COUNT	Вставляет количество используемых установок настольных ПК или серверов	Лицензия: общее количество установок программы превышает 110 % Лицензия: общее количество установок программы превышает 100%

Маркер	Описание	Тип сигнала опасности
%SEAT_PURCHASED_COUNT	Вставляет количество установок настольных ПК или серверов, доступное по лицензии	Лицензия: общее количество установок программы превышает 110 % Лицензия: общее количество установок программы превышает 100%
%THRESHOLD%	Указывает пороговое значение события	Обновление – устаревшие агенты Обновление – устаревшая вирусная база данных Smart Scan Обновление – устаревшие компоненты Security Server Службы Smart Protection – служба недоступна Недостаток ресурсов – оставшееся дисковое пространство Лицензия – количество установок программы превысило 110% Лицензия – количество установок программы превысило 100% События предупреждения: Все

Маркер	Описание	Тип сигнала опасности
%TO	Вставляет время и дату окончания события	Все события предупреждения, за исключением следующих: Защита от спама — количество обнаружений спама во всех полученных сообщениях превышает:

```
Тема: [Security Server - <$CSM_SERVERNAME>] [Требуется
действие] Антивирус. Нерешенные угрозы: %NUMBER
Сообщение: уведомление Trend Micro Worry-Free Business Security
* Антивирус. Нерешенные угрозы: %NUMBER
* Время отчета: %DATE_TIME
* Затронутые устройства: %DEVICE_COUNT
* Совет:
  Выполните сканирование при помощи инструмента Trend Micro HouseCall.
```

```
Тема: [Security Server - A-сервер] [Требуется действие]
Антивирус. Нерешенные угрозы: 5
Сообщение: уведомление Trend Micro Worry-Free Business Security
* Антивирус. Нерешенные угрозы: 5
* Время отчета: 14 февраля 2018 г.
* Совет:
  Выполните сканирование при помощи инструмента Trend Micro HouseCall.
```

Глава 11

Управление глобальными параметрами

В этой главе описываются глобальные параметры агентов и настройки системы для сервера Security Server.

Глобальные параметры

В веб-консоли можно настроить глобальные параметры для сервера Security Server и агентов Security Agent.

Вкладка	Описание
Прокси-сервер	Если для соединения с Интернетом используется прокси-сервер, укажите настройки прокси-сервера для следующих служб: • Обновления компонентов и уведомления о лицензии. • Службы Web Reputation, «Контроль действий» и Smart Scan Подробную информацию см. в разделе *Настройка параметров прокси-сервера сети Интернет на странице 11-3*.
SMTP	Параметры SMTP-сервера применимы ко всем уведомлениям и отчетам, генерируемым сервером Security Server. Подробную информацию см. в разделе *Настройка параметров SMTP-сервера на странице 11-4*.
Настольный ПК или сервер	Настройки безопасности применяются ко всем агентам Security Agent. Подробную информацию см. в разделе *Настройка параметров рабочей станции или сервера на странице 11-5*.
Система	Системные настройки позволяет автоматически удалять неактивных агентов, проверять соединения с агентами и управлять папками карантина. Подробную информацию см. в разделе *Настройка системных параметров на странице 11-11*.

Вкладка	Описание
Исключения	Списки исключений позволяют переопределять параметры политики, определенные службой Web Reputation, контролем действий и прогнозным машинным обучением. Подробную информацию см. в разделе *Настройка параметров списка исключений на странице 11-15*.

Настройка параметров прокси-сервера сети Интернет

Если сервер Security Server и агенты для подключения к Интернету используют прокси-сервер, укажите параметры прокси-сервера для использования следующих служб.

- **Security Server**. Обновления компонентов и обслуживание лицензии.
- **Агенты Security Agent**: служба Web Reputation, контроль действий, Smart Feedback, интеллектуальное сканирование Smart Scan и фильтрация URL-адресов.
- **Агенты Messaging Security Agent** (только Advanced) служба Web Reputation и защита от спама

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. Настройте необходимые параметры на вкладке **Прокси-сервер**
   - Прокси-сервер Security Server

Примечание

Агенты Messaging Security Agent также используют параметры прокси-сервера Security Server.

- Использовать прокси-сервер для обновлений и уведомлений о лицензии
- Использовать прокси-протокол SOCKS 4/5
- Адрес: Адрес IPv4/IPv6 или имя компьютера
- Порт
- Аутентификация на прокси-сервере
  - Имя пользователя
  - Пароль

- Прокси-сервер Security Agent
  - Использовать входные данные для прокси-сервера обновлений

Примечание

Агенты Security Agent используют прокси-сервер и порт Internet Explorer для подключения к Интернету. Выберите эту функцию, только если Internet Explorer на клиентских компьютерах и Security Server имеют одинаковые учетные данные для входа.

  - Имя пользователя
  - Пароль

3. Нажмите кнопку **Сохранить**.

Настройка параметров SMTP-сервера

Параметры SMTP-сервера применимы ко всем уведомлениям и отчетам, генерируемым Worry-Free Business Security.

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. При необходимости настройте параметры на вкладке **SMTP**:
   - **SMTP-сервер**: Укажите IPv4-адрес, IPv6-адрес или имя SMTP-сервера.
   - **Порт**
   - **Включить аутентификацию на сервере SMTP**
     - Имя пользователя
     - Пароль
3. Чтобы убедиться в том, что настройки верны, нажмите **Отправить тестовое сообщение электронной почты**. Если отправка не удалась, измените настройки или проверьте состояние сервера SMTP.
4. Нажмите кнопку **Сохранить**.

Настройка параметров рабочей станции или сервера

Параметры настольного ПК или сервера относятся к глобальным настройкам Worry-Free Business Security. Настройки каждой группы перекрывают эти параметры. Если параметры той или иной группы не настроены, то используются параметры настольного ПК или сервера. Например, если для определенной группы не разрешено ни одного URL-адреса, то к ней применяется список разрешенных URL-адресов, указанный на этом экране.

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. При необходимости настройте параметры на вкладке **Настольный ПК или сервер**:

Настройки	Описание

Чувствительность к местоположению	Благодаря чувствительности к местоположению администратор имеет возможность настраивать параметры безопасности в зависимости от способа подключения клиента к сети.
	
	Чувствительность к местоположение контролирует параметры подключений «В офисе» и «Вне офиса».
	
	Security Agent автоматически определяет местоположение клиента на основании информации с веб-консоли и контролирует веб-сайты, посещаемые пользователями. Ограничения зависят от местоположения пользователя.
	
	• **Включить чувствительность к местоположению**: эти настройки влияют на параметры подключения «В офисе» и «Вне офиса» брандмауэра, работу службы Web Reputation и частоту обновления по расписанию.
	
	• **Информация о шлюзе**: клиенты и подключения из этого списка будут использовать параметры для внутреннего соединения при удаленном подключении к сети (с помощью VPN) и включенной чувствительности к местоположению.
	
	  • IP-адрес шлюза
	
	  • MAC-адрес. Добавление MAC-адреса значительно повышает безопасность, разрешая подключение только настроенному устройству.
	
	Для удаления программы нажмите значок удаления (x).

Настройки	Описание
Уведомление службы поддержки	Уведомление службы поддержки размещается в Security Agent и сообщает пользователю о том, с кем необходимо связаться для получения поддержки. Настройте следующие параметры необходимым образом: • **Метка службы технической поддержки** • **Адрес электронной почты службы технической поддержки** • **Дополнительная информация**. Это окно всплывает при наведении курсора на метку

Настройки	Описание
Общие параметры сканирования	• **Отключить службу Smart Scan** Переводит все агенты Security Agent в обычный режим сканирования. Функция Smart Scan будет недоступна до следующей активации. Для переключения одной или нескольких групп Security Agent перейдите в раздел **Устройства** > **{группа}** > **Политика настройки** > **Метод сканирования**. **Примечание** Инструкции по переключению Security Agent между методами сканирования см. в *Настройка способов сканирования на странице 5-6*. • **Разрешить отложенное сканирование для файловых операций** При включении этого параметра временно повышается производительность системы. **ПРЕДУПРЕЖДЕНИЕ!** Разрешение отложенного сканирования может сделать систему уязвимой для угроз. • **Исключить разделы Shadow Copy**: службы Shadow Copy и «Снимок тома» создают резервные копии или снимки файла или папки на определенном томе в автоматическом или ручном режиме. • **Исключить папку базы данных Security Server:** агенты, установленные на сервере Security Server, не выполняют проверку собственных баз данных при сканировании в режиме реального времени. По умолчанию программа WFBS не сканирует свою собственную базу данных. Компания Trend Micro рекомендует сохранить такой выбор, чтобы предотвратить возможное разрушение базы данных в ходе сканирования. • **Исключить папки сервера Microsoft Exchange, если программа установлена на сервере Microsoft Exchange** Запрещает агентам, установленным на сервере Microsoft Exchange, сканирование папок Microsoft Exchange. • **Исключить папки контроллера домена Microsoft**: агенты, установленные на контроллере домена, не выполняют сканирование папок контроллера домена. В этих папках хранится информация о пользователях, имена пользователей, пароли и другие важные данные.

Настройки	Описание
Параметры антивирусного сканирования	• **Настроить параметры сканирования для крупных сжатых файлов** Укажите максимально допустимый размер файла и количество файлов в сжатом файле, при превышении которых сканирование выполняться не будет. • **Очищать сжатые файлы**: агенты будут пытаться удалять зараженные файлы из сжатого файла. • **Сканировать до {} уровн. OLE**: агенты будут сканировать указанное количество уровней связывания и внедрения объектов (OLE). OLE позволяет пользователям создавать объекты одного применения и связывать их с другим применением или внедрять в другое применение. Например, файл XLS можно внедрить в файл DOC. • **Добавить функцию сканирования вручную в контекстное меню Windows на клиентских компьютерах**: в контекстное меню добавляется ссылка **Сканировать с помощью агента Security Agent**. После этого правый щелчок мышью на файле или папке (на рабочем столе или в проводнике Windows) позволяет запустить сканирование вручную.
Параметры поиска шпионских и нежелательных программ	• **Сканировать на наличие объектов cookie**. Программа Security Agent выполняет сканирование на наличие файлов cookie. • **Включить в журнал шпионского ПО обнаружение объектов cookie** Записывать каждый случай обнаружения объекта cookie в журнал шпионских программ.
Параметры брандмауэра	Установите флажок **Отключить брандмауэр и удалить драйверы**, чтобы удалить клиентский брандмауэр Worry-Free Business Security и связанные с ним драйверы. **Примечание** После отключения брандмауэра связанные с ним настройки будут недоступны, пока он не будет включен повторно.

Настройки	Описание
Защита от веб-угроз HTTPS	Включите эту функцию, чтобы выполнять проверку URL-адресов HTTPS на основе параметров службы Web Reputation и службы фильтрации URL-адресов в Chrome, Firefox и Microsoft Edge. **Примечание** Эта функция не требует дополнительную надстройку браузера. По умолчанию Worry-Free Business Security проверяет URL-адреса HTTPS в Internet Explorer при помощи надстроек браузера.
Параметры сигналов тревоги	**Отображать значок предупреждения на панели задач Windows, если файл вирусной базы данных не обновлялся в течение {} дн.**: на клиентских компьютерах отображается значок предупреждения, если файл базы данных не обновлялся в течение указанного количества дней.
Пароль для удаления Security Agent	• **Разрешить пользователю клиента удалять Security Agent без пароля.** • **Запрашивать у пользователя клиента пароль при попытке удалить Security Agent.**
Пароль для выхода из программы Security Agent и снятия блокировки	• **Разрешить пользователям клиента закрывать и разблокировать Security Agent на своем компьютере без пароля.** • **Запрашивать у пользователей клиента пароль при попытке закрыть и разблокировать Security Agent.** **Примечание** Разблокирование Security Agent позволяет пользователю переопределять все параметры, настроенные в разделе **Устройства** > **{группа}** > **Политика настройки** > **Права агента**.

Настройки	Описание
Предпочтительный IP-адрес	Эта настройка доступна только на Security Server с двойным стеком и применяется только для агентов с двойным стеком. После установки или обновления агентов они регистрируются на сервере Security Server, используя IP-адрес. Выберите один из следующих вариантов: • **вначале IPv4, затем IPv6**: агенты используют сначала свой адрес IPv4. Если агент не может зарегистрироваться с помощью своего адреса IPv4, он использует свой адрес IPv6. Если регистрация не удалась в обоих случаях, агент выполняет повторную попытку, используя приоритетный для данного выбора IP-адрес. • **вначале IPv6, затем IPv4**: агенты используют сначала свой адрес IPv6. Если агент не может зарегистрироваться с помощью своего адреса IPv6, он использует свой адрес IPv4. Если регистрация не удалась в обоих случаях, агент выполняет повторную попытку, используя приоритетный для данного выбора IP-адрес.

3. Нажмите кнопку **Сохранить**.

Настройка системных параметров

Раздел **Система** экрана **Глобальные параметры** содержит параметры автоматического удаления неактивных агентов, проверки соединения с агентами и управления папкой карантина.

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. При необходимости настройте параметры на вкладке **Система**:

Настройки	Описание
Удаление неактивного агента Security Agent	При использовании программы удаления Security Agent на клиенте автоматически отправляется уведомление серверу Security Server. Когда сервер Security Server получает такое уведомление, он удаляет значок клиента из дерева групп безопасности. Это показывает, что клиента больше нет. Однако если агент Security Agent удаляется иным способом, например путем форматирования жесткого диска компьютера или удаления файлов клиента вручную, сервер Security Server не будет уведомлен об удалении, и агент Security Agent будет отображаться как неактивный. Если пользователь произведет выгрузку клиента или отключит агент на длительное время, сервер Security Server также будет отображать Security Agent как неактивный. Чтобы в дереве групп безопасности отображались только активные клиенты, настройте Security Server для автоматического удаления неактивных агентов Security Agent из дерева. • **Разрешить автоматическое удаление неактивных агентов Security Agent**: включается режим автоматического удаления клиентов, которые не установили соединение с сервером Security Server в течение определенного периода времени (в днях). • **Автоматически удалять неактивный Security Agent через {} дней**: Количество дней отсутствия активности клиента до удаления его из веб-консоли.

Настройки	Описание

Проверка соединения агента	Программа Worry-Free Business Security отображает состояние соединения клиента в дереве групп безопасности с помощью значков. Однако в определенных обстоятельствах дерево групп безопасности может перестать правильно отображать состояние соединения агента. Например, если сетевой кабель клиента будет случайно выдернут, агент не сможет уведомить Trend Micro Security Server о переходе в автономное состояние. Это агент будет отображаться в дереве групп безопасности как находящийся в сети.
	
	Проверить подключение «агент-сервер» можно вручную или с помощью проверки в веб-консоли.
	
	Примечание
	Функция «Проверить соединение» не дает возможности выбрать определенные группы или агенты. Она проверяет всех агентов, зарегистрированных на сервере Security Server.
	
	• **Выполнять проверку соединения по расписанию**: включается проверка соединения между агентом и сервером по расписанию.
	  ◦ **Ежечасно**
	  ◦ **Ежедневно**
	  ◦ **Еженедельно, каждые**
	  ◦ **Время начала:** время начала проверки.
	• **Проверить сейчас**: Немедленно протестировать соединение.

Настройки	Описание
Обслуживание карантина	По умолчанию агенты Security Agent отправляют зараженные файлы на карантин в следующую папку на Security Server: `<папка установки Security Server>\PCCSRV\Virus` Если вам нужно изменить папку (например, если на диске недостаточно места), введите полный путь, например, `D:\Quarantined Files`, в поле **Папка карантина**. При изменении папки убедитесь, что такие же изменения произведены в разделе **Устройства** > **{группа}** > **Политика настройки** > **Поместить в карантин**, иначе агенты будут продолжать отправлять файлы в `<папка установки Security Server>\PCCSRV\Virus`. Кроме того, настройте следующие параметры обслуживания: • **Размер папки карантина**. Размер папки карантина в мегабайтах. • **Максимальный размер одного файла**: максимальный размер одного файла, помещенного в папку карантина, в мегабайтах. • **Удалить все помещенные в карантин файлы**: удаляются все файлы из папки карантина. Если папка заполнена и загружается новый файл, то он не будет сохранен. Если вы не хотите, чтобы агенты отправляли помещенные в карантин файлы на сервер Security Server, укажите новую папку в разделе **Устройства** > **{группа}** > **Политика настройки** > **Поместить в карантин** и игнорируйте все параметры обслуживания. Инструкции см. в разделе *Папка карантина на странице 5-20*.

Настройки	Описание
Установка Security Agent	**Папка установки агента Security Agent**: во время установки вам будет предложено указать папку установки Security Agent, в которую будет устанавливаться каждый агент Security Agent. Если необходимо, измените каталог, введя полный путь. В эту папку будут устанавливаться только будущие агенты, существующие агенты сохранят свой текущий каталог. Используйте одну из следующих переменных для указания пути установки: • `$BOOTDISK`: Буквенная метка загрузочного диска • `$WINDIR`: Папка установки Windows • `$ProgramFiles`: папка программ

3. Нажмите кнопку **Сохранить**.

