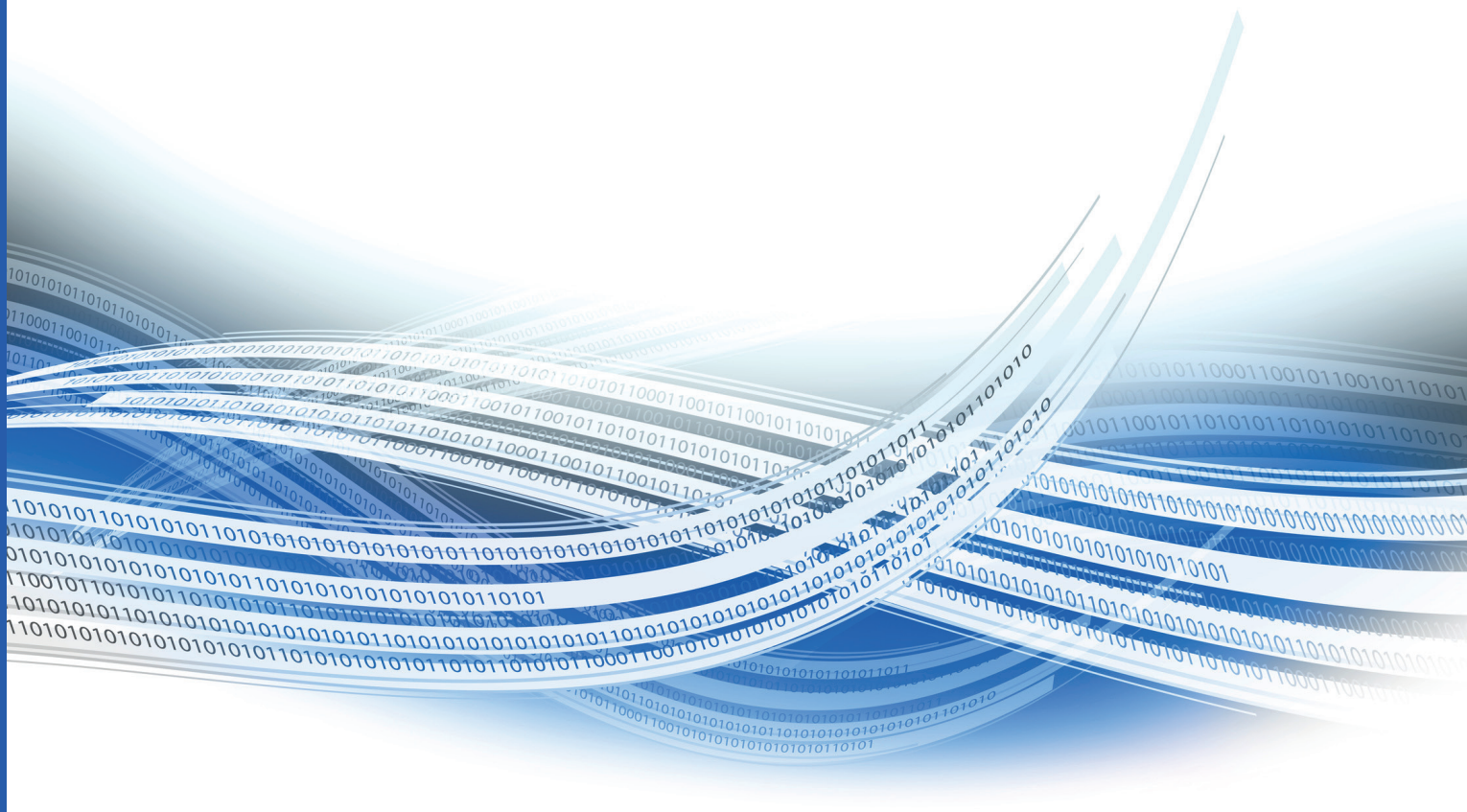
PCS AG
Communication Services



# UNIQUE IIS Protector

## Manual

Microsoft Partner
Gold Application Development

# UNIQUE IIS Protector

**V. 2.01.1010**

**Virus Protection for Microsoft Internet Information Server**

Welcome to UNIQUE IIS Protector

To protect the Microsoft Internet Information Server against the increasing virus threat, we designed and developed the UNIQUE IIS Protector. The content which will be uploaded to the Microsoft Information Server will be checked in real terms via the Symantec Scan Engine. A redundant handling of multiple Scan Engines is also possible as a setup of an email notification system based on a multilevel log system. The protection for the Internet Information Server can be configured user-defined. By request defined websites can be protected (e.g. external website) or can be left unprotected (e.g. Intranet) within the Internet Information Server. In case a virus is found, you can use a precast template to give feedback to the user or create an http redirection. Dependent on the protocol (e.g. http) the handling can be configured individually. The version 6 and 7 of the Internet Information Server are supported, in a 32bit as well as in a 64bit environment.

PCS AG
support@pcs-ag.de
Version 2.01.1010

## Index

# 1. Requirements

Operating System:

Microsoft Windows Server 2003 / 2003 R2 x86 or x64
Microsoft Windows Server 2008 x86 or x64
Microsoft Windows Server 2008 R2

Software:

Microsoft Internet Information Server 6.0 / 7.0 / 7.5 32bit or 64bit
Symantec Scan Engine 5.1 or higher available in your network environment

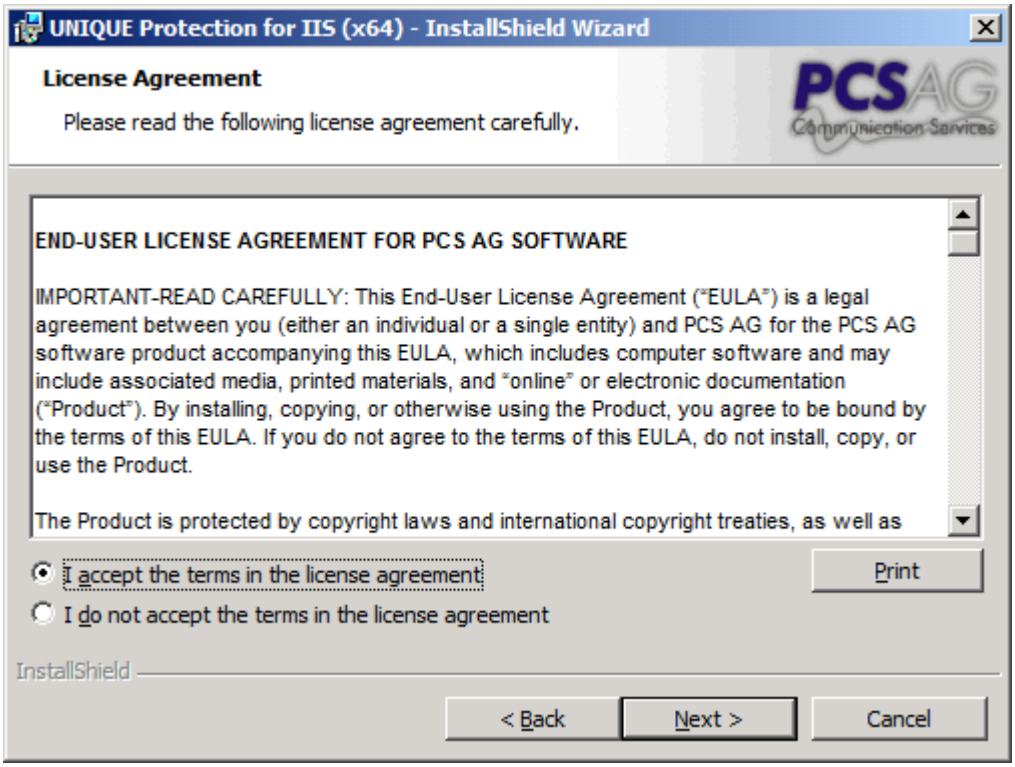
Memory:

