GFI WebMonitor 4 for ISA Server

Руководство

GFI Software

http://www.gfi.ru/
E-mail: info@gfi.ru

Версия 4.0 – последнее обновление 25 февраля 2008 г.

Содержание

Введение

Ознакомление с GFI WebMonitor

GFI WebMonitor – это комплексное средство мониторинга, дополняющее функциональность Microsoft ISA Server для обеспечения возможности контроля и фильтрации сетевого трафика пользователей (серфинга и загрузок) в режиме реального времени. Кроме этого, система позволяет блокировать соединения, а также проверять трафик на наличие вирусов, троянов, шпионских программ и фишинга.
Это идеальное решение для прозрачного контроля привычек пользователей. Решение также позволяет обеспечить соответствие регулятивным нормам без вмешательства пользователей.

Версии

GFI WebMonitor 4 поставляется в трех версиях. Каждая версия отвечает различным требованиям системных администраторов:
Версия WebFilter: Фильтрация веб-трафика и веб-сайтов в соответствии с встроенной базой данных WebGrade. Это настраиваемая база данных классификации сайтов, определяющая доступ по пользователю/группе/IP-адресу/времени.
Версия WebSecurity: Обеспечение высокой степени защиты веб-трафика. Это достигается благодаря встроенному модулю контроля и множественным антивирусным механизмам, а также модулям поиска шпионских программ.
Версия UnifiedProtection: Это WebFilter и
и WebSecurity в одном пакете.

Как работает GFI WebMonitor?

Функции GFI WebMonitor можно разбить на четыре логических шага:

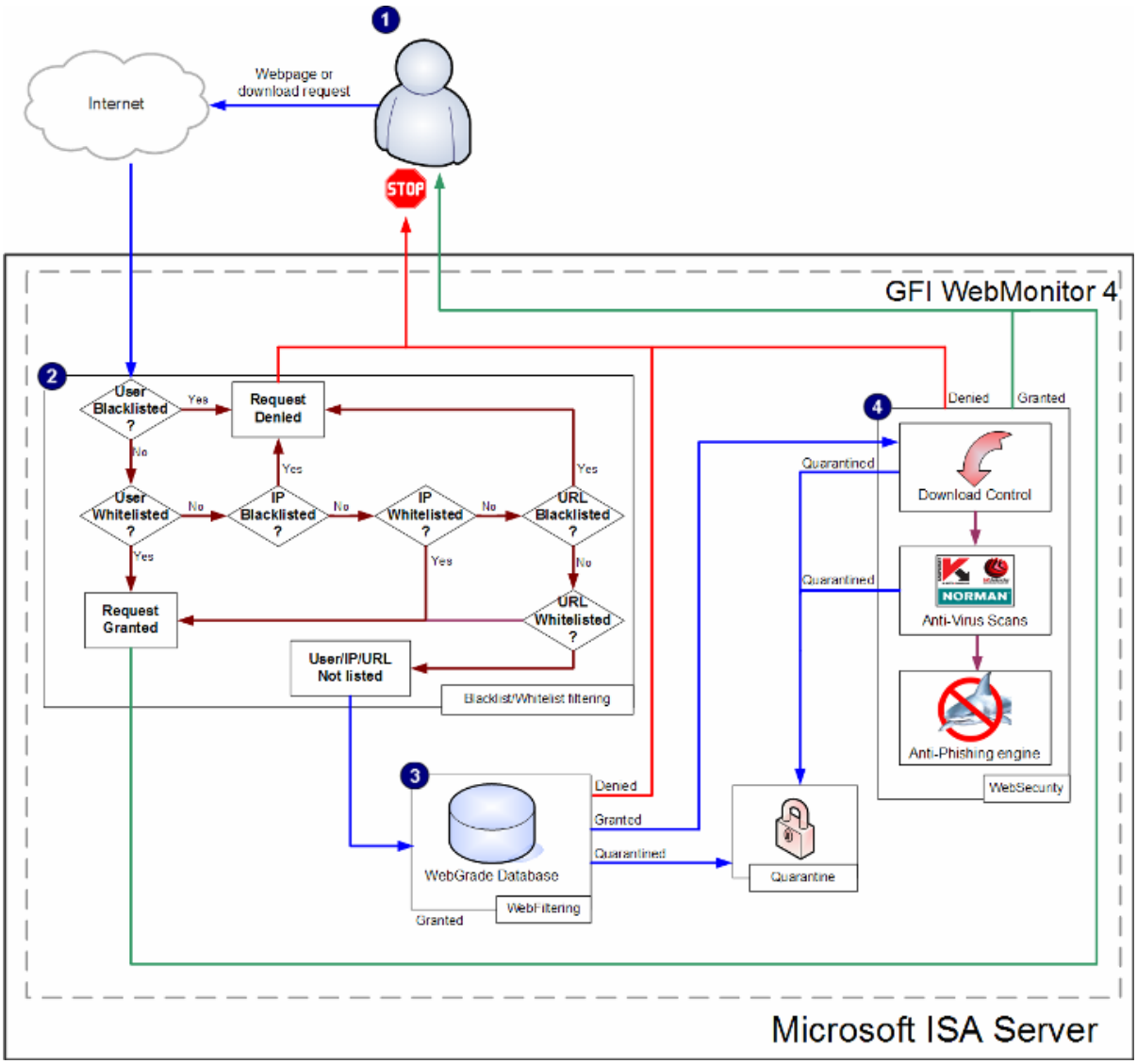


Рис. 1 - Как работает GFI WebMonitor?

Этап 1 – инициализация запроса: на этом этапе пользователи запрашивают веб-страницу или загрузку через Интернет. Входящий трафик, сгенерированный запросом пользователя, принимается Microsoft ISA Server, который в свою очередь передает весь полученный трафик GFI WebMonitor (запросы веб-страниц, загрузки изображений, загрузки файлов).

Этап 2 - фильтрация по «черному» и «белому» спискам: этот этап включает внутренний механизм фильтрации по «черному» и «белому» спискам GFI WebMonitor, который анализирует идентификаторы пользователей, исходящий IP-адрес и запрошенный URL.

- Веб-трафик, запрошенный помещенными в «черный» список пользователями и IP-адресами или от помещенных в «черный» список URL-адресов, немедленно отклоняется.
- Веб-трафик, запрошенный помещенными в «белый» список пользователями и IP-адресами, или от помещенных в «белый» список URL-адресов, автоматически получает доступ и направляется пользователю.
- Запросы, не помещенные ни в «черный», ни в «белый» список, направляются для обработки модулю WebFilter.

Этап 3 - модуль WebFilter: Модуль WebFilter анализирует некатегоризированный трафик сети, полученный от механизма фильтрация по «черному» и «белому» спискам категоризированных веб-сайтов. Веб-трафик отклоняется или разрешается согласно политикам, установленным в соответствии с категориями веб-сайтов, включенных в базу данных WebGrade.

Политики могут быть настроены на направление трафика на карантин; чтобы системные администраторы позже могли одобрить/отклонить трафик согласно потребностям и требованиям. Если изолированный веб-трафик одобрен вручную, изолированный URL-адрес помещается во временный «белый» список, так чтобы у пользователей был доступ к этому ресурсу.

ПРИМЕЧАНИЕ: Модуль WebFilter только доступен только в версии WebFilter и версии UnifiedProtection GFI WebMonitor. В случае использования версии WebSecurity веб-трафик непосредственно направляется от фильтров по «черному» и «белому» спискам к модулю WebSecurity.

Этап 4 - модуль WebSecurity: Модуль WebSecurity анализирует веб-трафик проходящий через модуль управления загрузкой и сканирует входящий материал на вирусы, шпионское ПО и другой вредоносный код. Зараженный материал автоматически отклоняется или изолируется на основе политик.
Веб-трафик также проверяется на наличие фишинга в соответствии с обновляемой базой данных. При обнаружении фишинга данные автоматически блокируются. Одобренные данные отправляются пользователю через ISA Server.

ПРИМЕЧАНИЕ: Модуль WebSecurity доступен только в версии WebSecurity и версии UnifiedProtection GFI WebMonitor. В случае использования версии WebFilter веб-трафик передается пользователю, не проходя процессы, включенные в модуль WebSecurity.

Основные функции

- GFI WebMonitor включает следующие функции:
- Контроль веб-активности в режиме реального времени.
- Немедленное блокирование веб-доступа и загрузок в процессе.
- Защита веб-трафика с помощью множественных и обновляемых антивирусных механизмов и антишпионского ПО.
- Тесная интеграция с Microsoft ISA Server в качестве веб-фильтра.
- Без дублирования функциональных возможностей Microsoft ISA Server.
- Простая установка с минимальными требованиями к конфигурации.
- Проверка сигнатуры типа файла – файлы с переименованными расширениями автоматически распознаются.
- Уведомления о важных событиях по электронной почте.
- Современная база данных WebGrade обеспечивает проверку всех запросов веб-сайта по обширной базе данных.
- Политики контроля загрузок.
- «Белый» и «черный» списки URL-адресово, пользователей и IP-адресов, отменяющие политики WebFilter и WebSecurity.
- Отчеты по использованию трафика по пользователям/веб-сайтам.
- Карантин опасных файлов и содержимого.

- Веб-интерфейс.

Схема лицензирования GFI WebMonitor

GFI WebMonitor 4 основан на подписке с функциями, которые становятся недоступными, когда подписка заканчивается.

В таблице ниже указано, какие функции будут доступны в определенной версии, и будут ли эти функции доступны по истечении подписки.

Функция	Версия	Подписка с истекающим сроком
Мониторинг	Все версии	Доступно
«Белый» список	Все версии	Не доступно
«Черный» список	Все версии	Не доступно
Политики веб-фильтрации	Версия WebFilter	Не доступно
Мониторинг трафика	Версия WebFilter	Не доступно
Политики управления загрузкой	Версия WebSecurity:	Не доступно
Политики поиска вирусов и шпионского ПО	Версия WebSecurity:	Доступно без обновлений
Обновления антивируса	Версия WebSecurity:	Не доступно
Механизмы антифишинга	Версия WebSecurity:	Не доступно
Карантин	Все версии	Доступно
Создание отчетов	Все версии	Доступно

Истечение лицензии

Лицензии на GFI WebMonitor 4 истекают по двум причинам:

- Окончание подписного периода
- Превышение количества пользователей

При превышении количества пользователей, системным администраторам предоставляется 15-дневный льготный период, в течение которого они должны приобрести новые лицензии. По истечении льготного периода все функции GFI

WebMonitor 4 (за исключением мониторинга и антивирусного сканирования) блокируются.

Оценка продукта GFI WebMonitor

Вы можете загрузить и испытать полную версию GFI WebMonitor 4 без ключа в течение 10 дней. Однако вы можете попросить 30-дневный ключ продукта, заполнив соответствующую форму на веб-сайте GFI. Кроме этого, бесплатно предоставляется техническая поддержка по электронной почте. 30-дневный ключ для оценки будет выслан по электронной почте после загрузки продукта. В процессе оценочного периода все функции GFI WebMonitor 4 будут доступны.

Установка GFI WebMonitor

Введение

Эта глава предоставляет информацию, относящуюся к установке GFI WebMonitor 4

Системные требования

Установите GFI WebMonitor на компьютерах, которые отвечают следующим аппаратным и программным системным требованиям:

WebFilter Edition – минимальные аппаратные требования

- Процессор: 1,8 ГГц
- ОЗУ: 1 ГБ
- Жесткий диск: 2 ГБ доступного пространства

WebSecurity Edition – минимальные аппаратные требования

- Процессор: 1,8 ГГц
- ОЗУ: 1 ГБ
- Жесткий диск: 10 Гбайт доступного пространства

GFI WebMonitor UnifiedProtection Edition – минимальные аппаратные требования

- Процессор: 1,8 ГГц
- ОЗУ: 2 ГБ
- Жесткий диск: 12 Гбайт доступного пространства

ПРИМЕЧАНИЕ: Спецификации размера жесткого диска для каждой версии необходимы для установки и управления GFI WebMonitor. Во внимание принимается кэш загрузок, пространство, необходимое для сканирования и файлы истории. Однако это только показательно; возможно, вам потребуется распределить дополнительное дисковое пространство в зависимости от среды и количества контролируемых пользователей.

Программные требования – все версии

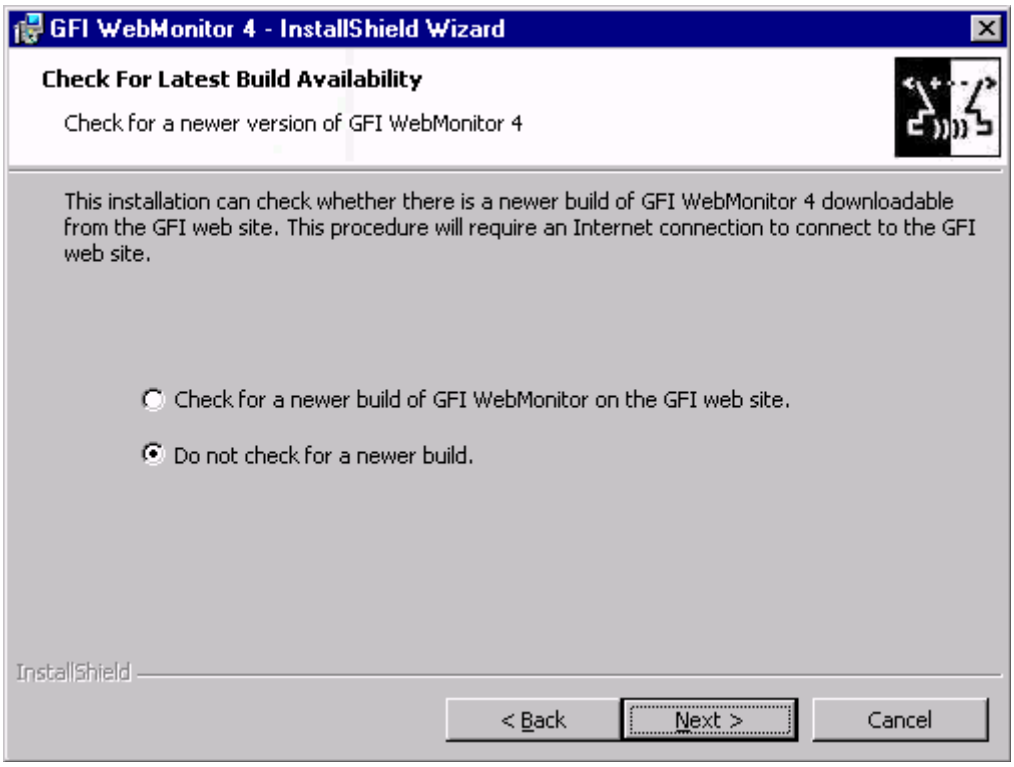
- Операционная система Windows 2000 Server (SP4) или Windows 2003
- Microsoft ISA Server 2004 (SP3) или выше
- Microsoft Internet Explorer 6 или выше
- .NET framework 2.0

ПРИМЕЧАНИЕ: GFI WebMonitor может быть установлен только на машине с Microsoft ISA Server.

Процедура установки

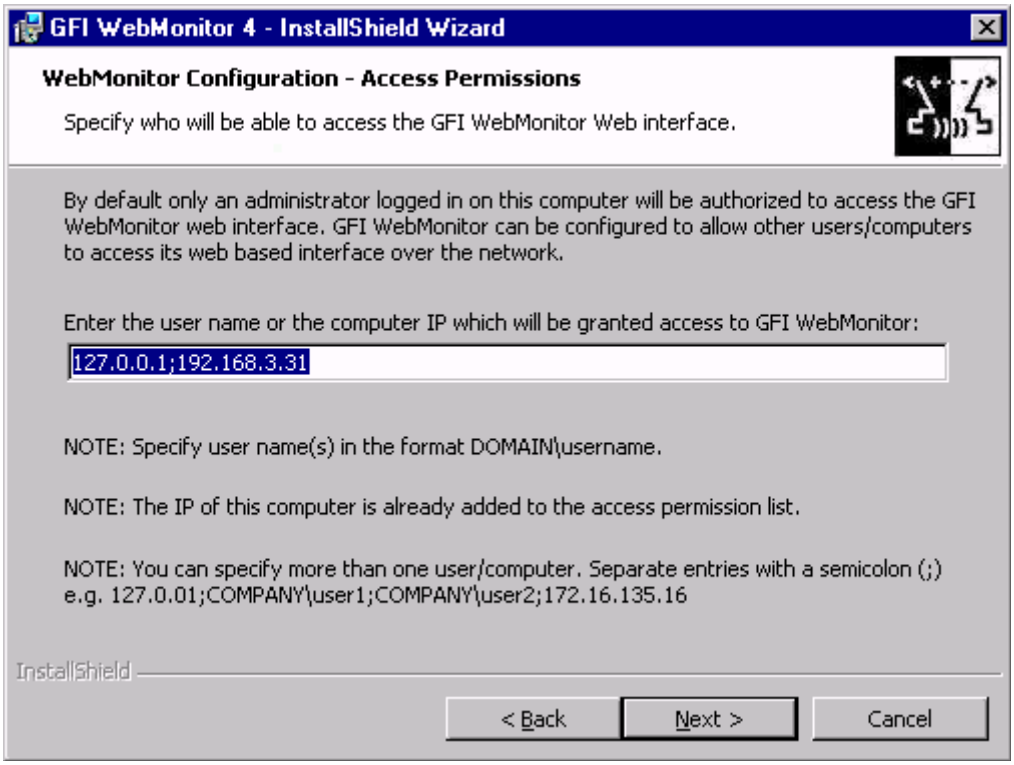
Чтобы установить GFI WebMonitor 4:

1. Дважды щелкните webmonitor4.exe и нажмите Next (Далее).
2. Выберите, требуется ли более новая версия GFI WebMonitor 4 и нажмите кнопку Next (Далее).



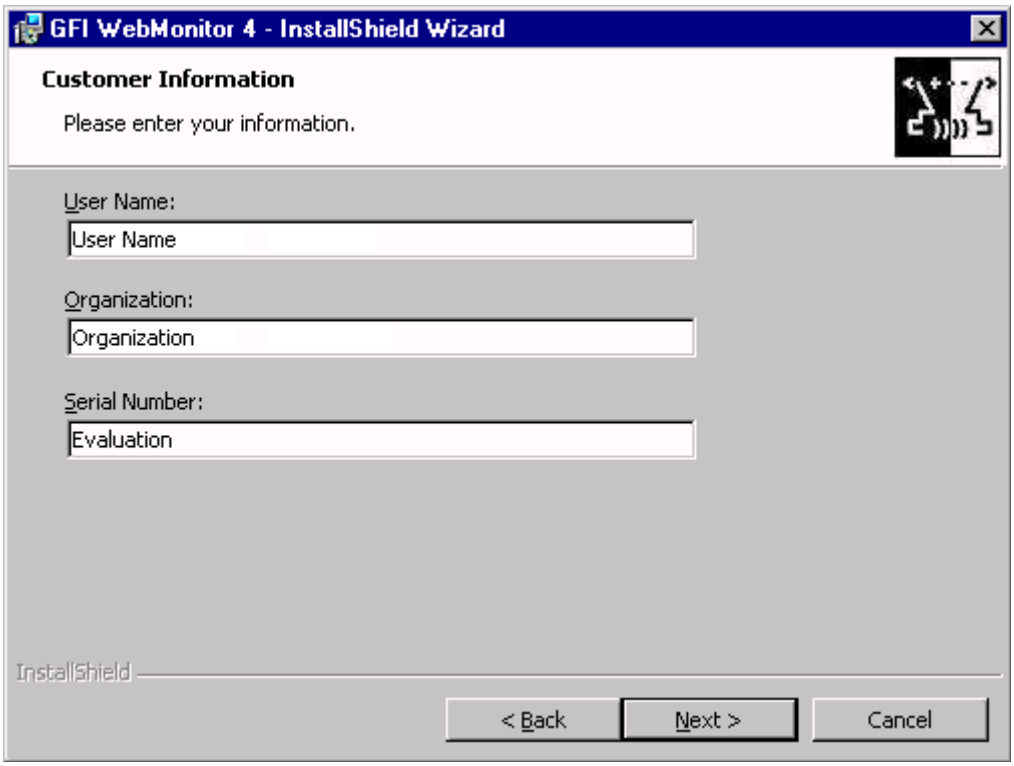
Снимок 1 – Поиск более новой версии GFI WebMonitor

3. Тщательно прочтите лицензионное соглашение. Чтобы продолжить установку, выберите I accept the terms in the license agreement (я принимаю условия лицензионного соглашения) и нажмите Next (Далее).



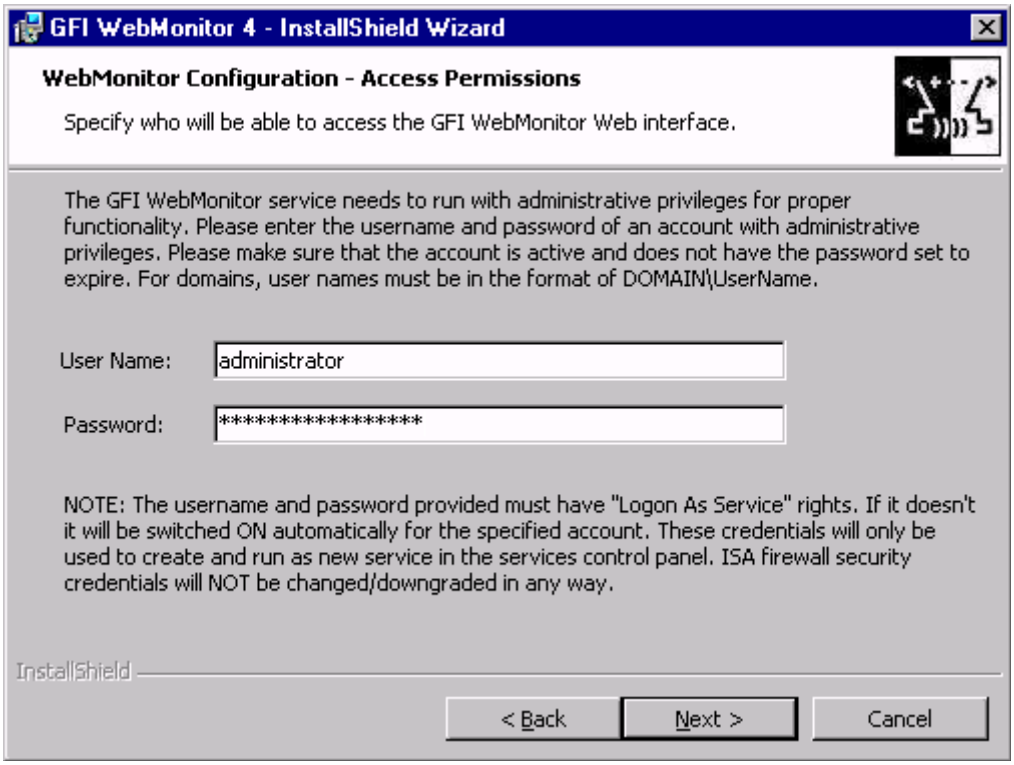
Снимок 2 – разрешения на доступ GFI WebMonitor

4. Определите имя пользователя или IP-адрес, которому будет предоставлен доступ к веб-интерфейсу GFI WebMonitor и нажмите Next (Далее).



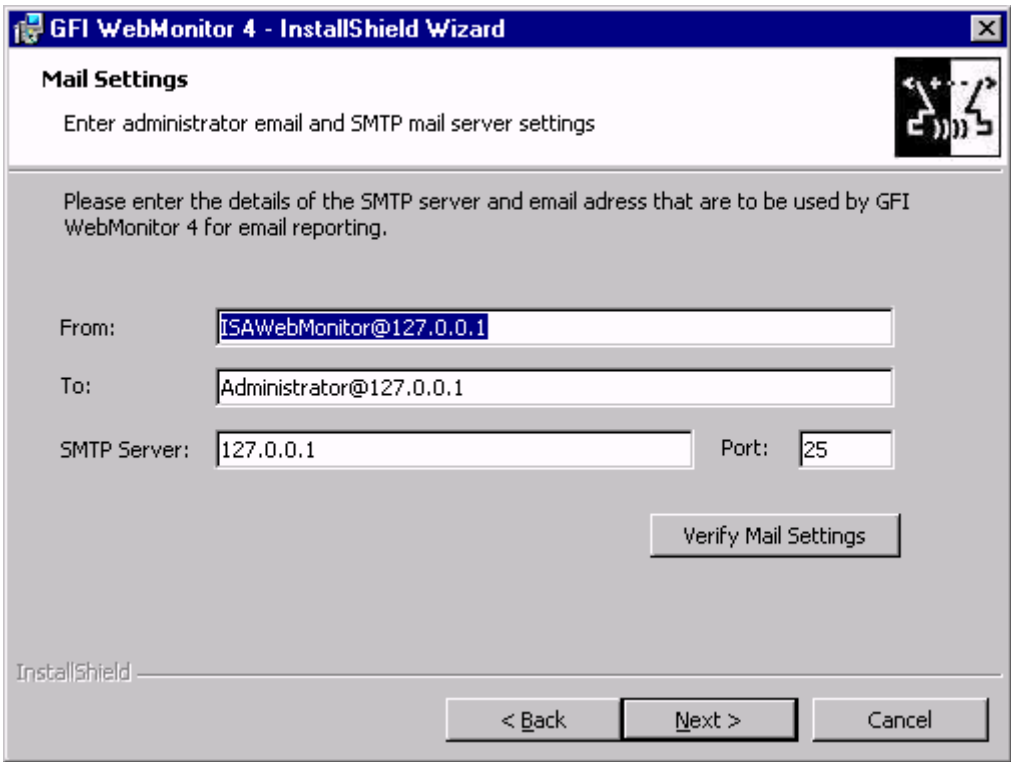
Снимок 3 – лицензионные сведения GFI WebMonitor

5. Введите имя пользователя, организацию и лицензионный ключ. Если вы хотите оценивать продукт в течение 10 дней, оставьте оценочный ключ, заданный по умолчанию. Нажмите кнопку Next (Далее).



Снимок 4 – учетные данные GFI WebMonitor

6. Введите учетные данные, которые будут использоваться для запуска сервиса GFI WebMonitor. Нажмите кнопку Next (Далее).



Снимок 5 – параметры настройки почтового сервера SMTP GFI WebMonitor

7. Введите параметры почтового сервера SMTP и адрес электронной почты для уведомления администратора. Нажмите кнопку Next (Далее).
8. Задайте альтернативный установочный путь или нажмите Next (Далее) для использования пути по умолчанию.
9. Нажмите Install (Установка), чтобы завершить установку.

Запуск GFI WebMonitor

После установки выберите GFI WebMonitor: Пуск > Программы > GFI WebMonitor > GFI WebMonitor.

Альтернативно, веб-консоль GFI WebMonitor можно запустить через веб-обозреватель, используя URL-адрес или IP-адрес, который указывает на дистрибутив WebMonitor GFI на ISA Server.

Пример: http://<IP-адрес_isa-сервера>:1007

Загрузка базы данных WebGrade

По умолчанию, база данных WebGrade не включена в установочный пакет WebMonitor GFI. После установки GFI WebMonitor загружается и устанавливается новейшая версия базы данных.

Загрузка антивирусных сигнатур

По умолчанию антивирусные сигнатуры не включены в установочный пакет WebMonitor GFI. После установки GFI WebMonitor автоматически загружаются и устанавливается новейшие сигнатуры для поддерживаемых механизмов сканирования.

Обновление предыдущей версии

Основные операционные и обрабатывающие технологии, на которых построен GFI WebMonitor 4, отличаются от предыдущих версий GFI WebMonitor. Поэтому предыдущие версии не могут быть импортированы в GFI WebMonitor 4.

