



# UNIQUE IIS Protector Manual



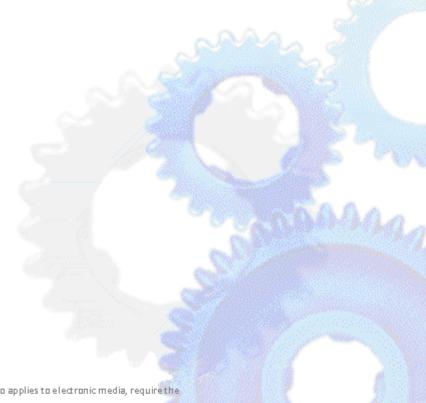
# **UNIQUE IIS Protector**

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 userdefined. 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 Copyright by PCS AG

#### Index

1.	Requirements	Page 3
2.	Installation / Setup	Page 3
3.	Configuration	Page 7
	3.1. Global Settings	Page 8
	3.2. Internet Information Server	Page 10
	3.3 Scan Extensions	Page 11
	3.3.1. Settings HTTP Upload Extension	Page 12
	3.3.1.1. Configuration Template HTTP Upload Extension	Page 13
	3.4. Symantec Scan Engine	Page 14
	3.5. Notification	Page 16
	3.5.1. Configuration mail template	Page 16
4.	Integrated Help	Page 17
5.	FAQ	Page 17
6.	About PCS AG	Page 17



PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

# 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

explicit approval of PCS AG.

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

🙀 UNIQUE Protection for IIS (	×	
	Welcome to the InstallShield Wizard for UNIQUE Protection for IIS (x64)	20 C
PCSAG	The InstallShield(R) Wizard will install UNIQUE Protection for IIS (x64) on your computer. To continue, click Next.	2-2
Communication Services	WARNING: This program is protected by copyright law and international treaties.	50000
	Version: 2.01.1010	
	< Back Next > Cancel	
PCS AG <u>support@pcs-ag.de</u> Version 2.01.1010 Copyright by PCS AG Reproduction and copying of any kind, even in	part, this also applies to electronic media, require the	

🙀 UNIQUE Protection for IIS (x64) - InstallShield Wizard	×			
License Agreement Please read the following license agreement carefully.				
END-USER LICENSE AGREEMENT FOR PCS AG SOFTWARE				
IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and PCS AG for the PCS AG software product accompanying this EULA, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("Product"). By installing, copying, or otherwise using the Product, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install, copy, or use the Product.				
The Product is protected by copyright laws and international copyright treaties, as well as	-			
I accept the terms in the license agreement     Print				
C I <u>d</u> o not accept the terms in the license agreement				
InstallShield				
< <u>B</u> ack <u>N</u> ext > Cancel				

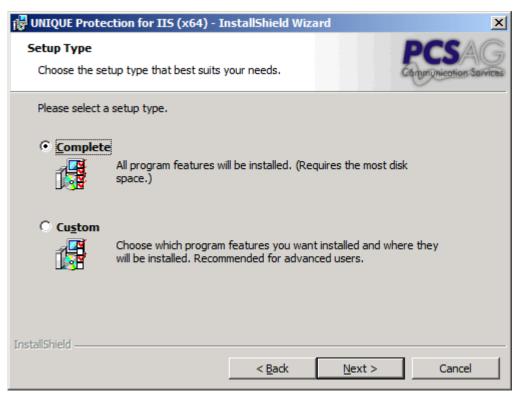
Read and accept the license agreement and click Next.

If you do not accept the license agreement, setup cannot be continued.

🔀 UNIQUE Protection for IIS (x64) - In	stallShield Wizard		×	
Customer Information Please enter your information.		PC	SAG cotion Services	
User Name:				
Your Name				
Organization: Your Organisation		_		
I four organisation				
				6003
InstallShield				
	< <u>B</u> ack	Next > (	Cancel	

Enter your Name and Organization and click Next.





Select Complete and click Next.