1 GB RAM
60 MB Hard Disk space for Installation
additional Hard Disk space for Logfiles

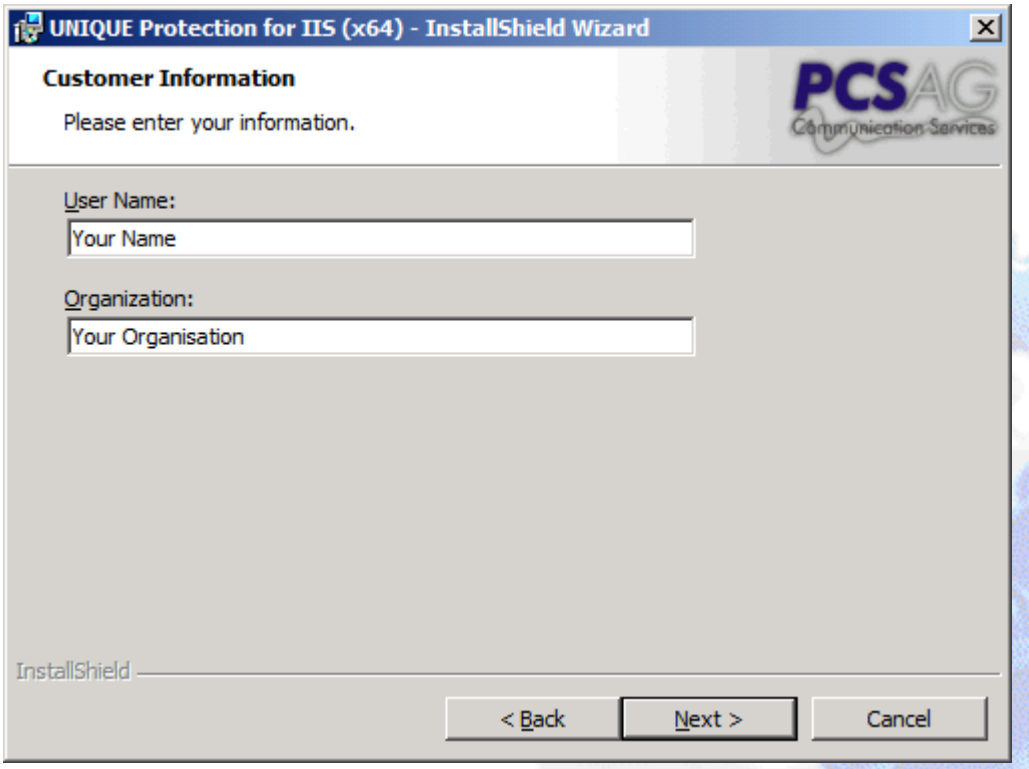
# 2. Installation

Installation of Unique IIS Protector will be started using the setup.exe installer.

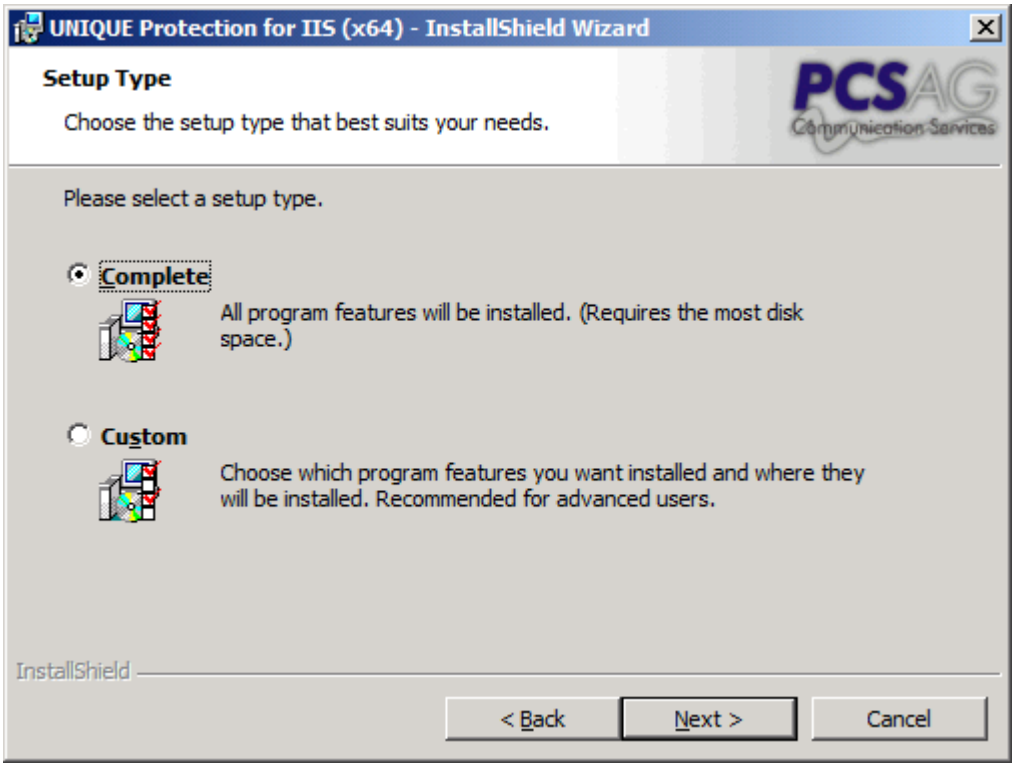
Click *Next* to start installation.