Настройка параметров списка исключений

Процедура

1. Перейдите к **Администрирование** > **Глобальные параметры**.
2. Щелкните вкладку **Исключения** и настройте указанные далее параметры при необходимости.

Раздел	Описание
Служба Web Reputation и фильтрация URL-адресов	• **Список разрешенных URL-адресов**: веб-сайты (и их поддомены), не проверяемые службой Web Reputation и службой фильтрации URL-адресов.

Раздел	Описание
	Примечание Список разрешенных URL-адресов имеет приоритет над списком заблокированных. Если URL-адрес совпадает с записью из списка разрешенных URL-адресов, агенты разрешают доступ к этому URL-адресу, даже если он есть в списке заблокированных URL-адресов. Разрешенные/заблокированные URL-адреса, заданные для конкретной группы, переопределяют глобальные параметры исключений. • **Список заблокированных URL-адресов**: веб-сайты (и их поддомены), которые всегда блокируются службой фильтрации URL-адресов. • **Список исключенных процессов**:Процессы, исключенные из проверок службы Web Reputation и фильтрации URL-адресов. Введите критические процессы, которые ваша компания считает надежными. **Совет** Когда выполняется обновление списка исключенных процессов, а сервер развертывает обновленный список для агентов, все активные соединения HTTP на клиентском компьютере (через порт 80, 81, или 8080) на несколько секунд будут отключены. Выполняйте обновление списка исключенных процессов в период наименьшей рабочей нагрузки. • **Исключаемые IP-адреса**: IP-адреса (например, 192.168.0.1), не проверяемые службой Web Reputation и службой фильтрации URL-адресов. Введите важные IP-адреса, считающиеся доверенными в вашей организации.

Раздел	Описание
	• **Отправьте журналы Web Reputation и URL-фильтрации на сервер безопасности**
Список исключений прогнозного машинного самообучения	Настройте глобальный список исключений файлов прогнозного машинного самообучения, чтобы агенты Security Agent не распознавали эти файлы как вредоносные. Введите значение хэша SHA-1 файла, чтобы исключить файл из области сканирования. При необходимости можно добавить примечание о причине исключения или указать имена файлов, связанные со значением хэша.

3. Нажмите кнопку **Сохранить**.

Глава 12

Использование журналов и отчетов

В этой главе описано использование журналов и отчетов для мониторинга системы и анализа степени защиты.

Журналы

В программе Worry-Free Business Security ведутся всесторонние журналы об инцидентах, связанных с вирусами, вредоносными, шпионскими и нежелательными программами, различных событиях и обновлениях. С помощью этих журналов можно оценивать политики защиты организации, выявлять клиенты, подвергающиеся большему риску заражения, и проверять, успешно ли были установлены обновления.

Примечание

Для просмотра файлов с расширением .CSV можно использовать редакторы электронных таблиц, например, Microsoft Excel.

В программе Worry-Free Business Security ведутся журналы следующих видов.

- Журналы событий веб-консоли
- Журналы настольного ПК или сервера
- Журналы сервера Microsoft Exchange (только Advanced)

Таблица 12-1. Тип журнала и его содержимое

Тип (объект, создавший запись в журнале)	Содержимое (тип журнала, из которого извлекается информация)
События консоли управления	• Сканирование вручную (запускается с веб-консоли) • Обновления (обновления Security Server) • События консоли

Тип (объект, создавший запись в журнале)	Содержимое (тип журнала, из которого извлекается информация)

Настольный ПК или сервер	• Журналы вирусов
	  • Сканирование вручную
	  • Сканирование в режиме реального времени
	  • Сканирование по расписанию
	• Журналы шпионских и нежелательных программ
	  • Сканирование вручную
	  • Сканирование в режиме реального времени
	  • Сканирование по расписанию
	• Журналы предиктивного машинного самообучения
	• Журналы Web Reputation
	• Журналы фильтрации URL-адресов
	• Журналы контроля действий
	• Журналы обновлений
	• Журналы сетевых вирусов
	• Журналы событий
	• Журналы контроля устройств
	• Обновить журналы развертывания
	• Журналы ПО для вымогательства
	  • Антивирусная защита
	  • Контроль действий
	  • Web Reputation
	  • Фильтрация URL-адресов
	  • Прогнозное машинное самообучение

Тип (объект, создавший запись в журнале)	Содержимое (тип журнала, из которого извлекается информация)
Сервер Exchange (только Advanced)	• Журналы вирусов • Журналы блокировки вложений • Журналы фильтрации содержимого / предотвращения потери данных • Журналы обновлений • Журналы резервного копирования • Журналы архивирования • Журналы событий сканирования • Журналы частей сообщений, неподлежащих сканированию • Журналы Web Reputation • Журналы событий мобильных устройств

Запрос журнала

Выполнение запросов журнала для сбора информации из базы данных журнала событий. Для настройки и выполнения запросов используйте окно **«Запрос журнала»**. Результаты можно экспортировать в файл .CSV или распечатывать.

Агент Messaging Security Agent (только Advanced) отправляет журналы на сервер Security Server каждые пять минут (независимо от времени создания журнала).

Процедура

1. Перейдите в **Отчеты** > **Запрос журнала**.
2. При необходимости обновите следующие параметры:

- **Период**
  - **Предустановленный период**
  - **За указанный период**: Ограничение запроса конкретными датами.
- **Тип**: Содержимое журналов всех типов см. в разделе *Журналы на странице 12-2*.
  - **События консоли управления**
  - **Настольный ПК или сервер**
  - **Сервер Exchange** (только Advanced)
- **Содержимое**: Доступные параметры зависят от параметра **Тип** журнала.

3. Нажмите **Просмотр журналов**.
4. Для того чтобы сохранить журнал в виде CSV-файла, нажмите кнопку **Экспорт**. Для просмотра файлов формата CSV используйте редакторы электронных таблиц.

Отчеты

Можно создавать однократные отчеты вручную или настроить сервер Security Server для создания отчетов по расписанию.

Отчеты можно распечатывать или отправлять по электронной почте администратору и другим получателям.

Данные, содержащиеся в отчете, зависят от количества журналов, доступных на Security Server во время создания отчета. Количество журналов изменяется, поскольку новые журналы добавляются, а существующие удаляются. В разделе **Отчеты** > **Обслуживание** вы можете удалить журналы вручную или установить расписание их удаления.

Работа с однократными отчетами

Процедура

1. Перейдите в раздел **Отчеты** > **Однократные отчеты**.
2. Выполните следующие задачи.

Задача	Шаги
Создать отчет	a. Нажмите кнопку **Добавить**. Появится новое окно. b. Укажите следующее: • **Имя отчета** • **Период**: Ограничение отчета определенными датами. • **Содержимое**: Для выбора всех угроз установите флажок **Выбрать все**. Для выбора отдельной угрозы установите соответствующий флажок. Щелкните значок «плюс» (+), чтобы развернуть данный раздел. • **Отправить отчет** • **Получателям**: Введите адреса электронной почты получателей, разделяя их точкой с запятой (;). • **Формат**: Выберите PDF-файл или ссылку на HTML-отчет. При выборе PDF файл PDF будет прикреплен к сообщению электронной почты. c. Нажмите кнопку **Добавить**.

Задача	Шаги
Просмотр отчета	В столбце «Имя отчета» перейдите по ссылкам к отчету. При переходе по первой ссылке открывается отчет в формате PDF, а при переходе по второй — в формате HTML. Данные, содержащиеся в отчете, зависят от количества журналов, доступных на Security Server во время создания отчета. Количество журналов изменяется, поскольку новые журналы добавляются, а существующие удаляются. В разделе **Отчеты** > **Обслуживание** можно удалить журналы вручную или установить расписание удаления журналов. Для получения дополнительных сведений о содержании отчета см. *Анализ отчетов на странице 12-12*.
Удаление отчетов	a. Выберите строку, содержащую ссылки на отчет. b. Нажмите кнопку **Удалить**. **Примечание** Для автоматического удаления отчетов перейдите на вкладку **Отчеты** > **Обслуживание** > **Отчеты** и установите максимальное число отчетов, сохраняемых в Worry-Free Business Security. По умолчанию сохраняется 10 однократных отчетов. При превышении этого числа Security Server удаляет отчеты, начиная с самого давнего.

Работа с запланированными отчетами

Процедура

1. Выберите **Отчеты** > **Запланированные отчеты**.
2. Выполните следующие задачи.

Задача	Шаги
Создание шаблона запланированного отчета	a. Нажмите кнопку **Добавить**. Появится новое окно. b. Укажите следующее: • **Имя шаблона отчета** • **Расписание**: ежедневно, еженедельно или ежемесячно, а также время формирования отчета Если для создания ежемесячных отчетов выбраны числа 31, 30 или 29, а в месяце меньшее количество дней, WFBS не будет создавать отчет в этом месяце. • **Содержимое**: Для выбора всех угроз установите флажок **Выбрать все**. Для выбора отдельной угрозы установите соответствующий флажок. Щелкните значок «плюс» (+), чтобы развернуть данный раздел. • **Отправить отчет** • **Получателям**: Введите адреса электронной почты получателей, разделяя их точкой с запятой (;). • **Формат**: Выберите PDF-файл или ссылку на HTML-отчет. При выборе PDF файл PDF будет прикреплен к сообщению электронной почты. c. Нажмите кнопку **Добавить**.

Задача	Шаги
Просмотр запланированных отчетов	a. В строке, содержащей шаблон, на основе которого создаются запланированные отчеты, нажмите **История отчетов**. Откроется новое окно. b. В столбце «Просмотр» нажмите на ссылки на отчет. При переходе по первой ссылке открывается отчет в формате PDF, а при переходе по второй — в формате HTML. Данные, содержащиеся в отчете, зависят от количества журналов, доступных на Security Server во время создания отчета. Количество журналов изменяется, поскольку новые журналы добавляются, а существующие удаляются. В разделе **Отчеты** > **Обслуживание** можно удалить журналы вручную или установить расписание удаления журналов. Для получения дополнительных сведений о содержании отчета см. *Анализ отчетов на странице 12-12*.
Задачи обслуживания шаблона	
Изменение параметров шаблона	Нажмите на шаблон и затем измените параметры в открывшемся окне. Для отчетов, созданных после сохранения изменений, будут использоваться новые параметры.
Включение/ отключение шаблона	Щелкните по значку под столбцом «Включено». Отключите шаблон, если вы хотите временно остановить создание запланированных отчетов, и включите его снова при необходимости.

Задача	Шаги
Удаление шаблона	Выберите шаблон и нажмите кнопку **Удалить**. Удаление шаблона не удаляет запланированные отчеты, созданные на основе этого шаблона, но ссылки на отчеты больше не будут доступны из веб-консоли. Доступ к отчетам можно получить непосредственно с компьютера, на котором установлен сервер Security Server. Отчеты будут удалены только в том случае, если вы вручную удалите их с компьютера или если Security Server автоматически удаляет отчеты в соответствии с параметрами автоматического удаления запланированных отчетов, заданными на вкладке **Отчеты** > **Обслуживание** > **Отчеты**. Для автоматического удаления шаблонов перейдите на вкладку **Отчеты** > **Обслуживание** > **Отчеты** и установите максимальное число шаблонов, сохраняемое Worry-Free Business Security. По умолчанию сохраняется 10 шаблонов. При превышении этого числа Security Server удаляет шаблоны, начиная с самого давнего.
Задачи обслуживания отчета	

Задача	Шаги
Отправка ссылки на запланированные отчеты	Отправьте ссылку на запланированные отчеты (в формате PDF) по электронной почте. Для доступа к файлу PDF получателям нужно перейти по ссылке в сообщении электронной почты. Убедитесь, что получатели могут подключиться к серверу Security Server, иначе файл не будет отображаться. **Примечание** Электронная почта содержит только ссылку на файл PDF. Сам файл PDF не прикрепляется к сообщению. a. В строке, содержащей шаблон, на основе которого создаются запланированные отчеты, нажмите **История отчетов**. Откроется новое окно. b. Выберите отчеты и нажмите кнопку **Отправить**. В вашем клиенте электронной почты по умолчанию откроется новое сообщение со ссылкой на отчет.
Удаление запланированных отчетов	a. В строке, содержащей шаблон, на основе которого создаются запланированные отчеты, нажмите **История отчетов**. Откроется новое окно. b. Выберите отчеты и нажмите кнопку **Удалить**. **Примечание** Для автоматического удаления отчетов перейдите на вкладку **Отчеты** > **Обслуживание** > **Отчеты** и установите максимальное число запланированных отчетов для каждого шаблона, сохраняемое Worry-Free Business Security. По умолчанию сохраняется 10 запланированных отчетов. При превышении этого числа Security Server удаляет отчеты, начиная с самого давнего.

Анализ отчетов

Отчеты Worry-Free Business Security включают следующую информацию: Отображаемая информация может меняться в зависимости от установленных параметров.

Таблица 12-2. Содержание отчета

Пункт	Описание
Антивирусная защита	**Сводная информация о вирусах для настольных ПК и серверов** В отчетах о вирусах содержится подробная информация о количестве и типах обнаруженных вирусов и вредоносного ПО и о принятых мерах безопасности, а также список наиболее часто обнаруживаемых вирусов и вредоносного ПО. Щелкните имя вируса/вредоносного программы для открытия новой страницы веб-браузера и перехода в энциклопедию вирусов Trend Micro, где можно получить дополнительную информацию об этом вирусе или вредоносном ПО.
	5 первых зараженных настольных ПК и серверов Приводится список из 5 компьютеров или серверов с наибольшим количеством сообщений об обнаружении вирусов или вредоносного ПО. Частые заражения вирусами или вредоносным ПО одного и того же клиента могут свидетельствовать о том, что компьютер представляет собой серьезную угрозу безопасности, и это требует тщательного исследования.

Пункт	Описание
Антишпионское ПО	**Сводная информация о шпионских и нежелательных программах, обнаруженных на настольных ПК и серверах** В отчетах о шпионских и нежелательных программах содержится подробная информация об обнаруженных шпионских и нежелательных программах на клиентах, в том числе количество случаев обнаружения и действия, выполненные программой WFBS. Отчет включает также круговую диаграмму, отображающую процентное соотношение всех проведенных мероприятий по антишпионскому ПО.
	5 первых настольных ПК и серверов с обнаруженными шпионскими и нежелательными программами В отчете приводится также список из 5 наиболее часто встречающихся шпионских программ и Grayware и 5 компьютеров или серверов с наибольшим количеством обнаруженных шпионских и нежелательных программ. Подробные сведения о каждой шпионской и нежелательной программе можно получить, щелкнув по имени программы. Откроется новая страница веб-браузера с информацией о соответствующих шпионских и нежелательных программах с веб-сайта компании Trend Micro.
Сводная информация о защите от спама (только Advanced)	**Сводная информация о нежелательной почте** В отчетах приводится информация о количестве спама и фишинг-почты, обнаруженном при сканировании почтовых сообщений, а также список отмеченных ложных тревог.
Прогнозное машинное самообучение	**Топ-5 программ, нарушающих политики прогнозного машинного самообучения**
	Топ-10 компьютеров, нарушающих политики прогнозного машинного самообучения
Web Reputation	**10 компьютеров, первых по частоте нарушения политик служб Web Reputation**

Пункт	Описание
Категория URL-адреса	**5 категорий URL, наиболее часто нарушающих политики** Список наиболее часто посещаемых категорий веб-сайтов, нарушающих политику.
	10 компьютеров, первых по частоте нарушения политик категорий URL
Контроль действий	**Первые 5 программ по нарушению политик контроля действий**
	Первые 10 компьютеров по нарушению политик контроля действий
Контроль устройств	**Первые 10 компьютеров по нарушению политик контроля устройств**
Сводная информация о фильтрации содержимого (только Advanced)	**Сводная информация о фильтрации содержимого** В отчетах приводится информация об общем количестве сообщений, отфильтрованных программой Messaging Security Agent.
	10 наиболее часто нарушаемых правил фильтрации содержимого Список из 10 наиболее часто нарушаемых правил фильтрации. Настройте правила фильтрации с учетом этой информации.
Сетевые вирусы	**10 наиболее часто обнаруживаемых сетевых вирусов** Список из 10 сетевых вирусов, наиболее часто обнаруживаемых общим драйвером брандмауэра. Щелкните имя вируса для открытия новой страницы в веб-браузере и перехода в энциклопедию вирусов Trend Micro, где можно получить дополнительную информацию об этом вирусе.
	10 наиболее часто подвергающихся атаке компьютеров Список компьютеров в сети, наиболее часто сообщающих о заражении.

