InfoWatch TMG Adapter. Руководство по установке и конфигурированию

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

08.09.2017

СОДЕРЖАНИЕ

1 Введение 2

2 Обзор TMG Adapter 3

2.1 Функции TMG Adapter 3

2.2 Состав TMG Adapter 3

2.3 Требования к программному обеспечению TMG Adapter 4

3 Установка и удаление TMG Adapter 4

3.1 Подготовка к установке решения 4

3.2 Установка решения 5

3.3 Первичная настройка решения 6

3.4 Запуск решения 7

3.5 Удаление решения 7

3.6 Настройка InfoWatch Traffic Monitor 7

4 Администрирование TMG Adapter 7

4.1 Настройка IW TMG Adapter 7

4.2 Настройка режима блокировки 8

4.2.1 Параметры режима блокировки 9

4.2.2 Страница блокировки 9

4.3 Счётчики производительности 9

4.4 Известные проблемы и их решение 10

4.4.1 Ошибка прав доступа при установке решения 11

4.4.2 Ошибка соединения с ICAP-сервером после установки решения 11

4.4.3 Отсутствие имени пользователя в Management Console 12

4.4.4 Отсутствие записей о загрузке файлов в Management Console 12

4.4.5 Неработающая загрузка файлов 13

4.4.6 Счётчики производительности TMG Adapter 13

4.4.7 Невозможность отправки писем загрузки файлов на определённых сервисах 13

Введение

В настоящем руководстве представлены сведения по установке, настройке и администрированию интеграционного решения TMG Adapter.

Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов InfoWatch Traffic Monitor Server с установленным компонентом InfoWatch ICAP и для администраторов Microsoft Forefront Thread Management Gateway 2010 (TMG), настраивающих интеграцию между этими продуктами.
Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Microsoft Windows и Linux, а также знакомых с основами администрирования InfoWatch Traffic Monitor. Кроме этого необходимо знание основ администрирования Microsoft Forefront TMG 2010.

Обзор TMG Adapter

В этой главе:

- Функции TMG Adapter;
- Состав TMG Adapter;
- Требования к программному обеспечению TMG Adapter.

2.1 Функции TMG Adapter

TMG Adapter (TMGA) предназначен для обеспечения взаимодействия InfoWatch Traffic Monitor и Microsoft Forefront TMG 2010. TMGA является дополнительным модулем Microsoft Forefront TMG 2010 типа Web Filter (фильтр).
TMGA позволяет решать задачу перехвата исходящих HTTP(S)-запросов и передачу копии трафика на InfoWatch Traffic Monitor по протоколу ICAP. Перехват исходящего трафика может осуществляться, как в неблокирующем, так и в блокирующем режиме. Это означает, что в первом случае результаты работы ICAP-сервера никак не влияют на прохождение трафика. А во втором — запросы, содержащие конфиденциальные данные, не будут переданы на удалённый сервер. При этом пользователю будет показано соответствующее уведомление.

2.2 Состав TMG Adapter

IW TMG Adapter состоит из следующих модулей:

1. модуль TMG Web Filter, осуществляющего перехват (и, при необходимости, блокировку) исходящего трафика и его отправку на IWTM;

2. модуль счётчиков производительности, позволяющий получать информацию о работе фильтра в реальном времени.

2.3 Требования к программному обеспечению TMG Adapter

Для работы TMG Adapter необходимо следующее программное обеспечение:

1. Microsoft Forefront TMG 2010;
2. InfoWatch Traffic Monitor 3.5, 4.x, 5.x, 6.x + компонент InfoWatch ICAP.

Установка и удаление TMG Adapter

В этой главе даны пошаговые инструкции по установке, первичной настройке и удалению интеграционного решения.
Установка производится на сервере Microsoft Forefront TMG 2010. Установка производится автоматически, с помощью инсталляционного пакета.
Для установки необходимы права:

- локального администратора;
- администратора массива (Forefront TMG Array Administrator), если установка производится на одиночный сервер TMG или серверы standalone массива;
- администратора enterprise (Forefront TMG Enterprise Administrator), если установка производится на серверы массива, администрируемого Enterprise Management Server.

Глава содержит следующую информацию:

- Подготовка к установке решения;
- Установка решения;
- Первичная настройка решения;
- Запуск решения;
- Удаление решения;
- Настройка InfoWatch Traffic Monitor.

