TrafficLog Documentation

(The following graphics are screen shots from Microsoft® ISA Server 2006 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate TrafficLog, which is the property of Collective Software.)

Table of Contents

Requirements

- ISA Server 2004/2006
- Microsoft .NET Framework version 2 should be installed on each ISA server.

Installation of TrafficLog

Install Procedure

1. Close the ISA management console if it's open.
2. Execute the TrafficLog.msi file. This will stop your firewall service, install the filter and interface software, register the filter, and then re-start the firewall service.
3. If you are installing over a remote desktop session, keep in mind that when the firewall service stops and restarts your RDP connection may be frozen, dropped or timed out. If an error occurs during the installation and the firewall service cannot be restarted, you will need to access the console to troubleshoot further (see below).
4. You must run the installer on each ISA server in an array separately, so they will all have the filter files installed and registered.
5. If the installation completes with no errors, then you can proceed to the configuration section.

Troubleshooting

The installation normally completes without errors. However there are a few possible failure modes that can occur for this complex install process.

Install rolls back (with red error message at the end)

If you are presented with an error message on the final screen, then check out the application event log, which often will contain details on why the installation failed. The problem may be immediately solvable from this information, or you may need to work with Collective support for additional troubleshooting assistance.

Frozen or hung install

The installer tries to start the firewall service after it is done registering the filter components. In rare cases, everything may register properly but there could still be a problem preventing the firewall service from starting. In this situation, the installation may appear to hang on the “Starting services...” item. This is because it is trying repeatedly to start the service, and failing. In fact if you look at the application event log, you will see several errors from the firewall service as it tries to start. These messages may help identify the cause of the problem.

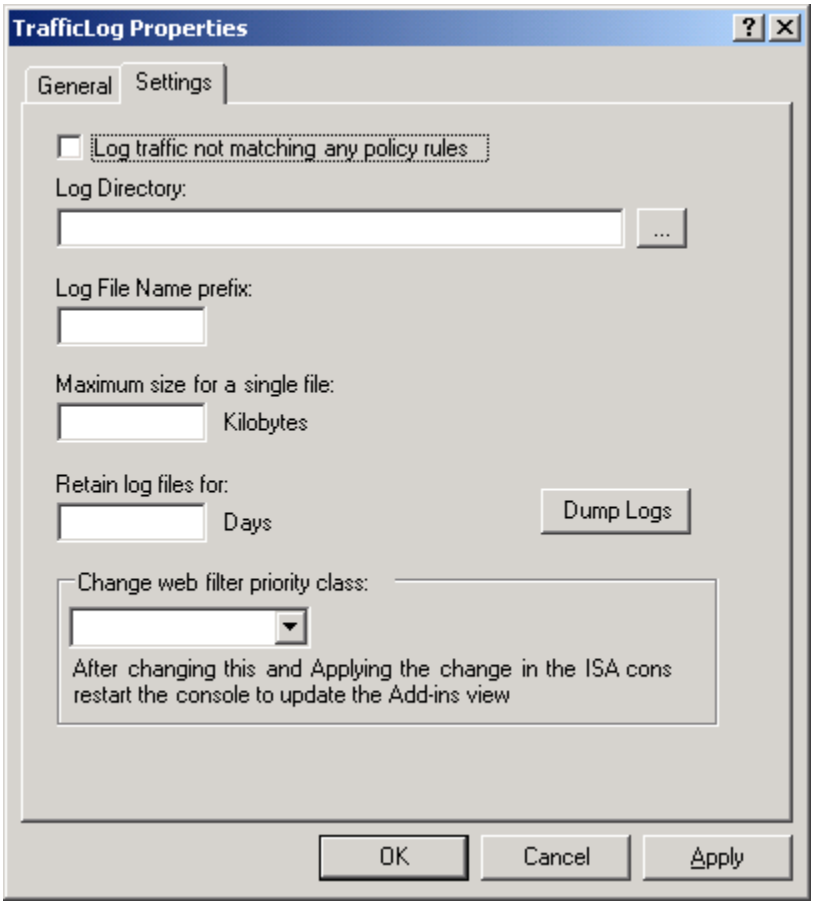
The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that change). This will cause the installer to quickly give up, and it should then correctly roll back the installation while leaving the firewall service down. After this happens you can then re-enable and restart the firewall service.

This kind of problem should not normally occur, and will probably require additional troubleshooting by Collective support. However if you are able to fix the problem you

can re-run the install safely after completing this procedure.

Setting Log File information

In Add-ins, Web Filters, right click the “TrafficLog” line and select Properties. The settings tab is shown below:



Log traffic not matching policy rules

Some traffic such as form authentication and “denied” screens are sent between ISA and the browser without matching a specific policy rule. Select this option to log it; by default it will be skipped. Note that the non-rule traffic seen by the logger may depend on its order in the filter hierarchy.