Выполнение задач обслуживания для отчетов и журналов

Процедура

1. Выберите **Отчеты** > **Обслуживание**.
2. Выполните следующие задачи.

Задача	Шаги
Укажите максимальное количество хранимых отчетов и шаблонов.	Вы можете ограничить количество однократных отчетов, запланированных отчетов (для шаблона) и шаблонов, доступных на Security Server. При превышении этого числа Security Server удаляет отчеты и шаблоны, начиная с самого давнего. a. Откройте вкладку **Отчеты**. b. Введите максимальное количество хранимых однократных отчетов, запланированных отчетов и шаблонов.
Настройка автоматического удаления журналов	a. Откройте вкладку **Автоматическое удаление журналов**. b. Выберите типы журналов и укажите максимальный «возраст» журналов. Журналы старше этого значения будут удалены.
Удаление журналов вручную	a. Откройте вкладку **Удаление журналов вручную**. b. Для каждого типа журнала введите максимальный «возраст» журналов. Журналы старше этого значения будут удалены. Для удаления всех журналов введите `0`. c. Нажмите кнопку **Удалить**.

3. Нажмите кнопку **Сохранить**.

Глава 13

Выполнение административных задач

В этой главе описывается выполнение административных задач, например просмотр лицензии продукта, работа с Plug-in Manager и удаление сервера Security Server.

Изменение пароля веб-консоли

Компания Trend Micro рекомендует использовать для веб-консоли надежные пароли. Надежный пароль содержит не менее восьми символов, одну или несколько прописных букв (от A до Z), одну или несколько строчных букв (от a до z), одну или несколько цифр (от 0 до 9), а также специальные символы и знаки препинания (!@#$%^&,.:;?). В качестве стойкого пароля нельзя использовать имя пользователя или включать имя пользователя в пароль. Кроме того, он не должен состоять из имени или фамилии пользователя, даты его рождения или других данных, легко идентифицирующих пользователя.

Процедура

1. Перейдите к **Администрирование** > **Пароль**.
2. При необходимости обновите следующие параметры:
   - **Старый пароль**
   - **Новый пароль**
   - **Подтверждение пароля**: Для подтверждения повторно введите новый пароль.
3. Нажмите кнопку **Сохранить**.

Работа с Plug-in Manager

Plug-in Manager по мере доступности отображает в веб-консоли программы для сервера Security Server и агентов. После этого можно устанавливать программы и управлять ими в веб-консоли, в том числе устанавливать подключаемые модули клиентов на агентах. Загрузите и установите Plug-in Manager в **Администрирование** > **Подключаемые модули**. После установки можно проверить наличие доступных

подключаемых программ. Дополнительные сведения см. в документации для Plug-in Manager и подключаемых модулей.

Управление лицензией продукта

В окне лицензии на продукт можно продлить или обновить лицензию, а также просмотреть подробную информацию о лицензии.

Экран «Лицензия на продукт» содержит информацию о лицензии. В зависимости от настроек, выбранных при установке, у вас может быть полностью лицензионная или демонстрационная версия. В любом случае ваша лицензия дает вам право на соглашение об обслуживании. После истечения срока действия соглашения об обслуживании защита клиентов в сети станет ограниченной. Не забывайте просматривать окно «Лицензия на продукт» и своевременно продлевать лицензию.

Примечание

Компоненты продуктов компании Trend Micro в зависимости от региона могут иметь различные лицензии. Сводная информация о компонентах, которые разрешено использовать в соответствии с существующим ключом регистрации и кодом активации, будет выведена после установки. Для проверки лицензии на компоненты свяжитесь с поставщиком или продавцом.

Продление лицензии

Продлить срок действия лицензии Worry-Free Business Security или выполнить обновление до полностью лицензированной версии можно, оплатив продление лицензии. для полной версии требуется код активации.

Продление лицензии продукта возможно двумя способами:

- В веб-консоли откройте окно текущего статуса и следуйте инструкциям на экране. Эти инструкции появляются в течение 60 дней до и 30 дней после истечения срока действия лицензии.

- Для продления лицензионного соглашения свяжитесь с торговым представителем или распространителем компании Trend Micro.

  Торговые представители могут оставить свои контактные данные в файле на сервере Security Server. Просмотрите файл в:

  ```
  {папка установки Security Server}\PCCSRV\Private
  \contact_info.ini
  ```

  Примечание

  `{Папка установки сервера Security Server}` — это обычно папка `C:\Program Files\Trend Micro\Security Server`.

  Представитель Trend Micro обновит вашу регистрационную информацию с помощью специальных инструментов регистрации продуктов Trend Micro.

  Сервер Security Server запрашивает сервер регистрации и получает новую дату истечения срока действия регистрации непосредственно от него. При продлении лицензии не требуется вводить новый код активации вручную.

Активация новой лицензии

Код активации Worry-Free Business Security зависит от типа лицензии.

Таблица 13-1. Код активации в зависимости от типа лицензии

Тип лицензии	Код активации
Полностью лицензионная версия Worry-Free Business Security Standard	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Полностью лицензионная версия Worry-Free Business Security Advanced	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

Примечание

При появлениив опросов о коде активации обращайтесь на веб-сайт службы технической поддержки компании Trend Micro по адресу:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Чтобы изменить тип лицензии, введя новый код активации, воспользуйтесь окном лицензии на продукт.

1. Откройте **Администрирование** > **Лицензия на продукт**.
2. Выберите команду **Введите новый код**.
3. Введите новый код активации в поле.
4. Нажмите кнопку **Активировать**.

Настройка параметров обновления продукта

Настройте Worry-Free Business Security, чтобы выполнять обновление продукта автоматически.

Процедура

1. Выберите пункт **Администрирование** > **Обновление продукта**.

   Откроется вкладка **Параметры**.

2. В разделе **Параметры обновления** выберите пункт **Включить загрузку обновлений продукта**.

3. Укажите действие, которое следует выполнять после выпуска нового пакета обновления.

   - **Загрузить**: автоматическая загрузка пакета обновления в папку загрузок согласно настроенному расписанию.
   - **Загрузить и установить**: автоматическая загрузка и установка пакета обновления согласно настроенному расписанию.

4. Укажите, когда следует выполнять действие.

Примечание

Для процедуры установки может потребоваться некоторое время. После ее завершения перезапустите Security Server. Выберите время, когда установка пакета обновления создаст наименьшие неудобства.

5. Нажмите кнопку **Сохранить**.

Настройка уведомлений об обновлениях продукта

Worry-Free Business Security может сообщать пользователям об обновлениях продукта, когда доступна новая версия, пакет обновления или исправление. Можно задать уведомления об обновлениях продукта, имеющие следующие типы.

- Security Agent. Уведомление показывается возле области уведомлений на локальном компьютере
- Электронная почта

Процедура

1. Выберите пункт **Администрирование** > **Обновление продукта**.
2. Нажмите кнопку **Уведомления**.
3. Чтобы получать уведомления от Security Agent, настройте параметры в разделе **Security Agent: уведомление**.
   a. Нажмите кнопку **Добавить**.
   b. Выберите из списка агенты Security Agent.
   c. Нажмите кнопку **Сохранить**.

4. Чтобы получать уведомления об обновлениях продукта по электронной почте, укажите получателей в разделе **Уведомление по электронной почте**.

Примечание

Для получения уведомлений по электронной почте необходимо настроить вкладку **SMTP** в разделе **Администрирование** > **Глобальные параметры**.

5. Нажмите кнопку **Сохранить**.

Участие в программе обратной связи Smart Feedback Program

Для получения дополнительных сведений о программе Smart Feedback см. *Smart Feedback на странице 1-6*.

Процедура

1. Перейдите к **Администрирование** > **Smart Protection Network**.
2. Нажмите **Подключить модуль Trend Micro Smart Feedback**.
3. Для отправки информации о потенциальных угрозах безопасности в файлах на клиентских компьютерах установите флажок **Включить отзыв о подозрительных программных файлах**.

Примечание

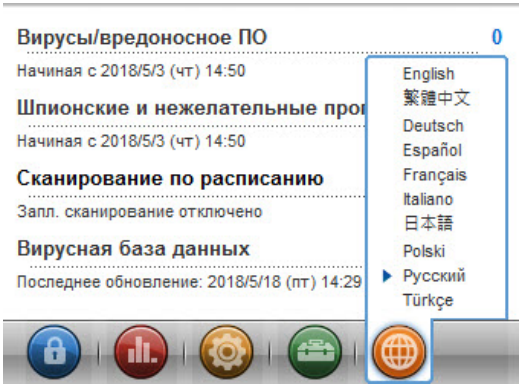
Отправляемые файлы не содержат пользовательских данных и отправляются только для анализа угроз.

4. Чтобы компания Trend Micro могла получить представление о вашей компании, выберите тип **отрасли**.

5. Нажмите кнопку **Сохранить**.

Изменение языка интерфейса агента

По умолчанию язык интерфейса агента будет соответствовать региональным настройкам ОС клиентской системы. Пользователи могут изменить язык через интерфейс агента.



Сохранение и восстановление параметров программы

Можно сделать копию базы данных Security Server и важных файлов конфигурации для выполнения отката Security Server. Если у вас возникли проблемы и вы хотите переустановить сервер Security Server или вернуться к предыдущей конфигурации, сделайте копию.

Процедура

1. Остановите основную службу Trend Micro Security Server Master Service.

2. Вручную скопируйте следующие файлы и папки в другое место.

ПРЕДУПРЕЖДЕНИЕ!

Не используйте при выполнении этой задачи программы резервного копирования.

`<путь установки Security Server>\PCCSRV`

- `ofcscan.ini`: Содержит глобальные параметры.
- `ous.ini`: Содержит таблицу источника обновления для разворачивания антивирусных компонентов.
- Папка `Private`: Содержит параметры брандмауэра и источника обновлений.
- `Pccnt\Common\OfcPfw.dat`: Содержит параметры брандмауэра.
- `Download\OfcPfw.dat`: Содержит параметры установки брандмауэра.
- Папка `Log`: Содержит системные события и журнал проверки соединения.
- Папка `Virus`: папка карантина WFBS для зараженных файлов.
- Папка `HTTDB`: содержит базу данных WFBS.

3. Удаление сервера Security Server. См. *Удаление сервера Security Server на странице 13-10*.
4. Выполните установку с нуля. См. *Руководство по установке и обновлению* Worry-Free Business Security.
5. После окончания работы основной программы установки остановите Trend Micro Security Server Master Service на конечном компьютере.
6. Обновите версию вирусной базы данных из резервной копии:
   a. Получите текущую версию вирусной базы данных с нового сервера.

```
<путь установки Security Server>\PCCSRV\Private
\component.ini. [6101]

ComponentName=Virus pattern

Version=xxxxxx 0 0
```

b. Обновите версию вирусной базы в резервной копии файла.

```
\Private\component.ini
```

Примечание

Если вы изменяете путь для установки сервера Security Server, укажите новый путь в файлах резервных копий `ofcscan.ini` и `\private\ofcserver.ini`.

7. Замените базу данных Worry-Free Business Security и соответствующие файлы в папке `PCCSRV` на целевом компьютере созданными ранее резервными копиями.

8. Перезапустите основную службу Trend Micro Security Server Master Service.

Удаление сервера Security Server

Удаление сервера Security Server влечет за собой удаление сервера Scan Server.

Worry-Free Business Security использует программу удаления для безопасного удаления сервера Trend Micro Security Server с компьютера. Перед удалением сервера Security Server удалите агент на всех клиентах.

Удаление Trend Micro Security Server не приводит к удалению агентов. Перед удалением сервера Trend Micro Security Server администраторы должны удалить или переместить все агенты на другой Security Server. См. *Удаление агентов на странице 3-41*.

Процедура

1. На компьютере, на котором установлен сервер, выберите **Пуск** > **Панель управления** > **Установка и удаление программ**.
2. Выберите **Trend Micro Security Server** и нажмите кнопку **Изменить/Удалить**.

   Появится окно подтверждения.
3. Нажмите кнопку **Далее**.

   Программа удаления главного модуля (программа удаления сервера) запросит пароль администратора.
4. Введите в текстовое поле пароль администратора и нажмите **OK**.

   Мастер удаления приступит к удалению файлов сервера. После удаления сервера Security Server появится сообщение с подтверждением.
5. Для завершения работы программы удаления нажмите кнопку **OK**.

Глава 14

Использование инструментов управления

В этой главе описано использование инструментов администратора, средств клиента и дополнений.

Типы инструментов

В программу Worry-Free Business Security включен набор инструментов, помогающий выполнять различные задачи, включая конфигурацию сервера и управление клиентом.

Примечание

Административные и клиентских инструменты не могут быть запущены из веб-консоли. Дополнения можно загрузить с веб-консоли.

Инструкции по использованию этих инструментов приведены в соответствующих разделах ниже.

Эти инструменты подразделяются на три категории:

- **Административные инструменты**
  - **Настройка сценария входа в сеть** (`SetupUsr.exe`): Автоматизирует установку Security Agent. См. *Установка с использованием программы настройки сценариев входа на странице 3-12*.
  - **Сканер уязвимостей** (`TMVS.exe`): Обнаружение незащищенных компьютеров в сети. См. *Установка с использованием сканера уязвимостей на странице 3-22*.
  - **Агент Remote Manager Agent**: Позволяет продавцам управлять программой Worry-Free Business Security через централизованную веб-консоль. См. *Установка агента Trend Micro Remote Manager (для пользователей портала Customer Licensing Portal) на странице 14-4*.
  - **Утилита Trend Micro Disk Cleaner**: Удаляет ненужные резервные файлы Worry-Free Business Security, файлы журналов и неиспользуемые файлы баз данных. См. *Сохранение дискового пространства на странице 14-15*.
  - **Scan Server Database Mover**: безопасно переносит базу данных Scan Server на другой диск. См. *Перенос базы данных сервера Scan Server на странице 14-18*.

- **Клиентские инструменты**
  - **Упаковщик клиента** (`ClnPack.exe`): Создает самораспаковывающийся файл, содержащий агент Security Agent и компоненты. См. *Установка с использованием Client Packager на странице 3-15*.
  - **Восстановление зашифрованных вирусов и шпионских программ** (`VSEncode.exe`): Открывает зараженные файлы, зашифрованные программой Worry-Free Business Security. См. *Восстановление зашифрованных файлов на странице 14-19*.
  - **Инструмент переназначения клиентов** (`IpXfer.exe`): Переводит агентов с одного сервера Security Server на другой. См. *Перемещение агентов на странице 4-12*.
  - **Повторное создание идентификатора клиента Security Agent** (`WFBS_WIN_All_ReGenID.exe`): Используйте программу ReGenID для повторного создания идентификатора клиента Security Agent с учетом того, является ли агент клонированным компьютером или виртуальной машиной. См. *Использование инструмента ReGenID на странице 14-24*.
- **Дополнения**: позволяют администраторам просматривать динамические сведения о компонентах безопасности и системе в консолях поддерживаемых операционных систем Windows. Это та же информация высокого уровня, которая отображается на экране «Текущее состояние». См. *Управление дополнениями SBS и EBS на странице 14-25*.

Примечание

Некоторые инструменты, доступные в предыдущих версиях программы Worry-Free Business Security, недоступны в этой версии. Для получения этих инструментов обратитесь в службу технической поддержки Trend Micro.

Агент Trend Micro Remote Manager

Агент Trend Micro Remote Manager позволяет дилерам и партнерам управлять продуктом Worry-Free Business Security с помощью консоли Trend Micro Remote Manager. Агент Remote Manager можно установить на сервере Security Server после завершения установки этого сервера или позже.

Требования для установки:

- GUID (глобальный уникальный идентификатор) агента Remote Manager
- Активное подключение к сети Интернет
- 50 МБ свободного пространства на диске

Следуйте процедурам, описанным в одном из следующих разделов:

- *Установка агента Trend Micro Remote Manager (для пользователей портала Customer Licensing Portal) на странице 14-4*
- *Установка агента Trend Micro Remote Manager (для пользователей Licensing Management Platform) на странице 14-6*

Установка агента Trend Micro Remote Manager (для пользователей портала Customer Licensing Portal)

Процедура

1. Получите GUID агента Remote Manager.
   a. На веб-консоли Remote Manager откройте раздел **Клиенты**.
   b. В столбце **Компания** выберите клиента.
   c. На вкладке **Продукты** выберите продукт Worry-Free Business Security.

d. Скопируйте GUID.

2. Перейдите к следующей установочной папке сервера Security Server:`PCCSRV\Admin\Utility\RmAgent` и запустите приложение `TMRMAgentforWFBS.exe`.

   Например: `C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Примечание

   Пропустите этот шаг, если вы запускаете установку из окна настройки Security Server.

3. Прочитайте лицензионное соглашение в мастере установки Trend Micro Remote Manager Agent. Если вы согласны с условиями, выберите вариант **Я принимаю условия лицензионного соглашения** и затем нажмите **Далее**.