Навигация в консоли GFI WebMonitor

Введение

Консоль WebMonitor's GFI – это веб-интерфейс, через который можно управлять любым аспектом его функциональных возможностей. С его помощью можно контролировать, блокировать и предоставлять доступ ко всему сетевому трафику сети.

Навигация в пользовательской консоли GFI WebMonitor

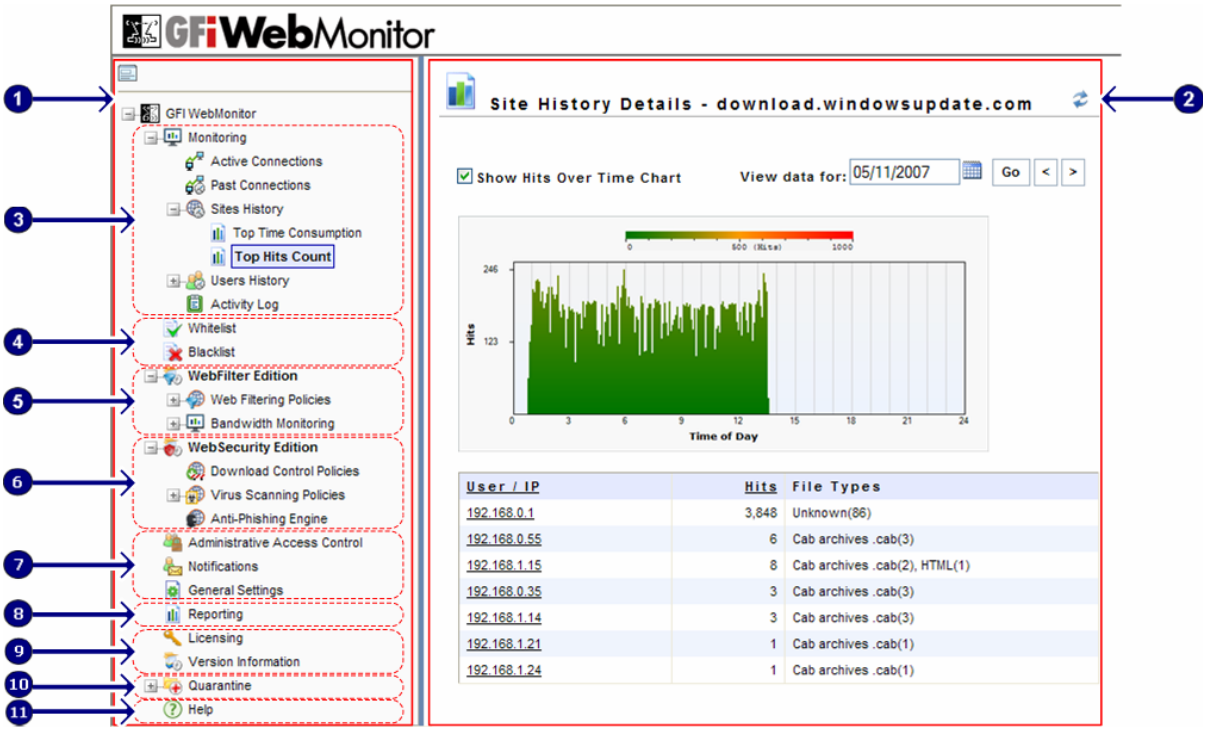


Рисунок 2 – Навигация в консоли GFI WebMonitor

1	Панель навигации – позволяет просматривать и использовать все функциональные возможности GFI WebMonitor.
2	Панель просмотра – позволяет просматривать веб-статистику, текущий и прошлый веб-трафик, а также параметры настройки GFI WebMonitor.
3	Узел мониторинга – обеспечивает доступ к функциям мониторинга веб-трафика GFI WebMonitor.
4	Узел «черный»/«белый» список – обеспечивает доступ к функциям «черного» и «белого» списков GFI WebMonitor.
5	Узел WebFilter– обеспечивает доступ к функциям WebFilter из GFI WebMonitor. А также доступ к параметрам настройки базы данных WebGrade.
6	Узел WebSecurity – обеспечивает доступ к функциям WebSecurity

	из GFI WebMonitor. А также доступ к различным экранам настройки параметров антивируса и управления загрузками.
7	Узел настройки – обеспечивает доступ ко всем функциям настройки и управления GFI WebMonitor. Включает управление доступом, настройкой уведомлений и общими настройками параметров.
8	Узел отчетов – обеспечивает доступ конфигурации создания отчетов из GFI WebMonitor.
9	Узлы лицензирования – обеспечивает доступ к управлению лицензией и информацией о версии.
10	Узел карантина – обеспечивает доступ к элементам, заблокированным GFI WebMonitor. Они располагаются в зависимости от времени блокирования.
11	Узел справки – обеспечивает доступ к справочной информации по всем аспектам функциональности GFI WebMonitor.

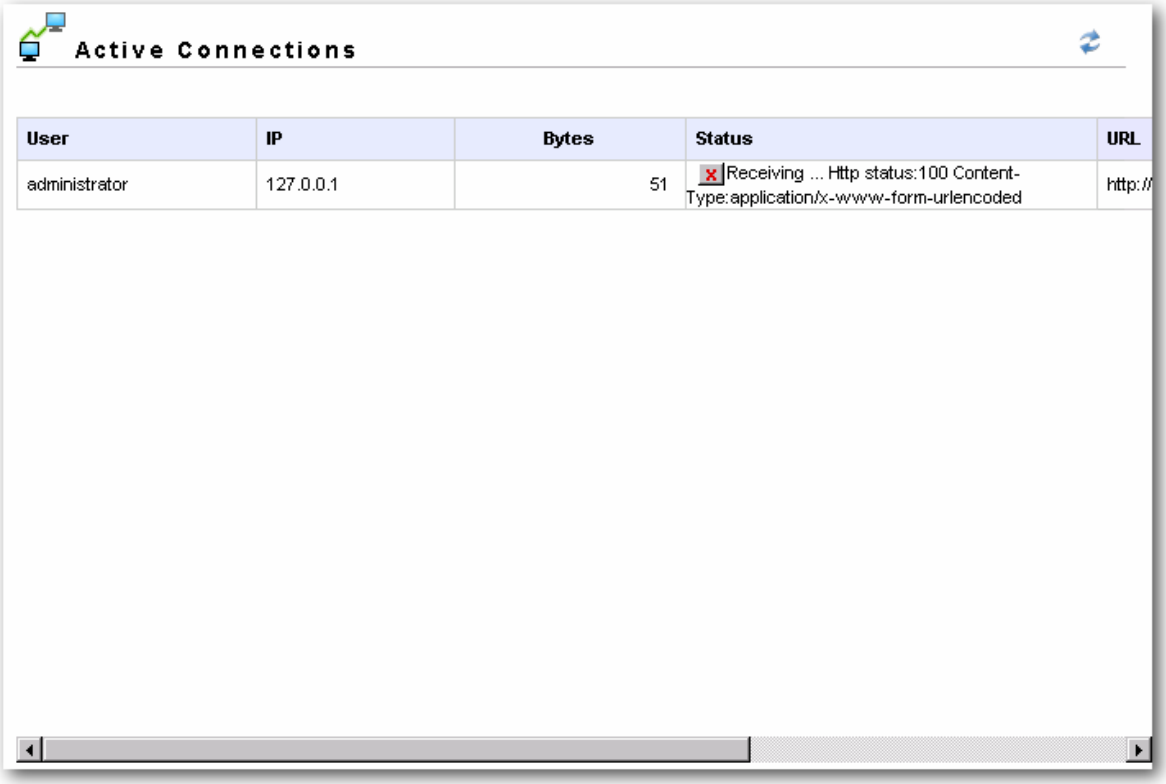
Начало работы: мониторинг Интернет-активности

Введение

С помощью узла мониторинга и его подузлов можно проверять текущие и прошлые веб-запросы, собранные и обработанные сервером Microsoft ISA. Через эти узлы можно просматривать данные, относящиеся к:

- Активным подключениям
- Последним подключениям
- Истории посещений сайтов
- Истории по пользователям
- Журналу регистрации активности

Активные соединения



Снимок 6 – Активные соединения

Доступ к представлению Active Connections (Активные соединения) осуществляется щелчком Monitoring Active Connections (Мониторинг активных соединений) в панели навигации.

В представлении «Активные соединения» отображается информация, связанная со всеми текущими активными TCP-соединениями, обработанными Microsoft ISA Server. Отображаемая информация включает:

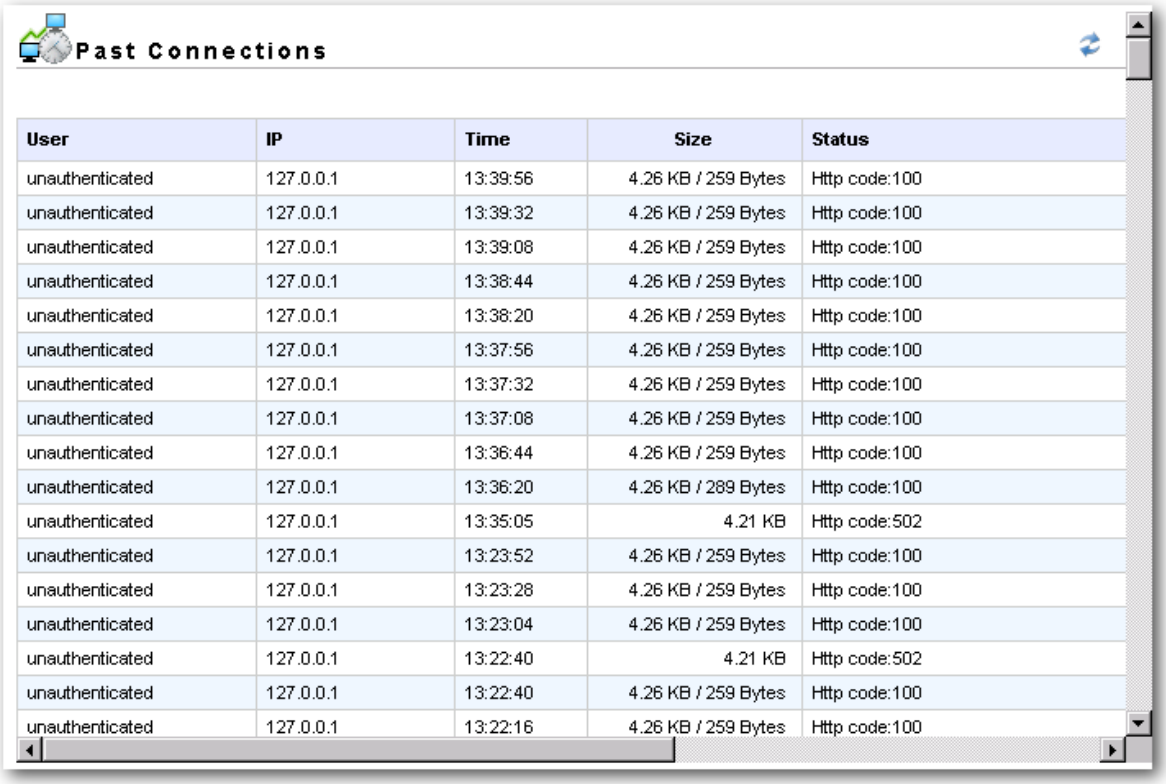
- Имя пользователя
- IP источника
- Получено/отправлено байт
- Детали соединения, такие как направление трафика и тип файла
- Данные о запрашиваемом URL-адресе

Через это представление можно прервать активные соединения с Интернетом. (например, прервать загрузку файла, потребляющую слишком много трафика). Чтобы прервать соединение, нажмите кнопку в столбце Status (Состояние) и загрузка будет прекращена.

ПРИМЕЧАНИЕ 1: Когда используется аутентификация ISA Server, имя пользователя учетной записи Windows будет отображено в столбце User (Пользователь). В другом случае имя пользователя отображается как неопределенное.

ПРИМЕЧАНИЕ 2: Отображаемая информация не обновляется автоматически. Чтобы обновить отображаемую информацию, щелкните кнопку обновления.

Последние соединения



User	IP	Time	Size	Status
unauthenticated	127.0.0.1	13:39:56	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:39:32	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:39:08	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:38:44	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:38:20	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:37:56	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:37:32	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:37:08	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:36:44	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:36:20	4.26 KB / 289 Bytes	Http code:100
unauthenticated	127.0.0.1	13:35:05	4.21 KB	Http code:502
unauthenticated	127.0.0.1	13:23:52	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:23:28	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:23:04	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:22:40	4.21 KB	Http code:502
unauthenticated	127.0.0.1	13:22:40	4.26 KB / 259 Bytes	Http code:100
unauthenticated	127.0.0.1	13:22:16	4.26 KB / 259 Bytes	Http code:100

Снимок 7 – Последние соединения

Доступ к представлению «Последние соединения» осуществляется щелчком Monitoring Past Connections (Мониторинг последних соединений) в панели навигации.

Представление последних соединений показывает последние 2000 соединений, обработанных Microsoft ISA Server. Отображаемая информация включает:

- Имя пользователя
- IP источника
- Время доступа к URL-адресу
- Получено/отправлено байт
- Подробности соединения, такие как тип файла
- Подробности доступа к URL-адресам

Информация отсортирована по времени, с последним URL-адресом сверху.

ПРИМЕЧАНИЕ 1: Когда используется аутентификация ISA Server, имя пользователя учетной записи Windows отображается в столбце User (Пользователь). В другом случае имя пользователя отображается как неопределенное.

ПРИМЕЧАНИЕ 2: Отображаемая информация не обновляется автоматически. Чтобы обновить отображаемую информацию, щелкните кнопку обновления.

История посещений сайтов

Узел Sites Histiory (История посещения сайтов) позволяет идентифицировать:

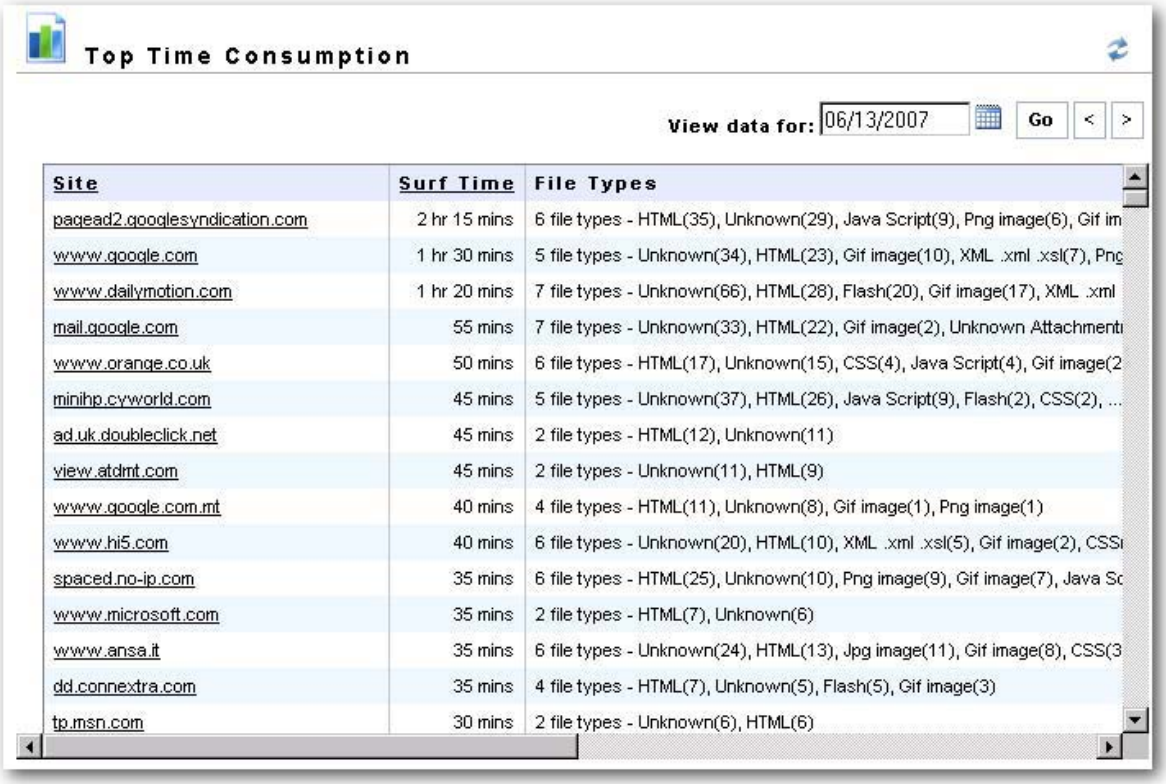
- Сайты, наиболее часто посещаемые сетевыми пользователями
- Полное время просмотра по каждому сайту.

Наибольшие затраты по времени

В представлении Top Time Consumption (Наибольшие затраты по времени) перечислены сайты, на которых сетевые пользователи провели большинство времени, по определенной дате. Отображаемая информация включает:

- Сайты, к которым осуществлялся доступ
- Время, потраченное на просмотр каждого сайта
- Типы файлов, к которым обращались с каждого сайта
- Пользователи/IP-адреса, которые обращались к сайту.

Список может быть отсортирован в алфавитном порядке по сайтам в порядке возрастания, или по проведенному времени в порядке убывания (сайт, на который было затрачено большинство времени сверху).



Снимок 8 История посещения сайтов: Наибольшие затраты по времени

Доступ к представлению Top Time Consumption (Наибольшие затраты по времени)» осуществляется щелчком Sites History > Top Time Consumption (История посещения сайтов > Наибольшие затраты по времени) в панели навигации.

По умолчанию, в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и нажмите Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, появится сообщение об ошибке.

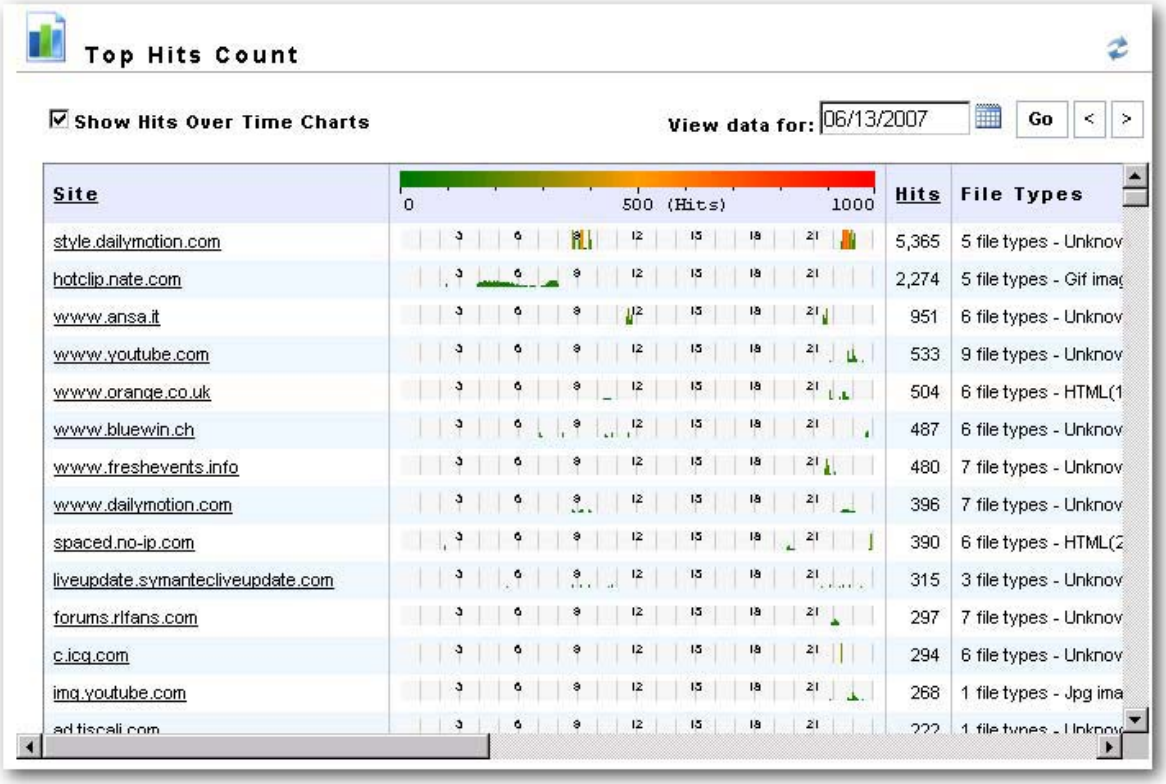
Вы можете также щелкнуть любой из сайтов в списке, чтобы открыть представление Site History Details (Детальная история посещений сайтов). Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Количество запросов

В представлении Top Hits Count (Количество запросов) перечислены сайты, наиболее часто запрашиваемые пользователями за определенную дату. Отображаемая информация включает:

- Запрашиваемые сайты
- Количество обращений к каждому сайту (то есть, количество запросов)
- Типы запрашиваемых с каждого сайта файлов
- Пользователи/IP-адреса, которые обращались к сайту
- Графические представления запросов сайта по времени

Список может быть отсортирован в алфавитном порядке в порядке возрастания, по сайтам, или в порядке убывания по популярности (сайт с наибольшим числом обращений вверху).



Снимок 9 – История посещений сайтов: Количество запросов

Доступ к представлению «Количество запросов» осуществляется щелчком Sites History > Top Time Consumption (История посещения сайтов > Количество запросов) в панели навигации.

Для графического отображения запросов по времени выберите Show Hits Over Time Charts (Графическое отображение запросов).

По умолчанию в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и щелкните Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, отображается сообщение об ошибке.

Вы можете также нажать на любой из перечисленных сайтов, чтобы просмотреть детальную историю посещений сайтов. Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

История по пользователям

В представлении Users History (История по пользователям) представлены детальные данные по пользователям, которые провели большую часть времени, просматривая сайты, и данные о сайтах, к которым наиболее часто обращались. Подузел Users History (История по пользователям) разделен на два подузла:

- Наиболее активные пользователи
- Количество запросов

Наиболее активные пользователи

Снимок 10 – История по пользователям: Наиболее активные пользователи

Доступ к представлению «Наиболее активные пользователи» осуществляется выбором Users History > Top Surfers (История пользователей > Наиболее активные пользователи) в панели навигации.

В представлении «Наиболее активные пользователи» отображается время, проведенное сетевыми пользователями, по определенной дате. Отображаемая информация включает:

- Пользователи/IP, которые просматривали сайты

- Время, затраченное на просмотр сайтов
- Сайты, к которым обращался каждый пользователь

Список может быть отсортирован по пользователю/IP-адресу в алфавитном порядке, по возрастанию, или по времени, проведенному, затраченному на просмотр сайтов, по убыванию (сайт, на который было затрачено наибольшее количество времени, расположен вверху).

- Чтобы отсортировать элементы по пользователю/IP-адресу, щелкните заголовок столбца User/IP (Пользователь/IP-адрес).
- Чтобы отсортировать элементы по времени, затраченному на просмотр сайтов, щелкните заголовок столбца Surf Time (Время в сети).

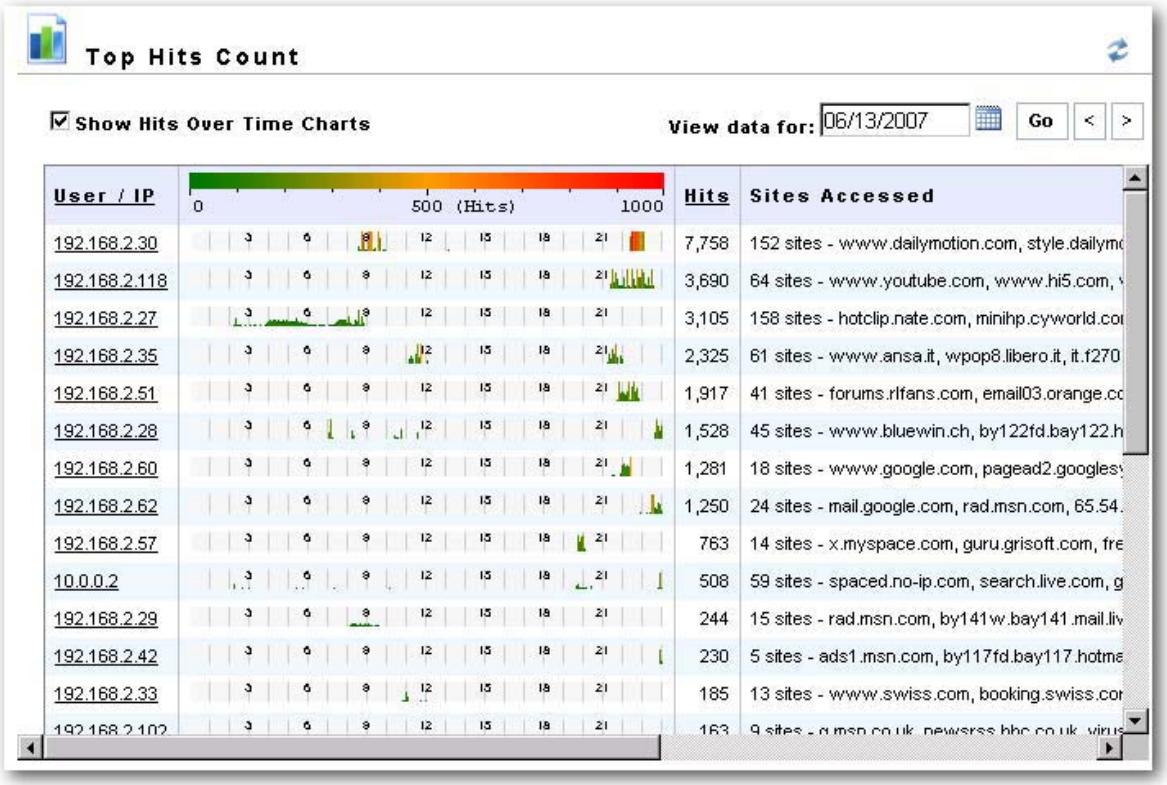
По умолчанию в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и нажмите Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, отображается сообщение об ошибке.

Вы можете также щелкнуть любого пользователя/IP-адрес, чтобы просмотреть User History Details (Детальная история по пользователям). Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Количество запросов



Снимок 11 – История по пользователям Количество запросов

Доступ к представлению «Количество запросов» осуществляется щелчком Sites History > Top Hits Count (История по пользователям > Количество запросов) в панели навигации.

В представлении «Количество запросов» отображаются пользователи с самым высоким количеством доступов к сайтам, по определенной дате. Отображаемая информация включает:

- Пользователи/IP-адреса, которые просматривали сайты
- Количество доступов к сайтам по каждому пользователю
- Сайты, к которым обращался каждый пользователь
- Графические представления запросов сайта по времени

Список может быть отсортирован по пользователям/IP-адресам в порядке возрастания, или по доступам к сайтам в порядке убывания (пользователь с наибольшим количеством доступов к сайтам сверху).

- Чтобы отсортировать элементы по пользователю/IP-адресу, щелкните заголовок столбца User/IP (Пользователь/IP-адрес).
- Чтобы отсортировать по доступам к сайтам, нажмите на заголовок столбца Hits (Запросы).

Чтобы графически отобразить запросы по времени для каждого из перечисленных сайтов, установите флажок Show Hits Over Time Charts. Диаграммы помогают идентифицировать время доступа к сайтам по каждому пользователю.