3.1 Подготовка к установке решения

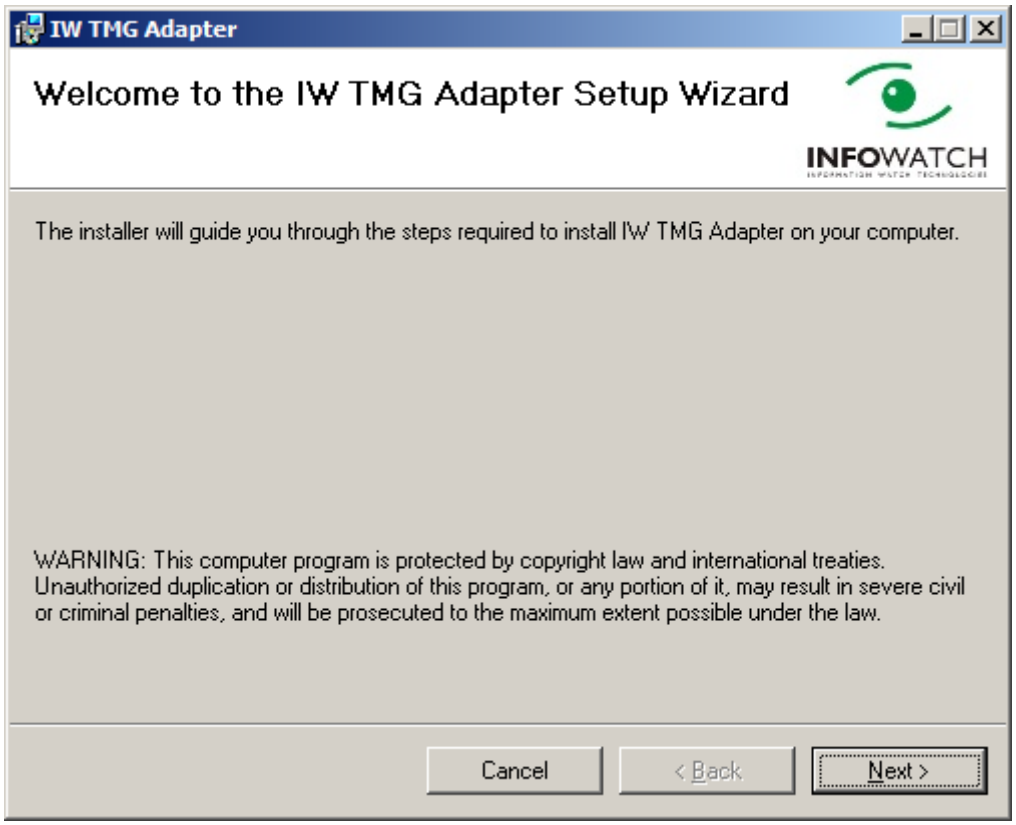
Перед установкой решения необходимо проделать следующие действия:

1. Если есть необходимость сохранять файлы логов TMGA, то создать каталог для сохранения этих файлов

2. Убедиться, что у созданного каталога есть права на запись для пользователя NETWORK SERVICE (от имени этого пользователя запускается служба Microsoft Forefront TMG Firewall)
3. Убедиться, что на диске, где расположен созданный каталог, достаточно свободного места для сохранения файлов логов. Размер файлов логов зависит от количества запросов в единицу времени, проходящих через фильтр, и от выставленного уровня логирования. Для работы в штатном режиме рекомендуется обеспечить наличие не менее 1 Гб свободного места.
4. Убедиться, что ICAP-сервер доступен с сервера, на котором установлен Microsoft Forefront TMG 2010. Для этого рекомендуется использовать инструмент Traffic Simulator, входящий в состав TMG. Если ICAP-сервер недоступен, то необходимо создать соответствующее разрешающее правило в Microsoft Forefront TMG Firewall.
5. Остановить службу Microsoft Forefront TMG Firewall.