4. Нажмите **Да**, чтобы подтвердить, что вы являетесь сертифицированным партнером.

5. Выберите пункт **У меня уже есть учетная запись Trend Micro Remote Manager, и я хочу установить агент**, затем нажмите кнопку **Далее**.

6. Определите свой сценарий.

Сценарий	Шаги
Новый пользователь	a. Выберите параметр **Связать с новым пользователем**. b. Нажмите кнопку **Далее**. Введите информацию пользователя. **Примечание** Если данный пользователь уже имеется в консоли TMRM и выбран параметр «Связать с новым пользователем», в дереве сети TMRM появятся два пользователя с одинаковым именем. Чтобы этого избежать, используйте приведенный ниже метод.

Сценарий	Шаги
Существующий пользователь	a. Выберите **Данный продукт уже есть в Remote Manager**. **Примечание** Служба WFBS уже должна быть добавлена в консоль TMRM. Инструкции см. в документации TMRM. b. Введите GUID.

7. Нажмите кнопку **Далее**.
8. Выберите **регион** и **протокол** и при необходимости введите информацию о прокси-сервере.
9. Нажмите кнопку **Далее**.

   Откроется окно «Путь установки».
10. Нажмите кнопку **«Далее»**, чтобы использовать папку установки по умолчанию.
11. Нажмите кнопку **Готово**.

    При успешном завершении установки и правильных настройках агент Remote Manager автоматически зарегистрируется на сервере Trend Micro Remote Manager. Агент Remote Manager должен отображаться на веб-консоли Remote Manager с обозначением «В сети».

Установка агента Trend Micro Remote Manager (для пользователей Licensing Management Platform)

Процедура

1. Получите код активации Worry-Free Business Security.
   a. На веб-консоли Remote Manager откройте раздел **Клиенты**.

b. В столбце **Компания** выберите клиента.

c. На вкладке **Продукты** выберите продукт Worry-Free Business Security.

d. Скопируйте код активации.

2. Обновите информацию о лицензии на Worry-Free Business Security.

   a. На веб-консоли Worry-Free Business Security откройте **Администрирование** > **Лицензия на продукт**.

   b. В разделе **Информация о лицензии** выберите пункт **Введите новый код**.

   c. Вставьте код активации в поле **Новый код активации**.

   d. Нажмите кнопку **Активировать**.

   e. Выберите пункт **Обновить информацию о лицензии**.

3. Перейдите к следующей установочной папке сервера Security Server:`PCCSRV\Admin\Utility\RmAgent` и запустите приложение `TMRMAgentforWFBS.exe`.

   Например: `C:\Program Files\Trend Micro\Security Server \PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Примечание

   Пропустите этот шаг, если вы запускаете установку из окна настройки Security Server.

4. Выберите пункт **У меня уже есть учетная запись Trend Micro Remote Manager, и я хочу установить агент**, затем нажмите кнопку **Далее**.

5. Выберите пункт **Связать с существующей лицензией на Licensing Management Platform**, затем нажмите кнопку **Далее**.

6. Укажите данные учетной записи Remote Manager и нажмите кнопку **Далее**.

7. Если необходимо, укажите сведения о прокси-сервере и нажмите кнопку **Далее**.

8. Если необходимо, укажите папку установки и нажмите кнопку **Далее**.

9. Нажмите кнопку **Готово**.

   При успешном завершении установки и правильных настройках агент Remote Manager автоматически зарегистрируется на сервере Trend Micro Remote Manager. Агент Remote Manager должен отображаться на веб-консоли Remote Manager с обозначением «В сети».

Управление агентами на управляемом сервере

В этом разделе описаны способы управления агентами на управляемом сервере.

Сообщения о состоянии агента

На управляемом сервере для агента отображается один из указанных далее значков на панели задач.

Таблица 14-1. Значки на панели задач

Значок	Описание
	Зеленый значок означает, что агент подключен к серверу связи Remote Manager. Агент работает в обычном режиме.
	Красный значок означает, что агент не подключен к серверу связи Remote Manager или что версия агента несовместима с сервером и должна быть обновлена.
	Значок с красной стрелкой означает, что агент завершил сеанс связи с Remote Manager.
	Значок с красным символом «X» означает, что агент выключен.

Изменение GUID агента на управляемом сервере

Если во время установки агента Remote Manager вы ввели неправильный GUID (глобальный уникальный идентификатор), удалите агент и снова установите его, указав правильный GUID. Если нет возможности выполнить эту процедуру, попробуйте сделать следующее.

Процедура

1. Откройте папку `C:\Program Files\Trend Micro \TMRMAgentForWFBS`.
2. Откройте файл `AgentSysConfig.xml` с помощью текстового редактора.
3. Найдите GUID, расположенный между параметрами `<AgentGUID>` и `</AgentGUID>`.
4. Измените GUID и сохраните файл.
5. В той же папке откройте файл `csmSysConfig.xml` с помощью текстового редактора.
6. Найдите GUID, расположенный между параметрами `<ProductGUID>` и `</ProductGUID>`.
7. Измените GUID и сохраните файл.
8. Щелкните правой кнопкой мыши значок агента Remote Manager на панели задач, затем выберите пункт **Перезапустить службу**.

Использование средства настройки агента

С помощью средства настройки агента можно изменять параметры конфигурации агента Remote Manager.

Выберите пункты **Пуск** > **Программы** > **Агент Trend Micro Remote Manager** > **Средство настройки агента** или щелкните правой кнопкой мыши значок на панели задач и выберите пункт **Настройка**.

Дополнительные сведения см. в разделе *Настройка агента на странице 14-10*.

Настройка агента

Меню настройки агента

Чтобы настроить агент, щелкните правой кнопкой мыши значок на панели задач. Откроется описанное ниже меню.

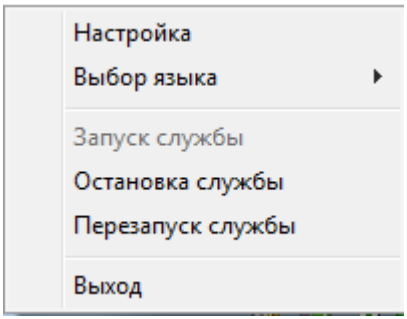


Иллюстрация 14-1. Всплывающее меню средства настройки агента

В меню доступны следующие пункты.

- **Настройка**: открывается окно настройки агента
- **Выбор языка**: вариант «Английский» присутствует всегда; также могут быть доступны другие языки.
- **Служба**: запуск, остановка, перезапуск
- **Выход**: при выходе из средства настройки служба Remote Manager не прекращает работу. Закрывается только средство настройки (и удаляется значок с панели задач). Средство можно снова запустить в любое время.

Главное диалоговое окно средства настройки

Щелкните правой кнопкой мыши значок на панели задач, затем выберите пункт **Настройка** в меню настройки агента. Откроется вкладка **Общие** средства настройки агента.

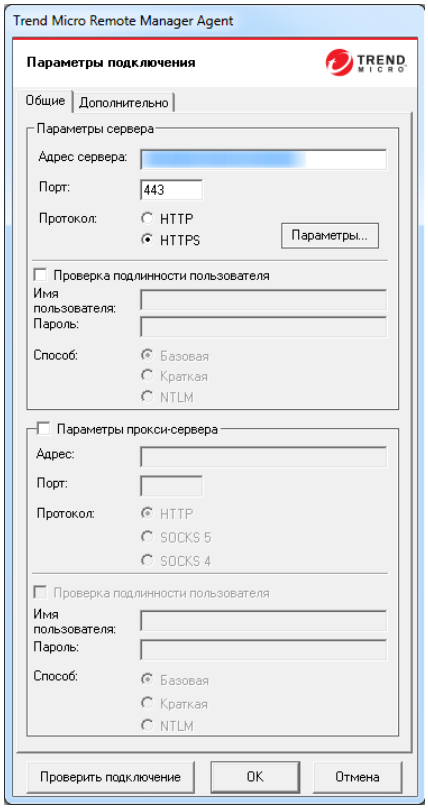


Иллюстрация 14-2. Вкладка «Общие» средства настройки агента

В окне настройки агента вам пока понадобятся только указанные далее разделы средства настройки.

- **Параметры сервера**: настройте связь с сервером, задав значения для следующих параметров.

- **Адрес сервера**: полное доменное имя (FQDN) сервера связи Remote Manager. Значение FQDN зависит от региона. Если вам необходимо изменить адрес сервера, обратитесь к специалисту службы поддержки.
- **Порт**: порт, который использует сервер Remote Manager для связи с агентом. Должно быть указано значение 80 для HTTP и 443 для HTTPS.
- **Протокол**: протокол, используемый для связи между сервером и агентом.

Важно

Компания Trend Micro не рекомендует изменять значения в полях **Адрес сервера** и **Порт**, если этого не требует ваш поставщик услуг технической поддержки.

- **Параметры прокси-сервера**: установите флажок **Параметры прокси-сервера**, чтобы активировать эту область, если сеть пользователя требует наличия прокси-сервера для связи с сервером Remote Manager.
  - **Адрес**: IP-адрес прокси-сервера.
  - **Порт**: порт прокси-сервера.
  - **Протокол**
- **Кнопка «Проверить подключение»**: кнопка **Проверить подключение** используется для проверки связи между агентом и сервером Remote Manager. Эта функция позволяет проверить, правильно ли работает основное соединение с сервером связи. Если оно не работает (когда средство настройки не может подключиться к серверу, появляется диалоговое окно), проблема может быть прежде всего связана с адресом или портом сервера связи либо с адресом или портом прокси-сервера.

Резервное копирование и восстановление параметров агента

Если вам необходимо удалить и снова установить агент с тем же идентификатором GUID в течение трех дней, сохраните параметры агента, чтобы избежать несогласованности в данных. Для этого выполните вручную резервное копирование файлов конфигурации, а после повторной установки агента замените файлы конфигурации резервными копиями.

Резервное копирование параметров

Процедура

1. На управляемом сервере щелкните правой кнопкой мыши значок агента на панели задач, затем выберите пункт **Остановка службы**, чтобы остановить службу агента.
2. Скопируйте все файлы с расширением `.xml`, `.dat` и `.ini` в папке установки `C:\Program Files\Trend Micro\TMRMAgentForWFBS` или `C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS`.
   - Файлы `.xml`
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - Файлы `.dat`

- MSA.dat
- logBuf.dat
- group.dat
- CSA.dat
- CriticalVA.dat

- Файлы .ini
  - csmStatusData.ini

3. Скопируйте все файлы в папке \Cache
4. Снова запустите службу агента.

Восстановление параметров

Процедура

1. Удалите агент локально.

   Примечание

   При локальном удалении агента отменяется его регистрация на сервере Remote Manager, в результате чего автоматически удаляются все данные, связанные с агентом. Чтобы сохранить регистрацию агента, перед его удалением измените адрес сервера в интерфейсе агента.

2. Установите агент заново. Используйте тот же GUID (его можно найти в файле agentSysConfig.xml).
3. На управляемом сервере щелкните правой кнопкой мыши значок агента на панели задач, затем выберите пункт **Остановка службы**, чтобы остановить службу агента.
4. Замените файлы конфигурации резервными копиями.

5. Щелкните правой кнопкой мыши значок агента на панели задач, затем выберите пункт **Запуск службы**, чтобы заново запустить службу агента.

Сохранение дискового пространства

Экономьте дисковое пространство на сервере Security Server и клиентских компьютерах с помощью средства очистки диска.

Запуск средства очистки на Security Server

Перед выполнением

Для экономии места на диске средство очистки дисков (`TMDiskCleaner.exe`) определяет и удаляет неиспользуемые файлы резервных копий, журналов и баз данных из следующих каталогов:

- `{Security Agent}\AU_Data\AU_Temp\*`
- `{Security Agent}\Reserve`
- `{Security Server}\PCCSRV\TEMP\*` (кроме скрытых файлов)
- `{Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\wss\*.log`
- `{Security Server}\PCCSRV\wss\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\Backup\*`
- `{Security Server}\PCCSRV\Virus\*` (удаление файлов, находящихся на карантине более двух недель, за исключением файла NOTVIRUS)
- `{Security Server}\PCCSRV\ssaptpn.xxx` (сохранение только последней версии базы данных)

- {Security Server}\PCCSRV\lpt$vpn.xxx (сохранение только трех последних версий базы данных)
- {Security Server}\PCCSRV\icrc$oth.xxx (сохранение только трех последних версий базы данных)
- {Security Server}\DBBackup* (сохранение только двух последних вложенных папок)
- {Messaging Security Agent}\AU_Data\AU_Temp*
- {Messaging Security Agent}\Debug*
- {Messaging Security Agent}\engine\vsapi\latest\pattern*

Процедура

1. На сервере Security Server перейдите к следующему каталогу:

   {Папка установка сервера}\PCCSRV\Admin\Utility\

2. Дважды щелкните файл **TMDiskCleaner.exe**.

   Откроется средство очистки диска Trend Micro Worry-Free Business Security.

   Примечание

   Файлы не могут быть восстановлены.

3. Нажмите **Удалить файлы**, чтобы просканировать и удалить неиспользуемые файлы резервных копий, журналов и баз данных.

Запуск средства очистки диска на Security Server с помощью интерфейса командной строки

Процедура

1. Откройте окно командной строки на сервере Security Server.

2. В окне командной строки введите следующую команду:

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide`: Выполнение средства в виде фонового процесса.
   - `/log`: Сохранение журнала операции в файле DiskClean.log в текущей папке.

     Примечание

     Параметр `/log` доступен только в том случае, если используется параметр `/hide`.

   - `/allowundo`: Перемещение файлов в корзину без необратимого удаления.

3. Для частого выполнения средства очистки настройте новую задачу в планировщике Windows. Для получения дополнительной информации см. документацию к Windows.

Сохранение дискового пространства на клиентских компьютерах

Процедура

- На рабочих станциях или серверах с установленными агентами Security Agent:
  - Удаляйте файлы, находящиеся на карантине.
  - Удаляйте журналы.
  - Запускайте инструмент Windows для очистки диска.
- На серверах Microsoft Exchange с установленными агентами Messaging Security Agent:
  - Удаляйте файлы, находящиеся на карантине.

- Удаляйте журналы.
- Запускайте инструмент Windows для очистки диска.
- Удаляйте архивные журналы.
- Удаляйте файлы резервного копирования
- Проверяйте размер базы данных Microsoft Exchange или журналов транзакций.

Перенос базы данных сервера Scan Server

Если на диске, на котором установлен сервер Scan Server, недостаточно пространства, используйте инструмент Scan Server Database Mover для безопасного перемещения базы данных Scan Server на другой диск.

Убедитесь, что компьютер с установленным сервером Security Server содержит несколько дисков и новый диск имеет не менее 3 ГБ доступного пространства. Подключенные диски не принимаются. Не переносите базу данных вручную и не используйте другие инструменты.

Процедура

1. На компьютере с сервером Security Server перейдите к `<папке установки Security Server>\PCCSRV\Admin\Utility`.
2. Запустите программу `ScanServerDBMover.exe`.
3. Щелкните **Изменить**.
4. Выберите **Обзор** и перейдите к целевому каталогу на другом диске.
5. Нажмите кнопку **ОК**, а затем кнопку **Завершить** после перемещения базы данных.

Восстановление зашифрованных файлов

Чтобы предотвратить открытие зараженных файлов, Worry-Free Business Security шифрует файлы в следующих случаях:

- перед помещением файла в карантин;
- при резервном копировании файла перед лечением.

Worry-Free Business Security содержит средство для расшифровки и последующего восстановления файла при необходимости получения из него информации. Файлы, которые могут быть расшифрованы и восстановлены программой Worry-Free Business Security:

Таблица 14-2. Файлы, доступные для расшифровки и восстановления в Worry-Free Business Security

Файл	Описание
Файлы карантина на клиентском компьютере	Эти файлы находятся в следующих каталогах: • `<папка установки Security Agent>\SUSPECT\Backup` или `<папка установки Security Agent>\quarantine`, (в зависимости от доступности). • `<папка установки Messaging Security Agent>\storage\quarantine` Эти файлы будут загружены в указанный папку карантина, которая, как правило, является папкой на сервере Security Server
Файлы карантина в указанной папке карантина	По умолчанию эта папка находится на компьютере с сервером Security Server (`<папка установки Security Server>\PCCSRV\Virus`). Чтобы изменить папку, перейдите на вкладку **Администрирование** > **Глобальные параметры** > **Система** и откройте раздел «Обслуживание карантина».

Файл	Описание
Резервные копии зашифрованных файлов	Это резервные копии зараженных файлов, которые агенты смогли вылечить. Эти файлы находятся в следующих папках: • <папка установки Security Agent>\Backup • <папка установки Messaging Security Agent>\storage\backup Для восстановления этих файлов пользователям необходимо переместить их в папку карантина на клиентском компьютере.