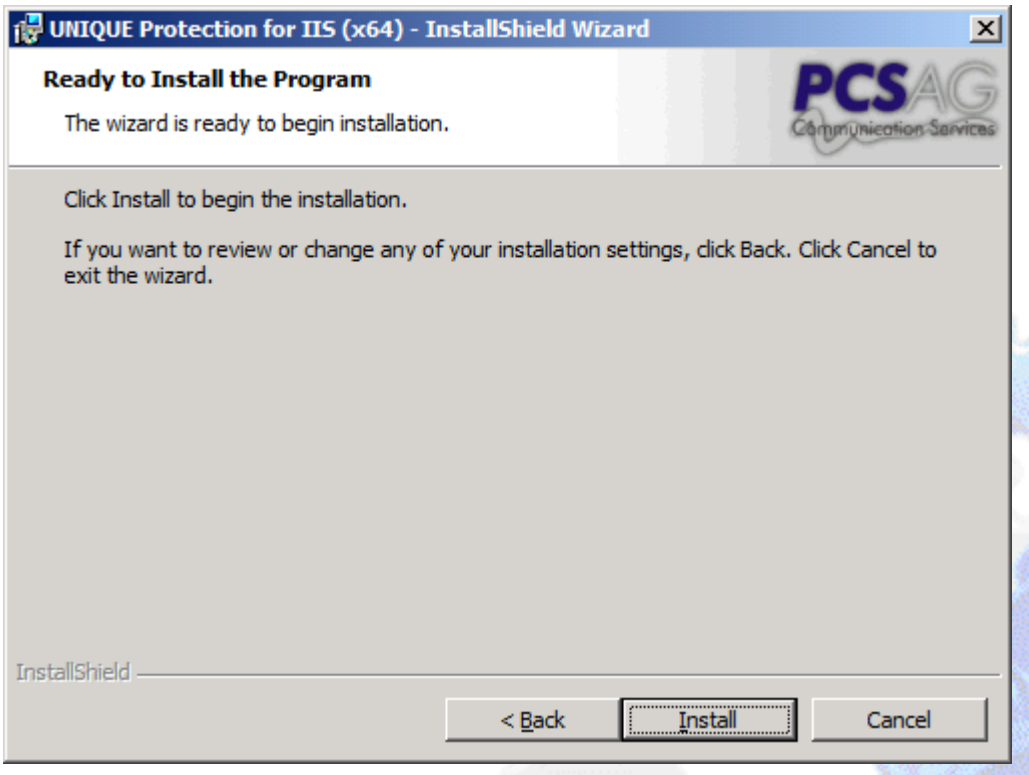

Read and accept the license agreement and click *Next*.
If you do not accept the license agreement, setup cannot be continued.



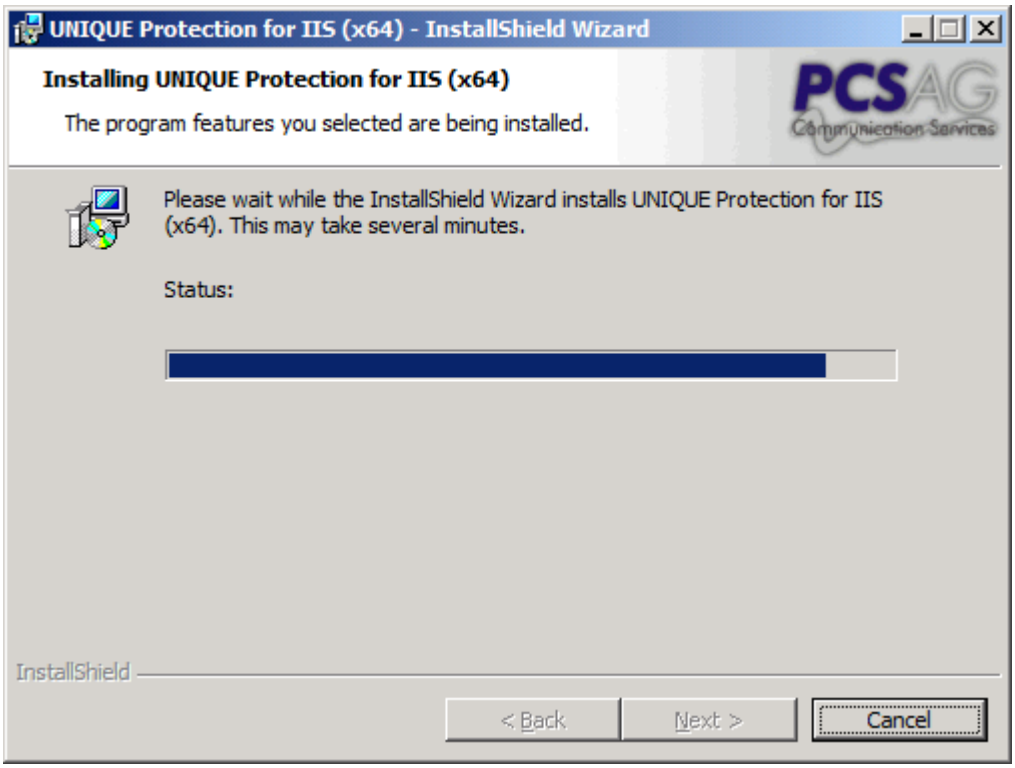

Enter your Name and Organization and click *Next*.




Select *Complete* and click *Next*.




Click *Install* to start copying files.



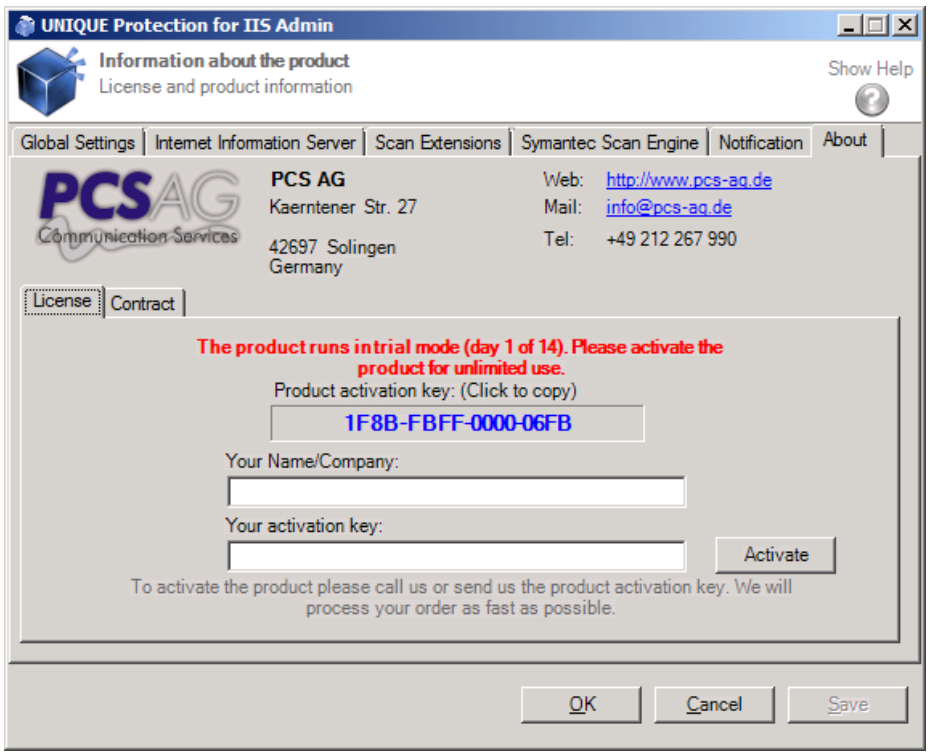

Files are being copied.


