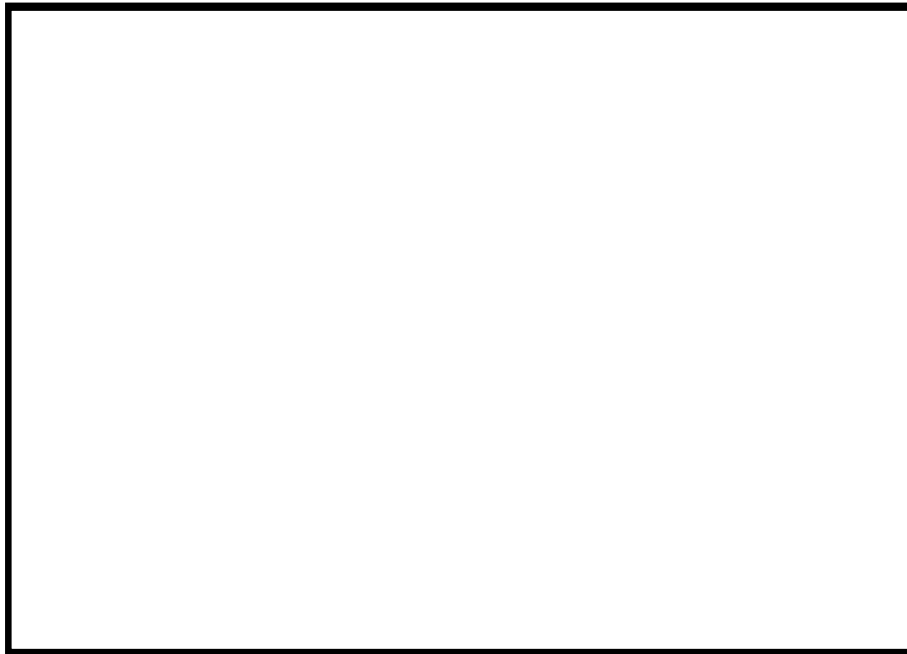


---

IISLogger 1.0

# User Manual

By Adiscon





# Contents

<b>About IISLogger 1.0</b>	<b>2</b>
Features.....	2
IIS Event Based Logging .....	2
Optimized for IIS.....	2
Ease of Use .....	2
System Requirements.....	2
<b>Getting Started</b>	<b>3</b>
Overview .....	3
Setup.....	3
Obtaining a Printable Manual .....	3
<b>How IISLogger Works</b>	<b>4</b>
IIS Workflow and Events.....	4
ISAPI Filter .....	4
Loggable Events.....	4
<b>Configuring IISLogger</b>	<b>6</b>
<b>Getting Help</b>	<b>7</b>
Frequently asked Questions .....	7
IISLogger Web Site.....	7
Support Forum.....	7
Email.....	7
Online Seminars .....	8
Phone .....	8
Fax .....	8
Software Maintenance.....	8
Non-Technical Questions.....	8
Product Updates .....	9
<b>Purchasing IISLogger</b>	<b>10</b>
The License.....	10
Pricing and Ordering .....	10
<b>Reference</b>	<b>11</b>
Version History .....	11
1.0 Final .....	11
Copyrights .....	11

<b>Glossary of Terms</b>	<b>13</b>
<b>Index</b>	<b>15</b>



# About IISLogger 1.0

**IISLogger** is an extension of the IIS logging process. The program generates additionally log data and forwards it via syslog. For IISLogger it is possible to log data even if the web request was not completely processed by the IIS. That offers the possibility to recognize hacker attacks.

**IISLogger** is a specialized tool for those that require full insight into the IIS process. If you are just interested in forwarding the W3C log files, please see [www.mwagent.com](http://www.mwagent.com) for a solution that probably better fits your needs.

---

## Features

### IIS Event Based Logging

IISLogger allows to log data at almost every event in IIS workflow. This allows in-depth logging of IIS activity.