ПРЕДУПРЕЖДЕНИЕ!

В результате восстановления зараженного файла вирус/вредоносная программа могут распространиться на другие файлы. Перед восстановлением файла изолируйте инфицированный клиентский компьютер и переместите важные файлы с него в резервное место хранения.

Расшифровка и восстановление файлов на Security Agent

Процедура

1. Откройте командную строку и перейдите в <папку установки Security Agent>.
2. Запустите файл VSEncode.exe, введя следующую команду:

   ```
   VSEncode.exe /u
   ```

   В открывшемся окне будет отображаться список файлов, находящихся в <папке установки Security Agent>\SUSPECT\Backup.

   Администраторы могут восстанавливать файлы, классифицированные на вкладке «Шпионские и нежелательные программы» как шпионские или нежелательные. На экране отображается список файлов, обнаруженных в папке: <папка установки Security Agent>\BackupAS.

3. Выберите файл для восстановления и нажмите **Восстановить**.

Примечание

Инструмент может одновременно восстанавливать только один файл.

4. В открывшемся окне укажите папку для восстановления файла.
5. Нажмите кнопку **OK**.

Примечание

После восстановления файла агент вновь сможет выполнять его сканирование и идентифицировать его как зараженный. Чтобы запретить сканирование файла, добавьте его в список исключений сканирований.

См. *Сканирование объектов и действий для Security Agent на странице 7-11*.

Файл будет восстановлен в указанной папке.

6. Нажмите **Закрыть**.

Расшифровка и восстановление файлов на сервере Security Server, в пользовательской папке карантина или в агенте Messaging Security Agent

Процедура

1. Если файл находится на компьютере с сервером Security Server, откройте командную строку и перейдите к `<папке установки сервера>\PCCSRV\Admin\Utility\VSEncrypt`.

   Если файл находится на клиентском компьютере с агентом Messaging Security Agent или в пользовательской папке карантина, перейдите к `<папке установки сервера>\PCCSRV\Admin\Utility` и

скопируйте папку VSEncrypt на клиентский компьютер или в пользовательскую папку карантина.

2. Создайте текстовый файл, затем введите полный путь к файлу, который требуется зашифровать или расшифровать.

   Например, для восстановления файлов в папке C:\My Documents\Reports, введите команду C:\My Documents\Reports*.* в текстовый файл.

   Файлы карантина на компьютере с сервером Security Server находятся в <папке установки сервера>\PCCSRV\Virus.

3. Сохраните текстовый файл с расширением INI или TXT. Например, сохраните его как ForEncryption.ini на диске C: .

4. Откройте командную строку и перейдите в каталог, где находится папка VSEncrypt.

5. Запустите файл VSEncode.exe, введя следующую команду:

   ```
   VSEncode.exe /d /i <папка с файлом INI или TXT>
   ```

   Где:

   <папка с файлом INI или TXT> — это путь к созданному файлу INI или TXT (например, C:\ForEncryption.ini).

6. Используйте другие параметры, чтобы выполнять различные команды.

Таблица 14-3. Восстановление параметров

Параметр	Описание
нет (без параметра)	Шифрование файлов
/d	Расшифровка файлов
/debug	Создайте журнал отладки и сохраните его на компьютере. На клиентском компьютере журнал отладки VSEncrypt.log создается в <папке установки агента>.

Параметр	Описание
/o	Перезапись зашифрованного или расшифрованного файла, если он уже существует.
/f <имя_файла>	Шифрование или расшифровка отдельного файла.
/nr	Не восстанавливать оригинальное имя файла.
/v	Отображение информации об инструменте
/u	Запускать пользовательский интерфейс инструмента
/r <папка_назначения>	Папка для восстановления файла
/s <исходное_имя_файла>	Имя исходного зашифрованного файла

Например, для расшифровки файлов в папке `Suspect` и создания журнала отладки необходимо указать в командной строке: `VSEncode [/d] [/debug]`. При шифровании или расшифровке файла программа Worry-Free Business Security создает в этой же папке зашифрованный или расшифрованный файл. Перед расшифровкой или зашифровкой файла, убедитесь, что он не заблокирован.

Восстановление почтовых сообщений в формате Transport Neutral Encapsulation

Формат Transport Neutral Encapsulation (TNEF) – это формат инкапсуляции сообщений, используемый в Microsoft Exchange/Outlook. Обычно этот формат находится во вложении к сообщению и обозначается `Winmail.dat`; Outlook Express автоматически скрывает данное вложение.

Дополнительные сведения см. в разделе https://support.microsoft.com/en-us/help/290809/.

Если агент Messaging Security Agent архивирует сообщения такого типа, и расширение файла меняется на .EML, Outlook Express отображает только тело почтового сообщения.

Использование инструмента ReGenID

При установке каждого агента Security Agent необходимо использовать глобальный уникальный идентификатор (GUID), позволяющий серверу Security Server однозначно идентифицировать клиентов. Дублирование GUID, как правило, происходит на клонированных клиентах или виртуальных машинах.

Если два или более агентов сообщают один и тот же GUID, запустите инструмент ReGenID для создания уникального GUID для каждого клиента.

Процедура

1. На сервере Security Server перейдите к следующему каталогу: `<папка установки сервера>\PCCSRV\Admin\Utility`.
2. Скопируйте файл `WFBS_WIN_All_ReGenID.exe` во временную папку на клиентском компьютере, где установлен Security Agent.

   Пример: `C:\temp`
3. Дважды щелкните файл `WFBS_WIN_All_ReGenID.exe` и следуйте инструкциям на экране.

   Инструмент остановит Security Agent и удалит клиент GUID.
4. Затем необходимо перезапустить агент Security Agent.

   Security Agent создаст новый клиент GUID.

Управление дополнениями SBS и EBS

Worry-Free Business Security содержит дополнения, позволяющие администраторам просматривать динамические сведения о состоянии агентов Security Agent в консолях следующих операционных систем Windows:

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

Установка дополнений SBS и EBS вручную

Во время установки Security Server на оконечном устройстве под управлением поддерживаемых операционных систем дополнения SBS или EBS устанавливаются автоматически. Чтобы использовать дополнение на другом оконечном устройстве, работающем под управлением поддерживаемых операционных систем, потребуется установить дополнение вручную.

Процедура

1. Войдите в веб-консоль Security Server.
2. Перейдите в **Администрирование** > **Инструменты управления**.
3. Нажмите **Дополнения**.
4. Щелкните соответствующую ссылку **Загрузить** для получения программы установки.
5. Скопируйте и запустите программу установки на целевом оконечном устройстве.

Использование дополнений SBS или EBS

Процедура

1. Откройте консоль SBS или EBS.
2. На вкладке **Безопасность** нажмите **Trend Micro Worry-Free Business Security** для просмотра информации о состоянии.

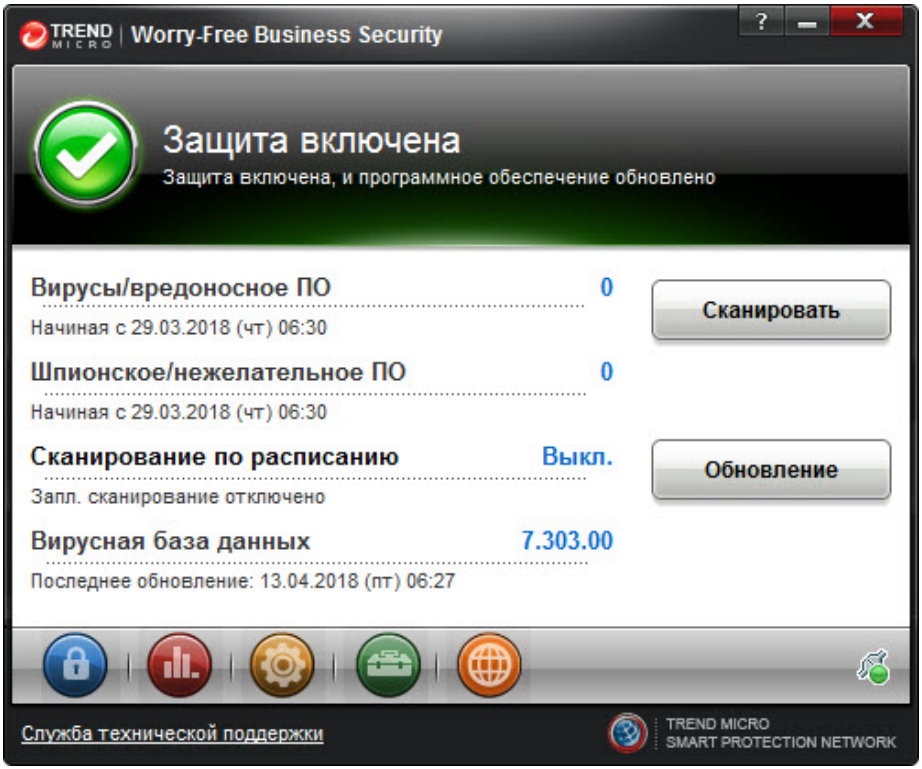
Приложение A

Значки Security Agent

В этом приложении описаны различные значки Security Agent, которые отображаются в клиентских системах.

Проверка состояния Security Agent

На следующем рисунке показана консоль агента Security Agent в состоянии, когда все функции обновлены и работают должным образом.



В следующей таблице перечислены значки главного интерфейса пользователя консоли Security Agent и их значения.

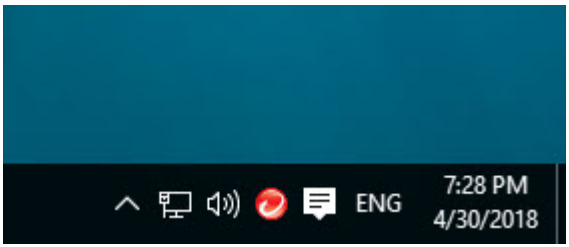
Таблица A-1. Значки главного интерфейса пользователя консоли Security Agent

Значок	Состояние	Объяснение и действие
	Защита включена. Защита включена, и программное обеспечение обновлено	Программное обеспечение обновлено и работает должным образом. Выполнение каких-либо действий не требуется.
	Перезагрузить компьютер. Перезагрузите компьютер для завершения удаления угроз безопасности	Агент Security Agent обнаружил угрозы, которые невозможно устранить немедленно. Перезагрузите компьютер для завершения устранения этих угроз.
	Защита подвержена риску. Обратитесь к администратору	Функция сканирования в режиме реального времени отключена, или защита подвержена риску по другой причине. Включите сканирование в режиме реального времени, и если это не решит проблему, обратитесь в службу поддержки.
	Обновить сейчас. Обновления не поступали на протяжении (количество) дней.	Вирусная база данных старше трех дней. Обновите Security Agent немедленно.

Значок	Состояние	Объяснение и действие
	Сканирование Smart Scan недоступно. Проверьте подключение к Интернету	Агент Security Agent не имел доступа к серверу Scan Server более 15 минут. Убедитесь в наличии подключения к сети, чтобы выполнить сканирование с использованием последних баз данных.
	Перезагрузить компьютер. Перезагрузите компьютер для завершения установки обновления	Перезагрузите компьютер для завершения обновления.
	Обновление программы. Идет обновление программного обеспечения защиты данных	Выполняется процесс обновления. Не отключайтесь от сети до его завершения.

Просмотр значков агентов Security Agent на панели задач Windows

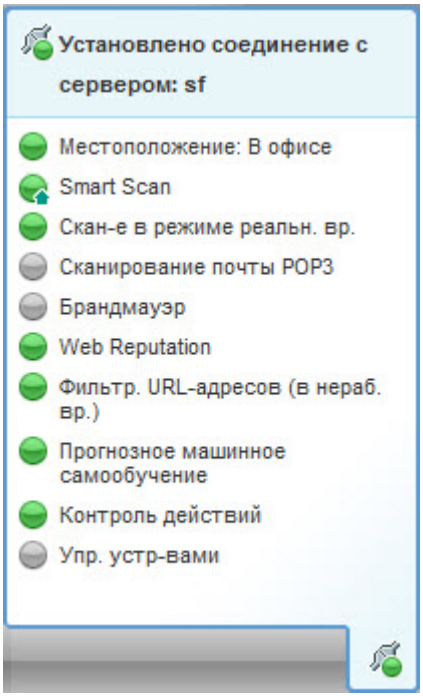
На панели задач Windows отображаются следующие значки агентов Security Agent:



Значок	Значение
	Состояние нормальное
	(Анимированный) Выполняется сканирование вручную или по расписанию. Агент Security Agent использует обычное сканирование или Smart Scan.
	Агент Security Agent выполняет обновление.
	Необходимо действие. • Сканирование в режиме реального времени отключено • Требуется перезагрузка для полной очистки от вредоносных программ • Модуль был обновлен, требуется перезагрузка • Для восстановления файлов, зашифрованных ПО для вымогательства, требуется перезагрузка • Необходимо обновление **Примечание** Откройте главную консоль агента Security Agent, чтобы увидеть требуемое действие.

Доступ к консоли Flyover

Консоль Flyover Security Agent откроется при наведении указателя мыши на небольшой значок справа в нижней части консоли Security Agent.



В таблице ниже перечислены значки панели Flyover консоли и их значения.

Таблица A-2. Значки панели Flyover консоли

Функция	Значок	Значение
Подключение		Подключено к Security Server
		Отсутствует подключение к Security Server, но сканирование в режиме реального времени запущено. Возможно, требуется обновить файл базы данных. Правой кнопкой мыши щелкните значок агента на панели задач Windows и выберите **Обновить сейчас**.
Расположение		В офисе (внутренняя сеть)
		Вне офиса (внешняя сеть)
Сканирование в режиме реального времени		Вкл.
		Выкл.
Сканирование почты POP3		Вкл.
		Выкл.

Функция	Значок	Значение
Smart Scan		Подключено к сети Trend Micro Smart Protection Network
		Не удалось подключиться к Smart Protection Network. Уровень защиты понижен, поскольку Агенты безопасности не удалось отправить запросы на сканирование. **Примечание** Убедитесь, что служба Smart Scan TMiCRCScanService запущена и программы Агенты безопасности подключены к Security Server.
		Smart Scan отключен. Использование обычного сканирования
• Брандмауэр • Web Reputation • Фильтрация URL-адресов • Контроль действий • Контроль устройств • Прогнозное машинное самообучение		Вкл.
		Выкл.

Приложение B

Поддержка IPv6 в Worry-Free Business Security

Данное приложение является обязательным к прочтению для пользователей, которые планируют развернуть Worry-Free Business Security в среде с поддержкой адресации IPv6. В этом приложении содержится информация о степени поддержки IPv6 в Worry-Free Business Security.

Компания Trend Micro предполагает, что читатель знаком с понятиями и задачами IPv6, включая создание сети, которая поддерживает адресацию IPv6.

Поддержка IPv6 в Worry-Free Business Security и Агенты безопасности

Поддержка IPv6 в Worry-Free Business Security начинается с версии 8.0. Более ранние версии Worry-Free Business Security не поддерживают адресацию IPv6. Поддержка IPv6 автоматически включается после установки или обновления сервера Security Server или агентов Security Agent и Messaging Security Agent, которые удовлетворяют требованиям IPv6.

Требования к серверу Security Server IPv6

IPv6 предъявляет к Security Server следующие требования.

- Если сервер будет управлять агентами IPv4 и IPv6, он должен иметь как IPv4, так и IPv6-адрес и должен идентифицироваться по имени хоста. Если сервер идентифицируется по адресу IPv4, агенты, имеющие только адрес IPv6, не смогут подключиться к нему. То же самое будет происходить, если клиентские компьютеры с адресами IPv4 будут подключаться к серверу, идентифицируемому по адресу IPv6.
- Если сервер будет управлять только агентами IPv6, минимальным требованием является наличие адреса IPv6. Сервер может идентифицироваться по имени хоста или по адресу IPv6. Когда сервер идентифицируется по имени хоста, то предпочтительнее использовать его полное доменное имя (FQDN). Это условие должно выполняться, так как в среде адресов IPv6 сервер WINS не сможет перевести имя хоста в соответствующий адрес IPv6.
- Убедитесь, что адрес IPv6 или IPv4 хоста можно получить с помощью, например, команды `ping` или `nslookup`.
- При установке Security Server на компьютер, имеющий только адрес IPv6, создайте прокси-сервер с двойным стеком, который может конвертировать между собой адреса IPv4 и IPv6 (например, DeleGate). Разместите прокси-сервер между Security Server и

Интернетом, чтобы позволить ему успешно подключаться к таким службам Trend Micro, как сервер ActiveUpdate, интерактивный сайт регистрации и Smart Protection Network.

Требования к агентам Messaging Security Agent

Агент Messaging Security Agent (только Advanced) может быть установлен на сервер с двойным стеком или на сервер Microsoft Exchange с адресом IPv6.