3.2 Установка решения

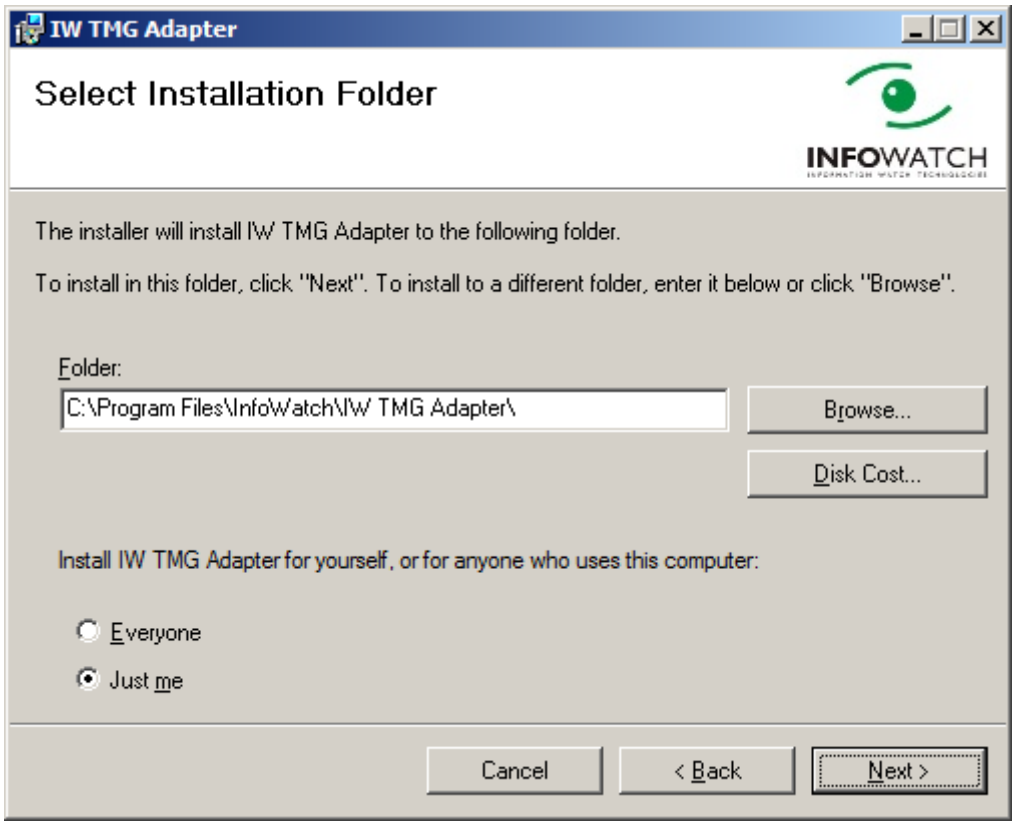
1. **Запустите установку**
   Запустить установочный файл `TMG Adapter.msi`.



2. **Задайте каталог установки**
   Задать каталог, где будет установлено решение TMG Adapter.

> **Важно!**

Использование каталога, название которого содержит спецсимволы или русские буквы приводит к нарушению работы сервера TMG.



3. **Выполните установку**
   Выполнить установку. Дождаться завершения работы инсталлятора.

3.3 Первичная настройка решения

После установки необходимо произвести первичную настройку решения. Настройка TMGA осуществляется редактированием файла tmga.ini, который представляет собой INI-файл конфигурации. Файл расположен в каталоге, куда было установлено решение TMG Adapter. После установки необходимо указать IP-адрес и порт для соединения с ICAP-сервером. Кроме того, для сохранения информации о проблемах, возникающих в процессе работы необходимо указать каталог для файлов логов. Также нужно убедиться, что у пользователя NETWORK SERVICES есть права на запись в данный каталог.
Помимо записи в файлы логов, сообщения с уровнями важности Information, Warning и Error будут продублированы в Event Log. В качестве источника таких сообщений указывается IW TMG Adapter.

Параметр	Описание
`IcapServerIp`	IP-адрес ICAP-сервера
`IcapServerPort`	Порт, по которому происходит соединение с ICAP-сервером

Параметр	Описание
`TracePath`	Путь для файлов логов и данных, передаваемых ICAP-серверу

3.4 Запуск решения

TMG Adapter запускается вместе со службой Microsoft Forefront TMG Firewall, поэтому для запуска решения необходимо запустить указанную службу.

3.5 Удаление решения

Удаление решения производится средствами ОС Windows из Панели Управления. Перед удалением необходимо остановить службу Microsoft Forefront TMG Firewall.