### Optimized for IIS

IISLogger is a high-performance ISAPI extension DLL. It places the smallest monitoring footprint possible for the given task on your server.

### Ease of Use

IISLogger is easy to install and configure.

---

## System Requirements

Any Windows-NT based operating system with IIS version 3 and above. To use the automated installer, a certain service pack level may be required. This can be avoided by a manual install. In any case, Adiscon recommends the highest service pack possible for all IIS installations that are exposed to the public Internet.

# Getting Started

---

## Overview

If you are new to IISLogger, we highly recommend watching the quick overview seminar available at

[http://seminars.adiscon.com/IISLogger-Overview/IISLogger-Overview\\_files/Default.htm](http://seminars.adiscon.com/IISLogger-Overview/IISLogger-Overview_files/Default.htm)

---

## Setup

*Setup is quick and easy. IISLogger uses a standard setup wizard.*

If you use the supplied setup program, everything needed is done automatically. Be sure, however, that you have installed IIS **before** you install IISLogger.

Note: Should you ever deinstall and then re-install IIS, IISLogger most probably needs to be re-installed, too.

---

## Obtaining a Printable Manual

A printable version of the manual can be obtained at

<http://www.iislogger.com/en/Manual/>

The manuals offered on this web-page are in PDF format for easy browsing and printing. The version on the web might also include some new additions, as we post manual changes – including new samples – frequently and as soon as they become available.

# How IISLogger Works

---

## IIS Workflow and Events

The way IIS processes HTTP requests is called the “IIS workflow”. During this processing, IIS raises events at certain stages.

You need to have a good understanding of what IIS workflow is in order to understand what IISLogger logs. To learn more about the IIS workflow, please visit <http://www.monitorware.com/Common/en/articles/iis-workflow.asp>

Workflow events are trapped by IISLogger and log data is emitted for each event. The specific events can be turned on and off via configuration. So there are potentially multiple log points per http request.

---

## ISAPI Filter

IISLogger uses a specific interface (ISAPI Filter) to receive event notifications from IIS. Due to ISAPI design, IISLogger will be loaded **by IIS** when IIS starts and will only be shut down when IIS terminates. IISLogger can **not** be started or stopped independently from IIS.

---

## Loggable Events

Log data can be generated during the following events:

- OnPreprocHeader - Notifies the filter that the server has pre-processed the client headers (has not yet begun to process the information contained within the headers!). This is typically the first event created by IIS.
- OnUrlMap – Event occurs whenever the server is converting a URL into a physical path.
- OnAuthentication - Occurs just before IIS attempts to authenticate the client.
- OnAuthComplete – After authentication is complete.



- OnSendResponse - Event occurs after the request is processed and before headers are sent back to the client.
- OnSendResponse - Event occurs after the request is processed and before headers are sent back to the client.
- OnEndOfRequest – Inform the filter when the request ends.
- OnLog - After the web request has been completed, the notification occurs just before IIS writes the request to the IIS log.
- OnEndOfNetSession - Notifies the filter that the session is closed.
- OnAccessDenied – Notifies, that access to a resource has been denied.

There are two other potentially useful log points, which are OnReadRawData and OnSendRawData. We do **not** support these log points because they have very high overhead and are not compatible with IIS 6 in native mode.

# Configuring IISLogger

There is a graphical configuration tool provided with IISLogger. Please use this to create your custom configuration.

# Getting Help

*IISLogger is very reliable. In the event you experience problems, find here how to solve them.*

Please note that all options (except priority support) are also open to evaluating customers. So do not hesitate to try them. Help is available in English and German language. Our local resellers may provide local language support. Please check with them.

---

## Frequently asked Questions

For a current list of Frequently Asked Questions (FAQ), please visit

<http://www.iislogger.com/en/FAQ/>

The FAQ area is continuously being updated.

---

## IISLogger Web Site

Visit the support area at

[www.iislogger.com/en/support/](http://www.iislogger.com/en/support/)

for further information. If for any reason that URL will ever become invalid, please visit [www.adiscon.com](http://www.adiscon.com) for general information.