Click *Finish* to complete installation. Enable the *Launch the program* checkbox to start the Unique IIS Protector automatically after setup.

# 3. Configuration

## a. Launch the Unique IIS Protector

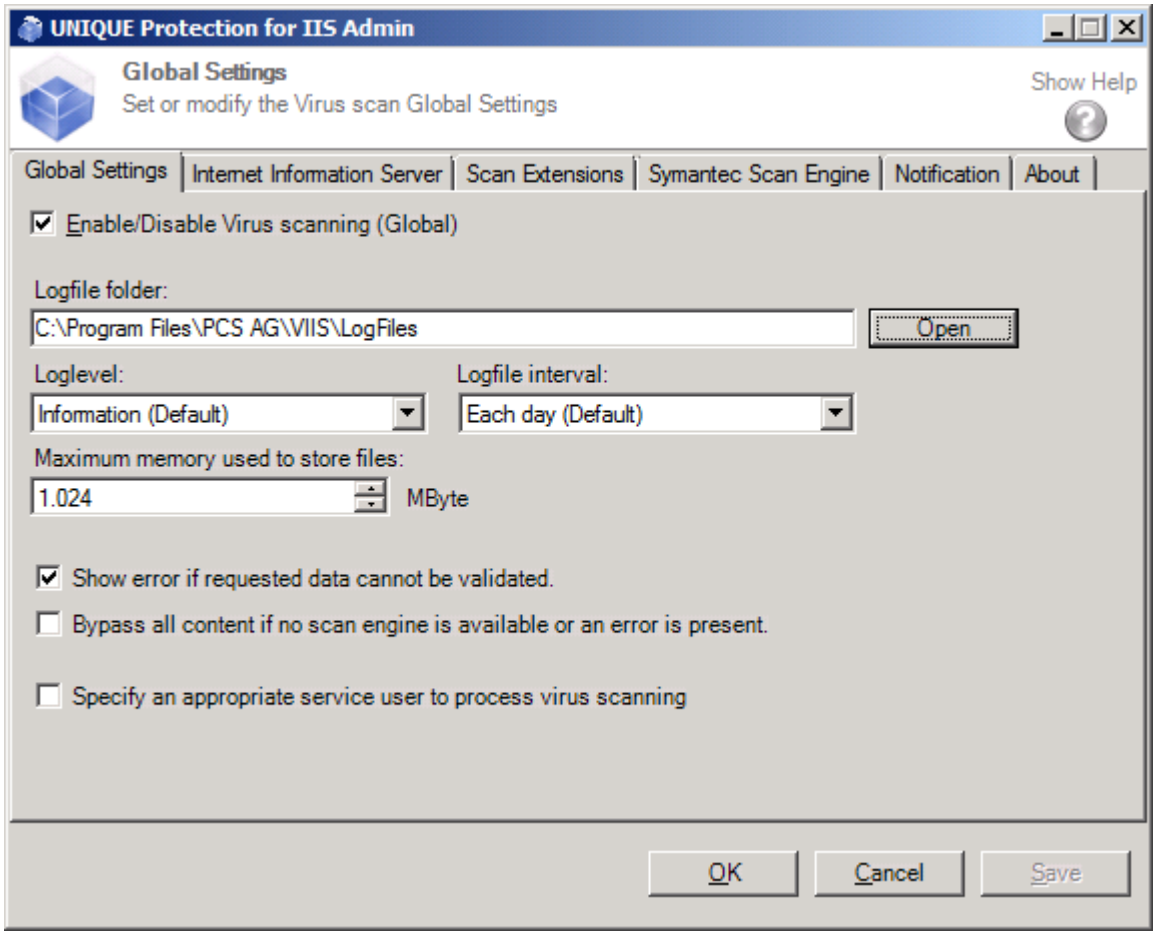
The following screen will come up after first start.




## b. Activation

The software can be used in trial mode for 14 days. After this period you will have to activate the Unique IIS Protector to continue scanning. To activate the Unique IIS Protector copy the activation key and send it by email to info@pcs-ag.de . You will then receive the necessary information for purchasing and licensing the product by one of our technical staff member.

## 3.1 Global Settings




To enable Virus scanning enable the checkbox *Enable/Disable Virus scanning (Global)* and click *Save*.
To disable Virus scanning disable the checkbox *Enable/Disable Virus scanning (Global*) and click *Save*.
Please note, that registering a Symantec Scan Engine is necessary (refer to 3.4)

To select a folder to store the logfiles, click on the button *Open*. Alternatively the path can be entered manually within the textbox in this format: device:\folder name. Please note that the specified folder must exist. The logfile data standard path is: *"%SystemRoot%\system32\LogFiles\PCSIISVirusScan"*

The *loglevel* defines which type of incidents will be written into the logfile.
The following log levels are available:

| Level | Description |
|---|---|
| *Verbose* | All incidents will be logged |
| *Information* | All incidents of this type will be logged: Information, Warnings, Errors and Fatal Errors |

| Level | Description |
|---|---|
| *Warnings* | All incidents of this type will be logged: Warnings, Errors and Fatal Errors |
| *Errors* | All incidents of this type will be logged: Errors and Fatal Errors |
| *Fatal Errors* | Only incidents of type Fatal Errors will be logged |

The default value is *Information*.

The logfile interval defines the time interval in which new logfiles will be generated. The following intervals are available:

| Interval | Description |
|---|---|
| *Only one* | All incidents will be written in a single data file |
| *Each hour* | A new logfile will be generated every hour |
| *Each day* | A new logfile will be generated every day |
| *Each week* | A new logfile will be generated every week |
| *Each month* | A new logfile will be generated every month |