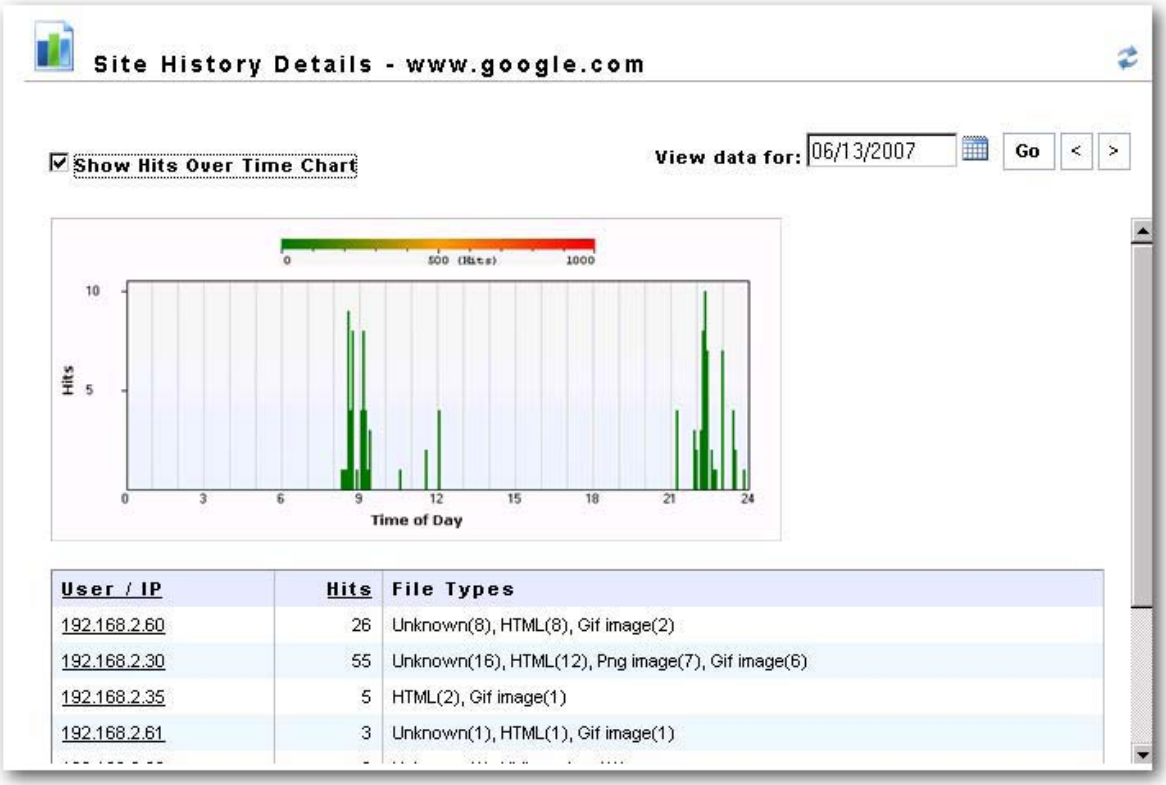
По умолчанию в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и нажмите Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, отображается сообщение об ошибке.

Вы можете также щелкнуть любого пользователя/IP-адрес, чтобы просмотреть User History Details (Детальная история по пользователям). Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Детальная история посещения сайтов



Снимок 12 – Детальная история посещения сайтов

Доступ к представлению Site History Details (Детальная история посещения сайтов) осуществляется щелчком Sites History (История посещений сайтов) (Top Time Consumption или Top Hits Count) из панели навигации. Из панели представления выберите один из перечисленных сайтов в столбце Site (Сайт).

В этом представлении отображается следующая информация:

- Все пользователи/IP-адреса, которые обращались к этому сайту по указанной дате
- Количество доступов к сайту по каждому пользователю
- Типы запрашиваемых файлов с сайта по каждому пользователю
- Графическое представление запросов сайта по времени, для всех пользователей
- Графическое представление запросов сайта по пользователям по времени, для каждого пользователя
- Графическое представление трафика по времени для каждого типа файла, для каждого пользователя.

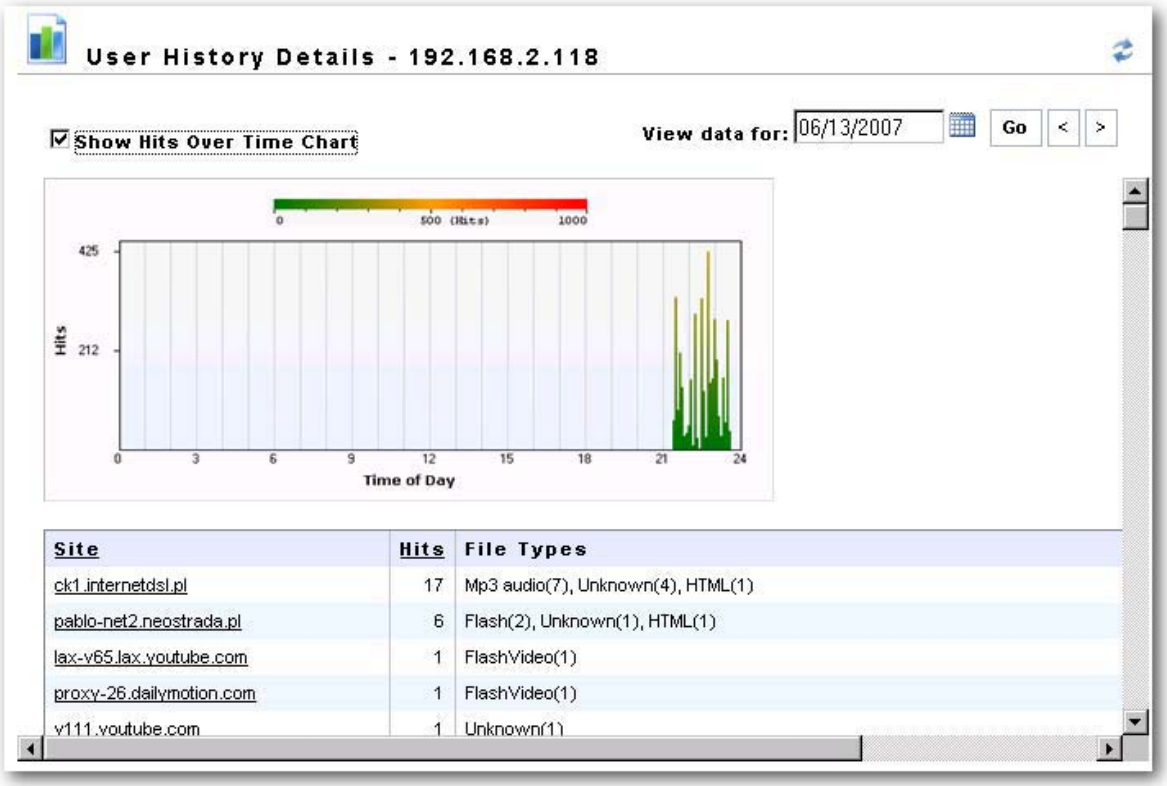
Чтобы графически отобразить запросы сайтов по времени для каждого пользователя, установите флажок Show Hits Over Time Chart. Эта диаграмма поможет идентифицировать период времени для указанных дат, в течение которых к сайту наиболее часто обращались пользователи.

Чтобы графически отобразить запросы сайтов по времени для определенного пользователя, наведите курсор мыши на число обращений для любого из перечисленных сайтов/IP-адресов. Во всплывшей диаграмме будет отображен пример доступа и частота для пользователя в течение дня.

Чтобы графически отобразить восходящий/нисходящий трафик по времени для определенного типа файла, для определенного сайта, наведите курсор мыши на тип файла, представленный для любого из перечисленных пользователей/IP-адресов.

Чтобы просмотреть детальную историю по пользователям можно также щелкнуть любого из перечисленных пользователей/IP-адресов. Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Детальная история по пользователям



Снимок 13 – Детальная история по пользователям

Доступ к представлению User History Details (Детальная история по пользователям) осуществляется щелчком Users History (История по пользователям) (Top Surfers или Top Hits Count) из панели навигации. В представлении выберите одного из перечисленных пользователей/IP-адрес в столбце User/IP.

В представлении User History Details (Детальная история по пользователям) отображаются следующие данные для определенного пользователя:

- Запрошенные сайты по указанной дате
- Количество доступов к сайту
- Запрошенные типы файлов
- Графическое представление запросов сайта по времени
- Графическое представление запросов определенного сайта по времени
- Графическое представление трафика по времени для каждого типа файла, для определенного сайта.

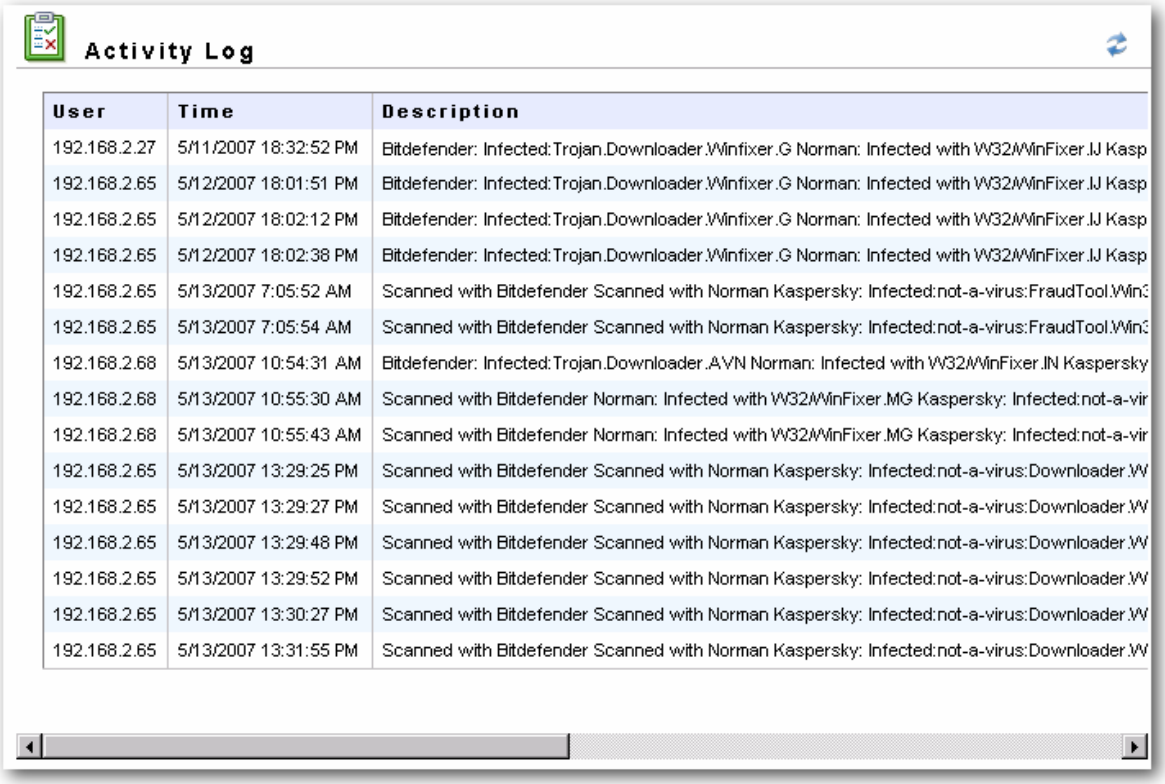
Чтобы графически отобразить запросы к сайтам по времени, выберите Show Hits Over Time Chart. Эта диаграмма поможет идентифицировать периоды для определенной даты, в которую осуществлялся доступ к перечисленным сайтам.

Чтобы графически отобразить запросы определенных сайтов для пользователя, наведите курсор мыши на число обращений для любого из перечисленных сайтов. Во всплывшей диаграмме будет отображен пример доступа к определенному сайту и частота для пользователя в течение дня.

Чтобы графически отобразить исходящий/восходящий трафик у загрузки/загрузки в течение долгого времени для определенного типа файла, для определенного пользователя, наведите курсор мыши на один из типов файлов.

Чтобы просмотреть детальную историю по пользователям, можно также щелкнуть любой из перечисленных сайтов. Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Журнал регистрации активности



User	Time	Description
192.168.2.27	5/11/2007 18:32:52 PM	Bitdefender: Infected:Trojan.Downloader.Winfixer.G Norman: Infected with W32/WinFixer.IJ Kasp
192.168.2.65	5/12/2007 18:01:51 PM	Bitdefender: Infected:Trojan.Downloader.Winfixer.G Norman: Infected with W32/WinFixer.IJ Kasp
192.168.2.65	5/12/2007 18:02:12 PM	Bitdefender: Infected:Trojan.Downloader.Winfixer.G Norman: Infected with W32/WinFixer.IJ Kasp
192.168.2.65	5/12/2007 18:02:38 PM	Bitdefender: Infected:Trojan.Downloader.Winfixer.G Norman: Infected with W32/WinFixer.IJ Kasp
192.168.2.65	5/13/2007 7:05:52 AM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:FraudTool.Win3
192.168.2.65	5/13/2007 7:05:54 AM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:FraudTool.Win3
192.168.2.68	5/13/2007 10:54:31 AM	Bitdefender: Infected:Trojan.Downloader.AVN Norman: Infected with W32/WinFixer.IN Kaspersky
192.168.2.68	5/13/2007 10:55:30 AM	Scanned with Bitdefender Norman: Infected with W32/WinFixer.MG Kaspersky: Infected:not-a-vir
192.168.2.68	5/13/2007 10:55:43 AM	Scanned with Bitdefender Norman: Infected with W32/WinFixer.MG Kaspersky: Infected:not-a-vir
192.168.2.65	5/13/2007 13:29:25 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W
192.168.2.65	5/13/2007 13:29:27 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W
192.168.2.65	5/13/2007 13:29:48 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W
192.168.2.65	5/13/2007 13:29:52 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W
192.168.2.65	5/13/2007 13:30:27 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W
192.168.2.65	5/13/2007 13:31:55 PM	Scanned with Bitdefender Scanned with Norman Kaspersky: Infected:not-a-virus:Downloader.W

Снимок 14 – Журнал регистрации активности GFI WebMonitor

Доступ к представлению Activity Log (Журнал регистрации активности) осуществляется щелчком узла Activity Log в панели навигации.

В представлении Activity Log (Журнал регистрации активности) показана вся активность GFI WebMonitor, связанная со следующими параметрами:

- Заблокированные или изолированные элементы
- Неуспешные процессы.

В представлении Activity Log (Журнал регистрации активности) отображены:

- Пользователь/IP-адрес
- Дата и время активности
- Описание активности и причина блокирования или изоляции
- Подробности о запрошенном URL-адресе.

WebFilter Edition – классификация сайтов и фильтрация содержимого

Введение

GFI WebMonitor использует WebFilter и базу данных WebGrade, чтобы управлять доступом в Интернет пользователей, групп или IP-адресов, на основе категории сайта. Категория определенного сайта определяется по базе данных WebGrade; если сайт перечислен в базе данных, GFI WebMonitor использует политику веб-фильтрации для определения выполняемого действия. Это может быть:

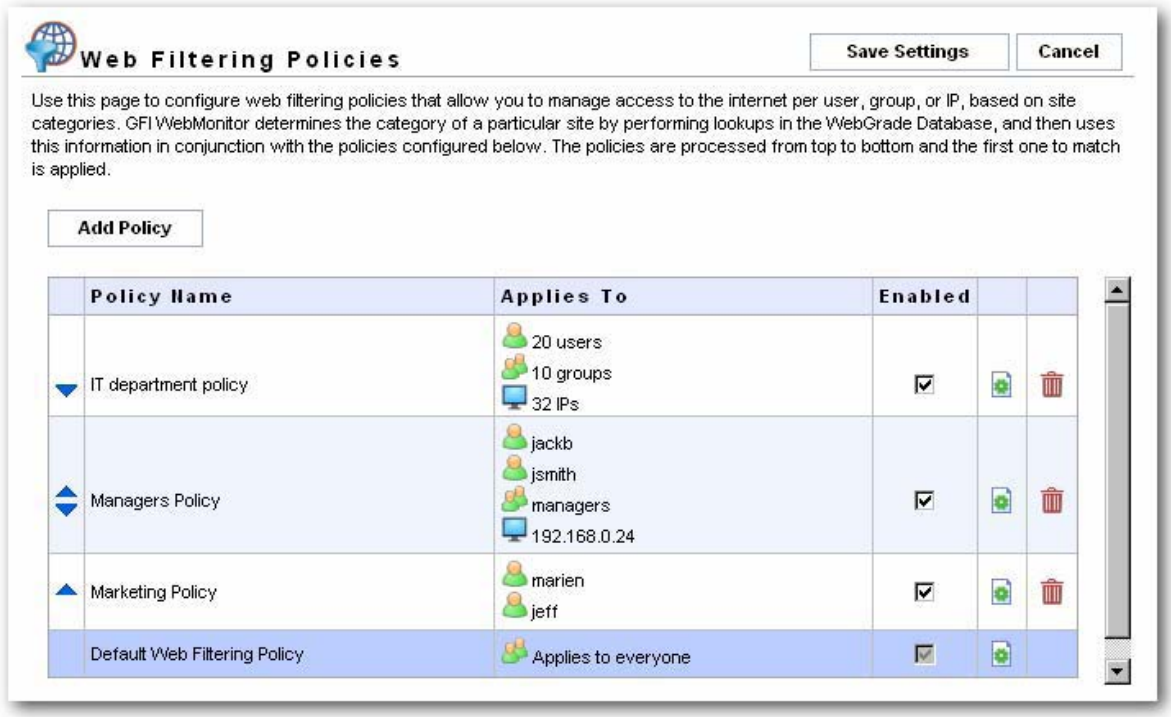
- Разрешение доступа к сайту
- Блокирование доступа к сайту и карантин файла URL
- Блокирование доступа к сайту и удаление URL.

Для применения к определенным периодам времени можно создавать политики; например политика может позволять пользователям получать доступ к сайтам новостей и развлечений во время обеда, но не в течение рабочих часов.

База данных WebGrade содержит более 60 категорий. К ним относятся порнография, игры, насилие и т.д. База данных обновляется на регулярной основе, и обновления автоматически загружаются в GFI WebMonitor.

Создание политик веб-фильтрации

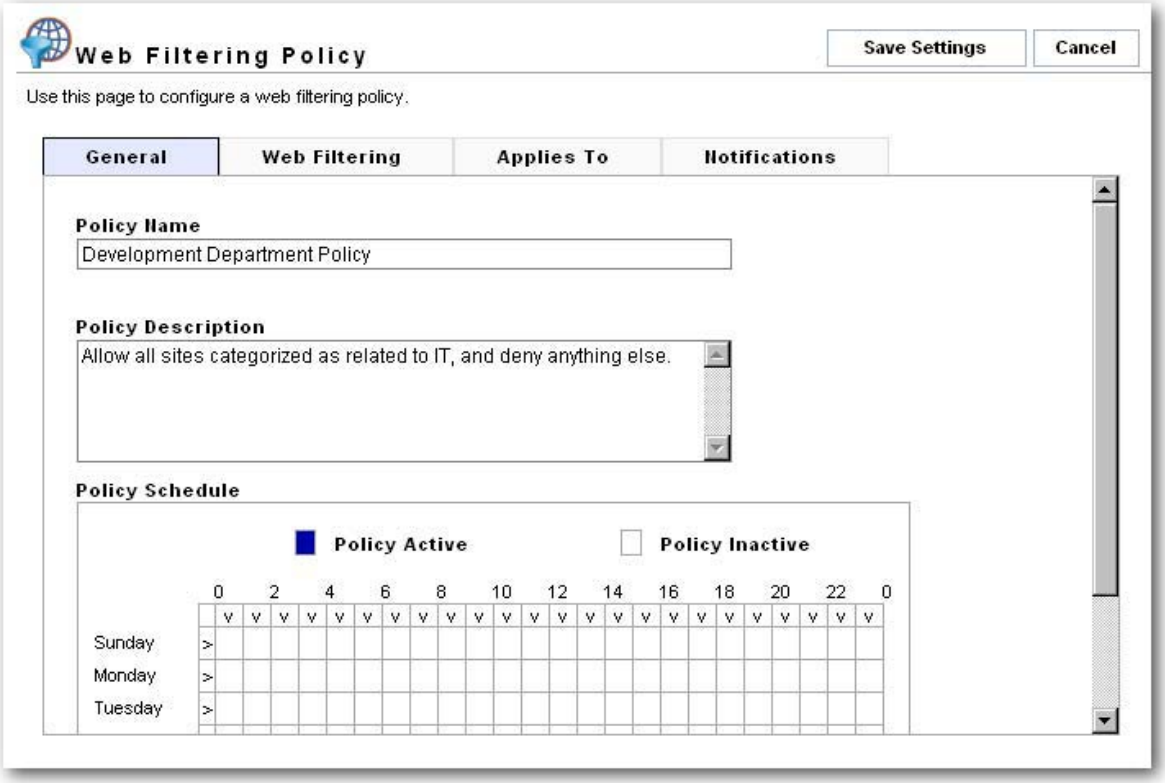
Добавление политик веб-фильтрации



Снимок 15 –Политики веб-фильтрации

Чтобы добавить политику веб-фильтрации:

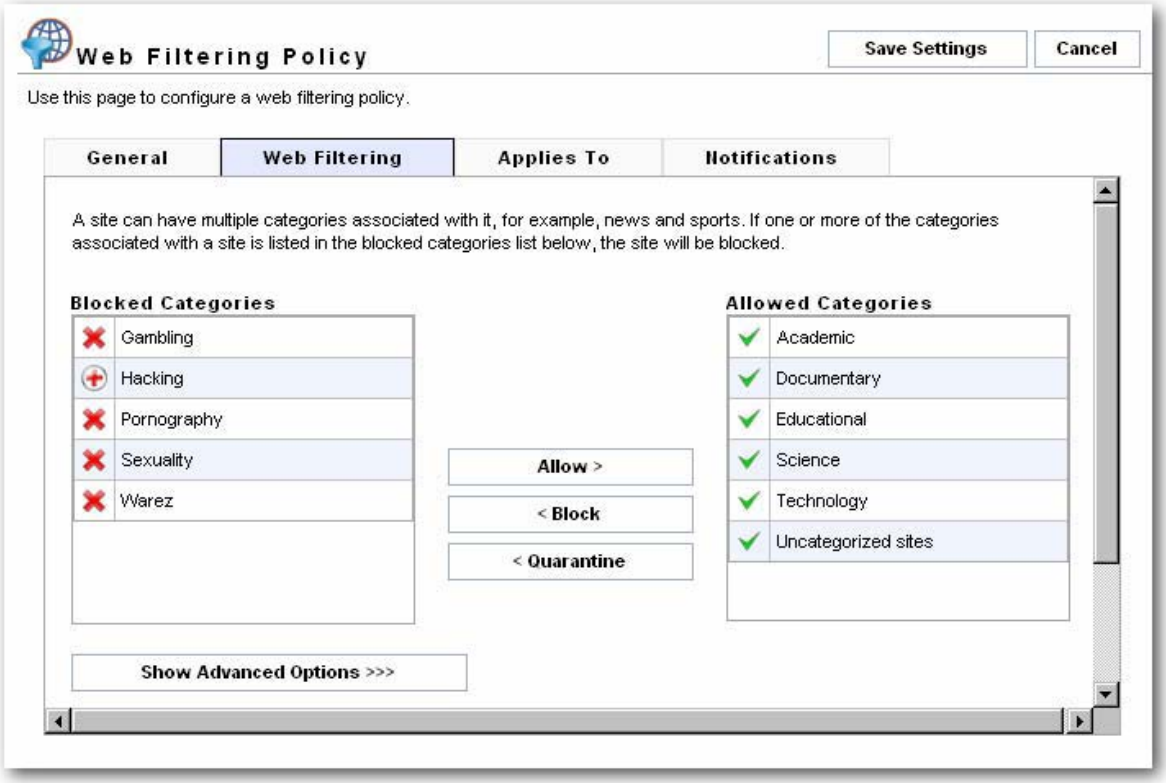
1. Щелкните WebFilter Edition > Web Filtering Policies из панели навигации.
2. Выберите Add Policy (Добавить политику).



Снимок 16 – Добавление политик веб-фильтрации: общие параметры настройки

3. Откройте вкладку General (Общие).

4. Введите имя и описание политики в поля Policy Name и Policy Description соответственно.
5. В поле Policy Schedule (Расписание политики) задайте время действия новой политики.

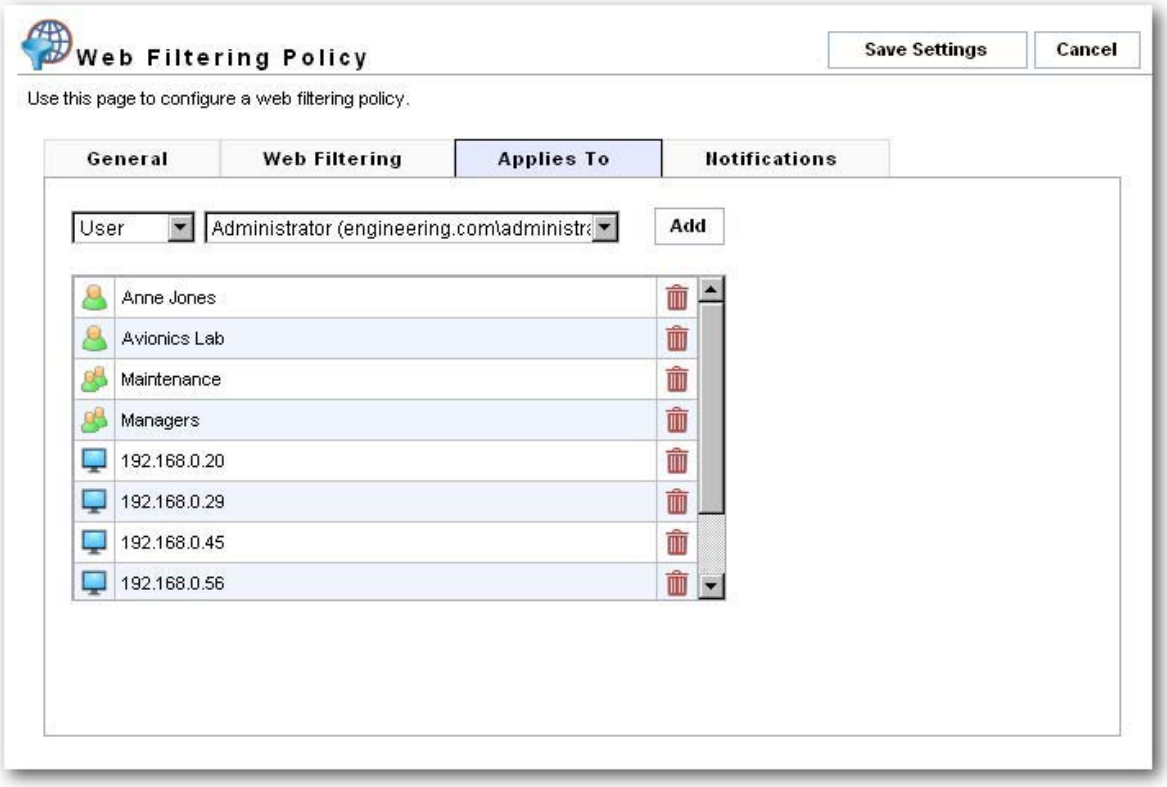


Снимок 17 – Добавление политик веб-фильтрации: категории веб-фильтрации

6. Откройте вкладку Web Filtering (Веб-фильтрация). Определите категории, применимые к новой политике и действиям:

- Чтобы разрешить категории: Выберите категории в списке Blocked Categories (Блокированные категории) и щелкните Allow (Разрешить).
- Чтобы заблокировать категории: Выберите категории в списке Allowed Categories (Разрешенные категории) и щелкните Block (Блокировать).
- Чтобы изолировать доступ: Выберите категории в списке Allowed Categories (Разрешенные категории) и щелкните Quarantine (Изолировать).