3.6 Настройка InfoWatch Traffic Monitor

Для корректного взаимодействия TMGA и IWTM необходимо, чтобы Traffic Monitor был настроен для перехвата HTTP-трафика, передаваемого по протоколу ICAP, при помощи модуля IW ICAP. Подробные инструкции по развёртыванию IWTM по данной схеме можно найти в документе «InfoWatch Traffic Monitor. Руководство по установке и конфигурированию». Для работы в блокирующем режиме необходимы соответствующие правки сценария анализа объектов на стороне InfoWatch Traffic Monitor. Информацию о необходимых правках можно найти в файле справки InfoWatch Traffic Monitor в разделе «Настройка параметров анализа объектов».

Администрирование TMG Adapter

Глава содержит следующие разделы:

- Настройка IW TMG Adapter;
- Настройка режима блокировки;
- Счётчики производительности;
- Известные проблемы и их решение.

4.1 Настройка IW TMG Adapter

Настройка TMGA осуществляется редактированием файла `tmga.ini`, который представляет собой INI-файл конфигурации. Файл расположен в каталоге, куда был установлен TMG Adapter. Параметры конфигурационного файла приведены в таблице ниже.

Параметр	Описание
LogLevel	Уровень логирования. Изменяется от 1 до 5. При нормальной работе должен равняться 3.
MaxIcapConnection	Максимальное количество открытых соединений с ICAP-сервером
IcapServerIp	IP-адрес ICAP-сервера
IcapServerPort	Порт, по которому происходит соединение с ICAP-сервером
IcapWaitTimeout	Время ожидания свободного соединения для передачи запроса на ICAP-сервер
IcapCheckInterval	Интервал проверки доступности ICAP-сервера, если он не был доступен при запуске фильтра
MaxRequestSize	Максимальный размер запроса в Кб, который будет передаваться на ICAP-сервер. Запросы большего размера передаваться на ICAP-сервер не будут.
CollectGetRequest	Нужно ли обрабатывать и передавать на ICAP-сервер GET-запросы (0 или 1)
BlockingMode	Режим блокировки запросов, содержащих конфиденциальную информацию (0 или 1)
AllowDataSendingOnNoIcap	Признак того, что при ошибке соединения с ICAP-сервером разрешается пересылать запросы на удалённый сервер (0 или 1)
AllowBigRequests	Признак того, что при превышении запросом параметра MaxRequestSize запрос разрешается пересылать на удалённый сервер
MaxAllowedAllocation	Максимально допустимый размер в Кб выделяемой под запрос памяти в Microsoft Forefront TMG
DbgDumpIo	Признак того, что нужно сбрасывать на диск данные, передаваемые ICAP-серверу
TracePath	Путь для файлов логов и данных, передаваемых ICAP-серверу

4.2 Настройка режима блокировки

При работе фильтра TMGA в режиме блокировки запросы, содержащие конфиденциальную информацию, не будут передаваться на удалённый сервер. Кроме того, пользователю будет показано уведомление о блокировке запроса. Возможна ситуация, когда вместо уведомления пользователь просто получает сообщение об ошибке либо со стороны используемого им сервиса (например, отправка писем на mail.ru), либо со стороны TMG.

В этой разделе:

- Параметры режима блокировки;
- Страница блокировки.

4.2.1 Параметры режима блокировки

Работа режима блокировки контролируется тремя переключателями в конфигурационном файле. Переключатель BlockingMode отвечает за включение/выключение режима блокировки в целом. Ещё два переключателя отвечают за поведение фильтра TMGA при возникновении внештатных ситуаций.
Переключатель AllowDataSendingOnNoIcap позволяет заблокировать все запросы (вне зависимости от того, содержится в них конфиденциальная информация или нет) при возникновении ошибки при общении с ICAP-сервером. В качестве ошибки может выступать как невозможность соединиться с ICAP-сервером, так и какая-либо ошибка, возникшая уже при непосредственной передаче данных. В случае возникновения подобной ошибки фильтр TMGA запишет информацию о ней в Event Log. Обратите внимание, что переключатель AllowDataSendingOnNoIcap совместно с переключателем CollectGetRequests и невозможностью соединиться с ICAP-сервером приведёт к полной невозможности использовать веб-браузеры, поскольку все запросы будут автоматически заблокированы.
Переключатель AllowBigRequests позволяет запретить все запросы, размер которых превышает значение параметра MaxRequestSize. Параметр MaxRequestSize ограничивает нагрузку на ICAP-сервер и InfoWatch Traffic Monitor, поскольку анализ больших запросов может занять продолжительное время. Если запрос превышает это значение, то на ICAP-сервер он посылаться не будет. Поэтому принять по нему вердикт, содержит он конфиденциальную информацию или нет, не представляется возможным. Блокировка (или наоборот разрешение) таких запросов производится с помощью ключа AllowBigRequests.