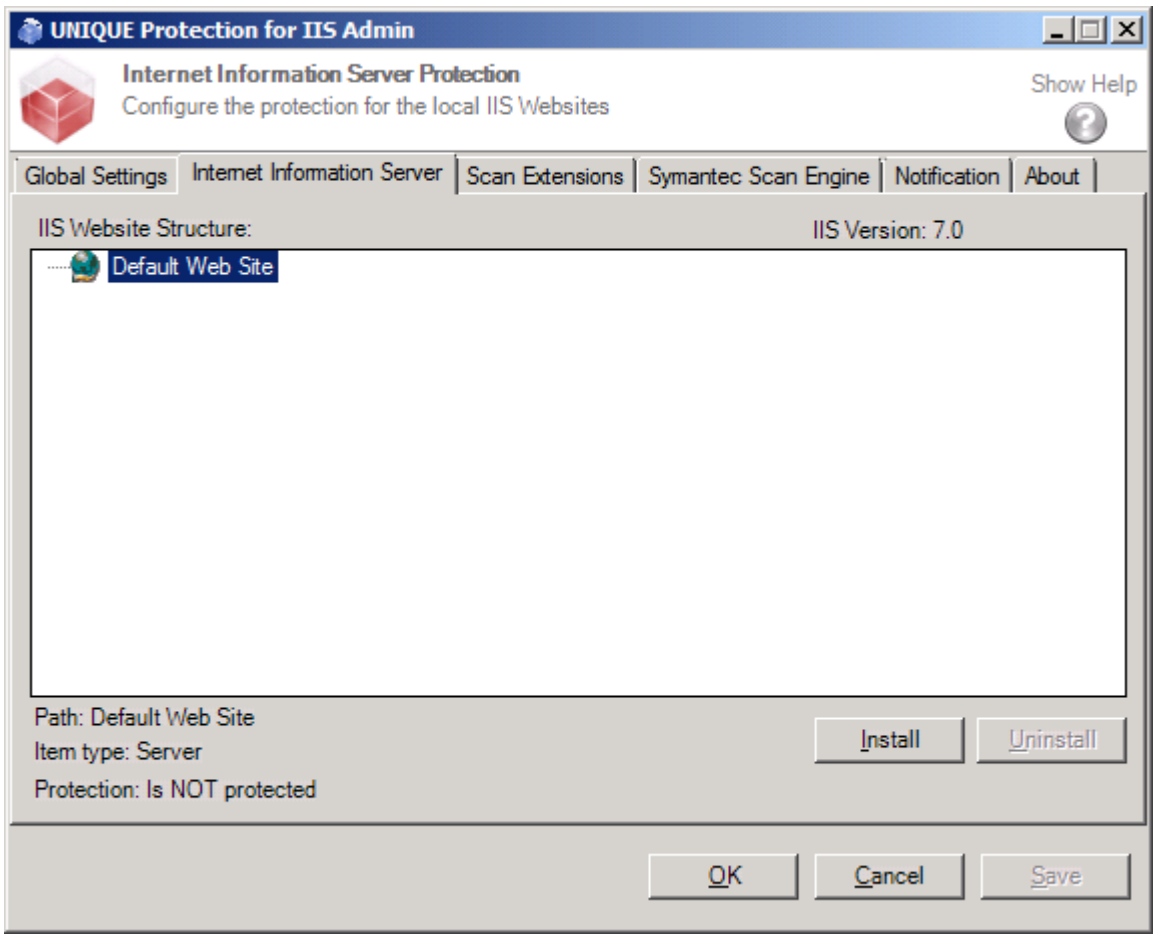
The default value is *Each day*.

The *maximum memory used to store files* option defines the maximum amount of temporally memory which can be used to store log files.

*Show error if requested data cannot be validated* defines whether the user will receive an information page containing the information for what kind of reason his request has been blocked (e.g. file contains a virus).

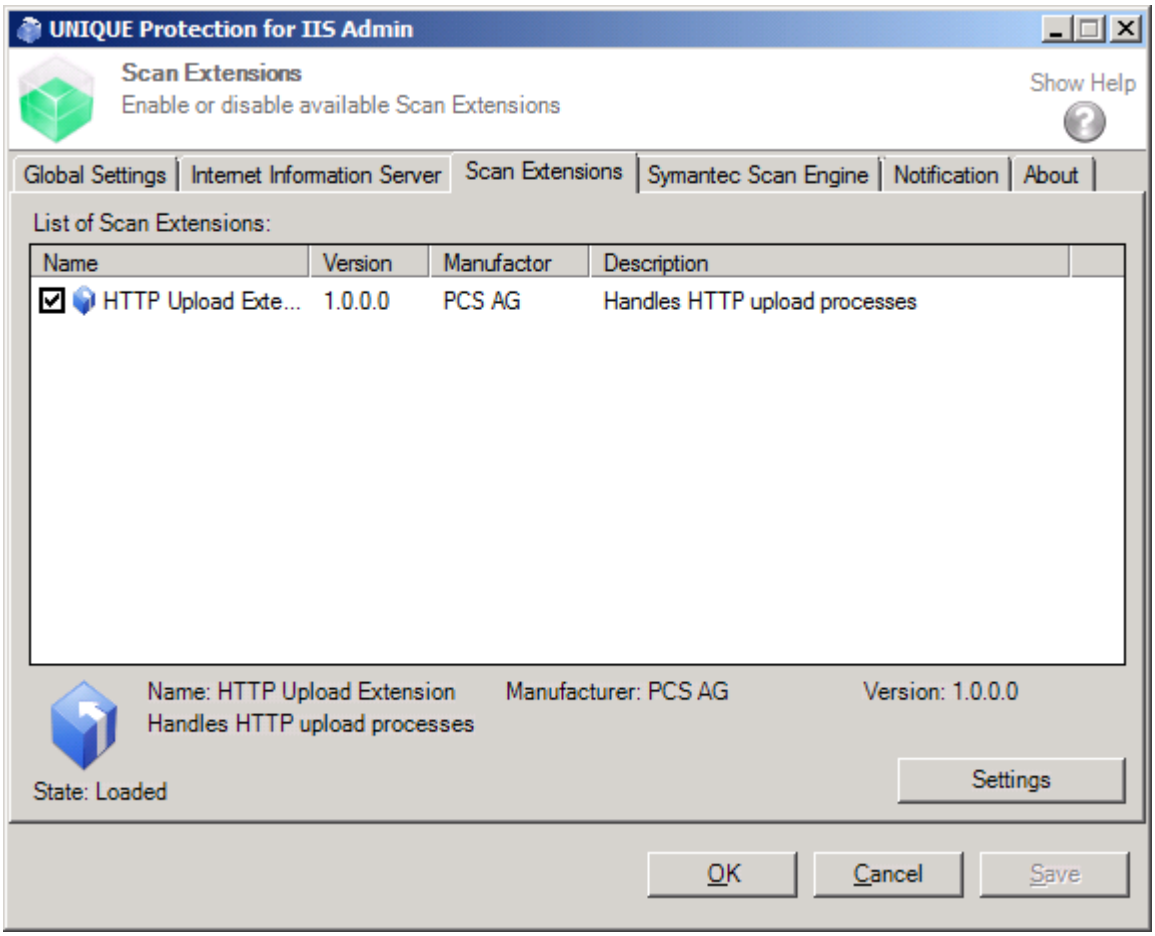
In case that all registered Symantec Scan Engines are offline or not available, and you want to ensure uploading functionality working properly during Scan Engine downtime, you can activate the option *Bypass all content if no scan engine is available or an error is present*.
Be aware, that enabling this option may lead to infection, because infected content will be bypassed when all Scan Engines are not available.
To define an individual service user to process virus scanning, enable the option *Specify an appropriate service user to process virus scanning* and enter the specific user in format DOMAIN \ USER (e.g. LOCALDOMAIN\SERVICEUSER).
Verify to enter the correct password and click *save*.
IMPORTANT: This user must not be network service.