ПРИМЕЧАНИЕ: Можно также создавать расширенные условия категории. Для получения дополнительной информации см. раздел «Создание расширенных условий политики веб-фильтрации».



Снимок 18 – Добавление политик веб-фильтрации: к кому относится

7. Откройте вкладку Applies To (Применяется к) и определите пользователя, группу и/или IP-адрес. Повторите для всех пользователей, групп и/или требуемых IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя, определите имя пользователя в формате DOMAIN\пользователь. Аутентификация ISA Server используется для проверки подлинности имени пользователя.

ПРИМЕЧАНИЕ 2: При добавлении групп аутентификация ISA Server используется для проверки подлинности имени группы.

Снимок 19 – Добавление политики веб-фильтрации: Уведомления

8. Откройте вкладку Notifications (Уведомления) и установите флажок Notify the following administrators when the site category infringes this policy (Уведомлять следующих администраторов при нарушении политики). Завершите установку вводом адреса электронной почты для уведомления администратора вместе с текстом уведомления. Также введите основной текст сообщения электронной почты в поле Send the following notification to the administrators (Отправить администраторам следующее уведомление).
9. При необходимости уведомления пользователя при нарушении политики установите флажок Notify the user accessing the site if the site category infringes this policy (Уведомлять пользователя при доступе к сайту, нарушающему политику) и введите текст сообщения.

ПРИМЕЧАНИЕ: Уведомление отправляется только в случае, если возможна аутентификация ISA Server, и пользователь, таким образом, может быть идентифицирован.

10. Завершите настройку политики нажатием Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Созданная политика будет отображена в основном представлении Web Filtering Policies (Политики веб-фильтрации).

Изменение политик веб-фильтрации

Чтобы изменить политику веб-фильтрации:

1. Щелкните WebFilter Edition > Web Filtering Policies из панели навигации.
2. Щелкните значок редактирования, расположенный рядом с политикой.
3. Для описания полей, которые можно редактировать, см. раздел Adding a Web Filtering Policy (Добавление политики веб-фильтрации).
4. Чтобы завершить изменение политики, щелкните Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Отключение политики веб-фильтрации

Чтобы отключить политику веб-фильтрации:

1. Щелкните WebFilter Edition > Web Filtering Policies из панели навигации.
2. Снимите флажок в столбце Enabled (Включено) для политики, которую требуется отключить, и нажмите Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Включение политики веб-фильтрации

1. Щелкните WebFilter Edition > Web Filtering Policies из панели навигации.
2. Установите флажок в столбце Enabled (Включено) для политики, которую требуется включить, и нажмите Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление политики веб-фильтрации

1. Щелкните WebFilter Edition > Web Filtering Policies в панели навигации.
2. Щелкните значок удаления для политики, которую требуется удалить, и нажмите кнопку Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Политика веб-фильтрации по умолчанию

GFI WebMonitor - WebFilter включает заданную по умолчанию политику веб-фильтрацию, которая применяется ко всем пользователям. Название политики

указано как Default Web Filtering Policy (Политика веб-фильтрации по умолчанию).

Эту политику можно изменить, однако ее нельзя отключить или удалить. Если вы хотите изменить политику по умолчанию политику, см раздел «Изменение политики веб-фильтрации».

ПРИМЕЧАНИЕ 1: Все политики, созданные пользователями, имеют приоритет над заданной по умолчанию.

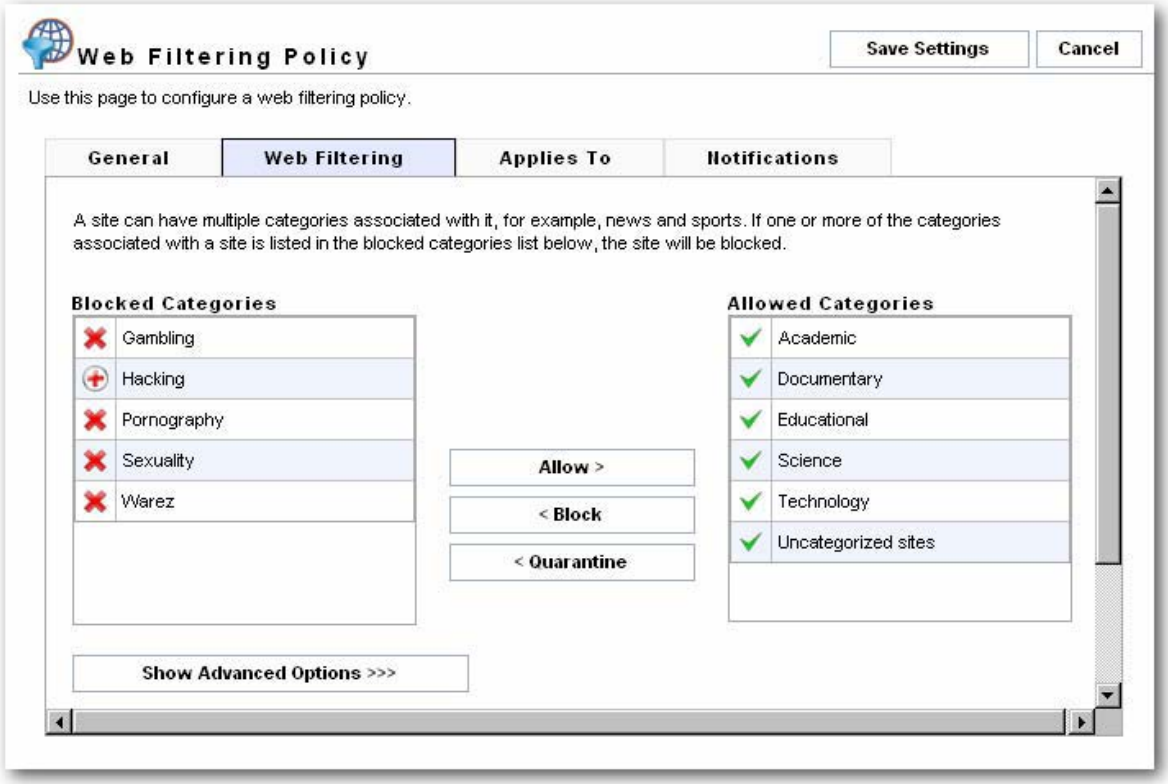
ПРИМЕЧАНИЕ 2: Определенные поля в заданной по умолчанию политике не могут быть изменены. Это Policy Name (Название политики), Policy Description (Описание политики) и поля на вкладке Applies To (Применяется к).

Создание расширенных условий политики веб-фильтрации

Расширенные условия политики веб-фильтрации предоставляют большую гибкость в определении сайтов, которые должны быть разрешены или заблокированы. Расширенные условия политики имеют приоритет над категориями, заданными в полях Allowed Categories (Разрешенные категории) и Blocked Categories (Заблокированные категории).

Добавление расширенного условия политики веб-фильтрации

Чтобы создать расширенное условие политики веб-фильтрации:



Снимок 20 – Политика веб-фильтрации

1. На вкладке Web Filtering (Веб-фильтрация) щелкните Show Advanced Options (Показать дополнительные параметры).

Снимок 21 – Создание расширенных условий политики веб-фильтрации

2. Чтобы открыть диалог Edit Properties (Изменить свойства), щелкните Add Condition (Добавить условие).
3. Определите комбинацию категорий, которые дадут возможность разрешать, блокировать или изолировать сайты.

Например, чтобы блокировать сайты, которые подпадают под категории «Для взрослых» и «Секс»:

a) Выберите Adult themes (Для взрослых) из списка Available Categories (Доступные категории) и щелкните Use Category (Использовать категорию)
b) Выберите Sexuality (Секс) из списка Available Categories (Доступные категории) и щелкните Use Category (Использовать категорию)
c) Выберите Block and Delete (Блокировать и удалить) из списка Perform this action (Выполнить действие): и нажмите OK, чтобы применить условие

4. Нажмите Save Settings (Сохранить настройки), чтобы завершить настройки.

ПРИМЕЧАНИЕ 1: При использовании расширенной политики сайты не блокируются, если сайт входит в индивидуальную категорию. В примере выше, сайт НЕ блокируется, если он попадает под категорию «Для взрослых». Аналогично, сайт НЕ блокируется, если он попадает только под категорию «Секс».

ПРИМЕЧАНИЕ 2: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Изменение расширенной политики веб-фильтрации

Чтобы изменить расширенную политику веб-фильтрации:

1. На вкладке Web Filtering (Веб-фильтрация) щелкните Show Advanced Options (Показать дополнительные параметры).
2. Щелкните расширенную политику, чтобы открыть диалог Edit Properties (Изменить свойства), где можно изменить условие.
3. Чтобы изменения вступили в силу, нажмите кнопку «ОК».

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

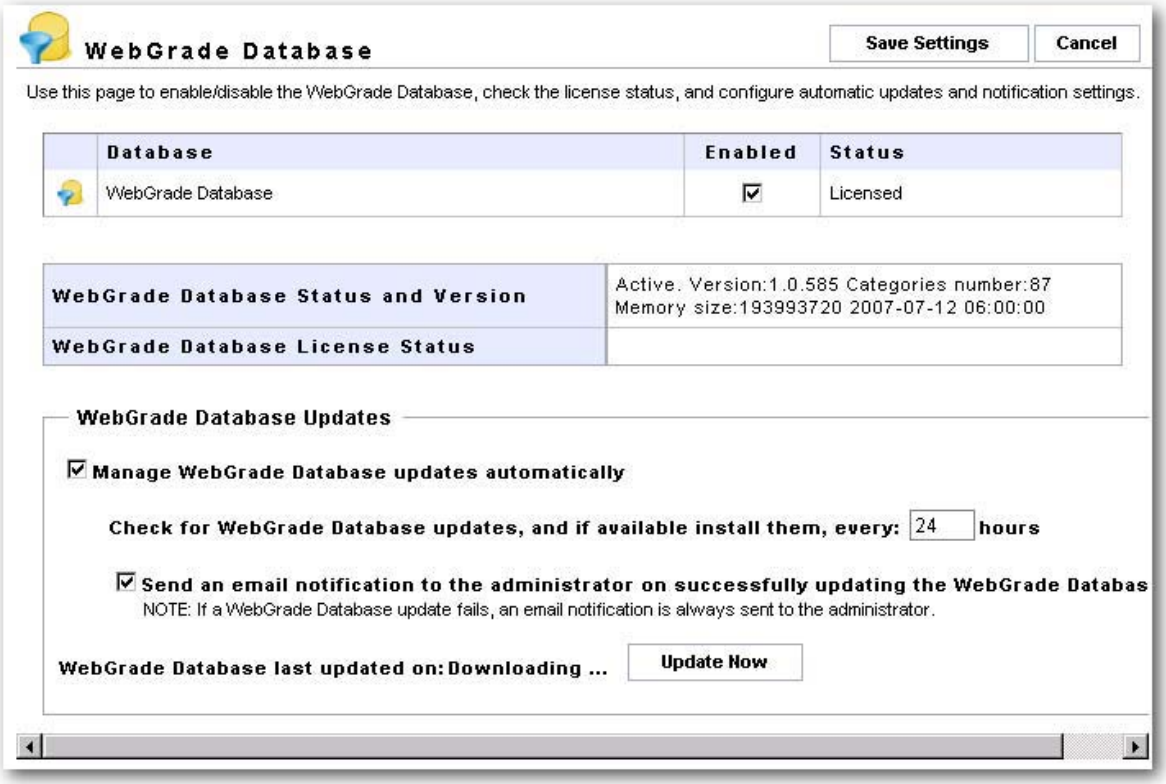
Удаление расширенной политики веб-фильтрации

Чтобы удалить расширенную политику веб-фильтрации:

1. На вкладке Web Filtering (Веб-фильтрация) щелкните Show Advanced Options (Показать дополнительные параметры).
2. Щелкните значок удаления, расположенный рядом политикой, выбранной для удаления.

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить настройки) не будет нажата, вы потеряете измененные параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Параметры настройки базы данных WebGrade



Снимок 22 – Параметры настройки базы данных WebGrade

Через представление настройки базы данных WebGrade можно:

- Включать/отключать базу данных
- Просматривать состояние базы данных, версию и лицензию
- Настраивать обновления базы данных

Доступ к представлению WebGrade Database (База данных WebGrade) осуществляется выбором WebFilter Edition > Web Filtering Policies > WebGrade Database в панели навигации.

Включение/отключение базы данных

Чтобы включить или отключить базу данных:

1. Щелкните WebFilter Edition > Web Filtering Policies > WebGrade Database
2. Установка и снятие флажка в столбце Enabled включает или отключает базу данных WebGrade.

ПРИМЕЧАНИЕ: Отключение базы данных WebGrade подразумевает, что политики веб-фильтрации не будут иметь информации о категориях сайтов.

Настройка обновлений базы данных

Используя флажки в области WebGrade Database Updates (Обновления базы данных WebGrade) параметров настройки базы данных WebGrade можно:

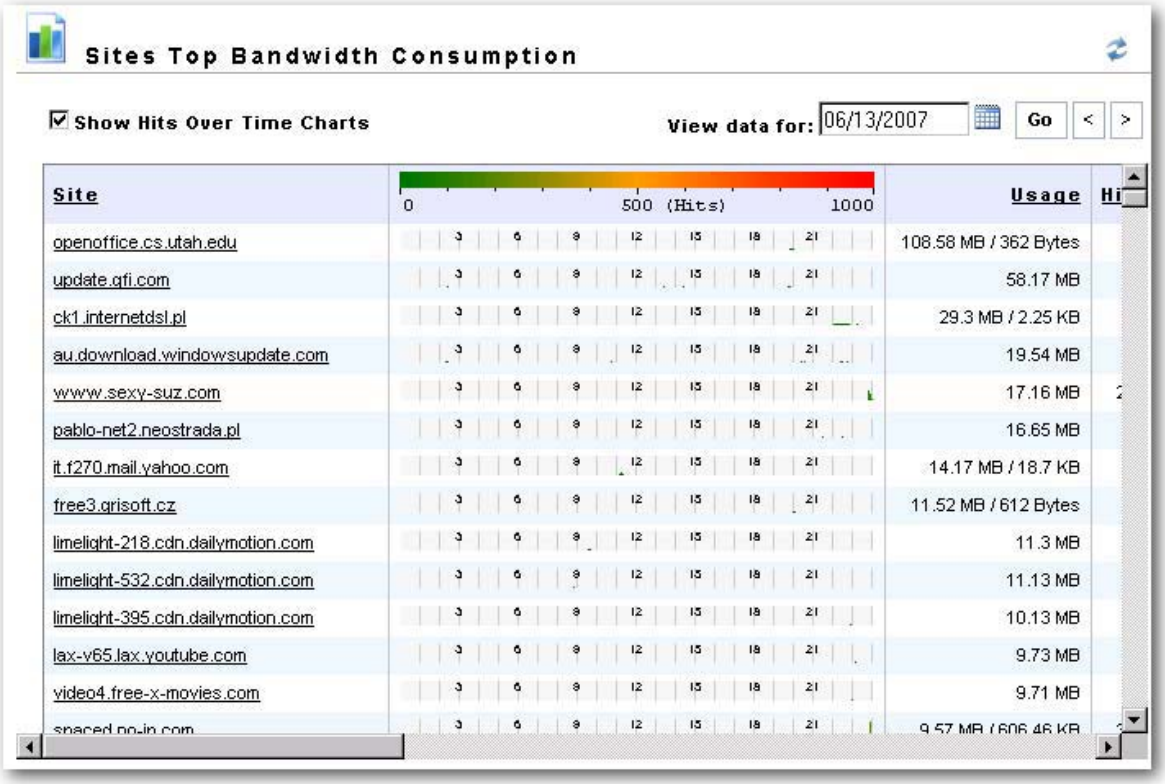
- Настраивать автоматическое или ручное обновление базы данных WebGrade

- Настраивать частоту установки доступных обновлений
- Настраивать отправку уведомлений после успешного обновления базы данных WebGrade
- Вручную обновлять базу данных WebGrade нажатием кнопки Update Now.

Мониторинг пропускной способности

Мониторинг пропускной способности используется для идентификации сайтов, с которых пользователями было загружено наибольший объем данных, а также этих пользователей. Эти данные доступны из этих двух подузлов под узлом Bandwidth Monitoring (Мониторинг пропускной способности):
Сайты, занимающие максимум пропускной способности
Пользователи, занимающие максимум пропускной способности

Сайты, занимающие максимум пропускной способности



Снимок 23 – Сайты, занимающие максимум пропускной способности

Доступ к представлению Sites Top Bandwidth consumption (Сайты, занимающие максимум пропускной способности) осуществляется щелчком WebFilter Edition > Sites Top Bandwidth Consumption в панели навигации.

В представлении Sites Top Bandwidth Consumption (Сайты, занимающие максимум пропускной способности) перечислены сайты, с которых пользователями был загружен наибольший объем данных, за определенную дату. Отображаемая информация включает:

- Сайты, к которым осуществлялся доступ
- Количество данных, загруженное с каждого сайта

- Количество обращений к каждому сайту (то есть, количество запросов)
- Типы запрашиваемых с каждого сайта файлов
- Пользователи/IP-адреса, которые обращались к сайту
- Категория сайта, определенные базой данных WebGrade
- Графические представления запросов сайта по времени.

По умолчанию список отсортирован по использованию, объему загруженных данных, в порядке убывания. Список может также быть отсортирован:

- В алфавитном порядке в порядке возрастания, щелчком заголовка столбца Site (Сайт)
- В порядке убывания популярности (сайт с наибольшим числом запросов сверху), щелчком заголовка столбца Hits (Запросы)

Чтобы графически отобразить запросы по времени для каждого из перечисленных сайтов, установите флажок Show Hits Over Time Charts. Эти графики позволяют идентифицировать периоды для определенной даты, в которую сайт запрашивался наиболее часто.

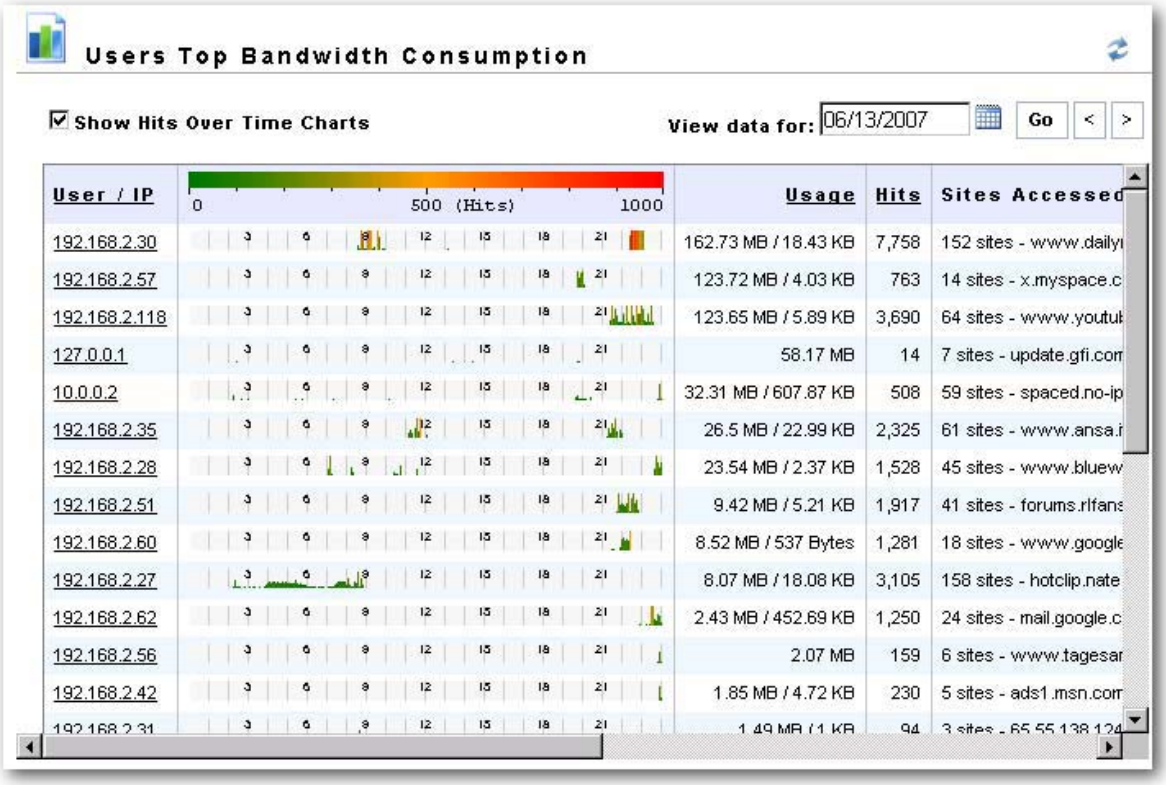
По умолчанию в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и нажмите Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, отображается сообщение об ошибке.

Вы можете также щелкнуть любой из сайтов в списке, чтобы открыть представление «Детальная история посещений сайтов». Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Пользователи, занимающие максимум пропускной способности



Снимок 24 – Пользователи, занимающие максимум пропускной способности

Доступ к представлению Users Top Bandwidth consumption (Пользователи, занимающие максимум пропускной способности) осуществляется щелчком WebFilter Edition > Users Top Bandwidth Consumption в панели навигации.

В представлении Users Top Bandwidth consumption (Пользователи, занимающие максимум пропускной способности) отображаются пользователи с самым высоким объемом загрузки по определенной дате. Отображаемая информация включает:

- Пользователи/IP-адреса, которые просматривали сайты
- Объем данных, загруженный каждым пользователем
- Количество доступов к сайтам по каждому пользователю
- Сайты, к которым обращался каждый пользователь
- Графические представления запросов сайта по времени.

По умолчанию список отсортирован по использованию, объему загруженных данных, в порядке убывания. Список может также быть отсортирован:

- В алфавитном возрастающем порядке по пользователю/IP-адресу, щелчком заголовка столбца User/IP (Пользователь/IP-адрес)
- В порядке убывания популярности (сайт с наибольшим числом запросов сверху), щелчком заголовка столбца Hits (Запросы)

Чтобы графически отобразить запросы по времени для каждого из перечисленных сайтов, установите флажок Show Hits Over Time Charts. Эта диаграмма помогает идентифицировать период времени для указанной даты, во время которой к сайту наиболее часто обращались пользователи.

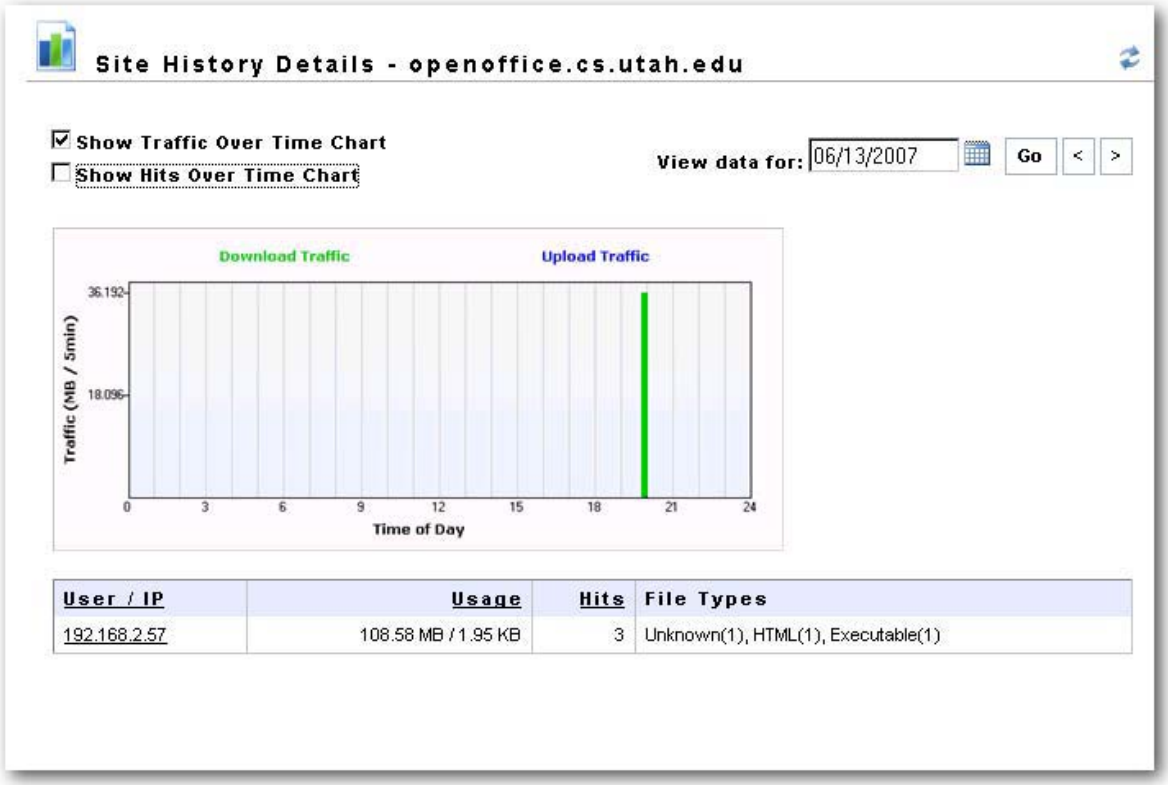
По умолчанию в этом представлении отображаются сегодняшние данные по умолчанию. Чтобы просмотреть данные за другие дни, используйте элементы управления в верхнем правом углу представления:

- Предыдущий день – щелкните кнопку «назад»
- Следующий день – щелкните кнопку «вперед»
- Определенная дата – нажмите кнопку календаря, выберите необходимую дату и нажмите Go (Искать).

ПРИМЕЧАНИЕ: Если данные для определенной даты не доступны, отображается сообщение об ошибке.

Вы можете также щелкнуть любой из сайтов в списке, чтобы открыть представление User History Details (Детальная история посещений сайтов). Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Детальная история посещения сайтов



Снимок 25 – Детальная история посещения сайтов

Доступ к представлению Site History Details (Детальная история посещения сайтов) осуществляется щелчком сайта, перечисленного в Sites Top Bandwidth Consumption (Сайты, занимающие максимум пропускной способности).

ПРИМЕЧАНИЕ: Более детально данные отображаются в представлении Site History Details (Детальная история посещения сайтов) через узел WebFilter Edition, но не через узел Monitoring (Мониторинг).