4.2.2 Страница блокировки

Страница, которая демонстрируется пользователю при блокировке его запроса, предоставляется ICAP-сервером, поэтому для информации по настройке этой страницы необходимо обратиться к документации по ICAP-компоненту InfoWatch Traffic Monitor.

4.3 Счётчики производительности

Для индикации процесса работы фильтра TMGA используется механизм счётчиков производительности (Performance Counters). Для просмотра значений счётчиков необходимо использовать оснастку Производительность (Performance Monitor snap-in) Microsoft Management Console. Счётчики, доступные в TMGA, приведены в таблице ниже.

Счётчик	Описание
HTTP requests	Число обработанных фильтром HTTP-запросов
HTTP requests per second	Число HTTP-запросов, обрабатываемых фильтром в секунду

Счётчик	Описание
GET request total	Полное число GET-запросов, обработанных фильтром
GET successes	Число GET-запросов, успешно переданных ICAP-серверу
GET failures	Число GET-запросов, которые не удалось передать ICAP-серверу
POST requests total	Полное число POST-запросов, обработанных фильтром
POST requests per second	Число POST-запросов, обрабатываемых фильтром в секунду
POST successes	Число POST-запросов, успешно переданных ICAP-серверу
POST failures	Число POST-запросов, которые не удалось передать ICAP-серверу
Bytes from TMG	Объём данных, в байтах, полученный фильтром от Microsoft Forefront TMG
Bytes from TMG per second	Объём данных, в байтах, который фильтр получает от Microsoft Forefront TMG в секунду
Bytes to ICAP	Объём данных, в байтах, переданный фильтром ICAP-серверу
Bytes to ICAP per second	Объём данных, в байтах, передаваемый фильтром ICAP-серверу в секунду
Available connections	Число свободных соединений, доступных в пуле соединений