### 3.2. Internet Information Server



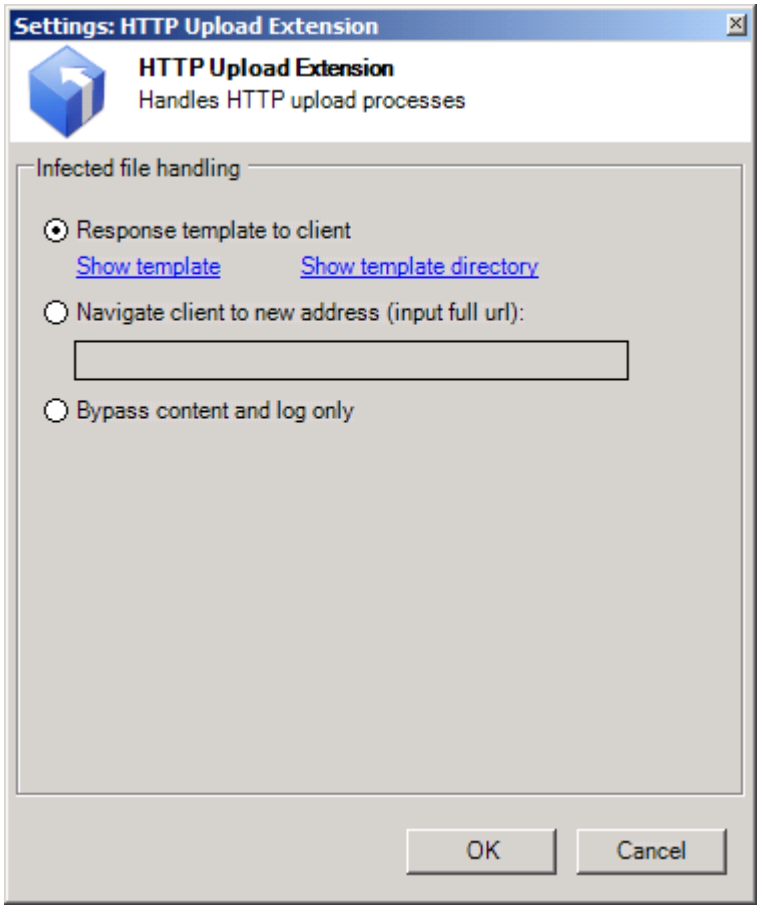

Inside the *Internet Information Server* tab you can install the protection for the websites of your IIS.
The website structure of IIS is listed inside the window as well as the Version number of IIS.
To active the protection to a website, simply select the website and click *Install.*
A red border will appear around the website icon to show that the protection is now active on this website. Also the protection state at the bottom will switch from *Is NOT protected* to *Is protected*.
To uninstall the protection for a website, select the website and click *Uninstall*.
The number of websites, which can be protected, is concurrently of unlimited number.

## 3.3 Scan Extensions




The tab *Scan Extensions* will list all available Scan Extensions. For the moment only *HTTP Upload extension* is available. More extensions will follow up. To configure the scan extensions settings, click *Settings*.

### 3.3.1 Settings HTTP Upload Extension




The HTTP Upload Extension settings page will allow you to define the action in a case of a virus found. The options are as follows:

*Response template to client*
In case a virus is found, a template can be responded to the client. Click *Show template* to display the current template or click *Show template directory* to open the folder containing the template files. How to edit template files, refer to 3.3.1.1

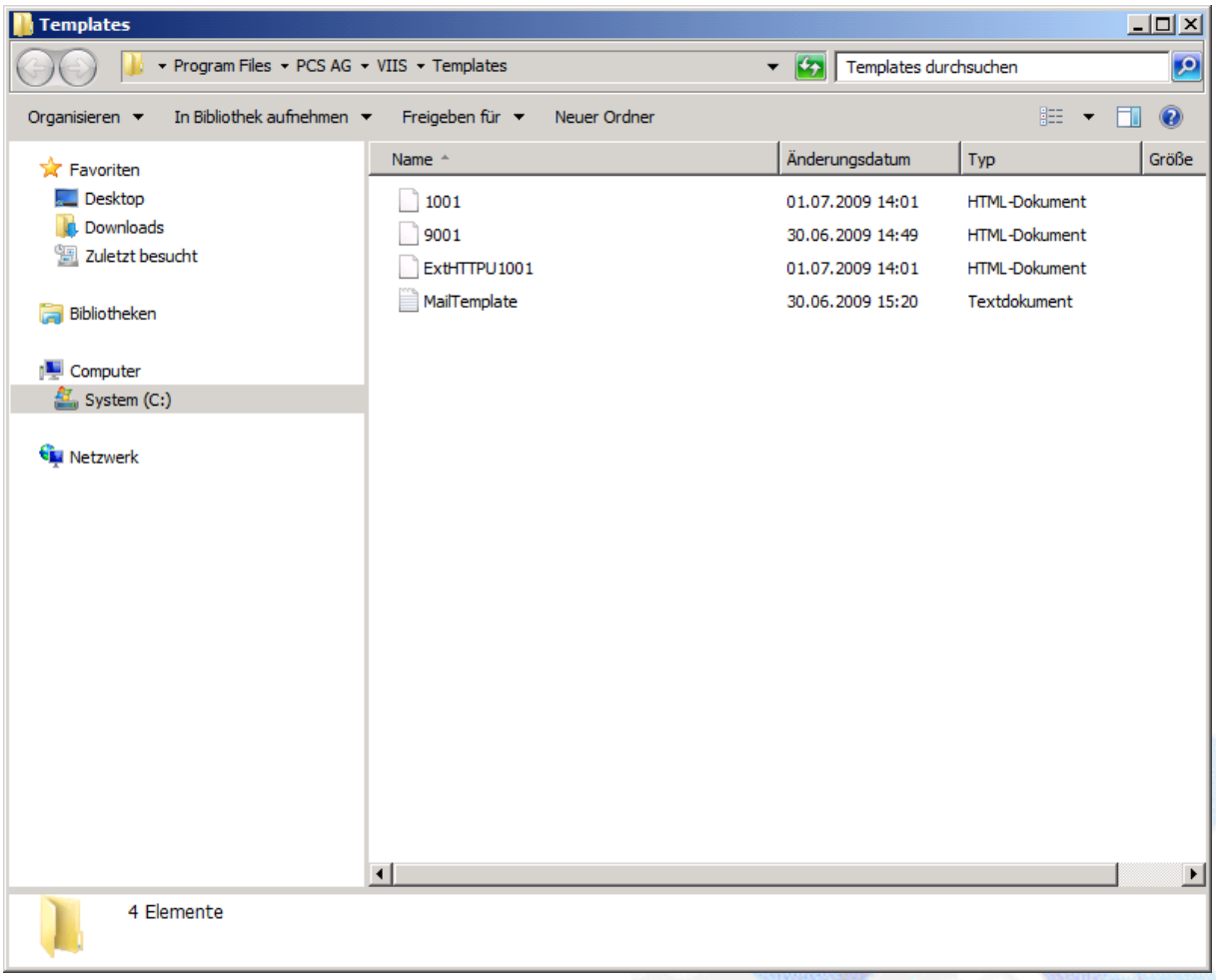
*Navigate client to new address (input full url)*
In case a virus is found, the client can be redirected to any http website. Activate the checkbox and enter the full url where the client should be redirected (e.g. http://www.website.dom)