В этом представлении отображается следующая информация для определенного сайта, по указанной дате:

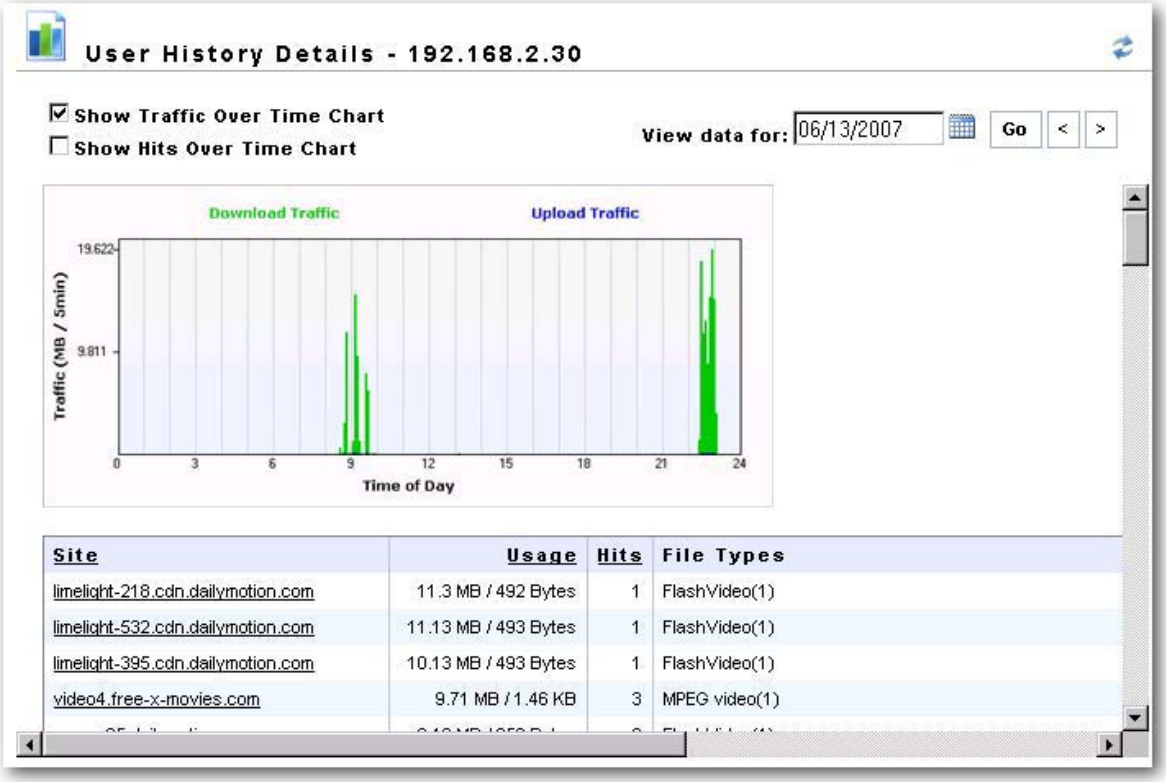
- Все пользователи/IP-адреса, которые обратились к тому сайту
- Объем данных, загруженных/переданных из/в сайт
- Количество обращений к сайту по каждому пользователю/IP-адресу
- Типы файла, запрашиваемых с сайта каждым пользователем/IP-адресом
- Графическое представление полного восходящего/нисходящего трафика, для всех пользователей/IP-адресов
- Графическое представление запрсов сайта по времени, по всем пользователям/IP-адресам
- Графическое представление восходящего/нисходящего трафика, для каждого пользователя/IP-адреса
- Графическое представление запросов сайта по времени, для каждого перечисленного пользователя/IP-адреса
- Графическое представление трафика по времени для каждого типа файлов, для каждого пользователя/IP-адреса.

Для графического представления различных элементов данных, отображенных в пределах этого представления:

- Выберите Show Traffic Over Time Chart (Показать диаграмму трафика по времени), чтобы графически отобразить входящий/исходящий трафик для всех пользователей. Эта диаграмма помогает идентифицировать период с наибольшим входящим/исходящим трафиком.
- Выберите Show Hits Over Time Chart (Показать диаграмму запросов по времени), чтобы графически отобразить запросы сайтов по времени для всех пользователей. Эта диаграмма поможет идентифицировать период времени для указанных дат, в течение которых к сайту наиболее часто обращались пользователи.
- Чтобы отобразить входящий/исходящий трафик по определенному пользователю, наведите курсор мыши на число, показывающее входящий/исходящий объем данных в столбце Usage (Использование). Диаграмма отображает информацию, связанную с входящим/исходящим объемом пользователя в течение дня.
- Чтобы отобразить запросы сайта по времени для определенного пользователя, наведите курсор мыши на число, отображающее количество запросов по пользователю/IP-адресу. Диаграмма отображает информацию, связанную с запросами и их частотой по пользователю в течение дня.
- Чтобы графически отобразить входящий/исходящий трафик по времени для определенного типа файла, наведите курсор мыши на тип файла, представленный для любого из перечисленных пользователей/IP-адресов.

Чтобы просмотреть детальную историю по пользователям можно также щелкнуть любого из перечисленных пользователей/IP-адресов. Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

Детальная история по пользователям



Снимок 26 – Детальная история по пользователям

Доступ к представлению User History Details (Детальная история по пользователям) осуществляется щелчком сайта, перечисленного в Users Top Bandwidth Consumption (Пользователи, занимающие максимум пропускной способности).

ПРИМЕЧАНИЕ: Более детально данные отображаются в представлении User History Details (Детальная история по пользователям) через узел WebFilter Edition, но не через узел Monitoring (Мониторинг).

В представлении User History Details (Детальная история по пользователям) показаны следующие данные для определенного пользователя/IP-адреса:

- Запрошенные сайты по указанной дате
- Объем загруженных/переданных данных из сайта/на сайт
- Количество доступов к сайту
- Запрошенные типы файлов
- Категория сайта, определенные базой данных WebGrade
- Графическое представление входящего/исходящего трафика
- Графическое представление запросов сайта по времени
- Графическое представление входящего/исходящего трафика, для каждого сайта
- Графическое представление запросов определенного сайта по времени
- Графическое представление трафика по времени для каждого типа файла, для определенного сайта.

Для графического представления различных элементов данных, отображенных в пределах этого представления:

- Выберите Show Traffic Over Time Chart (Показать диаграмму трафика по времени), чтобы графически отобразить входящий/исходящий трафик для всех сайтов. Эта диаграмма поможет идентифицировать периоды для определенной даты с наибольшим трафиком по пользователю/IP-адресу.
- Выберите Show Traffic Over Time Chart (Показать диаграмму трафика по времени), чтобы графически отобразить запросы по времени. Эта диаграмма поможет идентифицировать периоды для определенной даты, в которую осуществлялся доступ к перечисленным сайтам.
- Чтобы отобразить входящий/исходящий трафик по определенному сайту, наведите курсор мыши на число, показывающее входящий/исходящий объем данных в столбце Usage (Использование). Диаграмма отображает информацию, связанную с входящим/исходящим объемом пользователя по определенному сайту в течение дня.
- Чтобы графически отобразить определенные запросы сайтов по пользователю, наведите курсор мыши на число запросов сайтов. Диаграмма отображает информацию, связанную с указанным доступом и частотой по пользователю в течение дня.
- Чтобы графически отобразить входящий/исходящий трафик по времени для определенного типа файла, для определенного сайта, наведите курсор мыши на один из типов файлов.

Вы можете также щелкнуть любой из сайтов в списке, чтобы открыть представление «Детальная история посещений сайтов». Для получения дополнительной информации см. «Детальная история посещений сайтов» в этой главе.

WebSecurity Edition – сканирование файлов и контроль загрузок

Ознакомление с WebSecurity Edition

GFI WebMonitor WebSecurity проверяет и управляет файлами, загруженными из Интернета пользователями, группами или IP-адресами. GFI WebMonitor идентифицирует реальный тип загружаемого файла, а затем применяет политику управления загрузками для определения выполняемого действия. Это может быть:

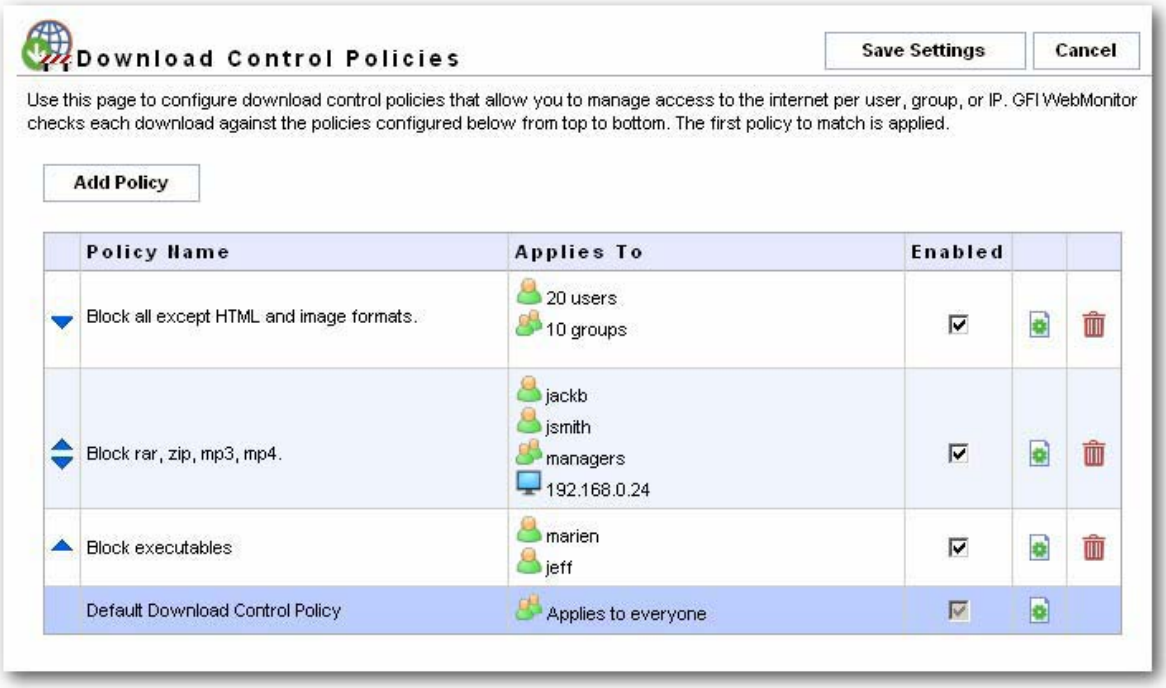
- Разрешение загрузки файла
- Блокирование загрузки файла и изоляция URL-адреса
- Блокирование загрузки файла и удаление все связанных URL-адресов.

Для разрешенных загрузок GFI WebMonitor применяет политики поиска вирусов и назначает параметры сканирования. Они могут включать следующее:

- Отображение процесса и состояния загрузки
- Сканирование загруженного файла с помощью любого из поддерживаемых сканеров
- Выполнение любого из следующих действий при обнаружении вируса:
    - Предупреждение с разрешением доступа к загруженному файлу
    - Блокирование доступа к загруженному файлу и карантин
    - Блокирование доступа к загруженному файлу и удаление.

WebSecurity также включает механизм антифишинга, который проверяет доступ к сайту по базе данных известных фишинговых URL-адресов. Если запрашиваемый URL-адрес будет найден, доступ к сайту блокируется.

Создание политик контроля загрузок



Снимок 27 – Политики управления загрузкой

Добавление политики контроля загрузок

Чтобы добавить политику управления загрузкой:

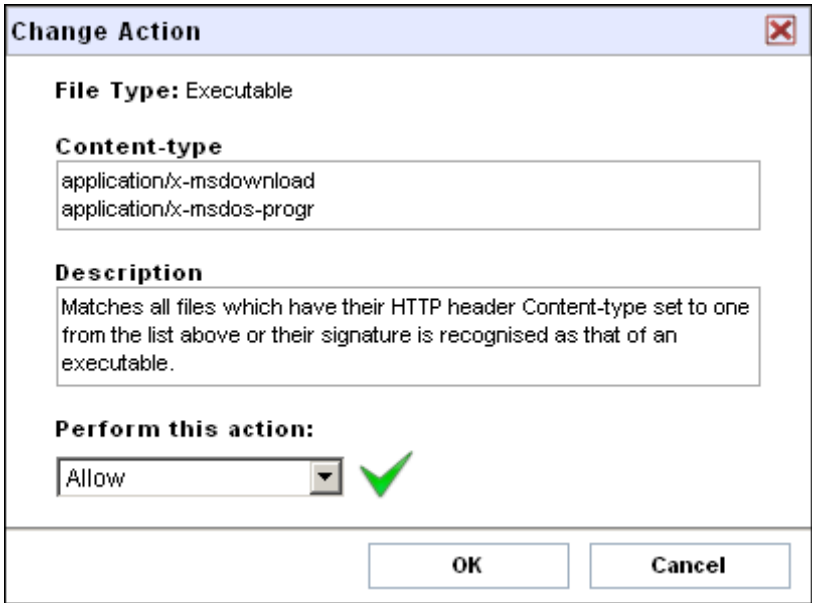
1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Щелкните Add Policy (Добавить политику).

Снимок 28 – Добавление политики управления загрузками

3. Откройте вкладку General (Общие).
4. Введите имя и описание политики в поля Policy Name и Policy Description соответственно.

Снимок 29 – Добавление новой политики управления загрузками: вкладка Download control (Управление загрузками)

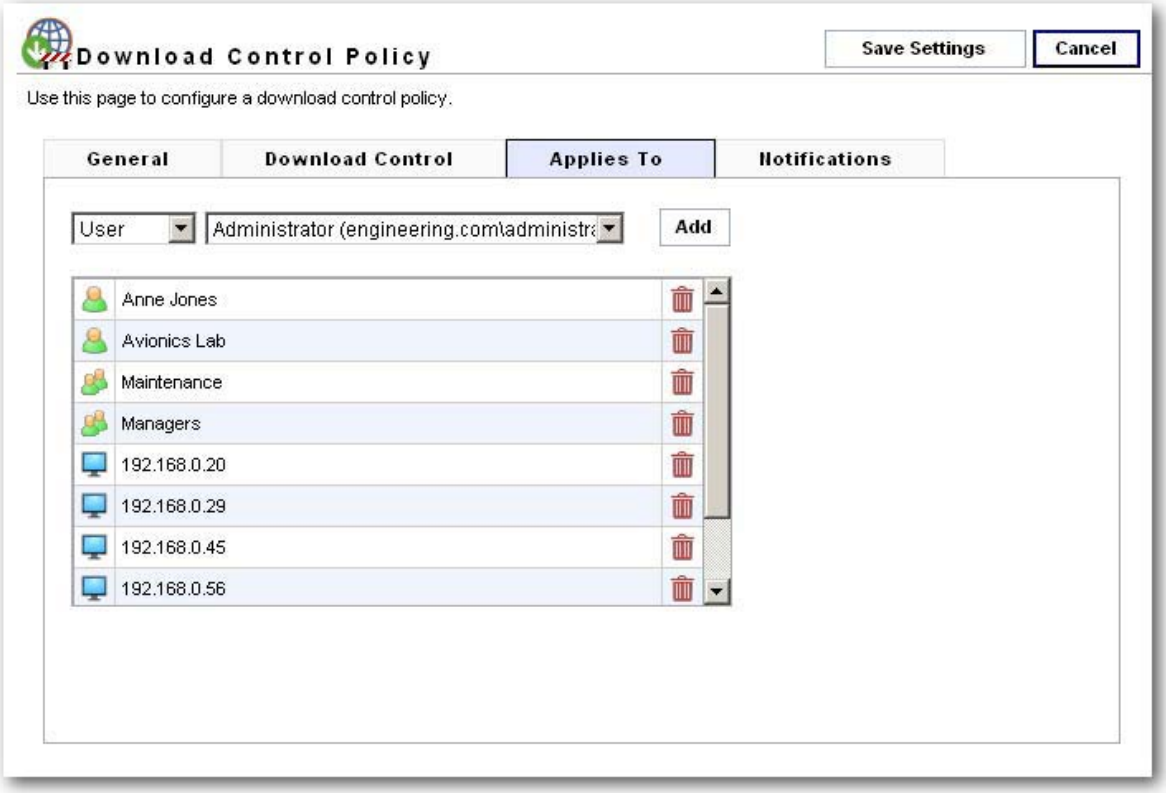
5. Откройте вкладку Download Control (Управление загрузками) и щелкните тип файла, который требуется контролировать.



Снимок 30 – Добавление новой политики управления загрузками: диалоговое окно Change Action (Изменение действия)

6. В диалоговом окне Change Action (Изменение действия) выберите действие из списка Perform this action: Доступные варианты:

- Allow (Разрешить)
- Block and Quarantine (Блокировать и изолировать)
- Block and Delete (Блокировать и удалить)

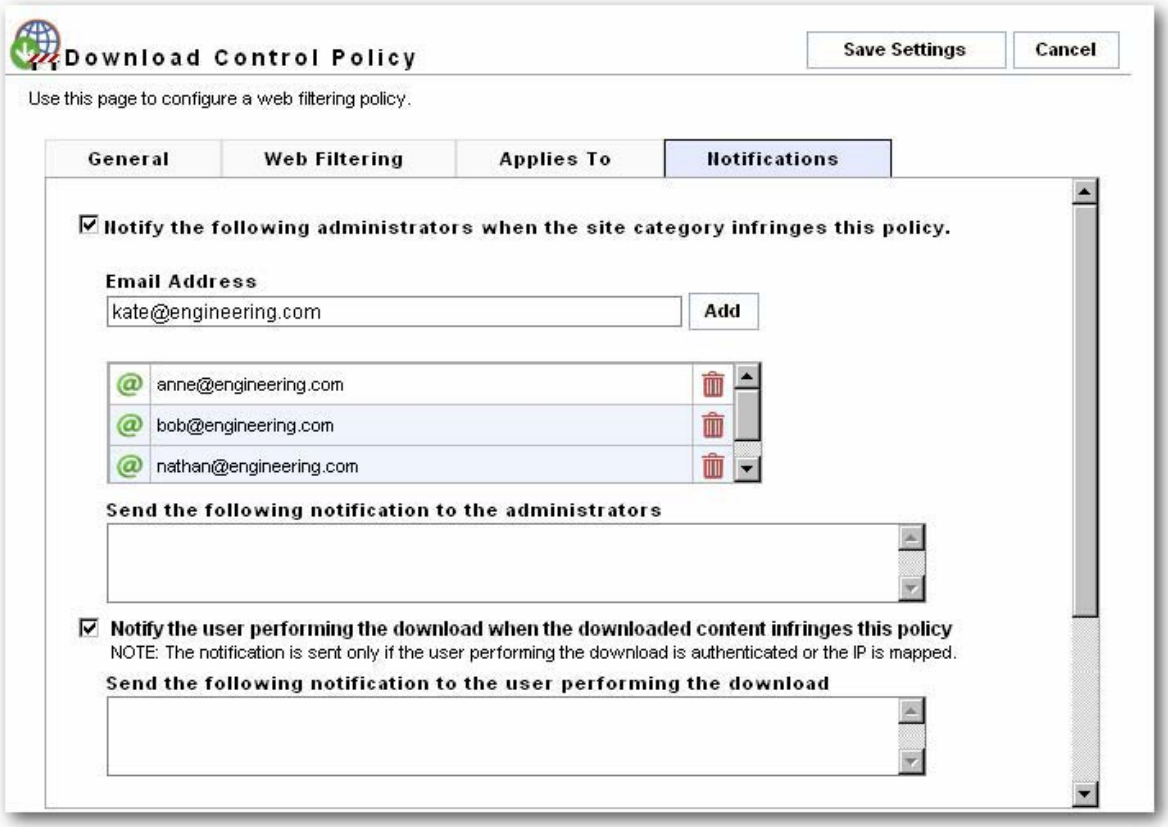


Снимок 31 – Политики управления загрузками: Вкладка Applies to tab (Применяется к)

7. Щелкните OK, откройте вкладку Applies To (Применяется к) и назначьте пользователя, группу и/или IP-адрес. Повторите для всех пользователей, групп и/или IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя, определите имя пользователя в формате DOMAIN\пользователь. Аутентификация ISA Server используется для проверки подлинности имени пользователя.

ПРИМЕЧАНИЕ 2: При добавлении групп аутентификация ISA Server используется для проверки подлинности имени группы.



Снимок 32 – Политики управления загрузками: вкладка Notification (Уведомление)

8. Откройте вкладку Notifications (Уведомления) и установите флажок Notify the following administrators when the download content infringes this policy (Уведомлять следующих администраторов при нарушении политики загрузок). Завершите настройку вводом адреса электронной почты для уведомления администратора вместе с текстом уведомления. Также введите основной текст для уведомления в поле Send the following notification to the administrators (Отправить администраторам следующее уведомление).
9. При необходимости отправки уведомлений пользователям при нарушении политики установите флажок Notify the user performing the download when the downloaded content infringes this policy (Уведомлять пользователей при нарушении политики загрузок) и введите текст уведомления.

ПРИМЕЧАНИЕ: Уведомление отправляется только в случае, если возможна аутентификация ISA Server, и пользователь, таким образом, может быть идентифицирован.

10. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Созданная политика будет отображена в основном представлении Download Control Policies (Политики управления загрузками).

Изменение политики управления загрузками

Чтобы изменить политику управления загрузками:

1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Щелкните значок редактирования, расположенный рядом с политикой.
3. Для описания полей для редактирования см. раздел Добавление политики управления загрузками в этой главе.
4. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Отключение политики управления загрузками

Чтобы отключить политику управления загрузками:

1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Снимите флажок в столбце Enabled (Включено) для политики, которую требуется отключить.
3. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Включение политики управления загрузками

Чтобы включить ранее отключенную политику управления загрузками:

1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Установите флажок в столбце Enabled (Включено) для политики, которую требуется отключить.
3. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление политики управления загрузками

Чтобы удалить политику управления загрузками:

1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Щелкните значок удаления, расположенный рядом политикой, выбранной для удаления.
3. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Политика управления загрузками по умолчанию

GFI WebMonitor - WebSecurity Edition включает политику управления загрузками по умолчанию, применяемую ко всем пользователям. Название политики представлено как Default Download Control Policy (Политика управления загрузками по умолчанию).

Эту политику можно изменять, но нельзя заблокировать или удалить. При необходимости изменить заданную по умолчанию политику см. раздел «Изменение политики управления загрузками» в этой главе.

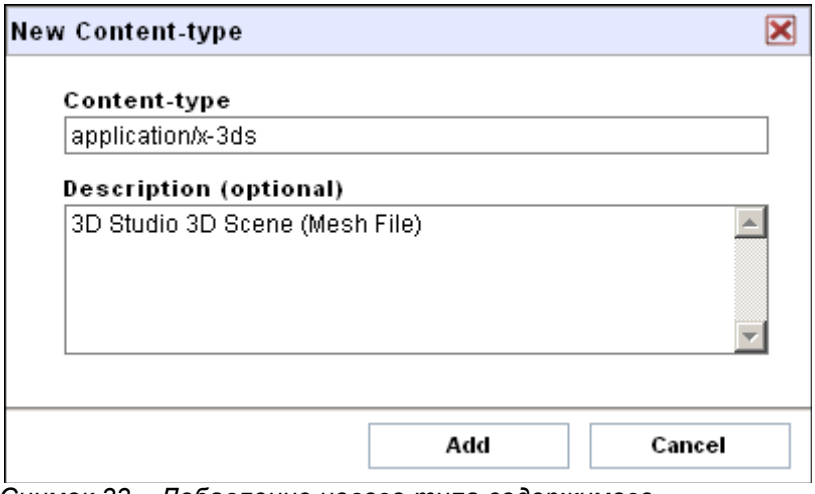
ПРИМЕЧАНИЕ 1: Вся созданная пользователем политика управления загрузками имеет приоритет над заданной по умолчанию политикой.

ПРИМЕЧАНИЕ 2: Определенные поля в заданной по умолчанию политике нельзя изменить. Это Policy Name (Название политики), Policy Description (Описание политики) и поля на вкладке Applies To (Применяется к).

Добавление типов содержимого

GFI WebMonitor - WebSecurity Edition включает большое количество общих типов файлов. Добавить тип файла, который не находится в предварительно заданном списке:

1. Щелкните WebSecurity Edition > Download Control Policies (Политики управления загрузкой) в панели навигации.
2. Щелкните Add Policy (Добавить политику), откройте вкладку Download Control (Управление загрузками) и щелкните Add Content-type (Добавить тип содержимого).



Снимок 33 – Добавление нового типа содержимого

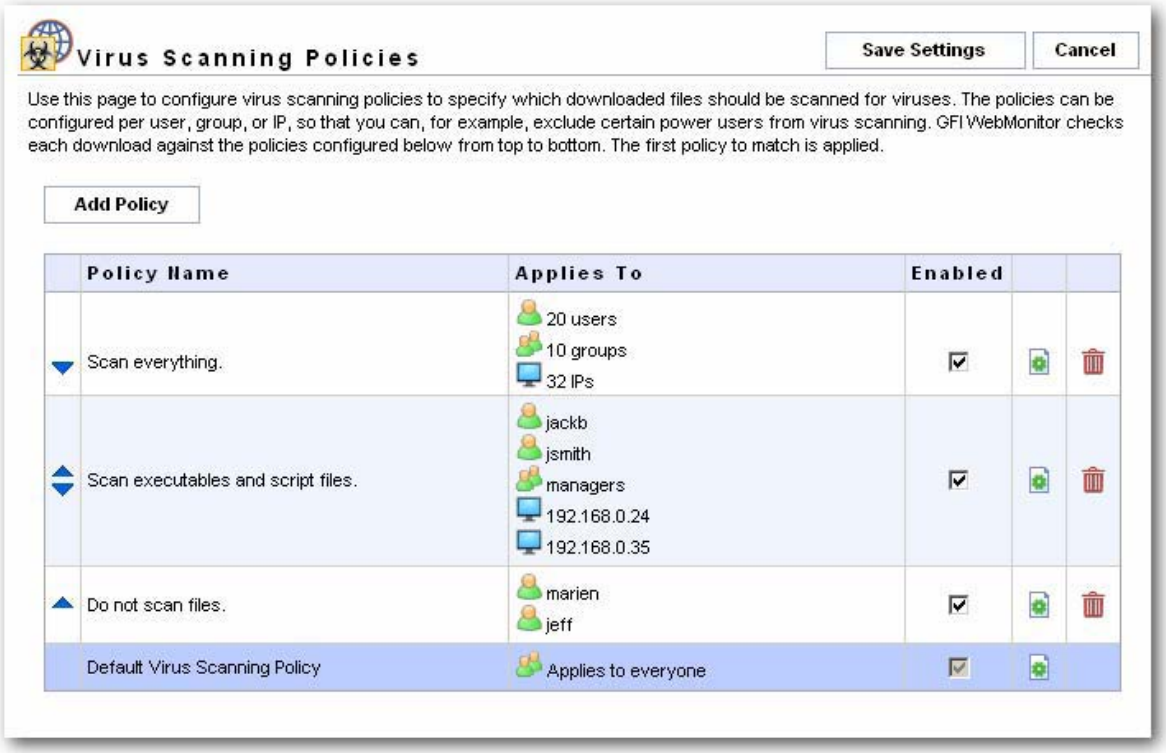
3. Введите тип содержимого в поле Content-Type в формате тип/подтип и щелкните Add (Добавить).

4. Завершите ввод нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ 1: Добавленные пользователями файлы не являются реальными типами файлов, как в случае с предварительно сконфигурированными типами файлов.