Желательно, чтобы агент Messaging Security Agent имел как IPv4, так и IPv6-адрес, поскольку некоторые из объектов, с которыми он взаимодействует, поддерживают только IPv4-адресацию.

Ограничения сервера только с адресом IPv6

В следующей таблице приведены ограничения для случаев, когда Security Server имеет только адрес IPv6.

Таблица B-1. Ограничения сервера только с адресом IPv6

Элемент	Ограничение
Управление агентами	Сервер, имеющий только адрес IPv6, не может: • развертывать агенты на клиентах, имеющих только адрес IPv4; • управлять агентами, имеющими только адрес IPv4.
Обновления и централизованное управление	Сервер, имеющий только адрес IPv6, не может обновляться с помощью источников обновления с адресом IPv4, таких как • Сервер Trend Micro ActiveUpdate • любого пользовательского источника обновлений с адресом IPv4.
Регистрация, активация и обновление продукта	Сервер, имеющий только адрес IPv6, не может подключиться к серверу регистрации Trend Micro Online Registration, чтобы зарегистрировать продукт, получить лицензию и активировать/продлить лицензию.

Элемент	Ограничение
Прокси-соединение	Сервер, имеющий только адрес IPv6, не может подключаться через прокси-сервер с адресом IPv4.
Подключаемые модули	В состав сервера, имеющего только адрес IPv6, входит Plug-in Manager, но развертывание любого из подключаемых модулей будет невозможно на: • агентах или компьютерах только с адресами IPv4 (из-за отсутствия прямого соединения); • агентах или компьютерах только с адресами IPv6 (так как ни один из подключаемых модулей не поддерживает IPv6).

Большинство из этих ограничений могут быть преодолены путем создания прокси-сервера с двойным стеком, который может конвертировать между собой адреса IPv4 и IPv6 (например, DeleGate). Установите прокси-сервер между Security Server и объектами, к которым он подключается, или объектами, которые он обслуживает.

Ограничения для Security Agent, использующих исключительно адреса IPv6

В следующей таблице указаны ограничения для Security Agent, использующих исключительно адреса IPv6.

Таблица B-2. Ограничения для Security Agent, использующих исключительно адреса IPv6

Элемент	Ограничение
Родительский Security Server	Агенты IPv6, имеющие только адрес IPv6, не могут управляться сервером Security Server с адресом IPv4.

Элемент	Ограничение
Обновления	Сервер Security Agent, имеющий только адрес IPv6, не может обновляться с помощью источников обновления с адресом IPv4, таких как: • Сервер Trend Micro ActiveUpdate • Security Server с адресом IPv4, • агент обновления Update Agent с адресом IPv4, • любого пользовательского источника обновлений с адресом IPv4.
Запросы сканирования и служба Smart Feedback	Агенты, имеющие только адрес IPv6, не могут отправлять запросы Trend Micro Smart Protection Network и использовать Smart Feedback.
Подключаемые модули	Агенты, имеющие только адрес IPv6, не могут устанавливать подключаемые модули, так как ни один из подключаемых модулей не поддерживает IPv6.
Прокси-соединение	Клиент Security Agent, использующий исключительно адреса IPv6, не может устанавливать соединение через прокси-сервер, использующий исключительно адреса IPv4.

Большинство из этих ограничений могут быть преодолены путем создания прокси-сервера с двойным стеком, который может конвертировать между собой адреса IPv4 и IPv6 (например, DeleGate). Разместите прокси-сервер между агентами Агенты безопасности и объектами, к которым они подключаются.

Настройка адресов IPv6

Веб-консоль позволяет настраивать адрес IPv6 или диапазон адресов IPv6. Ниже приведены некоторые правила настройки.

- Worry-Free Business Security принимает стандартные представления адресов IPv6.

  Это может произойти в следующих случаях.

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- Worry-Free Business Security также принимает локальные адреса IPv6, например:

```
fe80::210:5aff:feaa:20a2
```

ПРЕДУПРЕЖДЕНИЕ!

Соблюдайте осторожность при указании связанного локального адреса IPv6, потому что даже если решение Worry-Free Business Security сможет принять адрес, в определенных обстоятельствах оно не сможет его корректно обработать. Например, Агенты безопасности не могут обновляться с помощью источника обновления, если он находится в другом сегменте сети и идентифицируется по локальному адресу IPv6.

- Если адрес IPv6 является частью URL-адреса, заключайте его в квадратные скобки ([]).
- Для диапазонов адресов IPv6, как правило, требуется префикс и длина префикса. Для конфигураций, требующих указать сервер для запросов IP-адреса, ограничение длины префикса применяется для предотвращения проблем с производительностью, которые могут возникнуть, если сервер запрашивает значительное число IP-адресов. Например, для функции управления внешним сервером длина префикса может составлять только от 112 (65 536 IP-адресов) до 128 (2 IP-адреса).
- Некоторые параметры, связанные с адресами IPv6 или диапазоном адресов, будут развернуты для Агенты безопасности, но Агенты безопасности будут их игнорировать. Например, если в составленном списке источников Smart Protection указан сервер Smart Protection Server, идентифицированный своим адресом IPv6, клиенты Агенты безопасности, использующие исключительно

адреса IPv4, будут игнорировать этот сервер и подключаться к другим источникам Smart Protection.

Окна, отображающие IP-адреса

В этом разделе перечисляются места на веб-консоли, где отображаются IP-адреса.

- Дерево групп безопасности

  Всякий раз, когда отображается дерево групп безопасности, адреса IPv6 агентов, имеющих только эти адреса, появляются в столбце **IP-адрес**. Для агентов с двойным стеком адреса IPv6 отображаются, если они использовали для регистрации на сервере адреса IPv6.

  Примечание

  IP-адресами, которые агенты с двойным стеком используют при регистрации на сервере, можно управлять в разделе **Предпочтительный IP-адрес** на вкладке **Администрирование** > **Глобальные параметры** > **Настольный ПК или сервер**.

  При экспорте настроек агента в файл адреса IPv6 также экспортируются.

- Журналы

  IPv6-адреса агентов с двойным стеком и агентов, имеющих только адрес IPv6, отображаются в журналах.

Приложение C

Техническая поддержка

Ознакомьтесь с информацией о следующих разделах:

- *Ресурсы для поиска и устранения неисправностей на странице C-2*
- *Как связаться с Trend Micro на странице C-3*
- *Отправка подозрительного содержимого в компанию Trend Micro на странице C-5*
- *Другие ресурсы на странице C-6*

Ресурсы для поиска и устранения неисправностей

Прежде чем обращаться в службу технической поддержки, посетите следующие интернет-ресурсы компании Trend Micro.

Использование портала поддержки

Портал технической поддержки Trend Micro — это круглосуточный ресурс, работающий без выходных, который содержит самую актуальную информацию о распространенных и специфических проблемах.

Процедура

1. Перейдите по адресу https://success.trendmicro.com.
2. Выберите один из доступных продуктов или нажмите на соответствующую кнопку для поиска решений.
3. С помощью поля **Поддержка поиска** можно искать доступные решения.
4. Если решение не будет найдено, нажмите **Обратиться в службу поддержки** и выберите тип необходимой поддержки.

Совет

Чтобы отправить запрос на поддержку через Интернет, посетите следующий веб-сайт:

https://success.trendmicro.com/smb-new-request

Специалисты службы технической поддержки компании Trend Micro изучат ваш запрос и предоставят ответ в течение 24 часов с момента его отправки.

Энциклопедия угроз

В настоящее время большая часть вредоносных программ для обхода протоколов безопасности компьютеров использует смешанные угрозы, объединяющие две или более технологий. Trend Micro борется с такими комплексными вредоносными программами с помощью продуктов, которые формируют пользовательскую стратегию защиты. В энциклопедии угроз представлен развернутый список названий и симптомов различных смешанных угроз, который включает в себя известные вредоносные программы, спам, вредоносные URL-адреса и известные уязвимости.

На сайте https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware можно ознакомиться с информацией касательно следующего:

- вредоносные программы и вредоносный мобильный код, которые в данный момент пребывают в активном или «диком» состоянии;
- страницы со связанной информацией об угрозе, позволяющие сформировать полную историю веб-атаки;
- сообщения об интернет-угрозах, связанные с целевыми атаками и угрозами безопасности;
- веб-атаки и сведения о тенденциях в Интернете;
- еженедельные отчеты о вредоносных программах.

Как связаться с Trend Micro

Телефон и электронный адрес представителей компании Trend Micro:

Адрес	ООО «Тренд Микро Раша» 127055, Россия, Москва ул. Новослободская, д.24, стр.1 БЦ "Европа"

Телефон	+7 (495) 734-85-00
Адрес в Интернете	https://www.trendmicro.com
Эл. почта	support@trendmicro.com

- Список центров поддержки по всему миру:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Как связаться с Trend Micro:

  http://www.trendmicro.com.ru/about/contact/index.html

- Документация по продуктам Trend Micro:

  https://docs.trendmicro.com

Ускорение обработки запроса о поддержке

Для более эффективного решения проблем обеспечьте доступность следующей информации:

- действия, которые необходимо выполнить для воспроизведения проблемы.
- сведения об аппаратном обеспечении и сети;
- название производителя и модели компьютера и всех подключенных к нему устройств или видов оборудования;
- объем оперативной памяти и свободного места на диске;
- сведения об операционной системе и версии пакета обновления;
- версия установленного агента;
- серийный номер или код активации;
- подробное описание среды установки;
- точный текст полученного сообщения об ошибке.

Отправка подозрительного содержимого в компанию Trend Micro

Доступно несколько вариантов отправки подозрительного содержимого в компанию Trend Micro для дальнейшего анализа.

Email Reputation Services

Отправьте запрос о репутации указанного IP-адреса и укажите агент передачи сообщений для включения в глобальный утвержденный список:

https://servicecentral.trendmicro.com/en-us/ers/

Для отправки примеров сообщений в компанию Trend Micro см. следующую запись в базе знаний:

https://success.trendmicro.com/solution/1112106

Службы File Reputation

Соберите сведения о системе и отправьте содержимое подозрительных файлов в компанию Trend Micro:

https://success.trendmicro.com/solution/1059565

Для отслеживания заявки запишите ее номер.

Службы Web Reputation

Отправьте запрос о степени безопасности и типе содержимого URL-адреса сайта, заподозренного в фишинге или другом так называемом «распространении заражения» (источника преднамеренного распространения интернет-угроз, таких как шпионские программы и вирусы):

https://global.sitesafety.trendmicro.com/

Если назначенная степень является неправильной, отправьте запрос о реклассификации в компанию Trend Micro.

Другие ресурсы

Помимо решений и технической поддержки доступны различные вспомогательные интернет-ресурсы, которые помогут вам использовать новейшие решения, узнавать о новейших разработках и быть в курсе последних тенденций в сфере обеспечения безопасности.

Центр загрузок

Время от времени компания Trend Micro может выпускать пакеты исправлений для известных проблем или обновления для конкретных продуктов или служб. Для проверки на наличие доступных пакетов исправлений перейдите по адресу:

https://www.trendmicro.com/download/

При наличии пакета исправлений, который не применялся (указана дата выхода пакета исправлений), откройте файл Readme и проверьте, подходит ли он для вашей среды). Файл Readme также содержит инструкции по установке.

Отзывы и предложения по документации

Компания Trend Micro постоянно совершенствует свою документацию. Со всеми вопросами, замечаниями или предложениями относительно этого или любого другого документа компании Trend Micro обращайтесь на следующий сайт:

https://docs.trendmicro.com/en-us/survey.aspx

Приложение D

Использование терминов и понятий о продукте

Элементы, содержащиеся в этом приложении, представляют дополнительную информацию о продуктах и технологиях Trend Micro.

Критически важное исправление

Критически важное исправление в первую очередь решает проблемы безопасности установки для всех клиентов. Критически важные исправления для Windows содержат программу установки, в то время как другие исправления (не для Windows) обычно имеют сценарий установки.

Оперативное исправление

Оперативное исправление —— обходной путь или исправление одной проблемы, о которой сообщил клиент. Исправления зависят от проблемы и не предназначены для всех пользователей. Оперативные исправления Windows включают программу установки, в то время как исправления для других систем ее не включают (как правило, требуется остановка служебных программ, копирование файла для перезаписи файла установки и перезапуск служебных программ).

IntelliScan

IntelliScan — это способ определения файлов, подлежащих сканированию. Истинный тип исполняемых файлов (например, с расширением `.exe`) определяется на основании содержимого файла. Для неисполняемых файлов (например файлов с расширением `.txt`) тип определяется на основе их заголовков.

Использование функции IntelliScan дает следующие преимущества.

- Оптимизация производительности. Поскольку функция IntelliScan не требует значительных системных ресурсов, ее использование не влияет на выполнение других приложений на агент.
- Сокращение времени сканирования. Благодаря алгоритму определения типа файлов, функция IntelliScan подвергает процессу сканирования только уязвимые файлы. В силу этого

время работы в режиме сканирования всех файлов значительно сокращается.

IntelliTrap

IntelliTrap — это эвристическая технология Trend Micro, применяемая для обнаружения угроз, которые выполняют сжатие в реальном времени вместе другими вредоносными действиями, например упаковкой. Сюда входят вирусы, вредоносные программы, черви, «троянские кони», «черные ходы» и боты. Разработчики вирусов/вредоносных программ зачастую пытаются скрыть наличие кода путем использования различных схем сжатия. Технология сканирования вирусов IntelliTrap работает в реальном времени и использует правила и распознавание по шаблонам. IntelliTrap находит и удаляет известные вирусы и вредоносное ПО в сжатых файлах, содержащих до 17 уровней вложенности, запакованных с использованием любого из 16 известных типов сжатия.

Примечание

IntelliTrap пользуется тем же механизмом сканирования, что и программа проверки на вирусы. Таким образом, правила работы с файлами для IntelliTrap будут такими же, как правила, установленные администратором для программы проверки на вирусы.

Агенты регистрируют случаи обнаружения вредоносных программ и ботов в журнале IntelliTrap. Содержимое журнала IntelliTrap можно экспортировать и включать в отчеты.

При проверке на вредоносные программы IntelliTrap пользуется следующими компонентами:

- Модуль вирусного сканирования
- База данных IntelliTrap
- База исключений IntelliTrap

Система обнаружения вторжения

Система обнаружения вторжения сравнивает данные сетевых пакетов с базой данных и таким образом выявляет возможные атаки на локальный компьютер.

Система обнаружения вторжения служит для предотвращения следующих известных типов вторжений.

Система	Описание
Too Big Fragment (слишком большой фрагмент)	Атака типа «отказ в обслуживании», когда хакер направляет на целевой локальный компьютер пакет TCP/UDP завышенного размера. Такая атака может привести к переполнению буфера и, как следствие, зависанию или перезагрузке компьютера.
Ping of Death («смертельный» запрос)	Атака типа «отказ в обслуживании», когда хакер направляет на целевой локальный компьютер пакет ICMP/ICMPv6 завышенного размера. Такая атака может привести к переполнению буфера и, как следствие, зависанию или перезагрузке компьютера.
Conflicted ARP (конфликт протокола разрешения адресов)	Тип атаки, при котором злоумышленник посылает запрос Address Resolution Protocol (ARP) с совпадающими IP-адресами источника и назначения на целевой локальный компьютер. После этого целевой компьютер начинает в бесконечном цикле отправлять ответ ARP (свой MAC-адрес) самому себе, что приводит к зависанию или завершению работы
SYN Foold (синхронная атака)	Атака типа «отказ в обслуживании», при которой программа посылает на локальный компьютер множество пакетов синхронизации TCP (SYN), вследствие чего этот компьютер начинает непрерывно посылать множественные подтверждения синхронизации (SYN/ACK). Этот процесс может вызвать переполнение памяти компьютера, а в конечном итоге — сбой системы.
Overlapping Fragment (перекрывающиеся фрагменты)	Подобно атаке Teardrop, эта атака типа «отказ в обслуживании» отправляет на локальный компьютер перекрывающиеся фрагменты TCP. Это приводит к перезаписыванию данных заголовка в первом фрагменте TCP, позволяя ему проходить через брандмауэр. Это может повлечь за собой проникновение на локальный компьютер последующих фрагментов, содержащих вредоносный код.

Система	Описание
Teardrop (прорыв)	Подобно атаке перекрывающихся фрагментов, эта атака типа «отказ в обслуживании» работает с фрагментами IP. Некорректное значение смещения во втором или последующих IP-фрагментах может привести к сбою в работе операционной системы принимающего локального компьютера при попытке собрать фрагменты.
Tiny Fragment Attack (атака малыми фрагментами)	Тип атаки, при которой небольшой размер фрагментов TCP приводит к перемещению данных заголовка первого пакета TCP в следующий фрагмент. В результате маршрутизаторы, фильтрующие трафик, могут пропускать последующие фрагменты, которые могут содержать вредоносные данные.
Fragmented IGMP (фрагментированный протокол управления группами Интернет)	Атака типа «отказ в обслуживании», при которой пакеты IGMP посылаются на целевой локальный компьютер, который не в состоянии обработать их нужным образом. Такая атака может привести к зависанию или замедлению работы локального компьютера.
Land Attack (атака на папку локальной сети)	Тип атаки, при котором на локальный компьютер посылаются пакеты IP-синхронизации (SYN) с одинаковым адресом источника и назначения, вследствие чего этот компьютер начинает отправлять подтверждения синхронизации (SYN/ACK) самому себе. Такая атака может привести к зависанию или замедлению работы локального компьютера.