Log Directory

By default the logs will go into the ISALogs folder inside the ISA installation folder. You can change this behavior by selecting a different directory here.

Prefix

Logs are named uniquely based on the date and number of logs made on the current date. You can specify an additional prefix here for easier identification.

Max size

Logs will roll into a new file when this limit is reached. By default “today's” log file will be used for the entire day, no matter how big it gets.

Retain days

By default, logs are never deleted. If you set “2” here for example, logs from today and yesterday will be saved.

Filter priority class

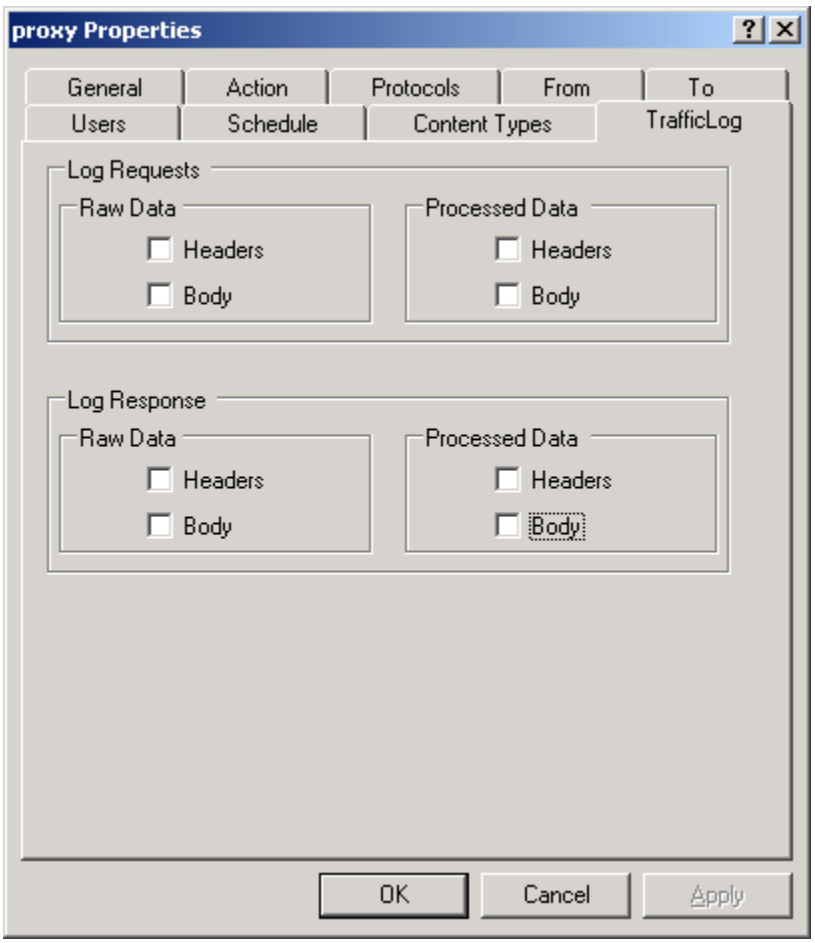
In order to catch the data that you want, it may be necessary to move the logger above or below other web filters in the list. For example to read form authentication traffic, the filter must be set at a higher priority than the form auth filter. (The form auth filter handles these connections and does not allow the traffic to reach lower filters).

If you are trying to see the output of a particular third party filter, you may want to move the logger below it. This way all traffic seen by the logger will already have been seen (and possibly modified) by the other filter first.

If you need to move the logger higher or lower than its “class” (H/M/L) allows, you can change the class here.

Logging Traffic

The properties page of each HTTP access or publishing rule will contain a TrafficLog tab:



By selecting various options you can control what type of data is logged.

At the time of this documentation, the logger does not make any distinction for binary data. This means binary data will be emitted into the log in raw form, and stop if any “0” bytes are in the data. This is considered a feature limitation presently.

Log behavior

- The log buffer is flushed to disk every 10 seconds.
- The filter holds the current log file open, so you won't be able to move, rename, or delete it until the filter closes it (on ISA shutdown, or upon moving to a new file)
- Changes applied to the rule policy do not affect active web sessions. Sessions always use a copy of the configuration from the moment the session began. So, to “retry” your scenario with changed logger settings, be sure to start with a fresh browser!

Support

The TrafficLog filter is made available to the ISA community at no charge, in the hope that it will be useful. We do not in general offer free support for it, nor can our technicians assist you in troubleshooting your ISA configuration issues.