---

## Support Forum

Share questions and answers with your peers! The forum is also monitored by Adiscon support staff.

To access the forum, point your browser at

<http://forum.adiscon.com/viewforum.php?f=24>

---

## Email

Please address all support requests to

[support@adiscon.com](mailto:support@adiscon.com)

An appropriate subject line is highly appreciated.

---

## Online Seminars

Adiscon offers a selection of online seminars. This selection is continuously being expanded. All available seminars can be found at:

<http://www.adiscon.com/Common/SeminarsOnline/>

*Please note: Windows Media Player is required to view the seminars.*

---

## Phone

**+49-2235-985004** (with "+" being the international dialing prefix, for example 011 in the US).

**Toll free from the US: 1-888-318-3395**

**Phone support is limited to those who purchased support incidents.** If you are interested in doing so, please email [info@adiscon.com](mailto:info@adiscon.com) for further details.

Please note that we are in the Central European Time zone (CET). That is 1 hour east of Greenwich Time. If it is 12pm in New York, it is 9pm at our office location. Our office hours are from 9am to 5pm. Therefore, we generally advise US customers to call in early mornings and Asian customers to call in late afternoon.

For best customer service, we highly recommend limiting phone calls to emergencies. We are checking our other support options regularly. Email support is available also during non-office hours, typically until 10pm CET.

---

## Fax

Please direct your faxes to

**+49-9349-928820**

**Toll free in the US: 1-888-900-3772**

with "+" being the international dialing prefix, e.g. 011 in the US and 00 in most other countries.

---

## Software Maintenance

Adiscon's software maintenance plan is called **UpgradeInsurance**. It offers unlimited free upgrades and priority support during its duration. It can be purchased for a period between 1 and 5 years.

To learn more about UpgradeInsurance, please visit

<http://www.adiscon.com/Common/en/products/upgrade-insurance-details.asp>

**Comment [Help1]:** UpgradeInsurance

---

## Non-Technical Questions

Please address all non-technical questions to

[info@adiscon.com](mailto:info@adiscon.com)

This email alias will answer all non-technical questions like pricing, licensing or volume orders.

---



---

## Product Updates

Please visit

[www.iislogger.com](http://www.iislogger.com)

for information about new and updated products.

# Purchasing IISLogger

All IISLogger features can be used for 30 days after installation without a license. However, after this period a valid license must be purchased. The process is easy and straightforward.

## The License

Please see license.txt for full license information. This file can be found in the ZIP file and is displayed during installation.

## Pricing and Ordering

For most current pricing information please visit

<https://secure.adiscon.com/eCommerce/SingleProdOrder.asp?ProdSKU=IISLogger>

This page can also be used to place your order online.

If you have any questions or would like to receive assistance, please let us know at [info@adiscon.com](mailto:info@adiscon.com).

# Reference

---

## Version History

### 1.0 Final

Release Date: 2002-12-12  
Initial

---

## Copyrights

This documentation as well as the actual IISLogger product is copyrighted by Adiscon GmbH, Germany. To learn more about other Adiscon products, please visit [www.adiscon.com/en/products/](http://www.adiscon.com/en/products/). To obtain information on the complete MonitorWare line of products, please visit [www.monitorware.com](http://www.monitorware.com).

Please note that IISLogger is part of the MonitorWare line of products. Please visit the MonitorWare site ([www.monitorware.com](http://www.monitorware.com)) to receive updates and information on all members of the family. The site also does have information on combining the individual components to build a complex distributed configuration.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other mentioned trademarks are for reference only. They belong to their respective owners.





# Glossary of Terms



# Index

## **C**

configuration 6

## **F**

Features 2

## **L**

license 10

## **M**

maintenance 8

## **O**

online seminar 8

ordering 10

## **P**

purchase 10

## **S**

seminar 8

setup 3

software maintenance 8

support

forum 7

online seminars 8

support options 7

## **U**

UpgradeInsurance 8