*Bypass content and log only*
In case a virus is found, content will be bypassed and the action will be logged. Please be aware, that infected content might be uploaded to the webserver!

#### 3.3.1.1. Configuration Template HTTP Upload Extension

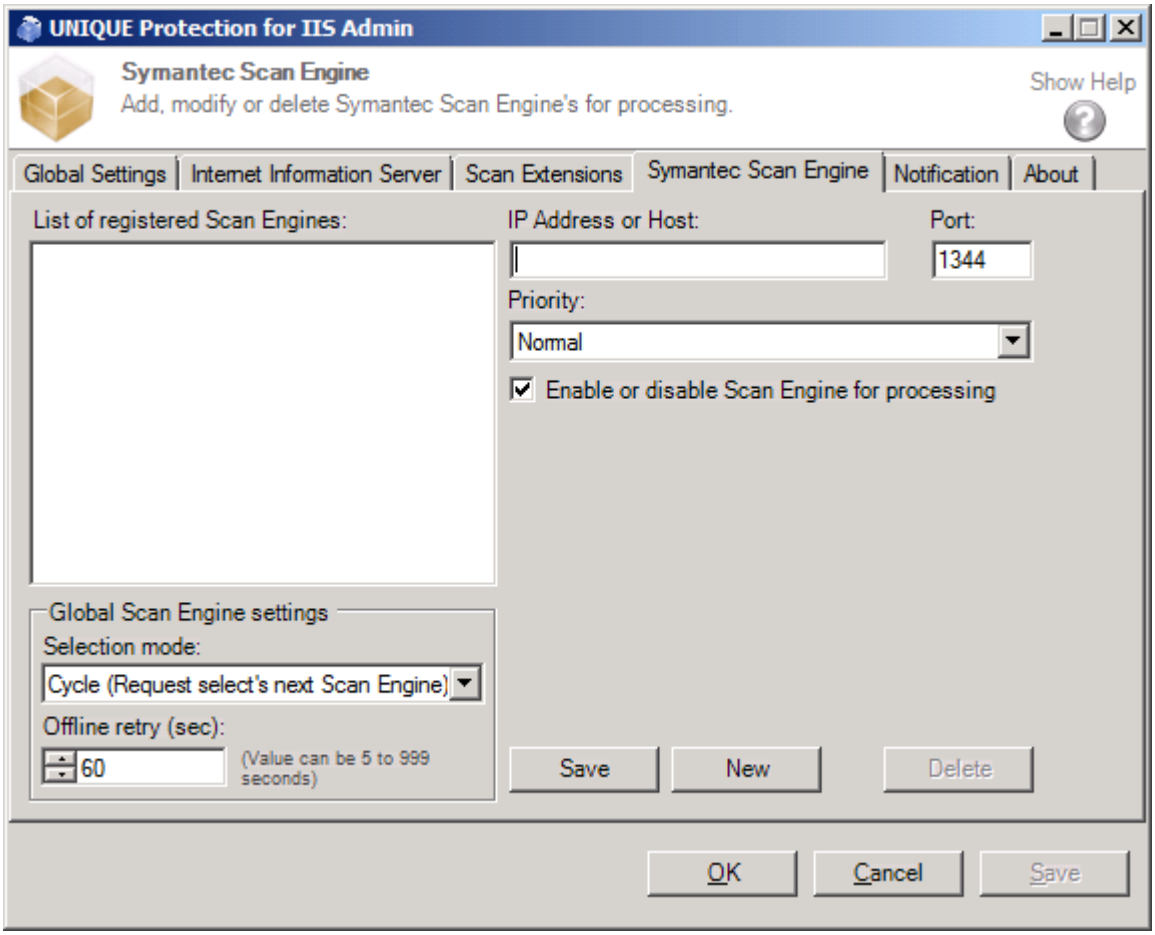
Click *Show template directory* in *HTTP Upload Extension settings* window. The installed templates will be listed as follows:

| | |
|---|---|
| 1001.htm | Template for Errors occurring during scan |
| 9001.htm | Template for Virus scan being not available |
| EXTHTTPU1001.htm | Template for Virus found |
| Mailtemplate.txt | Template for Email Notification |




To modify the templates, open it with any text or html editor.
IMPORTANT: Please note, that the wildcards within the square brackets are not allowed to be edited.
Refer also to 3.5 for editing Email template.

### 3.4. Symantec Scan Engine




Within the tab Symantec Scan Engine you can add, list, edit and remove Symantec Scan Engines to the system.

To add a new Symantec Scan Engine:
Enter the Scan Engine´s *IP address or Host*name and corresponding tcp *port*, its *priority* (only important when it is planned to add more than one Scan Engine) and its state (marked checkbox will enable Scan Engine for processing). Click *Save* and Scan Engine´s data will be analyzed and will be shown. (Data details: Scan Engine Version, Virus definition date, License, maximum connection).
Click *Save* in the main window of Unique IIS Protector Admin to save the Scan Engine configuration to the system.
All Scan Engines with state *(active)* are ready to be used for virus scanning.

To add a second Symantec Scan Engine:
Click new and simply repeat the steps above under consideration of the priority state, when priority mode is planned to be used.

Editing of Symantec Scan Engines
Any Scan Engine can be edited anytime. Just select the Scan Engine you want to edit, apply your changes and click *Save*.

Deletion of Symantec Scan Engines
Select the Scan Engine you want to delete and click *Save*.