ПРИМЕЧАНИЕ 2: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Создание политик поиска вирусов

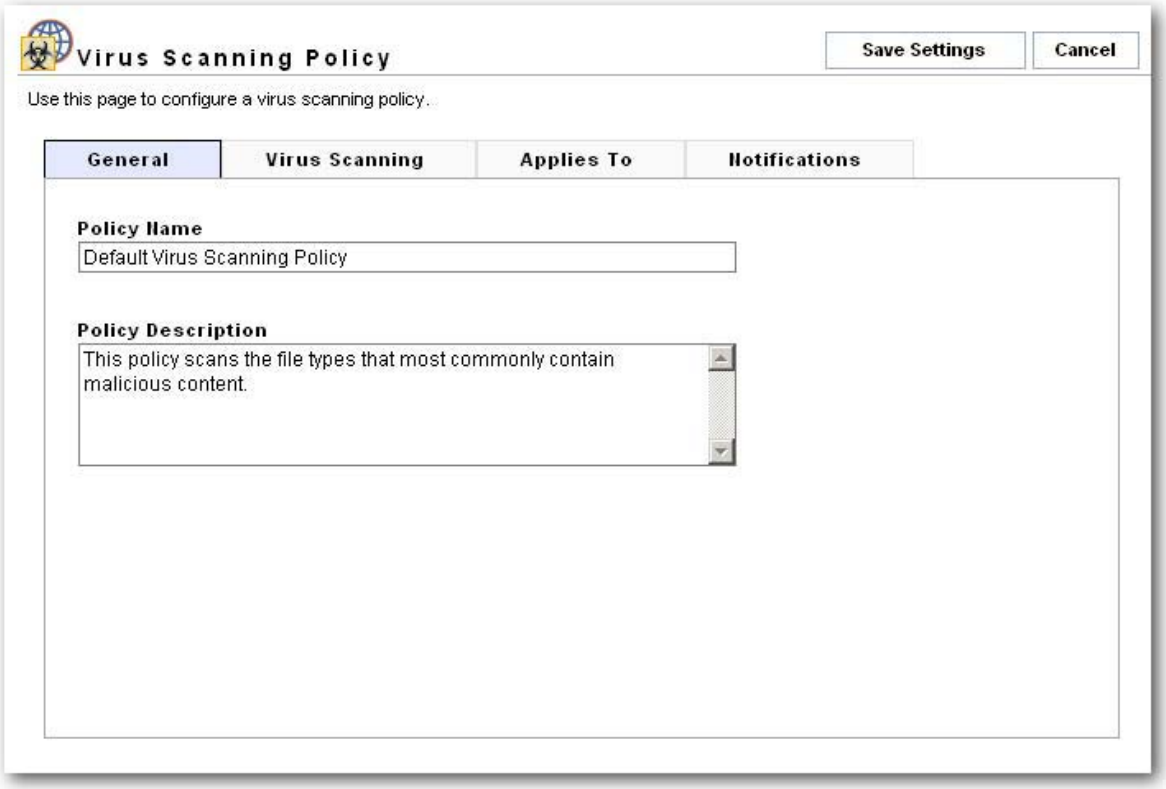


Снимок 34 – Политики поиска вирусов

Добавление политики поиска вирусов

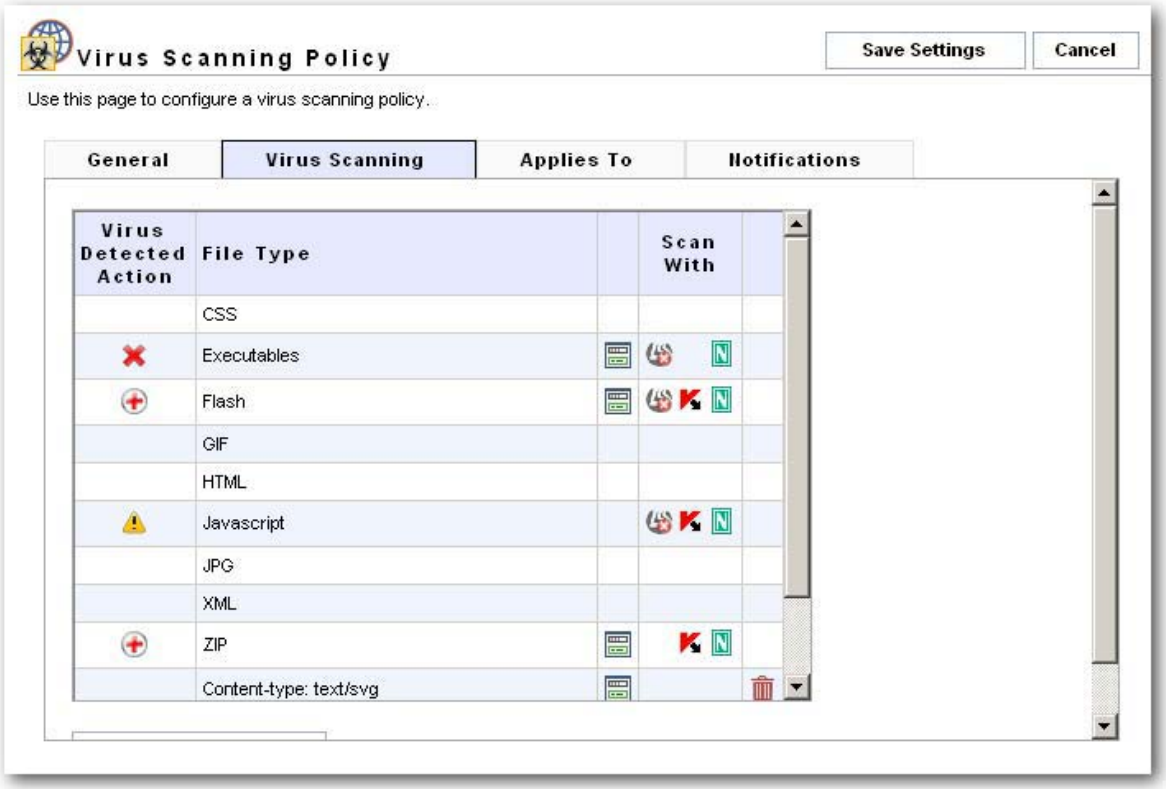
Чтобы добавить политику поиска вирусов:

1. Щелкните WebSecurity Edition > Virus Scanning Policies (Политики поиска вируов) в панели навигации.
2. Щелкните Add Policy (Добавить политику).
3. Откройте вкладку General (Общие).



Снимок 35 – Добавление новой политики поиска вирусов:

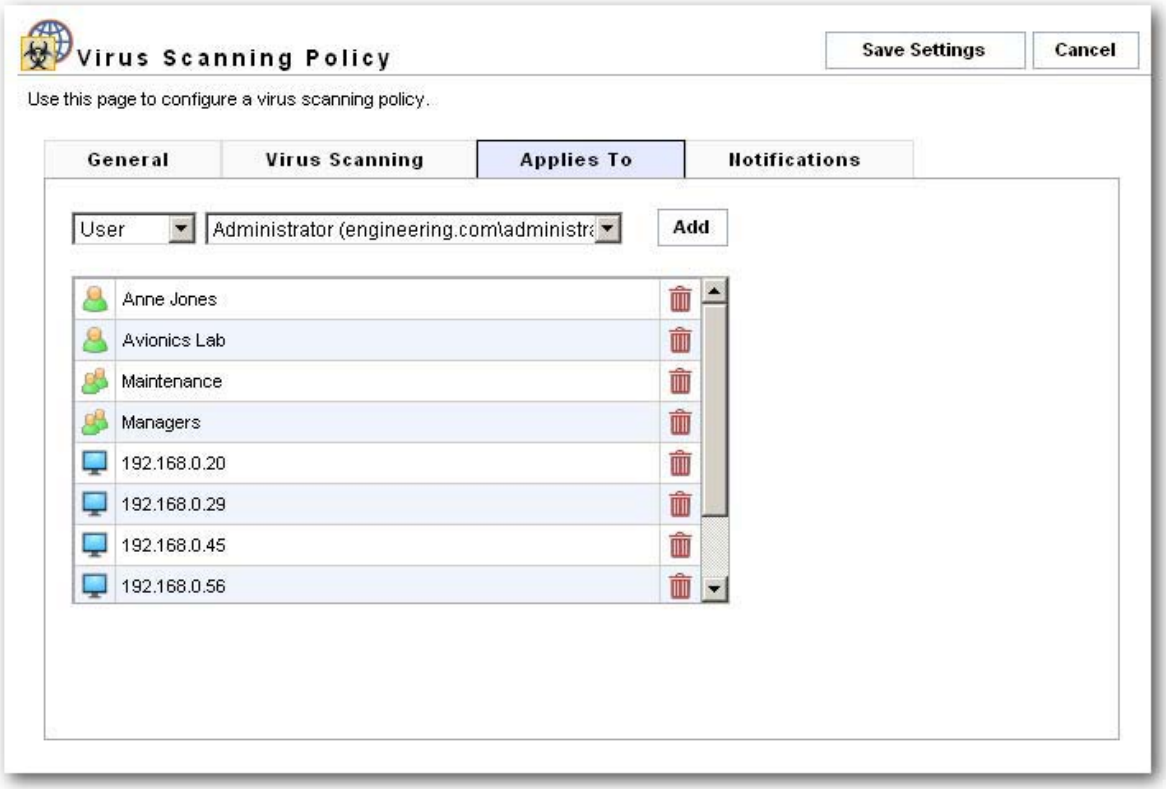
4. Введите имя и описание политики в поля Policy Name и Policy Description соответственно.



Снимок 36 – Добавление новой политики поиска вирусов: вкладка Virus scanning (Поиск вирусов)

5. Откройте вкладку Virus Scanning (Поиск вирусов) и щелкните тип файла, который требуется проверить. В диалоговом окне Change Action (Изменить действие) при необходимости выберите Display download progress and status (Отображение процесса и состояния загрузки) и выберите механизм сканирования. Кроме этого, выберите действие, которое требуется выполнить при обнаружении вируса. Это:

- Warn and Allow (Предупредить и разрешить)
- Block and Quarantine (Блокировать и изолировать)
- Block and Delete (Блокировать и удалить)

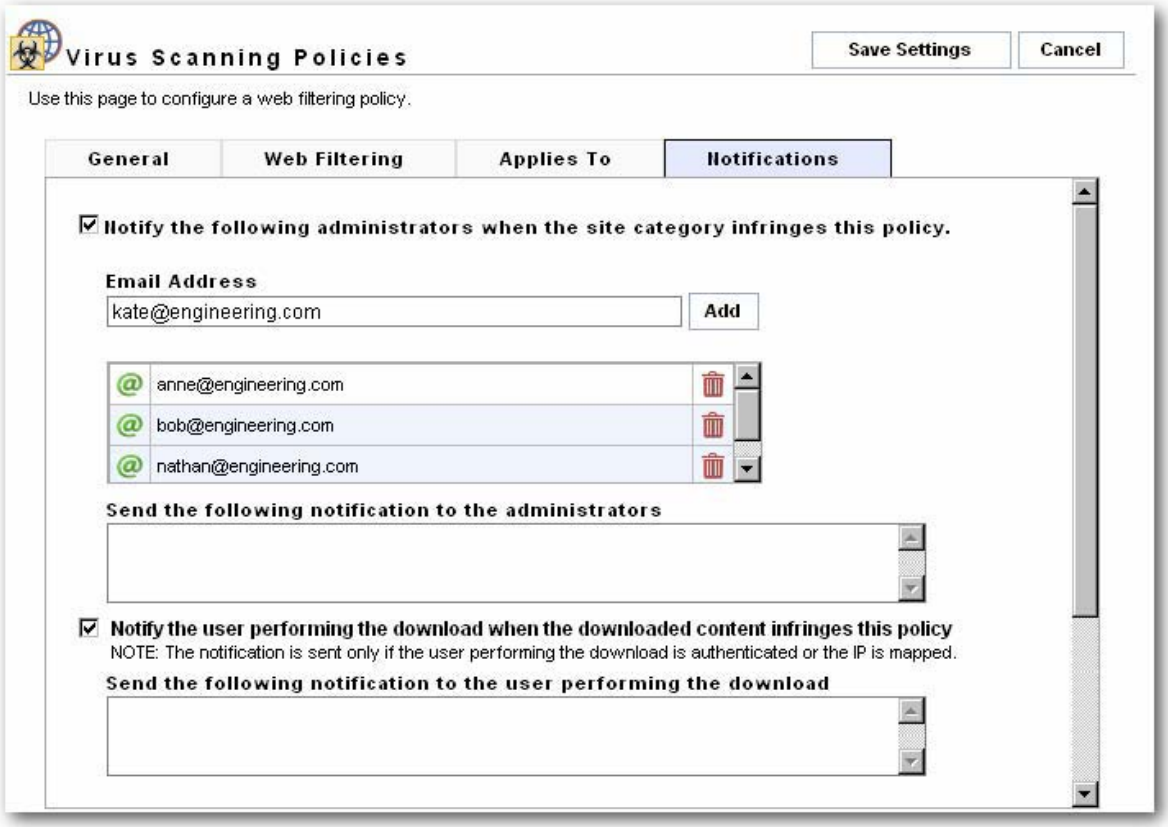


Снимок 37 – Добавление новой политики поиска вирусов: Вкладка Applies to tab (Применяется к)

6. Щелкните OK, откройте вкладку Applies To (Применяется к) и назначьте пользователя, группу и/или IP-адрес. Повторите для всех пользователей, групп и/или IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя, определите имя пользователя в формате DOMAIN\пользователь. Аутентификация ISA Server используется для проверки подлинности имени пользователя.

ПРИМЕЧАНИЕ 2: При добавлении групп аутентификация ISA Server используется для проверки подлинности имени группы.



Снимок 38 – Добавление новой политики поиска вирусов: вкладка Notification (Уведомление)

7. Откройте вкладку Notifications (Уведомления) и установите флажок Notify the following administrators when the download content infringes this policy (Уведомлять следующих администраторов при нарушении политики загрузок). Завершите установку вводом адреса электронной почты для уведомления администратора вместе с текстом уведомления. Также введите основной текст для уведомления в поле Send the following notification to the administrators (Отправить администраторам следующее уведомление).
8. При необходимости отправки уведомлений пользователям при нарушении политики установите флажок Notify the user performing the download when the downloaded content infringes this policy (Уведомлять пользователей при нарушении политики загрузок) и введите текст уведомления.

ПРИМЕЧАНИЕ 1: Уведомление отправляется только в случае, если возможна аутентификация ISA Server, и пользователь, таким образом, может быть идентифицирован.

9. Завершите настройку политики нажатием Save Settings (Сохранить настройки).

ПРИМЕЧАНИЕ 2: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Созданная политика будет отображена в основном представлении Virus Scanning Policies (Политики поиска вирусов).

Изменение политик поиска вирусов

Чтобы изменить политику поиска вирусов:

1. Щелкните WebSecurity Edition > Virus Scanning Policies (Политики поиска вирусов) в панели навигации.
2. Щелкните значок редактирования, расположенный рядом с политикой.
3. Для описания полей для редактирования см. раздел «Добавление политики поиска вирусов» в этой главе.
4. Завершите установку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Отключение политики поиска вирусов

Чтобы отключить политику поиска вирусов:

1. Щелкните WebSecurity Edition > Virus Scanning Policies (Политики поиска вирусов) в панели навигации.
2. Снимите флажок в столбце Enabled (Включено) для политики, которую требуется отключить.
3. Завершите отключение политики поиска вирусов нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Включение политики поиска вирусов

Чтобы включить политику поиска вирусов:

1. Щелкните WebSecurity Edition > Virus Scanning Policies (Политики поиска вирусов) в панели навигации.
2. Установите флажок в столбце Enabled (Включено) для политики, которую требуется включить.
3. Завершите включение политики поиска вирусов нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление политики поиска вирусов

Чтобы удалить политику поиска вирусов:

1. Щелкните WebSecurity Edition > Virus Scanning Policies (Политики поиска вирусов) в панели навигации.

2. Щелкните значок удаления, расположенный рядом политикой, выбранной для удаления.
3. Завершите удаление политики поиска вирусов нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Политика поиска вирусов по умолчанию

GFI WebMonitor - WebSecurity Edition включает политику поиска вирусов по умолчанию, применяемую ко всем пользователям. Название политики представлено как Default Virus Scanning Policy (Политика поиска вирусов по умолчанию).

Эту политику можно изменять, но нельзя заблокировать или удалить. При необходимости изменить заданную по умолчанию политику см. «Изменение политики поиска вирусов» в этой главе.

ПРИМЕЧАНИЕ 1: Любая созданная пользователем политика поиска вирусов имеет приоритет над заданной по умолчанию политикой.

ПРИМЕЧАНИЕ 2: Определенные поля в заданной по умолчанию политике нельзя изменить. Это Policy Name (Название политики), Policy Description (Описание политики) и поля на вкладке Applies To (Применяется к).

Механизмы сканирования

С помощью предсталвения Virus & Spyware Protection (Защита от вирусов и шпионских программ) можно:

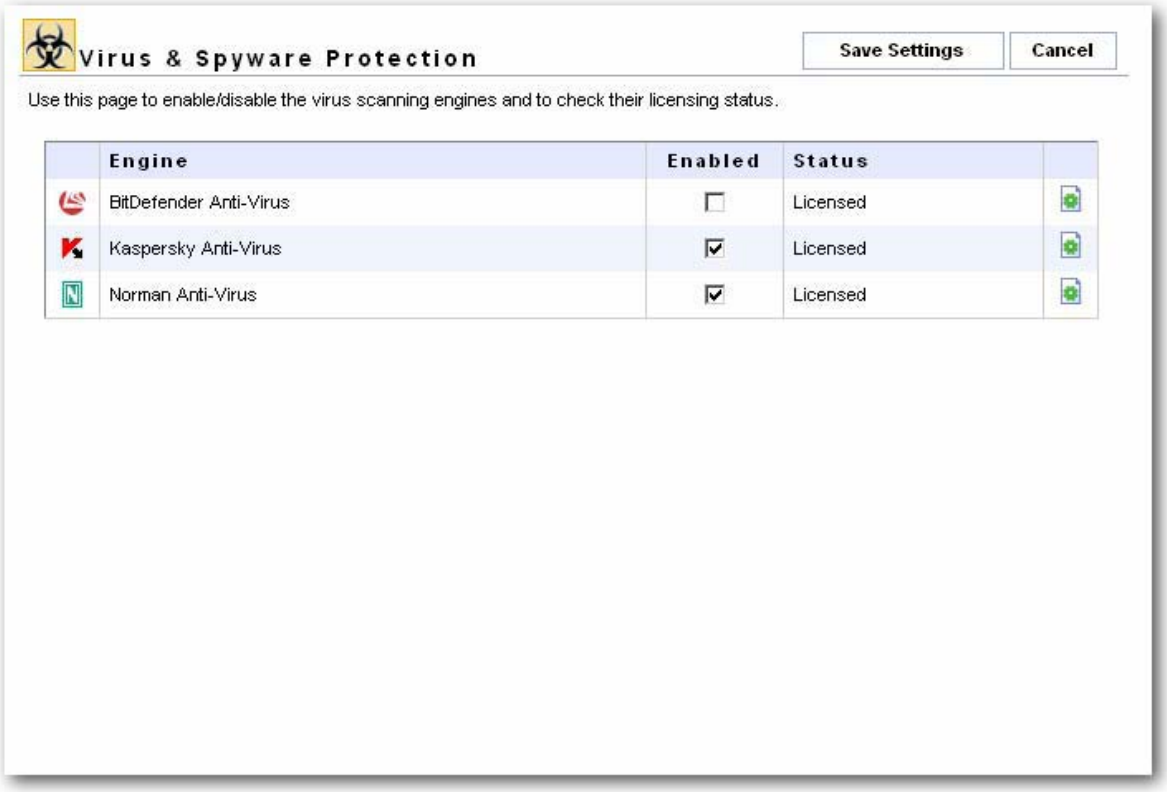
- Включить/выключить один или более поддерживаемых механизмов
- Просматривать состояние лицензии
- Настраивать обновления антивирусного механизма/сигнатур для каждого из механизмов сканирования

Для доступа к представлению Virus & Spyware Protection (Защита от вирусов и шпионских программ) выберите WebSecurity Edition > Virus Scanning Policies > Virus & Spyware Protection в панели навигации.

Включение/отключение механизмов сканирования

Чтобы включить или отключить один или более механизмов сканирования:

1. Выберите WebSecurity Edition > Virus Scanning Policies > Virus & Spyware Protection.



Снимок 39 – Защита от вирусов и шпионских программ

2. Установите или снимите флажок в столбце Enabled (Включено), чтобы включить или выключить проверку с помощью антивирусного сканера.

ПРИМЕЧАНИЕ: Отключение механизма сканирования означает, что GFI WebMonitor не будет использовать этот механизм.

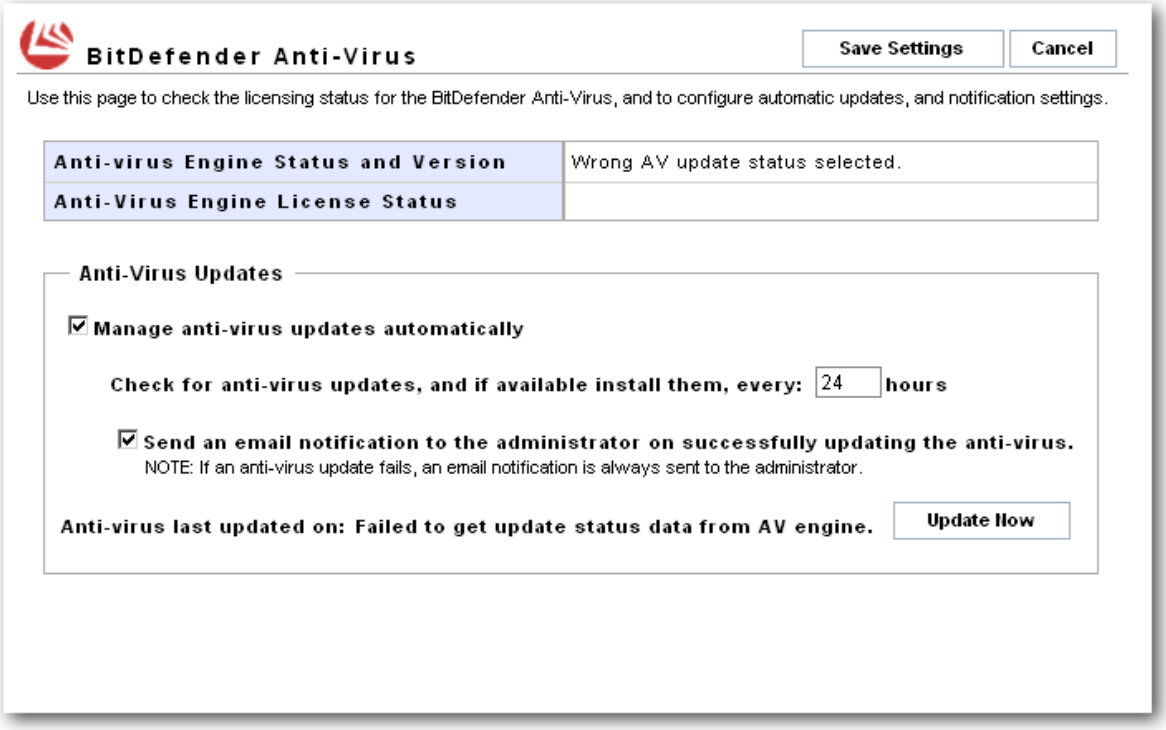
3. Завершите настройку механизма сканирования нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

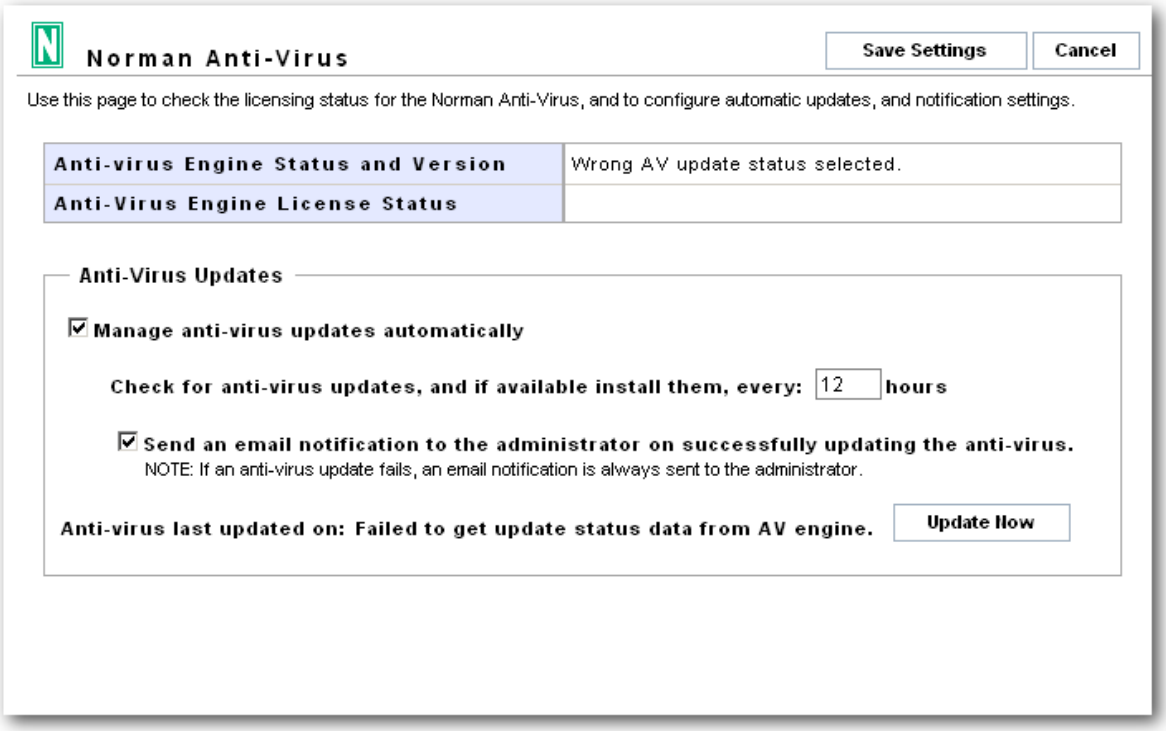
Настройка обновлений антивируса

Используя представление конфигурации для каждого из поддерживаемых механизмов сканирования можно:

- Просматривать состояние механизма сканирования, версию и лицензию
- Устанавливать или снимать флажки для автоматического или ручного обновления механизма сканирования/сигнатур
- Настраивать частоту установки доступных обновлений
- Устанавливать или снимать флажки, позволяющие настраивать уведомления, отправляемые после успешного обновления механизмов сканирования /сигнатур
- Вручную обновлять механизмы сканирования /сигнатуры нажатием кнопки Update Now.



Снимок 40 – Защита от вирусов и шпионских программ: свойства BitDefender

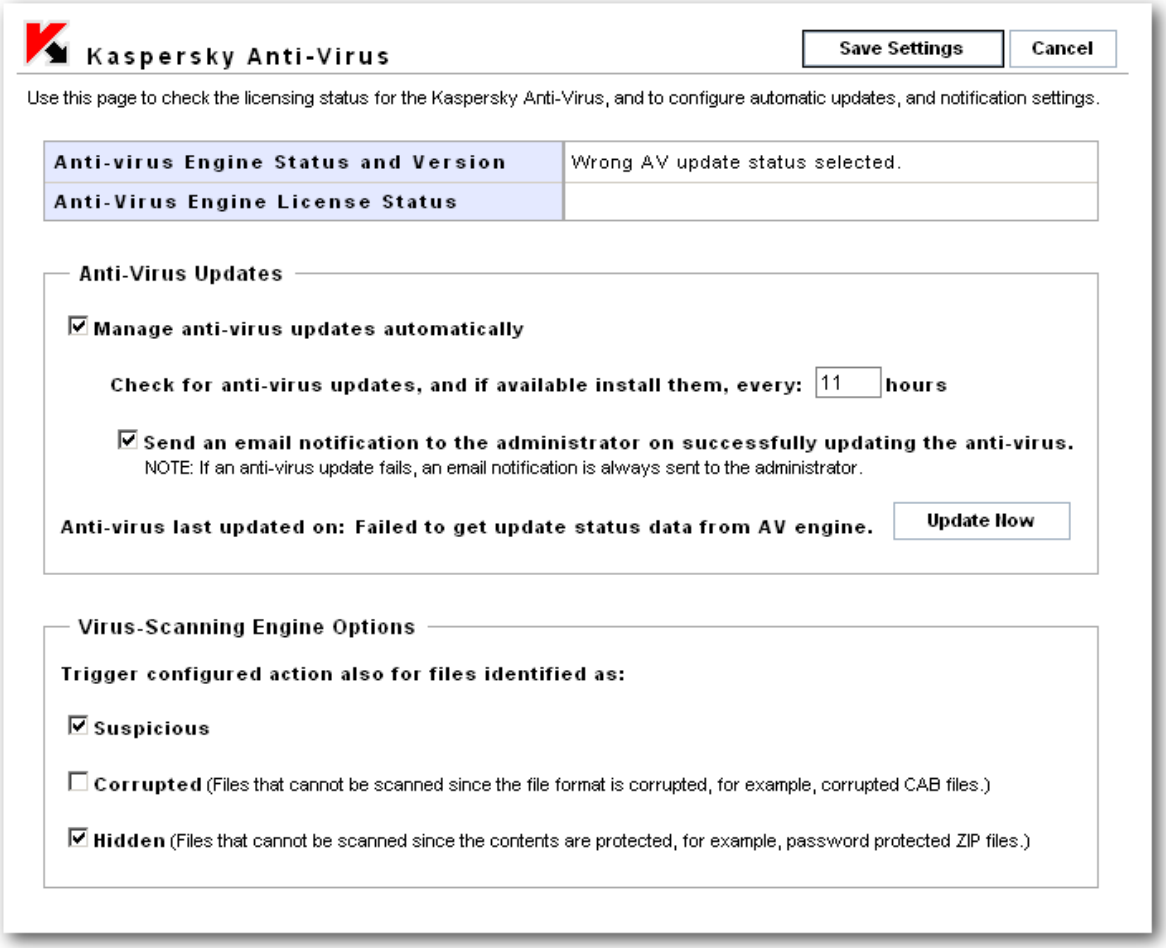


Снимок 41 – Свойства Norman Anti-Virus

Параметры механизма сканирования Kaspersky

Используя представление конфигурации для механизма сканирования Kaspersky, можно определить, должна ли применяться политика поиска вирусов, если файлы определяются как:

- Suspicious (Подозрительные)
- Corrupted (Поврежденные)
- Hidden (Скрытые)



Снимок 42 – Свойства Kaspersky Anti-Virus

1. Выберите WebSecurity Edition > Virus Scanning Policies > Virus & Spyware Protection.
2. Установите или снимите флажки, определяющие действия для файлов, определяемых как подозрительные, поврежденные или скрытые.
3. Завершите настройку нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Антифишинг

Используя механизм антифишинга можно:

- Включать/отключать антифишинг
- Просматривать лицензию механизма антифишинга
- Настраивать обновления базы данных антифишинга

Чтобы получить доступ к представлению Anti-Phishing Engine (Механизм антифишинга), выберите WebSecurity Edition > Anti-Phishing Engine в панели навигации.