Ключевые слова

В программе Worry-Free Business Security для фильтрации сообщений используются следующие ключевые слова.

- Слова («оружие», «бомбы» и т. д.)
- Числа (1, 2, 3 и т. д.)
- Специальные символы (&, №, + и т. д.)

- Короткие фразы («синяя рыба», «красный телефон», «большой дом» и т.д.)
- слова или фразы, которые соединены логическими операторами (яблоки .AND. апельсины);
- Слова или фразы, использующие регулярные выражения (регулярное выражение «.REG. м*л» соответствует словам «мал», «мол» и «мел», но не «миска» или «максимальный»).

Программа Worry-Free Business Security может импортировать существующий список ключевых слов из текстового файла (`.txt`). Импортированные ключевые слова помещаются в список ключевых слов.

Операторы с ключевыми словами

Операторы — это команды, объединяющие несколько ключевых слов. Операторы могут расширять или сужать условия. Операторы следует окружать точками (.). Это может произойти в следующих случаях.

```
яблоки .AND. апельсины и яблоки .NOT. апельсины
```

Примечание

Непосредственно перед оператором и после него ставится по точке. Между последней точкой и ключевым словом ставится пробел.

Таблица D-1. Использование операторов

Оператор	Принцип работы	Пример
любое ключевое слово	Агент Messaging Security Agent выполняет поиск содержимого с совпадением по слову	Введите слово и добавьте его в список ключевых слов

Оператор	Принцип работы	Пример
OR	Агент Messaging Security Agent выполняет поиск любого из ключевых слов, разделенных оператором OR Например, «яблоко OR апельсин». Агент выполняет поиск либо слова «яблоко», либо слова «апельсин». Если содержимое содержит любое из двух слов, то находится совпадение.	Введите `.OR.` между всеми словами, которые хотите включить в поиск. Например, «яблоко .OR. апельсин».
AND	Агент Messaging Security Agent выполняет поиск любого из ключевых слов, разделенных оператором AND Например, «яблоко AND апельсин». Агент выполняет поиск как слова «яблоко», так и слова «апельсин». Если в содержимом нет обоих слов, то совпадения не находится.	Введите `.AND.` между всеми словами, которые хотите включить в поиск. Например, «яблоко .AND. апельсин»
NOT	Messaging Security Agent исключает из поиска ключевые слова, стоящие после оператора NOT. Например, «.NOT. сок». Агент ищет содержимое, в котором нет слова «сок». Если сообщение содержит фразу «апельсиновая газировка», значит совпадение есть; если в нем есть фраза «апельсиновый сок», значит совпадения нет.	Введите `.NOT.` перед словом, которое хотите исключить. Например, «.NOT. сок»

Оператор	Принцип работы	Пример
WILD	Групповой (подстановочный) символ заменяет отсутствующую часть слова. Любые слова, оставшаяся часть которых может быть заменена подстановочным символом, считаются совпадениями. **Примечание** Агент Messaging Security Agent не поддерживает использование знака «?» в команде подстановочного символа «.WILD.».	Пользуйтесь оператором `.WILD.`, вводя его перед частью слова, которую вы ищете. Например, вы хотите найти все слова, содержащие «астро». В этом случае введите `.WILD.астро`. Все слова «гастроном», «астронавт» и «астроном» считаются совпадениями.
REG	Для обозначения регулярного выражения введите перед шаблоном оператор .REG. (например, .REG. г.*а). См. *Регулярные выражения на странице D-11*.	Введите `.REG.` перед шаблоном слова, которое вы ищете. Например, .REG. а.*е соответствует: «алле», «аве» и «акме», но не «алло», «анютины» или «антивирус»

Эффективное применение ключевых слов

Агент Messaging Security Agent предоставляет простые и при этом мощные средства создания очень специфичных фильтров. При создании правил фильтрации содержимого учтите следующее.

- По умолчанию Messaging Security Agent выполняет поиск точных совпадений с ключевыми словами. Используйте регулярные выражения для настройки поиска частичных совпадений с ключевыми словами. См. *Регулярные выражения на странице D-11*.
- Агент Messaging Security Agent по-разному анализирует несколько ключевых слов в одной строке, несколько ключевых слов в нескольких строках и несколько ключевых слов, разделенных знаками запятой, точки, переноса и другими знаками препинания. Дополнительную информацию о работе с ключевыми словами на нескольких строках см. в следующей таблице.

- Вы также можете настроить Messaging Security Agent для поиска синонимов фактических ключевых слов.

Таблица D-2. Как использовать ключевые слова

Ситуация	Пример	Соответствие / несоответствие
Два слова в одной строке	пистолеты бомбы	Соответствует: «Чтобы купить пистолеты, бомбы и другое оружие, щелкните здесь». Не соответствует: «Чтобы купить пистолеты и бомбы, щелкните здесь».
Два слова, разделенные запятой	пистолеты, бомбы	Соответствует: «Чтобы купить пистолеты, бомбы и другое оружие, щелкните здесь». Не соответствует: «Чтобы купить подержанные пистолеты, новые бомбы и другое оружие, щелкните здесь».

Ситуация	Пример	Соответствие / несоответствие
Несколько слов в нескольких строках	пистолеты бомбы оружие и боеприпасы	При выборе параметра **Любые указанные ключевые слова** Соответствует: «Продаются пистолеты» Также соответствует: «Покупайте пистолеты, бомбы и другое оружие» При выборе параметра **Все указанные ключевые слова** Соответствует: «Покупайте пистолеты, бомбы, оружие и боеприпасы» Не соответствует: «Покупайте пистолеты, бомбы, оружие, патроны» Также не соответствует: «Покупайте пистолеты, бомбы, оружие, боеприпасы»
Много ключевых слов в одной строке	пистолеты бомбы оружие боеприпасы	Соответствует: «Покупайте пистолеты, бомбы, оружие, боеприпасы» Не соответствует: «Покупайте патроны для пистолетов, оружия и новые бомбы»

Исправление

Исправление — это группа оперативных обновлений и исправлений безопасности, предназначенная для решения многих программных проблем. Компания Trend Micro делает исправления доступными на постоянной основе. Исправления Windows содержат программу

установки, в то время как другие (не Windows) исправления обычно имеют установочный скрипт.

Регулярные выражения

Регулярные выражения используются для выполнения поиска совпадений по строке. Некоторые общие примеры регулярных выражений см. в следующих таблицах. Чтобы задать регулярное выражение, добавьте перед шаблоном оператор «.REG.».

В Интернете есть ряд сайтов и учебников, посвященных этой теме. Один из них — это сайт PerlDoc:

http://www.perl.com/doc/manual/html/pod/perlre.html

ПРЕДУПРЕЖДЕНИЕ!

Регулярные выражения являются высокоэффективным инструментом поиска совпадений строк. По этой причине компания Trend Micro рекомендует администраторам, решившим использовать регулярные выражения, как следует освоить синтаксис регулярных выражений. Плохо написанные регулярные выражения могут оказать сильное отрицательное влияние на производительность. Trend Micro рекомендует начинать с простых регулярных выражений, не использующих сложного синтаксиса. При введении новых правил выполните архивацию и посмотрите, как агент Messaging Security Agent управляет сообщениями с помощью вашего правила. Если вы уверены, что у правила нет непредсказуемых последствий, можете изменить свое действие.

Примеры регулярных выражений

Некоторые общие примеры регулярных выражений см. в следующих таблицах. Чтобы задать регулярное выражение, добавьте перед шаблоном оператор «.REG.».

Таблица D-3. Подсчет и группировка

Элемент	Что это означает	Пример
.	Символ точки представляет любой символ, кроме символа начала строки.	Так, «гру.» соответствует словам «груша», «грусть», «группа», «груз» и т. д. «др.» соответствует «драже», «друг» и т.д.
*	Звездочка (*) заменяет ноль и более повторений предыдущего символа.	Так, «гр*» будет соответствовать «г», «гр», «грр», «гррр», «гррррр» и т. д.
+	Знак «плюс» (+) заменяет одно и более повторений предыдущего символа.	Так, «гр+» будет соответствовать результатам «гр», «грр», «гррр», «гррррр» и т. д., но не будет соответствовать «г».
?	Вопросительный знак (?) заменяет от нуля до одного повторения предыдущего символа.	Так, «гру?ша» будет соответствовать результатам «грша» и «груша», но не будет соответствовать словам «грууша», «груууша» и т. д.
( )	Скобки используются для группировки заключенных между ними знаков. Такая группа знаков считается неделимой.	Так, «гр(уша)+» будет соответствовать словам «груша», «грушауша», «грушаушауша» и т. д. Знак «+» применяется к подстроке, заключенной в скобки, поэтому регулярное выражение ищет сочетание «гр» со следующим за ним сочетанием «уша» (однократным или многократно повторяющимся).

Элемент	Что это означает	Пример
[ ]	В квадратные скобки заключается набор возможных вариантов символов.	Так, «а[бвгд]+» соответствует сочетаниям «аб», «ав», «аг», «ад», «абв», «адг», «адгб» и т. д. К группе символов внутри квадратных скобок применяется знак «+», поэтому regex ищет «а» со следующими за ним одним или более знаком из группы вариантов [бвгд]. «д[А-Я]» соответствует «дА», «дБ», «дВ» и так далее до «дЯ». Набор в квадратных скобках обозначает диапазон всех прописных букв между А и Я.
[^]	Знак «^» в квадратных скобках исключает весь указанный диапазон, и в этом случае regex будет искать все знаки, которые не входят в этот диапазон.	«д[^оауем]» соответствует «ды», «др» или «дд», «д9», «д#--д» перед любым одиночным символом за исключением гласной буквы.
{ }	Фигурные скобки задают определенное количество повторений предыдущего элемента. Единственная цифра в скобках значит, что только такое количество повторений будет считаться совпадением. Пара чисел, разделенных запятой, задают диапазон допустимых повторений предыдущего знака. Единственная цифра, за которой стоит запятая, задает диапазон от этого числа до бесконечности: верхней границы нет.	«да{3}» соответствует «дааа--д» перед 3-мя и только 3-мя экземплярами «а». «да{2,4}» соответствует «даа», «дааа», «дааaа» (но не «дааааа»)--д перед 2-мя, 3-мя или 4-мя экземплярами «а». «да{4,}» соответствует «дааaа», «дааааа», «дааааaа» и т. д.--д перед 4-мя экземплярами «а» или более.

Таблица D-4. Классы символов (краткая запись)

Элемент	Что это означает	Пример
\d	Любая цифра: эквивалент [0-9] или [[:digit]]	\d соответствует 1, 12, 123 и т. д., но не «1б7»--одна или несколько любых цифр.
\D	Любой знак, не являющийся цифрой: эквивалент [^0-9] или [^[:digit]]	\D соответствует «а», «аб», «аб&», но не «1» — любому одному или нескольким знакам, кроме цифр 0, 1, 2, 3, 4, 5, 6, 7, 8 или 9.
\w	Любая буква или цифра; функционально эквивалентно выражению [_А-Яа-я0-9] или [_[:alnum:]]	\w соответствует «а», «аб», «а1», но не «!&» — т. е. одному или более символам — буквам верхнего или нижнего регистра или цифрам, но не знакам препинания или служебным символам.
\W	Любой символ, отличный от буквы и цифры; функционально эквивалентно выражению [^_А-Яа-я0-9] или [^_[:alnum:]]	\W соответствует «*», «&», но не «алло» или «а1» — т. е. одному или более символам, которые не являются буквами или цифрами.
\s	Любое свободное место: пробел, новая строка, табуляция, неразрывный пробел и т. д.; эквивалент [[:space]]	«овощ\и» соответствует слову «овощ» перед символом пробела. Поэтому фаза «Я люблю овощ в супе» найдется по регулярному выражению, а фраза «Я люблю овощи в супе» не найдется.
\S	Любой символ, не являющийся пробелом; эквивалент [^[:space]]	«овощ\И» соответствует слову «овощ» со следующим за словом любым знаком, кроме пробела. Поэтому фраза «Я люблю овощи в супе» найдется по регулярному выражению, а фраза «Я люблю овощ в супе» не найдется.

Таблица D-5. Классы символов

Элемент	Что это означает	Пример
[:alpha:]	Любая буква	.REG. [[:alpha:]] соответствует «абв», «где», «ххх», но не 123 и @# $.
[:digit:]	Любая цифра; функционально эквивалентно \d	.REG. [[:digit:]] соответствует 1, 12, 123 и т. д.
[:alnum:]	Любая буква или цифра; функционально эквивалентно \w	.REG. [[:alnum:]] соответствует «абв», 123, но не ~!@.
[:space:]	Любое свободное место: пробел, новая строка, табуляция, неразрывный пробел и т. д.; эквивалент \s	.REG. (vegetable)[[:space:]] соответствует «овощ» перед символом пробела. Поэтому фраза «Я люблю овощ в супе» найдется по регулярному выражению, а фраза «Я люблю овощи в супе» не найдется.
[:graph:]	Любой знак, кроме пробела, управляющих символов и т. п.	.REG. [[:graph:]] соответствует 123, «абв», ххх><”, но не пробелам и не управляющим символам.
[:print:]	Любые знаки (схож с оператором [:graph:]) но включает знак пробела	.REG. [[:print:]] соответствует 123, «абв», ххх ><” и пробелам.
[:cntrl:]	Любые управляющие символы (например CTRL + C, CTRL + X)	.REG. [[:cntrl:]] соответствует 0x03, 0x08, но не «абв», 123, !@#.
[:blank:]	Знаки пробела и табуляции	.REG. [[:blank:]] соответствует символу пробела и символу табуляции, но не 123, «абв», !@#
[:punct:]	Знаки пунктуации	.REG. [[:punct:]] соответствует ; : ? ! ~ @ # $ % «&», «*», «‘», «“» и т. д. но не 123, «абв».

Элемент	Что это означает	Пример
[:lower:]	Любая буква нижнего регистра (Примечание. Параметр «Учитывать регистр» должен быть включен, в противном случае выражение будет функционально эквивалентно [:alnum:]).	.REG. [[:lower:]] соответствует «абв», «Деф», «сТресс», «До» и т. д., но не «АБВ», «ДЕФ», «СТРЕСС», «ДО», 123, !@#.
[:upper:]	Любая буква верхнего регистра (Примечание. Параметр «Учитывать регистр» должен быть включен, в противном случае выражение будет функционально эквивалентно [:alnum:]).	.REG. [[:upper:]] соответствует «АБВ», «ДЕФ», «СТРЕСС», «ДО» и т. д., но не «абв», «Деф», «Стресс», «До», 123, !@#.
[:xdigit:]	Цифры в шестнадцатеричном числе (0-9a-fA-F)	.REG. [[:xdigit:]] соответствует 0a, 7E, 0f и т. д.

Таблица D-6. Указатели шаблонов

Элемент	Что это означает	Пример
^	Означает начало строки	^(вопреки) соответствует любому фрагменту текста, который начинается с «вопреки». Так, предложение «вопреки тому, что я люблю овощи в супе» считается совпадением, но «тому, что я люблю овощи в супе, вопреки» — не считается.
$	Означает конец строки.	(вопреки)$ соответствует любому фрагменту текста, который заканчивается словом «вопреки». Так, предложение «вопреки тому, что я люблю овощи в супе» не будет считаться совпадением, но «тому, что я люблю овощи в супе, вопреки» — будет.

Таблица D-7. Управляющие последовательности и строковые константы

Элемент	Что это означает	Пример
\	Обозначение некоторых символов, имеющих специальное значение в регулярном выражении (например, «+»).	(1) .REG. C\\C\+\+ соответствует‘C \C++’. (2) .REG. * соответствует *. (3) .REG. \? соответствует ?.
\t	Обозначает знак табуляции.	(стресс)\t соответствует любому текстовому блоку, который содержит подстроку «стресс» сразу перед символом табуляции (ASCII 0x09).
\n	Обозначает начало новой строки. **Примечание** На разных платформах начало новой строки обозначается по-разному. В Windows это пара знаков — «возврат каретки» и «перевод строки». В Unix и Linux новая строка обозначается только символом перевода строки. В Macintosh новая строка обозначается только символом возврата каретки.	(стресс)\n\n соответствует любому фрагменту текста, в котором содержится подстрока «стресс», сразу за которой следуют два знака начала строки (0x0A в ASCII).
\r	Обозначает возврат каретки.	(стресс)\r соответствует любому текстовому блоку, который содержит подстроку «стресс» сразу перед одним символом возврата каретки (ASCII 0x0D).