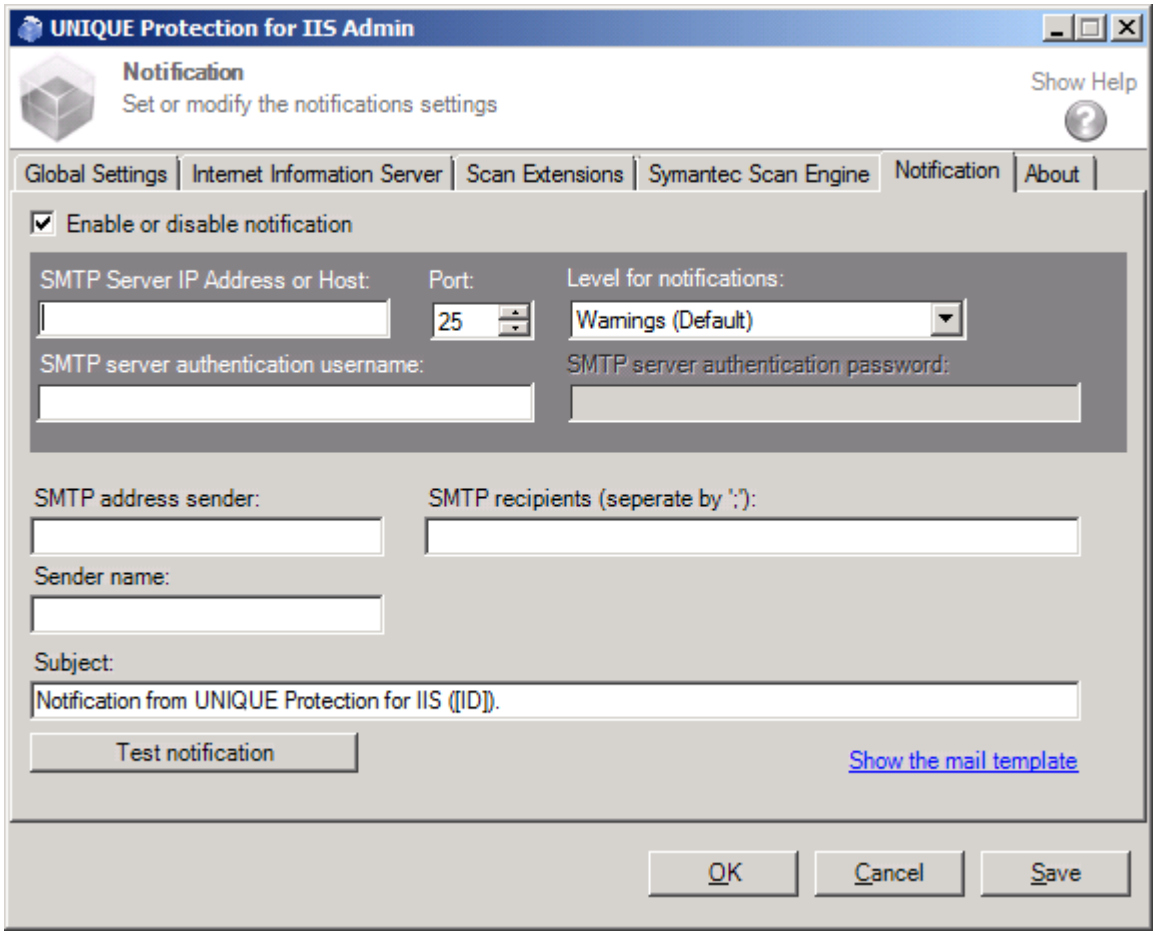
Priority Mode
The priority mode can be activated in Global Scan Engine settings in Symantec Scan Engine tab. When priority mode is enabled, Symantec Scan Engines will be used for scanning depending on their priority.
Example: Scan Engine 1 high priority – Scan Engine 2 low priority
In this case Scan Engine 1 will be used for scanning. Scan Engine 2 will only be used for scanning, when Scan Engine 1 is not available, busy or offline.

Cycle Mode
The cycle mode can be activated in Global Scan Engine settings in Symantec Scan Engine tab. When cycle mode is enabled, Symantec Scan Engines will be used for scanning in a cycle. Using cycle mode is recommended when handling a huge load of scanning. The load of a single Scan Engine will decrease when using multiple Scan Engines in cycle mode.

Offline retry (sec)
The option *Offline retry* defines the time interval in which Unique IIS Protector sends a heartbeat to the Scan Engine to check its availability.

Normal mode
Normal mode will use the first active Scan Engine being listed inside the list of registered Scan Engines.

## 3.5. Notification




The Email Notification will be setup within the Tab *Notification*. To activate the notification enter a valid IP address or host name in the field. If the SMTP Server requires an authentication, enter a user name and password. Enter a sender address, a minimum of one recipient address (multiple recipients need to be separated by a semicolon) and a display name for the sender.

The notification level defines which type of incidents will be sent. The notification level is as follows:

| Level | Description |
|---|---|
| *Verbose* | All incidents will be sent |
| *Information* | Incidents of the following types will be sent: Information, Warnings, Errors and Fatal Errors |
| *Warnings* | Incidents of the following types will be sent: Warnings, Errors and Fatal Errors |
| *Errors* | Incidents of the following types will be sent: Errors and Fatal Errors |
| *Fatal Errors* | Only Fatal Errors incidents will be sent |

The subject of the notification email can be customized as well as the Email template. The template can be edited by clicking on the button *Show Template*. Please note, that the wildcards within the square brackets are not allowed to be edited.
A test mail will be sent by clicking the button *Test Notification*. Please ensure, that the check box *Enable or Disable Notification* is activated and click on *Save*.

## 4. Integrated Help

Click on *Show Help* inside the Unique IIS Protector Admin to open the integrated help file content.

## 5. Frequently asked questions

Most common problems are security related!
Whenever problems are occurring, please check first the security configuration on the running web server.
Service users like IUSR_... or Network Service do not have access to the local filesystem, so that logfiles or eventlog entries cannot be created.
Verify the security rights for the specific folders (Logfile, Application) and if necessary, add the access rights.

If you need help please send a message to **support@pcs-ag.de**.

## 6. About PCS AG

As an IT solution provider the Solingen-based PCS AG endued comprehensive experience in the range of business consulting, software development as well as project and process management.

PCS AG
Communication Services
Kaerntener Strasse 27
42697 Solingen, Germany
Fon : +49(0) 2 12 - 2 67 99 0
Fax : +49(0) 2 12 - 2 67 99 99

E-Mail: info@pcs-ag.de

Internet: http://www.pcs-ag.de

**PCS AG** IS A GERMAN SOFTWARE DEVELOPER. WORLD'S FIRST MICROSOFT GOLD CERTIFIED PARTNER (CATEGORY: ECOMMERCE) AND 2001 MICROSOFT AWARD FOR CRM SOLUTIONS - TODAY MICROSOFT GOLD PARTNER IN THE CATEGORY „APPLICATION DEVELOPMENT".

PCS AG
Communication Services

**PCS AG** Merscheider Str. 94a, 42699 Solingen, Tel.: +49 (0) 212 250 83-0, Fax: +49 (0) 212 250 83-999
info@pcs-ag.de, www.pcs-ag.de