Включение/отключение механизма антифишинга

Чтобы включить или отключить механизм антифишинга:

1. Щелкните WebSecurity Edition > Anti-Phishing Engine.
2. Откройте вкладку General (Общие).

Снимок 43 – Свойства механизм антифишинга

3. Установите или снимите флажок Block access to phishing sites (Блокировать доступ к фишинговым сайтам), чтобы включить или отключить механизм антифишинга.

ПРИМЕЧАНИЕ 1: Отключение механизма антифишинга подразумевает, что GFI WebMonitor не может использовать механизм блокирования фишинговых сайтов.

4. Завершите настройку механизма антифишинга нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ 2: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Настройка обновлений базы данных антифишинга

Используя флажки в области Anti-Phishing Updates (Обновления антифишинга) в представлении Anti-Phishing Engine (Механизм антифишинга) можно:

- Настраивать автоматическое или ручное обновление базы данных антифишинга
- Настраивать частоту установки доступных обновлений
- Настраивать отправку уведомлений после успешного обновления базы данных антифишинга
- Вручную обновлять базу данных антифишинга нажатием кнопки Update (Обновить).

Чтобы настроить обновления базы данных антифишинга:

1. Щелкните WebSecurity Edition > Anti-Phishing Engine.
2. Откройте вкладку General (Общие).
3. Определите необходимые параметры настройки в области Anti-Phishing Updates (Обновления атнифишинга).
4. Завершите установку обновлений базы данных антифишинга нажатием Save Settings (Сохранить параметры).

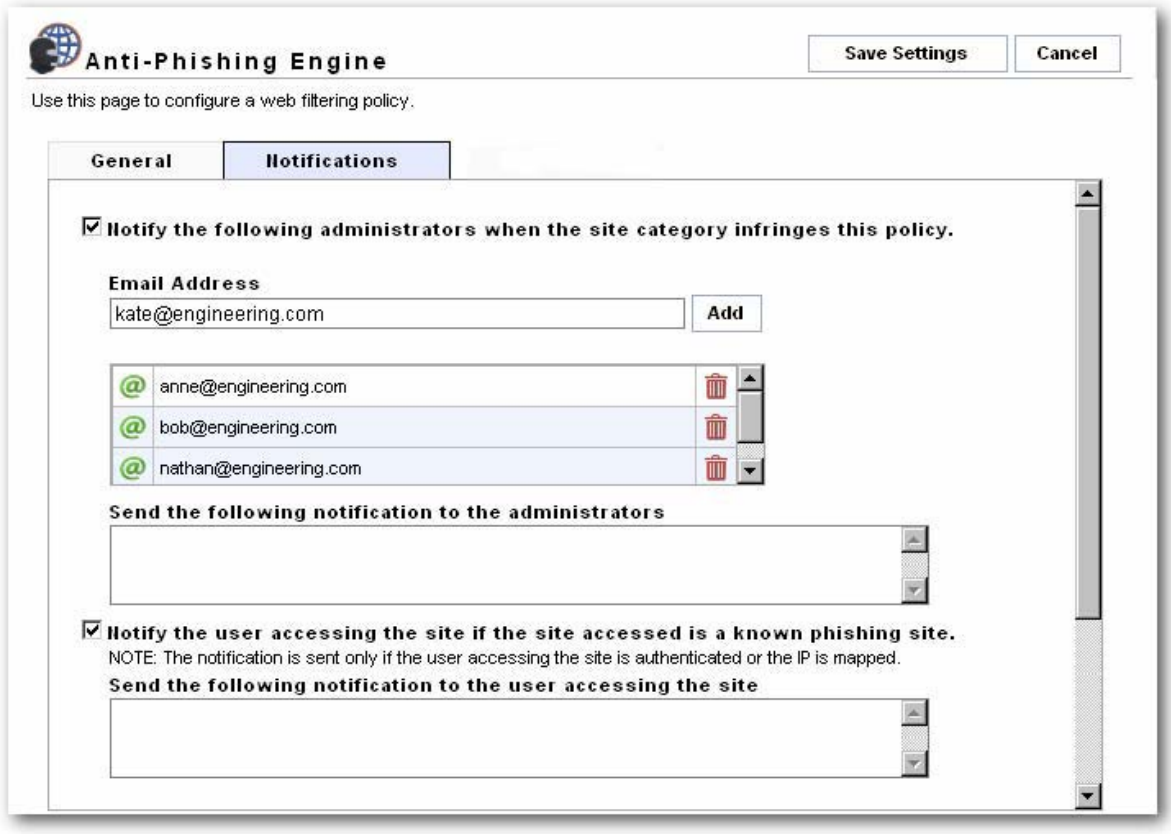
ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Настройка уведомлений антифишинга

На вкладке Notifications (Уведомления) в представлении Anti-Phishing Engine (Механизм антифишинга) можно установить отправку уведомлений при доступе к известному фишинговому сайту.

Чтобы включить уведомления:

1. Щелкните WebSecurity Edition > Anti-Phishing Engine.



Снимок 44 – Вкладка Notifications (Уведомления)

2. Откройте вкладку Notifications (Уведомления) и установите флажок Notify the following administrators when the site accessed is a known phishing site (Уведомлять следующих администраторов при доступе к известному фишинговому сайту). Завершите установку вводом адреса электронной почты для уведомления администратора вместе с текстом уведомления. Также введите основной текст для уведомления в поле Send the following notification to the administrators (Отправить администраторам следующее уведомление).
3. При необходимости уведомления пользователя при доступе к фишинговому сайту установите флажок Notify the user accessing the site if the site accessed is a known phishing site (Уведомлять пользователя при доступе к фишинговому сайту) и введите текст сообщения.

ПРИМЕЧАНИЕ: Уведомление отправляется только в случае, если возможна аутентификация ISA Server, и пользователь, таким образом, может быть идентифицирован.

4. Завершите настройку уведомлений нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Обработка заблокированных загрузок

Введение

GFI WebMonitor включает функцию каратнитина – ограниченную, безопасную и управляемую область хранения потенциально небезопасных загруженных файлов. Используя политику, можно блокировать и изолировать загруженные файлы/URL-адреса. Загруженные файлы могут быть изолированы в результате применения одной или более политик в следующих категориях:

- Политики управления загрузкой
- Политики веб-фильтрации
- Политики поиска вирусов

Администраторы должны выполнять обзор карантина, чтобы:

- Установить причину, по которой изолируется файл загрузки
- Определить, вреден ли файл или безопасен, и должен ли он быть удален или нет.

Если доступ будет разрешен, изолированные элементы передаются во временный «белый» список. В этом случае пользователям можно предоставить доступ к загруженным файлам через временный «белый» список.

Существует четыре различных представления изолированных элементов:

- Изолированные сегодня
- Изолированные вчера
- Изолированные на этой неделе
- Все изолированные элементы

Разрешенные или удаленные элементы

Просмотр изолированных элементов

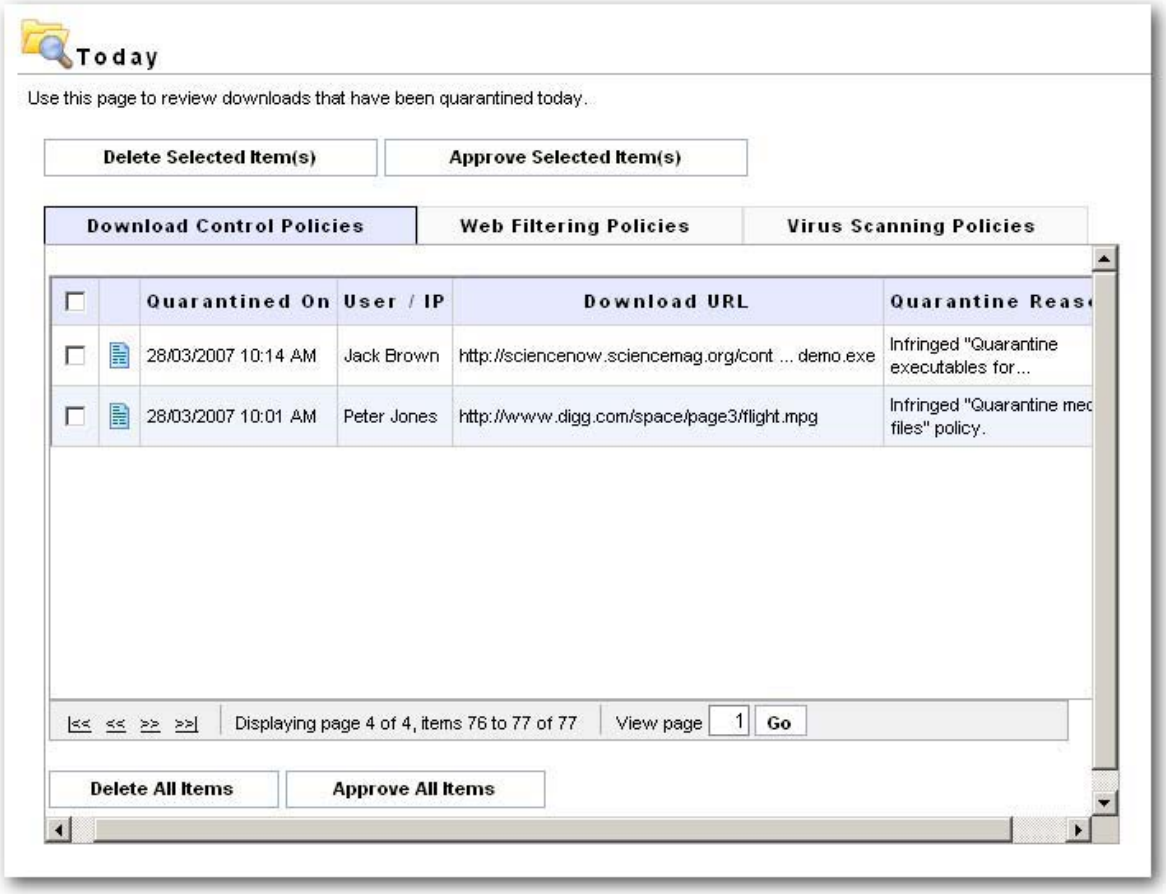
Следующая информация представлена для всех элементов в карантине:

- Дата и время, когда элемент был изолирован
- Пользователь/IP-адрес, который обратился к изолированному элементу
- Данные об URL-адресе изолированного элемента
- Причина изоляции элемента

Чтобы просмотреть изолированные элементы:

1. Чтобы просмотреть все элементы или выбранные за определенный период, выберите узел Quarantine (Карантин) в панели навигации и выберите одно из доступных представлений:

- Today (Сегодня)
- Yesterday (Вчера)
- This Week (На этой неделе)
- All Items (Все элементы)



Снимок 45 – Карантин

2. Выберите одну из доступных вкладок, чтобы просмотреть список элементов, изолированных для каждой соответствующей категории:

- Вкладка Download Control Policies (Политики управления загрузками)
- Вкладка Web Filtering Policies (Политики веб-фильтрации)
- Вкладка Virus Scanning Policies (Политики поиска вирусов)

Списки отсортированы в порядке убывания, с последним изолированным элементом сверху.

3. Чтобы просмотреть подробную информацию об элементе, щелкните значок деталей.
4. Чтобы вернуться к списку изолированных элементов, щелкните Go Back To List (Вернуться к списку).
5. Чтобы перемещаться по списку изолированных элементов, используйте значки навигации.

Разрешение изолированных элементов

Чтобы разрешить один или более изолированных элементов:

1. Щелкните узел Quarantine (Карантин) и выберите одно из доступных представлений, в зависимости от времени изоляции.
2. Откройте вкладку политики, где хранится изолированный элемент.
3. Щелкните значок деталей.

Снимок 46 – Разрешение изолированного элемента

4. Щелкните Approve Item (Разрешить элемент), чтобы загруженный файл был доступен всем пользователям, или Approve All Items (Разрешить все элементы), чтобы пользователям были доступны все элементы в карантине.

ПРИМЕЧАНИЕ 1: Адрес электронной почты пользователя отображается только в том случае, если осуществляется аутентификация через ISA Server, и если пользователь имеет действительное поле Active Directory.

ПРИМЕЧАНИЕ 2: С помощью флажка, связанного с каждой записью в карантине, можно включить «белый» список множества файлов.

ПРИМЕЧАНИЕ 3: Используйте эту функцию с большой осторожностью. При разрешении элемента из карантина веб-сайт исключается из всех политик GFI WebMonitor для определенного пользователя. Разрешение потенциально опасного файла может поставить сеть под угрозу.

Разрешенные элементы передаются во временный «белый» список. Для получения информации о «белом» списке см. главу «Разрешенные и запрещенные сайты».

ПРИМЕЧАНИЕ 4: Изолированные элементы, которые не разрешены по истечении 2 дней, автоматически удаляются.

Удаление изолированных элементов

Чтобы удалить один или более изолированных элементов:

1. Щелкните узел Quarantine (Карантин) и выберите одно из доступных представлений, в зависимости от времени изоляции.
2. Откройте вкладку политики, где хранится изолированный элемент.
3. Щелкните значок деталей.
4. Если загруженный файл требуется удалить, нажмите Delete Item (Удалить элемент).
5. Щелкните Delete Selected Item (Удалить выбранный элемент), чтобы удалить выбранный элемент, или Delete All Items (Удалить все элементы), чтобы удалить все элементы.

ПРИМЕЧАНИЕ 1: С помощью флажка, связанного с каждой записью в карантине, можно включить удаление множества файлов.

ПРИМЕЧАНИЕ 2: Изолированные элементы, которые не разрешены по истечении 2 дней, автоматически удаляются.

Разрешенные и запрещенные сайты

Введение

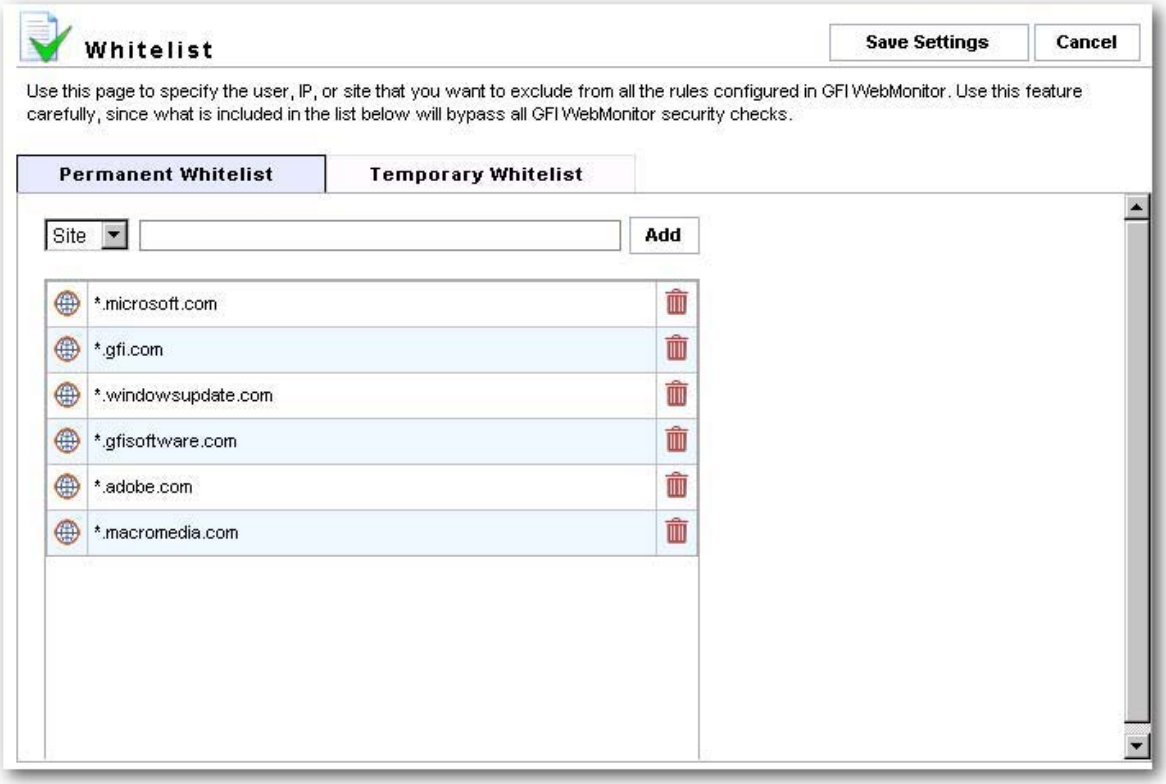
«Белые» и «черные» списки – это политики проверки содержимого, имеющие приоритет над всеми политиками WebFilter и WebSecurity Editions.

«Белый» список – это список сайтов, пользователей и IP-адресов, разрешенных администратором из всех политик GFI WebMonitor. Помимо постоянного «белого» списка существует временный, используемый для временного разрешения доступа к сайтам для пользователя или IP-адреса. Поскольку все политики WebFilter и WebSecurity отменяются, «белый» список следует использовать с большой осторожностью.

«Черный» список – список сайтов, пользователей и IP-адресов, которые всегда должны блокироваться независимо от политик, «белого» списка GFI WebMonitor.

«Черный» список имеет приоритет над «белым» списком GFI WebMonitor. Таким образом, если сайт входит в «черный» список и «белый» список одновременно, сайт будет заблокирован.

Создание «белого» списка



Снимок 47 – «Белый» список GFI WebMonitor

Для доступа к «белому» списку выберите узел «белый» список в панели навигации.

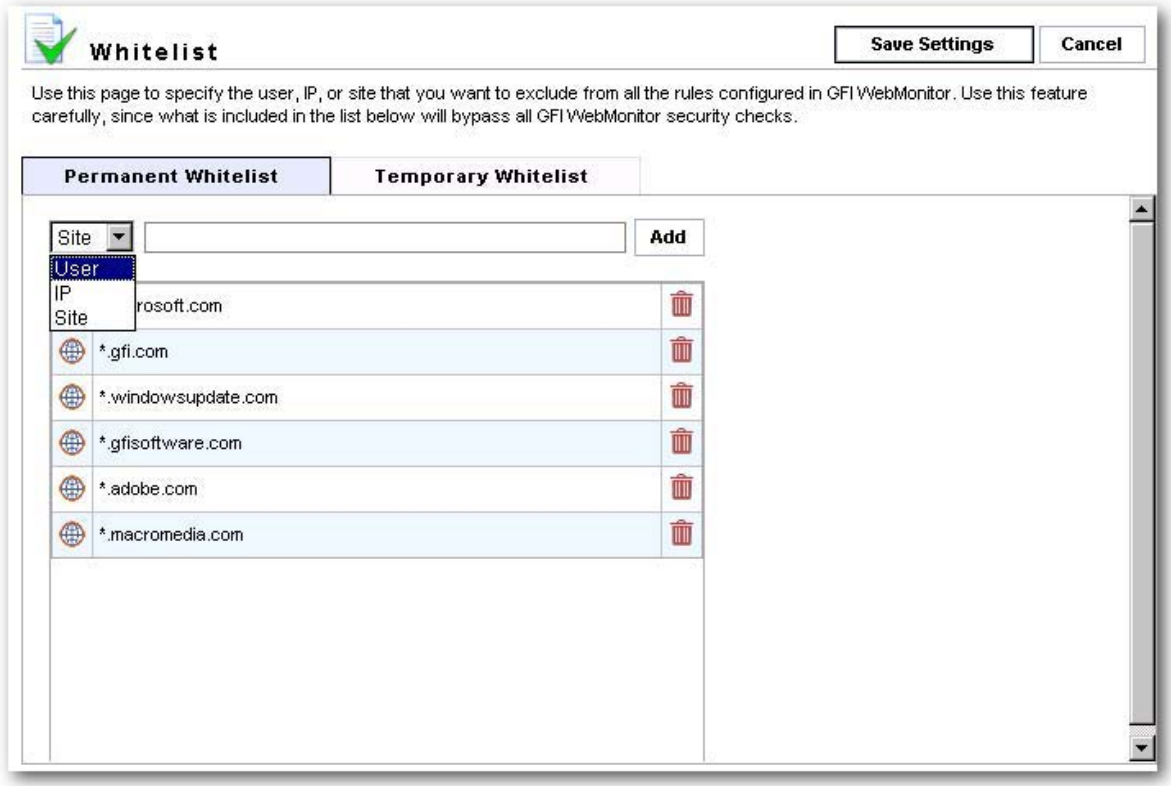
Предварительно настроенные элементы

По умолчанию GFI WebMonitor включает многие предварительно настроенные сайты в постоянный «белый» список. В него входят веб-сайты GFI, чтобы разрешить автоматическое обновление GFI WebMonitor, и веб-сайты Microsoft, чтобы разрешить автоматическое обновление Windows. Удаление любого из этих сайтов блокирует важные обновления.

Добавление элементов к постоянному «белому» списку

Чтобы добавить элемент к постоянному «белому» списку:

1. Выберите узел «белый» список и откройте вкладку Permanent Whitelist (Постоянный «белый» список).



Снимок 48 – Добавление элементов «белого» списка

2. В раскрывающихся списках выберите, будут ли пользователь, IP-адрес или сайт добавлены к «белому» списку и для какого пользователя, группы и/или IP-адреса будет применяться новый элемент «белого» списка. Повторите для всех пользователей, групп и/или IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя к «белому» списку, введите имя пользователя в формате DOMAIN\пользователь. Для проверки подлинности имени пользователя используется аутентификация ISA Server.

ПРИМЕЧАНИЕ 2: Добавляя сайт к «белому» списку, можно использовать подстановочные знаки. Для получения дополнительной информации см. раздел «Использование подстановочных знаков» в этой главе.

3. Чтобы добавить новый элемент к списку, щелкните Add (Добавить), а затем нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ 3: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление элементов из постоянного «белого» списка

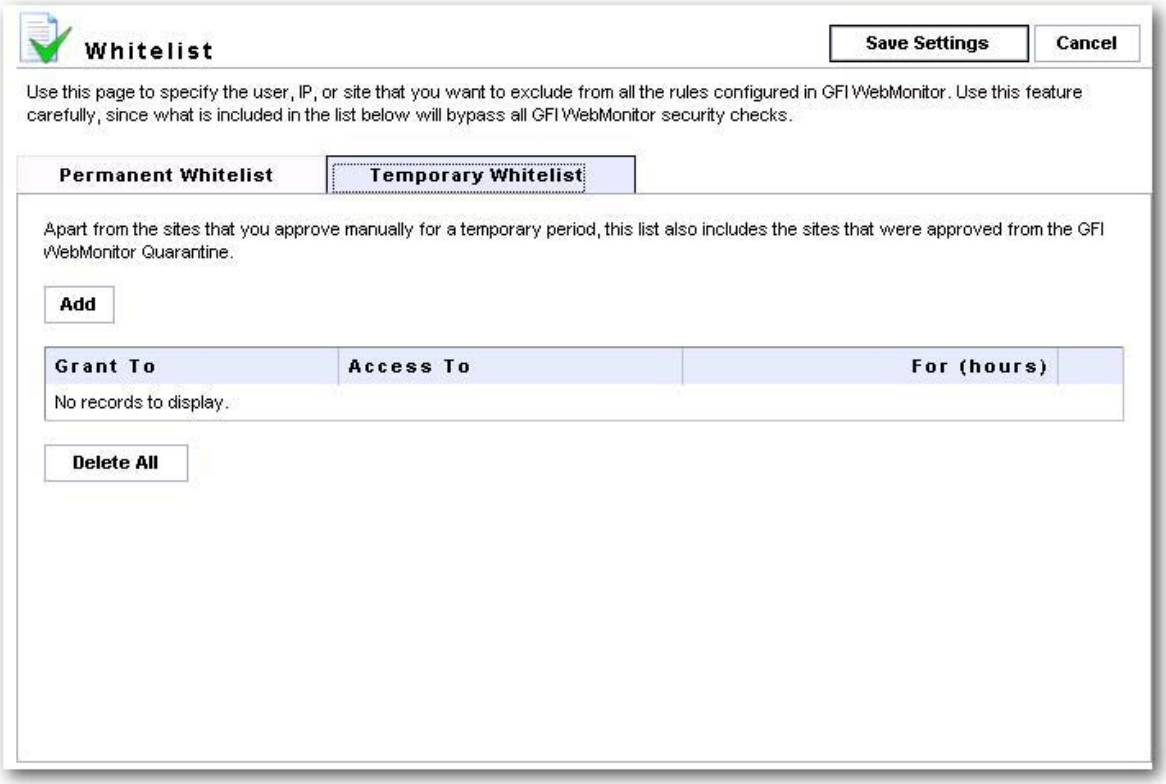
Чтобы удалить элемент из постоянного «белого» списка:

1. Выберите узел «белый» список и откройте вкладку Permanent Whitelist (Постоянный «белый» список).
2. Щелкните значок удаления, расположенный рядом элементом, выбранным для удаления.
3. Завершите удаление элементов «белого» списка нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

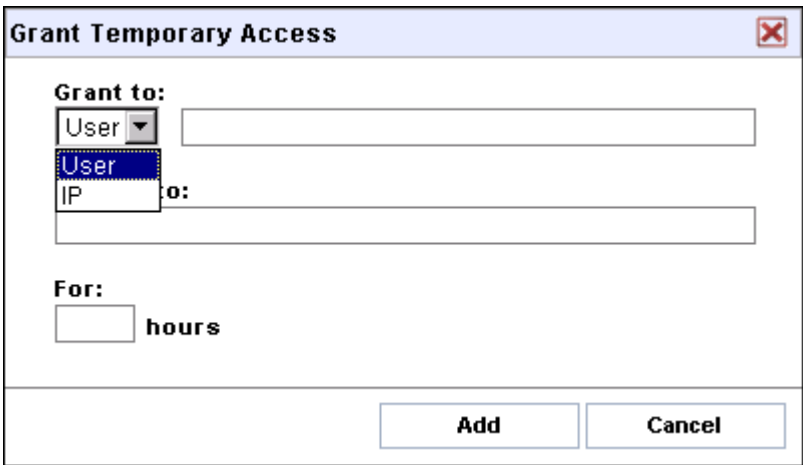
Добавление элементов к временному «белому» списку

Чтобы добавить элемент к временному «белому» списку:



Снимок 49 – Временный «белый» список

1. Выберите узел «белый» список и откройте вкладку Temporary Whitelist (Временный «белый» список).