Элемент	Что это означает	Пример
\b	Обозначает возврат на один символ со стиранием (backspace). OR Обозначает границы.	(stress)\b соответствует любому фрагменту текста, в котором содержится подстрока «stress», сразу за которой следует знак возврата на один символ со стиранием 0x08 в ASCII). Граница слова (\b) — это место между двумя символами, с одной стороны которого находится \w, а с другой — \W (в любом порядке), отсчитывая предполагаемые символы с начала или конца сроки как соответствующие \W (среди классов символов \b чаще обозначает backspace, чем границу слова). Например, следующее регулярное выражение может соответствовать номеру социальной страховки: .REG. \b \d{3}-\d{2}-\d{4}\b
\xhh	Обозначение символа ASCII с заданным шестнадцатеричным кодом (где hh обозначает двузначное шестнадцатеричное число).	\x7E(\w){6} соответствует любому фрагменту текста, в котором содержится ровно шесть буквенно-цифровых символов, перед которыми стоит тильда («~»). Поэтому находятся слова «~аб12вг», «~Ра3499», но не «~упс».

Генератор регулярных выражений

При определении параметров настройки правил для функции предотвращения потери данных имейте в виду, что генератор регулярных выражений может создавать только простые выражения в соответствии со следующими правилами и ограничениями.

- Переменными могут быть только буквы и цифры.

- Все остальные символы, такие как [-], [/] и так далее, могут быть только постоянными.
- Диапазоны переменных могут составлять только A-Z и 0-9; нельзя ограничивать диапазоны, например до A-D.
- В регулярных выражениях, создаваемых этим инструментом, учитывается регистр.
- Регулярные выражения, созданные при помощи данного средства, используются для поиска только положительных совпадений, но не отрицательных («если не совпадает»).
- Выражения на основе образца могут совпасть только с точно таким же количеством символов и пробелов, как и в образце. При помощи данного средства нельзя создавать шаблоны для поиска совпадения с «одним и более» из указанных символов или строк.

Сложный синтаксис выражений

Выражение с ключевым словом состоит из знаков — наименьших единиц сопоставления выражения с содержимым. Знак может быть оператором, логическим символом или операндом, то есть аргументом или значением, с которым работает оператор.

В число операторов входят .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., «.(.» и «.).». Операнд и оператор должны быть разделены пробелом. Кроме того, операнд может включать несколько знаков. См. *Ключевые слова на странице D-5*.

Использование регулярных выражений в работе

Следующий пример описывает работу фильтра по содержимому страховки, одного из фильтров по умолчанию.

[Format] .REG. \b\d{3}-\d{2}-\d{4}\b

Вышеуказанное выражение использует \b, символ возврата, за которым следует \d, любая цифра, затем {x}, обозначающий количество цифр, и, наконец, знак «-», обозначающий дефис. Этому выражению соответствует номер социального страхования. Нижеприведенная

таблица описывает строки, соответствующие данному регулярному выражению.

Таблица D-8. Числа, соответствующие регулярному выражению номера социального страхования

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Совпадения
333224444	Несовпадение
333 22 4444	Несовпадение
3333-22-4444	Несовпадение
333-22-44444	Несовпадение

При изменении выражения, как описано ниже,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

новое выражение соответствует следующей последовательности:

333 22 4444

Списки исключений из сканирования

Список исключений из сканирования для агентов Security Agent

Все программы компании Trend Micro внесены в список исключений и по умолчанию не сканируются.

Таблица D-9. Список исключений Security Agent

Название продукта	Путь установки
InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion` `ProgramDirectory=`

Название продукта	Путь установки
ScanMail eManager (ScanMail для Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Program Directory= C:\Program Files\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={диск для установки}:\INTERS~1
Плагин InterScan NSAPI	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=

Название продукта	Путь установки
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

Название продукта	Путь установки
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

Название продукта	Путь установки
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= Найдите путь к файлу exclusion.txt в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion\HomeDir Перейдите в каталог HomeDir (например, C:\Program Files\Trend Micro\Messaging Security Agent\). Откройте exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Списки исключений из сканирования для агентов Messaging Security Agent (только Advanced)

По умолчанию агент Messaging Security Agent, установленный на сервере Microsoft Exchange (2000 или более поздней версии), не сканирует базы данных Microsoft Exchange, файлы журналов Microsoft

Exchange, папки виртуального сервера и диск M. Список исключений хранится в:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

Остальные рекомендуемые папки Microsoft Exchange добавьте в список исключений вручную. См. http://support.microsoft.com/kb/245822/.

Исключения SBS 2003

Для SBS 2003 добавьте вручную следующее:

Исключения Microsoft Exchange	
База данных сервера Microsoft Exchange	`C:\Program Files\Exchsrvr\MDBDATA`
MTA-файлы Microsoft Exchange	`C:\Program Files\Exchsrvr\Mtadata`
Журналы отслеживания сообщений Microsoft Exchange	`C:\Program Files\Exchsrvr\server_name.log`
Microsoft Exchange SMTP Mailroot	`C:\Program Files\Exchsrvr\Mailroot`
Рабочие файлы Microsoft Exchange	`C:\Program Files\Exchsrvr\MDBDATA`
Служба репликации сайта	`C:\Program Files\Exchsrvr\srsdata`

	C:\Program Files\Exchsrvr\conndata
Исключения IIS	
Системные файлы IIS	C:\WINDOWS\system32\inetsrv
Папка сжатия IIS	C:\WINDOWS\IIS Temporary Compressed Files
Исключения контроллера домена	
Файлы базы данных Active Directory	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
Файлы базы данных NTFRS	C:\WINDOWS\ntfrs
Исключения служб Windows SharePoint	
Временная папка SharePoint	C:\windows\temp\FrontPageTempDir
Исключения папок Client Desktop	
Хранилище Windows	C:\WINDOWS\SoftwareDistribution\DataStore
Дополнительные исключения	
База данных съемных носителей (используется резервным копированием SBS)	C:\Windows\system32\NtmsData
Неотправленная почта коммуникатора SBS POP3	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
Входящая почта коммуникатора SBS POP3	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail

Хранилище Windows	`C:\WINDOWS\SoftwareDistribution\DataStore`
Хранилище базы данных DHCP	`C:\WINDOWS\system32\dhcp`
Хранилище базы данных WINS	`C:\WINDOWS\system32\wins`

Пакет обновления

Пакет обновления — набор критических обновлений, исправлений и новых функций, важных для обновления продукта. Обе версии (и Windows, и не-Windows) пакетов обновления имеют программу установки и сценарий установки.

Порт, используемый «троянскими конями»

Троянские порты обычно используются программами типа «троянский конь» для подключения к клиенты. Во время вирусной эпидемии Worry-Free Business Security блокирует порты со следующими номерами, которые могут быть использованы троянскими программами.

Таблица D-10. Троянские порты

Номер порта	Программа «троянский конь»	Номер порта	Программа «троянский конь»
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz

Номер порта	Программа «троянский конь»	Номер порта	Программа «троянский конь»
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Неизлечимые файлы

Модуль вирусного сканирования не может лечить следующие типы файлов.

Таблица D-11. Решения для неизлечимых файлов

Неизлечимый файл	Пояснение и решение
Файлы, зараженные троянскими программами	Троянские программы представляют собой программы, выполняющие непредсказуемые и несанкционированные действия вредоносного характера, такие как вывод сообщений, удаление файлов, либо форматирование дисков. Поскольку троянские программы не заражают файлы, их лечение не обязательно. Решение. Для удаления троянских программ используются механизм устранения ущерба и шаблон удаления повреждений.
Файлы, зараженные червями	Червь — это автономная программа (или группа программ), заражающая своими копиями или фрагментами другие клиент. Обычно черви распространяются через сеть или через вложения в сообщениях электронной почты. Черви не лечатся, так как являются автономными программами. Решение. Trend Micro рекомендует удалять червей.
Защищенные от записывания зараженные файлы	Решение. Снимите защиту от записи, чтобы разрешить лечение файла.
Файлы, защищенные паролем	Файлы, защищенные паролем (например, архивы или документы Microsoft Office, защищенные паролем). Решение. Снимите защиту паролем, чтобы разрешить лечение файла.
Резервные файлы	Файлы с расширениями RB0—RB9 являются резервными копиями зараженных файлов. В процессе лечения создаются копии зараженных файлов на случай их повреждения вирусом или вредоносной программой при лечении. Решение. При успешном лечении эти копии не понадобятся. На нормально работающем компьютере клиент резервный файл можно удалить.
Зараженные файлы в корзине	Работающая система может запретить удаление зараженного файла из корзины. Решение.

Неизлечимый файл	Пояснение и решение

	1. Перезагрузите клиент в режиме MS-DOS.
	2. Откройте приглашение командной строки.
	3. Для удаления файла введите следующее:
	`cd \`
	`cd recycled`
	`del *.* /S`
	Последняя команда удаляет все файлы в корзине.

Зараженные файлы во временных папках Windows или Internet Explorer.	Операционная система клиент может использовать файлы из временных папок Windows или Internet Explorer и поэтому запрещать их удаление. Эти файлы могут быть временными файлами, необходимыми для работы Windows.
	Решение.
	1. Перезагрузите клиент в режиме MS-DOS.
	2. Если зараженный файл находится во временной папке Windows, выполните следующие действия.
	a. Откройте командную строку и перейдите во временную папку Windows (путь по умолчанию: `C:\Windows\Temp`).
	b. Для удаления файла введите следующее:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	Последняя команда удаляет все файлы в папке Temp системы Windows.
	c. Перезапустите клиент в обычном режиме.
	3. Если зараженный файл находится во временной папке Internet Explorer, выполните следующие действия.
	a. Откройте командную строку и перейдите во временную папку Internet Explorer (путь по умолчанию: `C:\Users`

Неизлечимый файл	Пояснение и решение

	\<ваше имя пользователя>\AppData\Local \Microsoft\Windows\Temporary Internet Files).
	b. Для удаления файла введите следующее:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	Последняя команда удаляет все файлы в папке Temporary Internet Files.
	c. Перезапустите клиент в обычном режиме.

Сжатые файлы, использующие неподдерживаемый формат сжатия	Решение. Извлеките файлы из архива.
Заблокированные файлы или файлы, которые в данный момент выполняются	Решение. Разблокируйте файлы или дождитесь их выполнения.
Поврежденные файлы	Решение. Удалите файлы.

Индекс

A
AutoPcc.exe, 3-8, 3-12, 3-13

C
Client Packager, 3-9, 3-15, 3-16
    параметры, 3-15
    установка, 3-18
Conflicted ARP (конфликт протокола разрешения адресов), D-4

E
Early Boot Cleanup Driver, 8-9

F
Fragmented IGMP (фрагментированный протокол управления группами Интернет), D-5

I
IDS, D-4

L
Land Attack (атака на папку локальной сети), D-5

O
Overlapping Fragment (перекрывающиеся фрагменты), D-4

P
Ping of Death («смертельный» запрос), D-4
Plug-in Manager, 3-4

S
smart protection, 1-3
    Smart Protection Network, 1-3
Smart Protection Network, 1-3
smart scan, 5-5, 5-6
SYN Foold (синхронная атака), D-4

T
Teardrop (прорыв), D-5
Tiny Fragment Attack (атака малыми фрагментами), D-5
Too Big Fragment (слишком большой фрагмент), D-4

W
web reputation, 1-4, 3-4, 5-2
WFBS
    документация, xiv

А
Агент обновления, 3-4

Б
База данных IntelliTrap, 8-5
База данных контекстного сбора информации, 8-8
База данных контроля проверки программ, 8-11
База данных конфигурации контроля действий, 8-10
База данных обнаружения контроля действий, 8-10
База данных предотвращения эксплойтов браузера, 8-11
База данных применения политик, 8-11
База данных цифровых подписей, 8-11

База данных шпионских и нежелательных программ, 8-9
База исключений IntelliTrap, 8-5
брандмауэр
    преимущества, 5-32

В

веб-консоль, 2-4, 2-5
    информация, 2-4
    требования, 2-5
веб-страница установки, 3-7, 3-8
вероятный вирус/ вредоносная программа, 1-9
вирус/вредоносная программа, 1-9–1-11
    вероятный вирус/ вредоносная программа, 1-9
    Вирусы HTML, VBScript или JavaScript, 1-11
    Вирусы файлов .com и .exe, 1-10
    Вредоносный код ActiveX, 1-10
    Вредоносный код Java, 1-10
    загрузочный вирус (вирус загрузочного сектора), 1-10
    макровирус, 1-10
    Программа «троянский конь», 1-10
    программа-шутка, 1-9
    тестовый вирус, 1-11
    типы, 1-9–1-11
    упаковщик, 1-11
    червь, 1-11
Вирусная база данных, 8-5, 8-19
вирусы HTML, 1-11
вирусы JavaScript, 1-11
вирусы VBScript, 1-11
Вирусы файлов .com, 1-10
Вирусы файлов .exe, 1-10
Вредоносный код ActiveX, 1-10
Вредоносный код Java, 1-10

Д

действия при сканировании
    шпионские и нежелательные программы, 7-17
документация, xiv
Драйвер контроля действий, 8-10
дублирование компонентов, 8-14

З

загрузочный вирус, 1-10
задачи предварительной установки, 3-10, 3-19, 3-23
зашифрованные файлы, 14-19
защита внешних устройств, 8-10

И

интеллектуальная защита, 1-4
    Служба репутации файлов, 1-4
    Службы Web Reputation, 1-4
исправления, 8-12
исправления безопасности, 8-12

К

компоненты, 8-4
критические обновления, 8-12

М

макровирус, 1-10
Метод сканирования, 3-15
Механизм устранения ущерба, 8-7
Модуль вирусного сканирования, 8-6
Модуль контекстного сбора информации, 8-8

Модуль сканирования на наличие шпионских и нежелательных программ, 8-9

Н

Настройка сценария входа в сеть, 3-8, 3-12, 3-13
новые функции, 1-2

О

обнаружение руткитов, 8-10
обновление сервера
    дублирование компонентов, 8-14
    обновление вручную, 8-17
    обновление по расписанию, 8-17
Обработчик запросов контекстного сбора информации, 8-8
Общая база данных брандмауэра, 8-10
обычное сканирование, 5-5, 5-6
отзывы и предложения по документации, C-6

П

папка карантина, 5-20, 14-19
параметры DHCP, 3-26
поддержка
    более быстрое устранение проблем, C-4
Поддержка IPv6, B-2
    ограничения, B-3, B-4
    отображение адресов IPv6, B-7
политики безопасности
    сложность пароля
        требования, 6-65
поэтапное обновление, 8-14
Программа «троянский конь», 1-10
программа-шутка, 1-9
программы, 8-4

Р

Расширенная база данных сопоставления угроз, 8-9
Расширенный модуль сканирования нежелательных программ, 8-8
репутация файлов, 1-4

С

сетевые вирусы, 5-32
Система обнаружения вторжения, D-4
Сканер уязвимостей, 3-9, 3-22
    параметры DHCP, 3-26
    параметры пакетов, 3-33
    получение описания компьютера, 3-32
сканирование шпионских и нежелательных программ
    действия, 7-17
сложность пароля, 6-65
Служба контроля действий уровня ядра, 8-10
Службы Damage Cleanup Services, 3-4
Способы установки Security Agent, 3-7

Т

тестовый вирус, 1-11
тестовый скрипт EICAR, 1-11
типы сканирования, 3-4
Троянская программа, 8-7

У

угрозы безопасности, 1-12

шпионские и нежелательные программы, 1-12
удаление
с помощью программы удаления, 3-45
удаленная установка, 3-8
Унифицированная база данных анализатора сценариев, 8-12
упаковщик, 1-11
Установка Security Agent
с веб-консоли, 3-19
установка клиента
Client Packager, 3-15
использование сканера уязвимостей, 3-22
Настройка сценария входа в сеть, 3-12

Ф

Функция ActiveAction, 7-18

Ч

червь, 1-11

Ш

Шаблон механизма восстановления, 8-11
Шаблон Устранение повреждений, 8-7
шпионские и нежелательные программы, 1-12
adware (рекламная программа), 1-12
spyware («шпионские» программы), 1-12
программы для взлома паролей, 1-12
программы для набора номера, 1-12
программы для удаленного доступа, 1-12
программы-шутки, 1-12
хакерские инструменты, 1-12

Э

Энциклопедия вирусов, 1-9

TREND MICRO INCORPORATED

Тренд Микро (ЕМЕА) ул. Б.Никитская, 12-12/А1 стр.1 Лимитед (Филиал), 125009 Россия

Телефон: +7 (495) 988-89-22 Факс: +7 (495) 988-29-10 info@trendmicro.com

www.trendmicro.com

Item Code: WFRM108704/190701