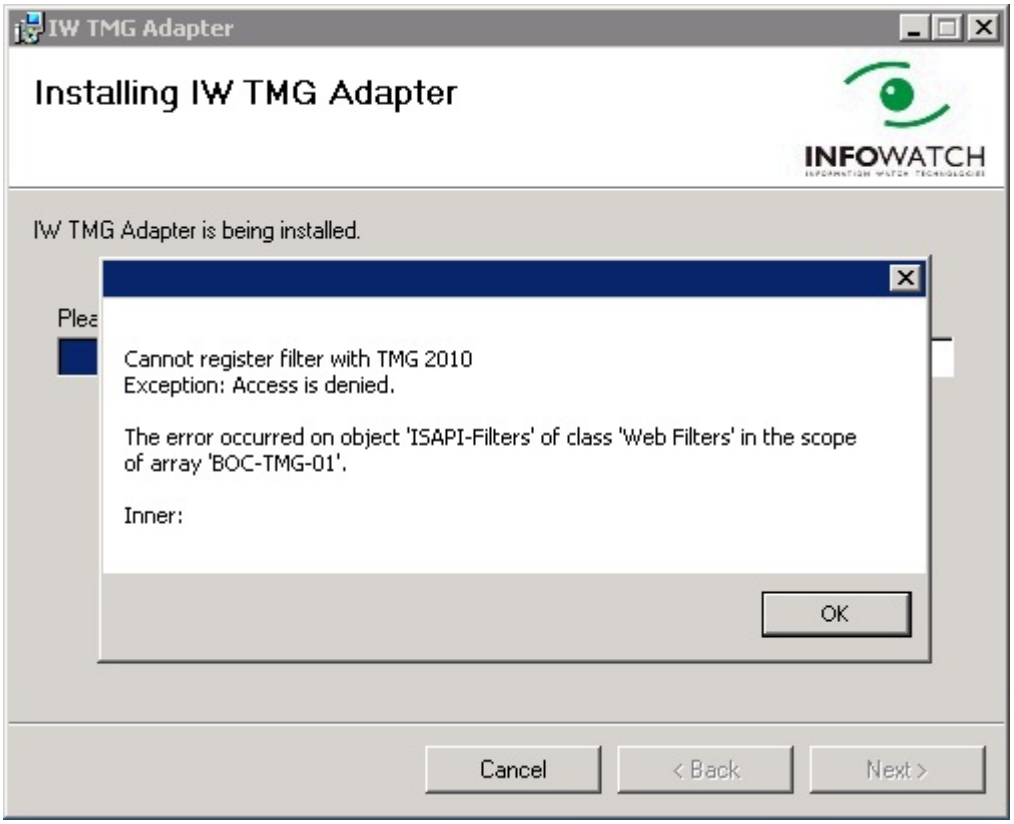
4.4 Известные проблемы и их решение

В этом разделе:

- Ошибка прав доступа при установке решения;
- Ошибка соединения с ICAP-сервером после установки решения;
- Отсутствие имени пользователя в Management Console;
- Отсутствие записей о загрузке файлов в Management Console;
- Неработающая загрузка файлов;
- Счётчики производительности TMG Adapter;
- Невозможность отправки писем загрузки файлов на определённых сервисах.

4.4.1 Ошибка прав доступа при установке решения

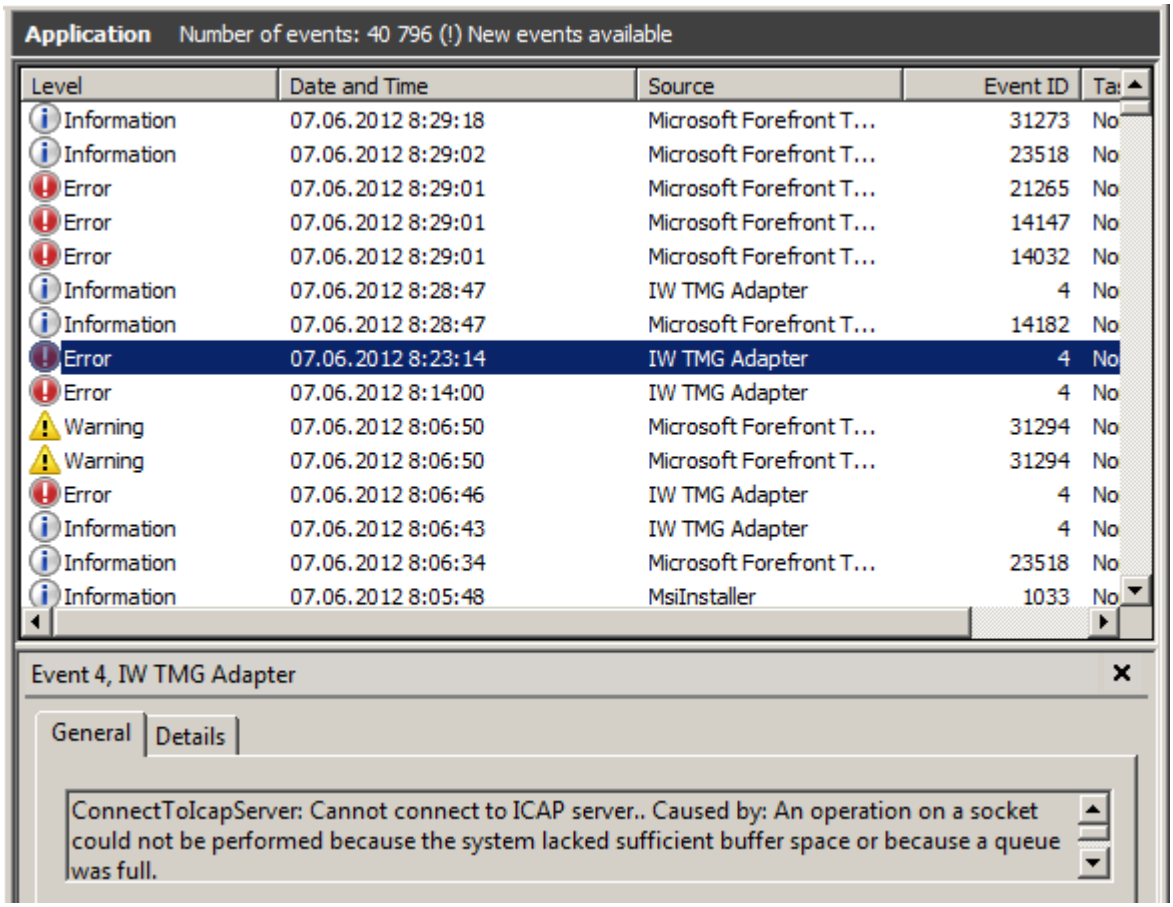
При установке решения от имени администратора массива на сервер массива, администрируемого Enterprise Management Server, может возникнуть ошибка прав доступа, показанная на изображении ниже.