Снимок 50 – Временный «белый» список: предоставление временного доступа

2. Нажмите Add (Добавить) и выберите предоставление временного доступа пользователю или IP-адресу. Введите данные о пользователе или IP-адресе для предоставления временного доступа, а также URL-адрес и время в часах.

ПРИМЕЧАНИЕ 1: При предоставлении временного доступа пользователю введите имя пользователя в формате DOMAIN\пользователь. Для проверки подлинности имени пользователя используется аутентификация ISA Server.

ПРИМЕЧАНИЕ 2: Добавляя сайт к «белому» списку, можно использовать подстановочные знаки. Для получения дополнительной информации см. раздел «Использование подстановочных знаков» в этой главе.

3. Чтобы добавить новый элемент к списку, щелкните Add (Добавить), а затем нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАЕНИЕ 3: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

ПРИМЕЧАЕНИЕ 4: Время в часах, в течение которого пользователю или IP предоставляется доступ к сайту, считается с момента нажатия Save Settings (Сохранить параметры).

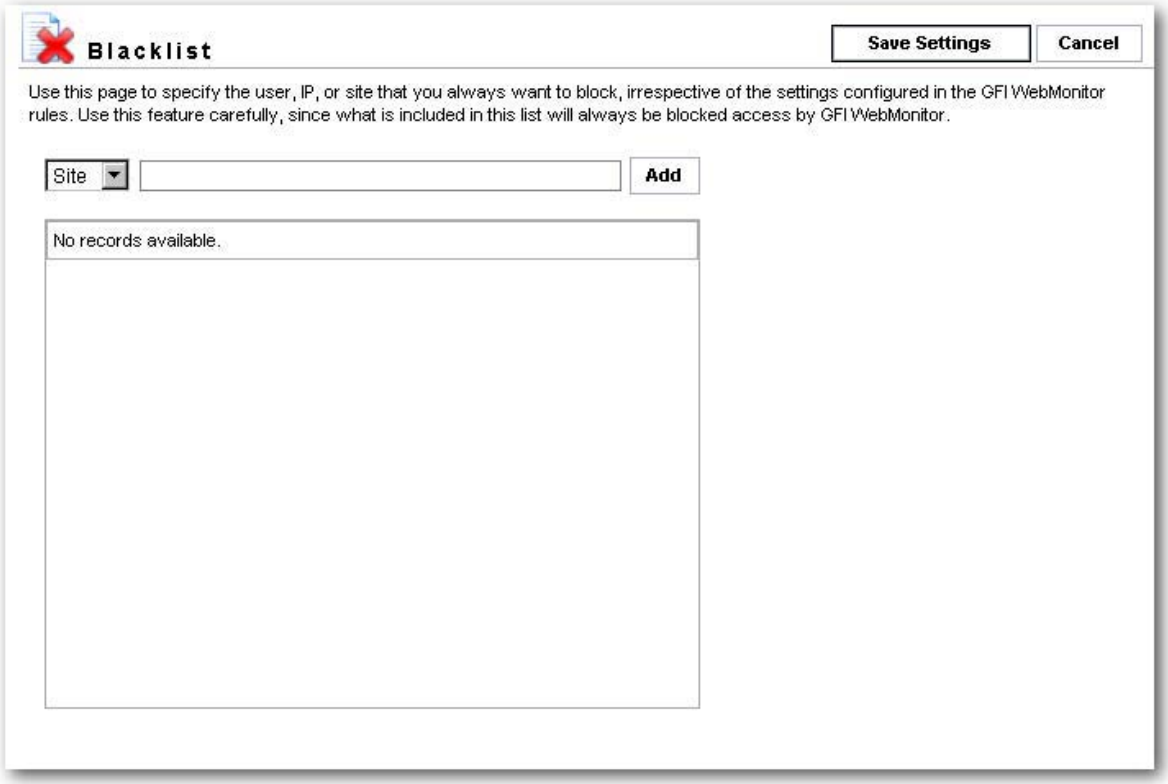
ПРИМЕЧАЕНИЕ 5: Время, оставшееся до прекращения доступа, отображается в столбце For (hours) (Для (часы)) в представлении Temporary Whitelist (Временный «белый» список).

Удаление элементов из временного «белого» списка

1. Выберите узел «белый» список и откройте вкладку Temporary Whitelist (Временный «белый» список).
2. Щелкните значок удаления, расположенный рядом элементом, выбранным для удаления.
3. Завершите удаление элементов «белого» списка нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Создание «черного» списка



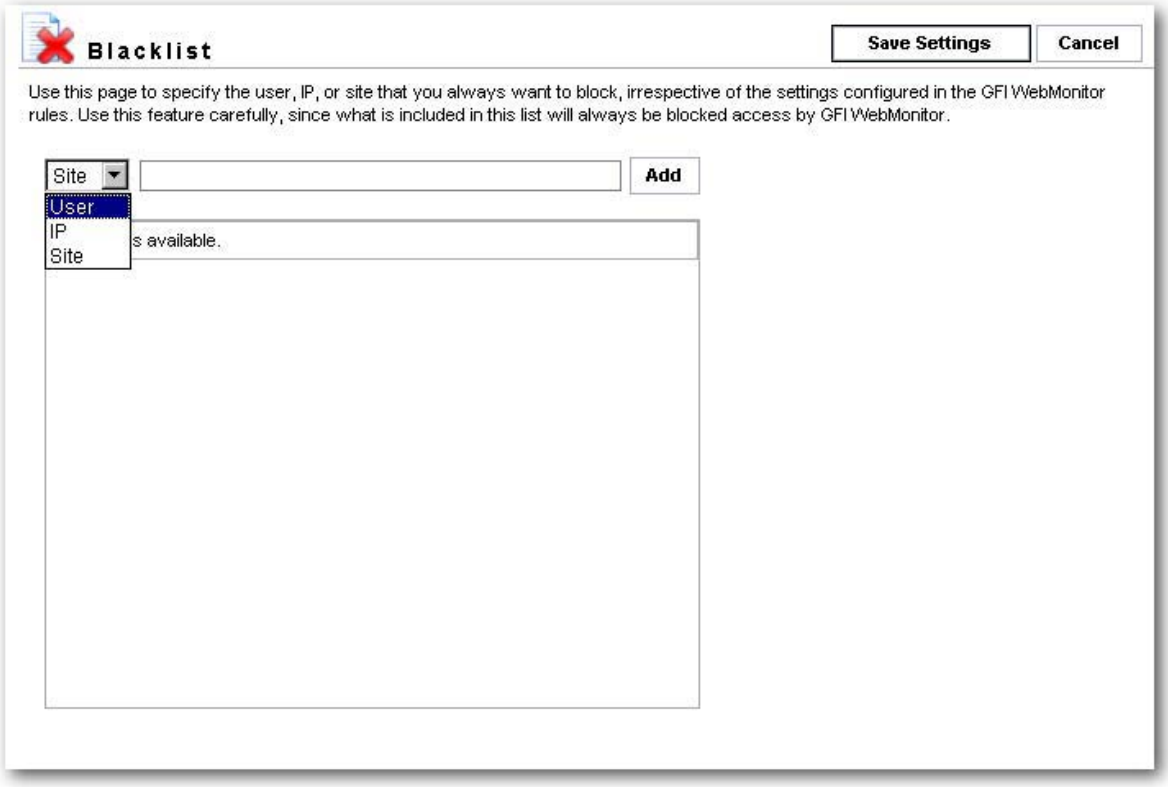
Снимок 51 – «Черный» список GFI WebMonitor

Чтобы получить доступ к «черному» списку, выберите узел Blacklist в панели навигации.

Добавление элементов «черному» списку

Чтобы добавить элемент к «черному» списку:

1. Выберите узел Blacklist в панели навигации.



Снимок 52 – Добавление элементов в «черный» список

2. В выпадающих списках выберите, будут ли пользователь, IP-адрес или сайт добавлены к «черному» списку и для какого пользователя, группы и/или IP-адреса будет применяться новый элемент «черного» списка. Повторите для всех пользователей, групп и/или IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя к «черному» списку, определите имя пользователя в формате DOMAIN\пользователь. Для проверки подлинности имени пользователя используется аутентификация ISA Server.

ПРИМЕЧАНИЕ 2: При добавлении сайта к «черному» списку можно использовать подстановочные знаки. Для получения дополнительной информации см. раздел «Использование подстановочных знаков» в этой главе.

3. Чтобы добавить новый элемент к списку, щелкните Add (Добавить), а затем нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ 3: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление элементов из «черного» списка

Чтобы удалить элемент из «черного» списка:

1. Выберите узел Blacklist в панели навигации.
2. Щелкните значок удаления, расположенный рядом элементом, выбранным для удаления.

3. Завершите удаление элементов «черного» списка нажатием Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Использование специальных символов

При добавлении сайта к «белому» или «черному» списку можно использовать подстановочные знаки как показано в примерах ниже:

Пример	Описание
*.com	Разрешить/заблокировать все домены верхнего уровня .com
*.website.com	Разрешить/заблокировать все субдомены website.com

Конфигурация GFI WebMonitor

Введение

GFI WebMonitor позволяет конфигурировать заданный по умолчанию набор параметров, используемых WebFilter и WebSecurity. Эти параметры настроены через три узла:

- Administrative Access Control (Управление контролем доступа): конфигурация доступа к веб-интерфейсу GFI WebMonitor для настройки и мониторинга.
- Notifications (Уведомления): конфигурация опций для уведомлений о важных событиях.
- General Settings (Общие параметры): конфигурация политик сохранения данных, загрузки кэша и временного «белого» списка.

Управление контролем доступа

Доступ к GFI WebMonitor основан на IP-адресе или проверки имени пользователя через ISA Server. Доступ разрешен только пользователям/IP-адресам из авторизованного списка.

Добавление пользователей/IP-адресов к списку доступа

Чтобы добавить пользователя или IP-адрес к списку доступа:

1. Выберите узел Administrative Access Control (Управление контролем доступа).

Снимок 53 – Настройка управления контролем доступа

2. В выпадающих списках выберите, будут ли пользователь, группа или IP-адрес добавлены к «белому» списку, и для какого пользователя, группы и/или IP-адреса будет применяться новый элемент «белого» списка. Повторите для всех пользователей, групп и/или IP-адресов.

ПРИМЕЧАНИЕ 1: Добавляя пользователя к списку управления доступа, определите имя пользователя в формате DOMAIN\пользователь. Для проверки подлинности имени пользователя используется аутентификация ISA Server.

3. Чтобы добавить новый элемент к списку, щелкните Add (Добавить), а затем нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ 2: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление пользователей/IP-адресов из списка доступа

Чтобы добавить пользователя или IP-адрес к списку доступа:

1. Выберите узел Administrative Access Control (Управление контролем доступа).
2. Щелкните значок удаления, расположенный рядом с пользователем/IP-адресом, которые требуется удалить.

3. Чтобы завершить удаление пользователей/IP-адреса нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Уведомления

Следующие уведомления о важных событиях отправляются администраторам:

- Изолированные элементы
- Отказы обновлений базы данных WebGrade, антивирусных сигнатур
- Успешные обновления базы данных WebGrade, антивирусных сигнатур
- Истечение срока лицензии на обновления базы данных WebGrade и антивирусных сигнатур.

Параметры конфигурации электронной почты

Чтобы настроить электронную почту:

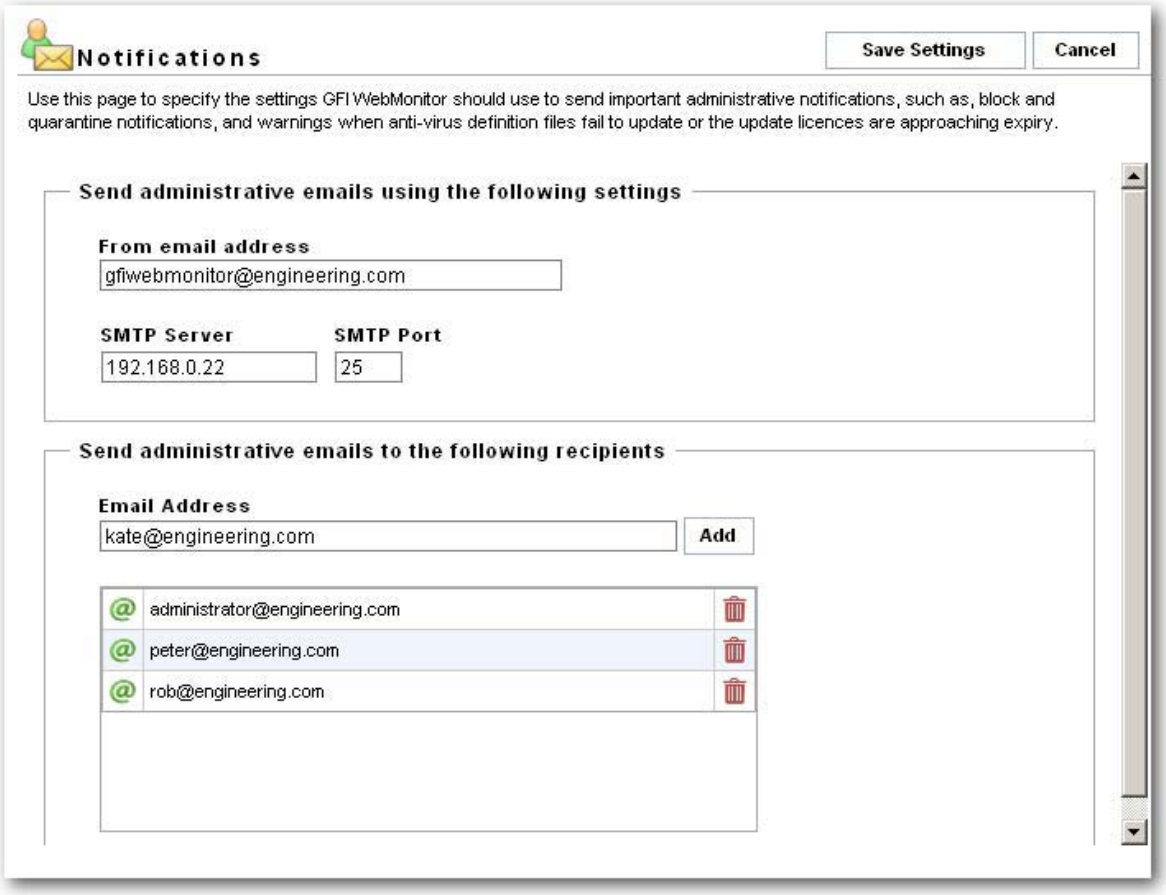
1. Выберите узел Notifications (Уведомления).
2. Перейдите к Send administrative emails using the following settings (Отправлять администраторам сообщения со следующими параметрами) и введите адрес, с которого будут отправляться уведомления, а также сервер SMTP и порт SMTP.
3. Чтобы завершить настройку параметров нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Параметры получателей электронной почты

Чтобы добавить получателей, которым будут отправляться уведомления:

1. Выберите узел Notifications (Уведомления).



Снимок 54 – Конфигурация уведомлений

2. Введите адрес электронной почты в поле Email Address и нажмите Add (Добавить).
3. Чтобы завершить настройку параметров нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Удаление получателей

1. Выберите узел Notifications (Уведомления).
2. Щелкните значок удаления, расположенный рядом с адресом, выбранным для удаления.
3. Чтобы завершить настройку параметров нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: Если кнопка Save Settings (Сохранить параметры) не будет нажата, вы потеряете параметры настройки, как только перейдете в другой раздел GFI WebMonitor.

Общие параметры

Используя узел General Settings (Общие параметры) можно:

- Определить период в днях, в течение которого данные об активности будут хранится в базе данных GFI WebMonitor. Эти данные используются для мониторинга и отчетов относительно:

    - Истории посещений сайтов и истории по пользователям
    - Сайты, занимающие максимум пропускной способности и пользователи, занимающие максимум пропускной способности.

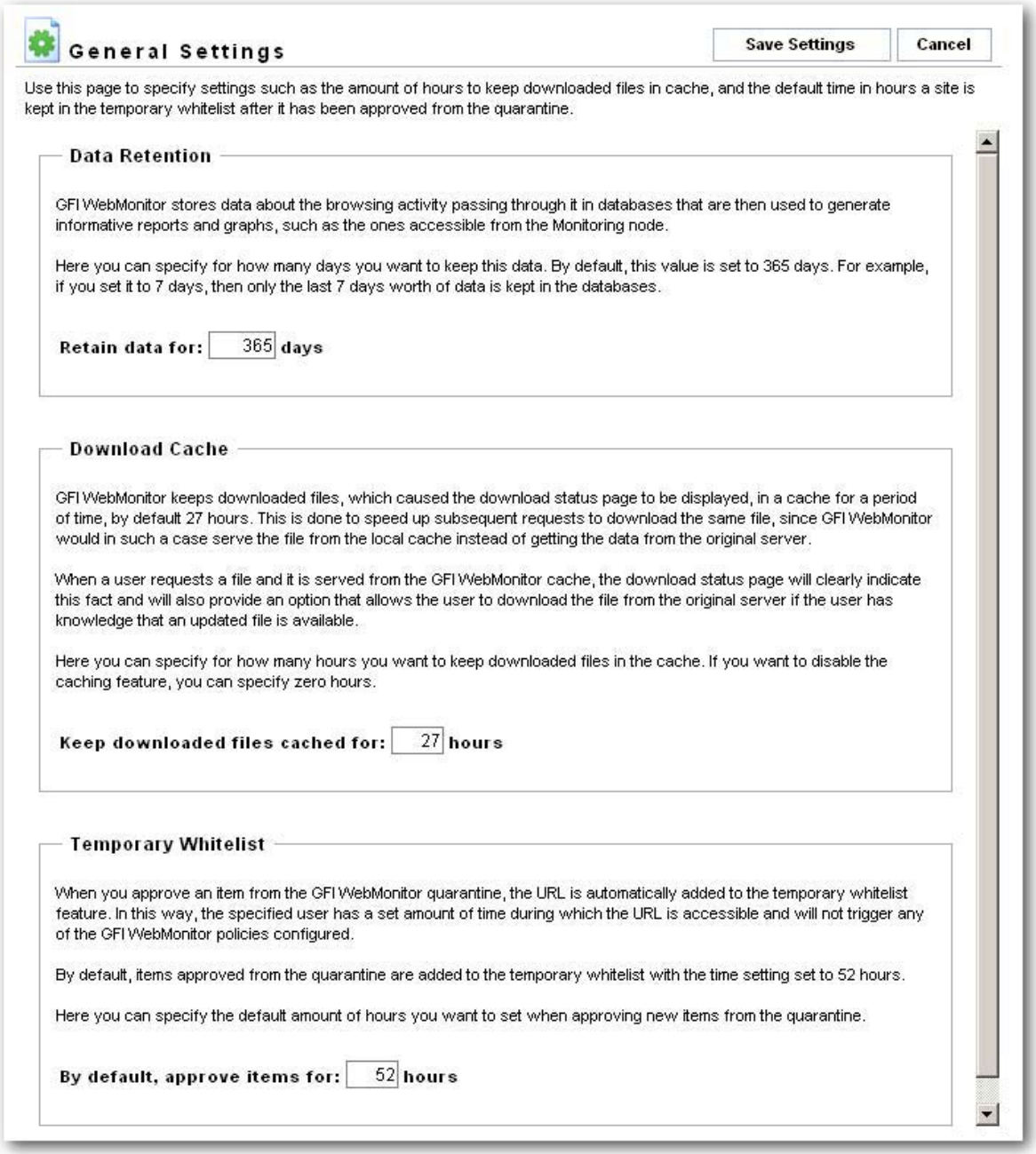
  По умолчанию установлен период в 365 дней.

- Определите период (в часах), в течение которого загруженные файлы будут храниться в локальном кэше. Хранение этих файлов в кэше ускорит последующие запросы этого же файла.

  По умолчанию установлено значение 27 часов. Если вы хотите отключить кэш, установите значение на ноль.

- Определите период (в часах), в течение которого разрешенные элементы карантина будут храниться во временном «белом» списке; это период, в течение которого разрешенный URL-адрес будет доступен.

  По умолчанию установлено значение 52 часа.



Снимок 55 – Настройка общих параметров

Настройка отчетов

Введение

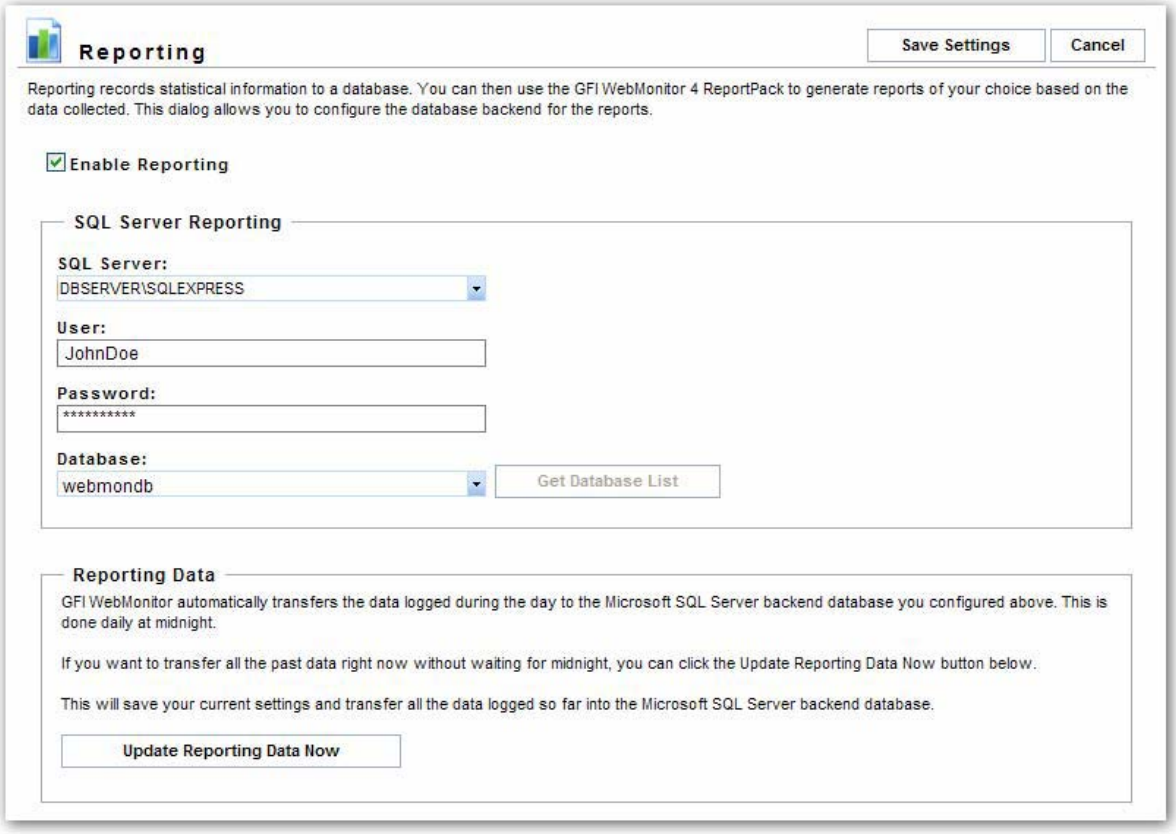
GFI WebMonitor позволяет хранить данные в базе данных для анализа статистической информации с помощью компонента отчетов GFI WebMonitor ReportPack. В этом разделе представлена следующая информация:

- Как включить или отключить сбор информации
- Настройка параметров отчетов

Включение функции создания отчетов

Чтобы включить сбор информации для создания отчетов:

1. Выберите узел Reporting (Отчеты).



Снимок 56 – Настройка отчетов в GFI WebMonitor

2. Чтобы включить функции создания отчетов, установите флажок Enable Reporting (Включить создание отчетов).
3. Введите данные о сервере SQL, базе данных и комбинацию пользователь/пароль, что позволит GFI WebMonitor подключиться и просматривать данные в базе данных.
4. Чтобы сохранить настройку отчетов нажмите Save Settings (Сохранить параметры).

ПРИМЕЧАНИЕ: В целях безопасности пароли могут быть задан только в машине, где установлен GFI WebMonitor.

Кнопка обновления данных отчета

Ежедневно в полночь GFI WebMonitor автоматически передает данные, зарегистрированные в базе данных Microsoft SQL Server. Однако бывают случаи, когда требуется вызвать процесс извлечения данных вручную:

- При обновлении версии GFI WebMonitor, поддерживающей отчеты.
- При миграции хранящихся в памяти данных в центральную базу данных
- Для проверки параметров конфигурации.

В этих случаях процесс извлечения данных осуществляется нажатием Update reporting data now (Обновить данные отчета).

ПРИМЕЧАНИЕ: Данные собираются в течение полных 24-часовых периодов с полуночи до полуночи. Нажатие Update reporting data now (Обновить данные отчета) не собирает данные за частичные периоды между полночью и временем нажатия кнопки.

Отключение функции создания отчетов

Чтобы отключить функции создания отчетов:

1. Выберите узел Reporting (Отчеты).
2. Чтобы отключить функцию создания отчетов снимите флажок в столбце Enable Reporting (Включить создание отчетов) и нажмите Save Settings (Сохранить настройки).

Разное

Введение

В этом разделе представлена следующая информация:

- Обновление лицензии GFI WebMonitor
- Обновление GFI WebMonitor

Ввод ключа лицензии после установки

После установки GFI WebMonitor введите ключ лицензии без переустановки и перенастройки продукта. Чтобы сделать это:

1. Выберите узел Licensing (Лицензирование) в панели навигации.
2. Введите ключ лицензии для одной из трех версий GFI WebMonitor в поле License Key.
3. Нажмите Verify License Key (Проверить ключ лицензии).

Проверка обновлений

Периодически GFI выпускает обновления подукта, котрые могут автоматически загружаться с веб-сайта GFI. Чтобы проверить доступность обновления:

1. Выберите узел Version Information (Информация о версии) в панели навигации.
2. Чтобы загрузить обновление, щелкните Check if a new build exists (Проверить обновления).

Устранение неисправностей

Введение

В этой главе описаны действия, которые следует выполнить для решения проблем. Основные источники информации, доступные для пользователей:

- Руководство – большинство проблем может быть решено при прочтении руководства.
- База знаний GFI – доступна на веб-сайте GFI.
- Сайт технической поддержки GFI.
- Посетите раздел расширенной поддержки пользователей GFI по адресу http://support.gfi.ru.
- Свяжитесь с нашей группой технической поддержки по телефону.

База знаний

GFI поддерживает Базу знаний, которая включает ответы на самые общие вопросы. Если у вас возникла проблема, пожалуйста, сначала проконсультируйтесь с Базой знаний. База знаний всегда содержит постоянно обновляемый список вопросов о поддержке и исправлениях.

Запрос информации по электронной почте

Вы всегда можете запросить интересующую вас информацию о продуктах по адресу электронной почты info@gfi.ru.