🕞 UNIQUE Protection for IIS (x64	4) - InstallShield Wizard	×	
Ready to Install the Program		PCSAG	
The wizard is ready to begin instal	llation.	Communication Services	
Click Install to begin the installatio	n.		
If you want to review or change a exit the wizard.	any of your installation settings, click Ba	ack. Click Cancel to	2
exit the wizard.			5
			255
			<u> </u>
			J. ST.
			also have
			100 A
InstallShield			RAAA.
	< <u>B</u> ack <u>I</u> nstall	Cancel	Property Service
Click Install to start copying files.		62-16	
PCS AG			
support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG			
Reproduction and copying of any kind, even in part,	this also applies to electronic media, requ	irethe	
explicit approval of PCS AG.			

100

🙀 UNIQUE P	rotection for IIS (x64) - InstallShield Wizard
	UNIQUE Protection for IIS (x64) ram features you selected are being installed.
1 <del>1</del>	Please wait while the InstallShield Wizard installs UNIQUE Protection for IIS (x64). This may take several minutes.
	Status:
InstallShield -	
	< Back Mext > Cancel

Files are being copied.

🖓 UNIQUE Protection for IIS (x64) - InstallShield Wizard			
	InstallShield Wizard Completed		
PCS AG Communication Services	The InstallShield Wizard has successfully installed UNIQUE Protection for IIS (x64). Click Finish to exit the wizard.		
	< Back <b>Finish</b> Cancel		

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

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

#### 3. Configuration

a. Launch the Unique IIS Protector

The following screen will come up after first start.

UNIQUE Protection for IIS Admin				
Information about the product License and product information	Show Help			
Global Settings Internet Information Server Scan Extensions Symantec Scan Engine Notification	About			
PCS AG     Web:     http://www.pcs-aq.de       Kaerntener Str. 27     Mail:     info@pcs-aq.de       42697 Solingen Germany     Tel:     +49 212 267 990				
The product runs in trial mode (day 1 of 14). Please activate the product for unlimited use. Product activation key: (Click to copy) 1F8B-FBFF-0000-06FB				
Your Name/Company:				
Your activation key:           Your activation key:         Activate           To activate the product please call us or send us the product activation key. We will				
process your order as fast as possible.				
<u>O</u> K <u>C</u> ancel	<u>S</u> ave			

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 <u>info@pcs-ag.de</u>. You will then receive the necessary information for purchasing and licensing the product by one of our technical staff member.

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

#### 3.1 Global Settings

UNIQUE Pro	tection for IIS Admin				_ 🗆 🗙
	al Settings modify the Virus scan Glob	al Settings			Show Help
Global Settings	Internet Information Server	Scan Extensions	Symantec Scan Engine	Notification	About
☑ <u>E</u> nable/Disa	able Virus scanning (Global	)			
Logfile folder:				······	
, -	s\PCS AG\VIIS\LogFiles			Open	
Loglevel:	( - I) =	Logfile interval:			
Information (De	_	Each day (Default			
Maximum mem	nory used to store files:	te			
<ul> <li>Show error if requested data cannot be validated.</li> <li>Bypass all content if no scan engine is available or an error is present.</li> </ul>					
Specify an appropriate service user to process virus scanning					
			<u>o</u> к <u>c</u>	ancel	<u>S</u> ave

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:

LevelDescriptionVerboseAll incidents will be loggedInformationAll 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.

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

### Page 10 of 17

#### 3.2. Internet Information Server

UNIQUE Presidente	otection for IIS Admin				
	rnet Information Server Pro igure the protection for the lo				Show Help
Global Settings	Global Settings Internet Information Server Scan Extensions Symantec Scan Engine Notification A				
IIS Website S	tructure:		IIS Ver	sion: 7.0	
	lt Web Site				
Path: Default Item type: Ser			<u>l</u> n	stall [	Jninstall
	NOT protected				
			<u>O</u> K <u>C</u> a	ancel	<u>S</u> ave

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.