При возникновении подобной ошибки необходимо после завершения установки удалить решение, а затем заново установить его от имени пользователя, имеющего права Forefront TMG Enterprise Administrator.

4.4.2 Ошибка соединения с ICAP-сервером после установки решения

После установки решения в Event Viewer появляются сообщения о невозможности соединения с ICAP-сервером следующего содержания: *Cannot connect to ICAP server. Caused by: An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.* На изображении ниже показано, как данная ошибка выглядит в Event Viewer.



Такая ошибка означает, что перед установкой решения не была остановлена служба Microsoft Forefront TMG Firewall. Для устранения ошибки необходимо перезапустить указанную службу.

4.4.3 Отсутствие имени пользователя в Management Console

После установки решения возможно появление в InfoWatch Management Console записей о перехвате HTTP-трафика по протоколу ICAP без указания имени авторизованного пользователя. Такая ситуация может быть обусловлена разрешающими правилами в Microsoft Forefront TMG 2010. Если в TMG существуют правила, разрешающие анонимный доступ (All Users), то запросы, которые были разрешены согласно этим правилам, будут отправляться на ICAP-сервер без данных об авторизации.

4.4.4 Отсутствие записей о загрузке файлов в Management Console

Если пользователь, использующий Microsoft Forefront TMG 2010, будет производить загрузку файлов на какие-либо веб-сервисы, то при превышении файлом определённого размера (зависящего от параметра MaxRequestSize в конфигурационном файле решения), информация о загрузке этого файла не будет передаваться на ICAP-сервер и, соответственно, не будет отображаться в Management Console.
При этом сообщения о таких событиях будут добавляться в Event Log. В качестве источника сообщения указывается IW TMG Adapter, уровень сообщения – Warning. В тексте сообщения указывается авторизованный пользователь и IP-адрес компьютера, с которого был совершён запрос, если Microsoft Forefront TMG 2010 сумел их определить.

4.4.5 Неработающая загрузка файлов

Возможна ситуация, когда при работе пользователей через Microsoft Forefront TMG 2010 у них некорректно работает загрузка файлов через плагин Adobe Flash в браузерах отличных от Microsoft Internet Explorer. Например, у пользователей может не работать прикрепление файлов к письмам на www.mail.ru, или загрузка изображений на сервис fotki.yandex.ru. Браузеры, отличные от Internet Explorer, не могут корректно провести авторизацию плагина Adobe Flash, поэтому TMG отклоняет соответствующие запросы. Решением данной проблемы является использование браузера Internet Explorer или создание на TMG правил, разрешающих анонимный доступ к конкретным сайтам, к которым обращается плагин Adobe Flash при загрузке файлов.

4.4.6 Счётчики производительности TMG Adapter

Возможна ситуация, когда после установки счётчиков производительности для TMG Adapter не получается просмотреть значения счётчиков (они не появляются в общем списке доступных счётчиков) или список счётчиков не содержит никаких значений. В этом случае необходимо в ключе реестра Windows «`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`» добавить параметр `Configuration Flags` типа `REG_DWORD` со значением `0x11`. Счётчики будут доступны после перезапуска Microsoft Management Console.

4.4.7 Невозможность отправки писем загрузки файлов на определённых сервисах

Если на фильтре TMGA включён режим блокировки, то при отправке писем или файлов через отдельные сервисы может возникнуть ошибка. Это связано с тем, что сервисы отправляют файлы/письма в фоновом режиме. Если такой запрос будет заблокирован ICAP-сервером, то сервис в фоне самостоятельно обработает ошибку и отобразит сообщение о невозможности отправки. В консоли InfoWatch Traffic Monitor такой запрос отображается, как заблокированный. Таким образом, подобное поведение связано с особенностями работы отдельных сервисов и фильтром TMGA контролироваться не может.