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

#### 3.3 Scan Extensions

UNIQUE Protection for 3	IIS Admin			
Scan Extensions Enable or disable available Scan Extensions				
Global Settings Internet Info	mation Server	Scan Extension	ns Symantec Scan Engine	Notification About
List of Scan Extensions:				
Name	Version I	Manufactor I	Description	
Vpload Exte	1.0.0.0	PCS AG	Handles HTTP upload proce	sses
Name: HTTP Upload Extension Manufacturer: PCS AG Version: 1.0.0.0 Handles HTTP upload processes				
State: Loaded				Settings
			<u>O</u> K <u>C</u>	ancel <u>Save</u>

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

Settings: HTTP Upload Extension	×
HTTP Upload Extension Handles HTTP upload processes	
Infected file handling	
<ul> <li>Response template to client</li> <li>Show template directory</li> <li>Navigate client to new address (input full url):</li> <li>Bypass content and log only</li> </ul>	
OK Cancel	

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!

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

#### 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 9001.htm EXTHTTPU1001.htm Mailtemplate.txt Templates	Template for Errors occurring duri Template for Virus scan being not Template for Virus found Template for Email Notification	-	thsuchen	
Organisieren 👻 In Bibliothek a	aufnehmen 🔻 Freigeben für 🔻 Neuer Ordner			
Favoriten	Name ^	Änderungsdatum	Тур	Größe
Nesktop	1001	01.07.2009 14:01	HTML-Dokument	
Downloads	9001	30.06.2009 14:49	HTML-Dokument	
🖳 Zuletzt besucht	ExtHTTPU 100 1	01.07.2009 14:01	HTML-Dokument	
詞 Bibliotheken	MailTemplate	30.06.2009 15:20	Textdokument	
Computer				
	•[			•
4 Elemente				

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.

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

## 3.4. Symantec Scan Engine

UNIQUE Protection for IIS Admin			_ 🗆 🗙
Symantec Scan Engine Add, modify or delete Symantec Scan Engine's for processing.			Show Help
Global Settings   Internet Information Server   Sc	an Extensions	Symantec Scan Engine	Notification About
List of registered Scan Engines:	IP Address o	r Host:	Port: 1344
	Normal		-
		r disable Scan Engine for	processing
Global Scan Engine settings			
Selection mode: Cycle (Request select's next Scan Engine)			
Offline retry (sec): 60 (Value can be 5 to 999 seconds)	Save	New	Delete
		<u>O</u> K <u>C</u> a	ncel <u>S</u> ave

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.

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

#### 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

UNIQUE Protection for IIS Admin	
Notification Set or modify the notifications settings	Show Help
Global Settings Internet Information Server Scan Extensions	Symantec Scan Engine Notification About
Enable or disable notification	
25 🕂 Wamir	or notifications: ngs (Default) server authentication password:
SMTP address sender: SMTP recipients (sep	perate by ';'):
Sender name:	
Subject:	
Notification from UNIQUE Protection for IIS ([ID]).	
Test notification	Show the mail template
	<u>OK</u> <u>Cancel</u> Save

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:

LevelDescriptionVerboseAll incidents will be sentInformationIncidents of the following types will be sent: Information, Warnings, Errors and Fatal<br/>ErrorsWarningsIncidents of the following types will be sent: Warnings, Errors and Fatal ErrorsErrorsIncidents of the following types will be sent: Errors and Fatal ErrorsFatal ErrorsOnly Fatal Errors incidents will be sent

PCS AG support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

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 <a href="mailto:support@pcs-ag.de">support@pcs-ag.de</a>.

#### 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 support@pcs-ag.de Version 2.01.1010 Copyright by PCS AG

ABOUT THIS MANUAL ALL RIGHTS RESERVED. EITHER THE SOFTWARE OR THE MANUAL MAY BE USED WITHOUT THE WRITTEN CONSENT OF PCS AG FULLY OR PARTIALLY REPRODUCED IN ANY FORM, REPRODUCED OR TRANSLATED. CHANGES AND DEVELOPMENTS RESERVED. ALMOST ALL SOFTWARE AND HARDWARE NAMES MENTIONED IN THIS DOCUMENTATI-ON ARE ALSO REGISTERED TRADEMARKS AND SHOULD BE CONSIDERED AS SUCH.

**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 Kärntener Str. 27, 42697 Solingen, Tel.: +49 (0) 212 26799-0, Fax: +49 (0) 212 26799-99 info@pcs-ag.de, www.pcs-ag.de