

## Helm 4 – Windows Firewall

WebHost Automation Ltd  
<http://www.webhostautomation.com/>  
January 2007  
Doc: HELM 4.0.0.0

---

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of WebHost Automation Ltd.*

*WebHost Automation Ltd may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from WebHost Automation Ltd, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2002. WebHost Automation Ltd. All rights reserved.*

*WebHost Automation, Helm, and the Helm Logo, are trademarks of WebHost Automation Ltd*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners*

# Table of Contents

<b>ABOUT HELM.....</b>	<b>3</b>
<b>IMPORTANT INFORMATION ABOUT THIS GUIDE .....</b>	<b>3</b>
<b>INSTALLING THE WINDOWS FIREWALL MODULE .....</b>	<b>4</b>
<b>WINDOWS FIREWALL.....</b>	<b>6</b>
<b>ENABLE AND DISABLE WINDOWS FIREWALL .....</b>	<b>7</b>
<b>SERVICE EXCEPTIONS.....</b>	<b>7</b>
<b>PORT EXCEPTIONS.....</b>	<b>8</b>
<b>ADDING A PORT EXCEPTION .....</b>	<b>8</b>
<b>DELETING A PORT EXCEPTION.....</b>	<b>9</b>

## About Helm

The Helm 4 Web Hosting Control System is an extremely powerful hosting automation solution for Windows 2000 and Windows .NET servers. Helm is developed by WebHost Automation Ltd, a United Kingdom-based corporation. Their main website is:

<http://www.webhostautomation.com>

## Important Information About This Guide

Because of the unique “unlimited user model” that Helm 4 employs, there is no longer a strict tier system. Therefore, the Administrator/Reseller/User layout that existed in the previous version of Helm no longer exists.

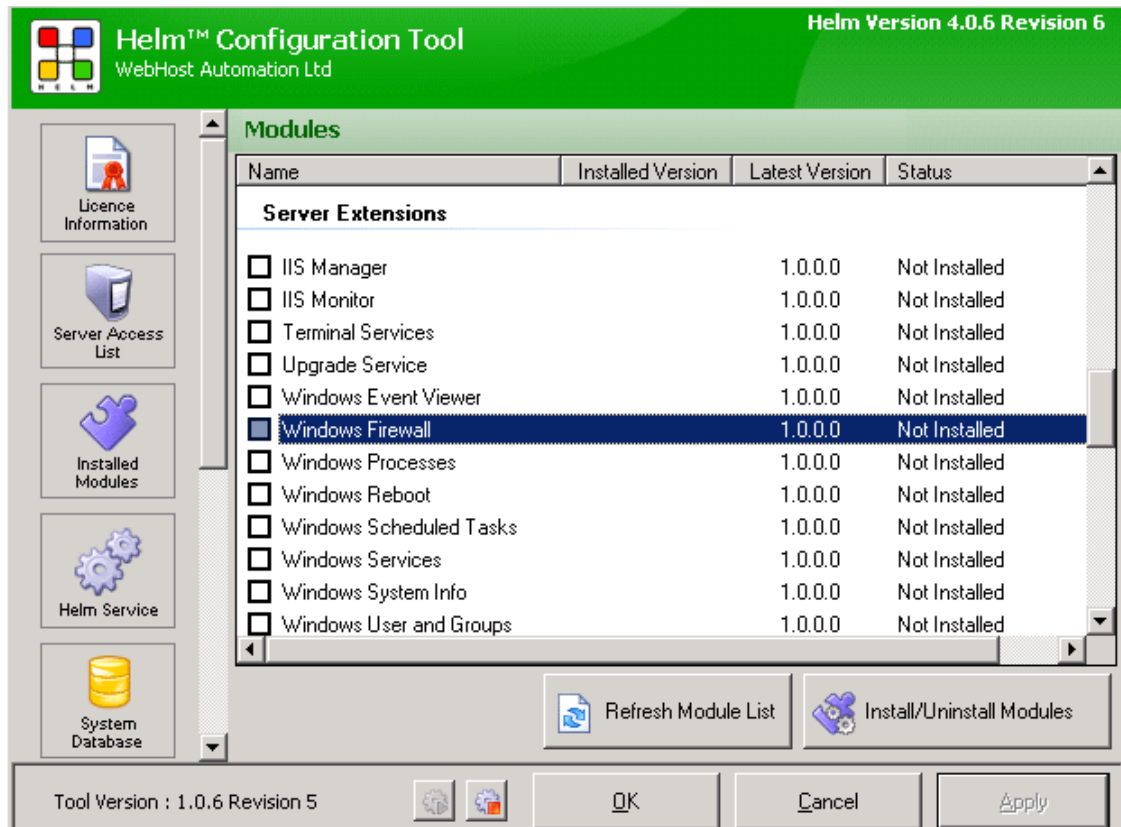
As well as this, the addition of Account roles and Login roles means that there are no longer strict permissions attributable to a specific user. Effectively, if a user has the correct permissions, they can see and/or do anything in Helm, even if they are not an administrator.

You should ensure that you have the correct permissions assigned to your login if you wish to make use of the functionality described in this document. You should contact your administrator for further information about this.

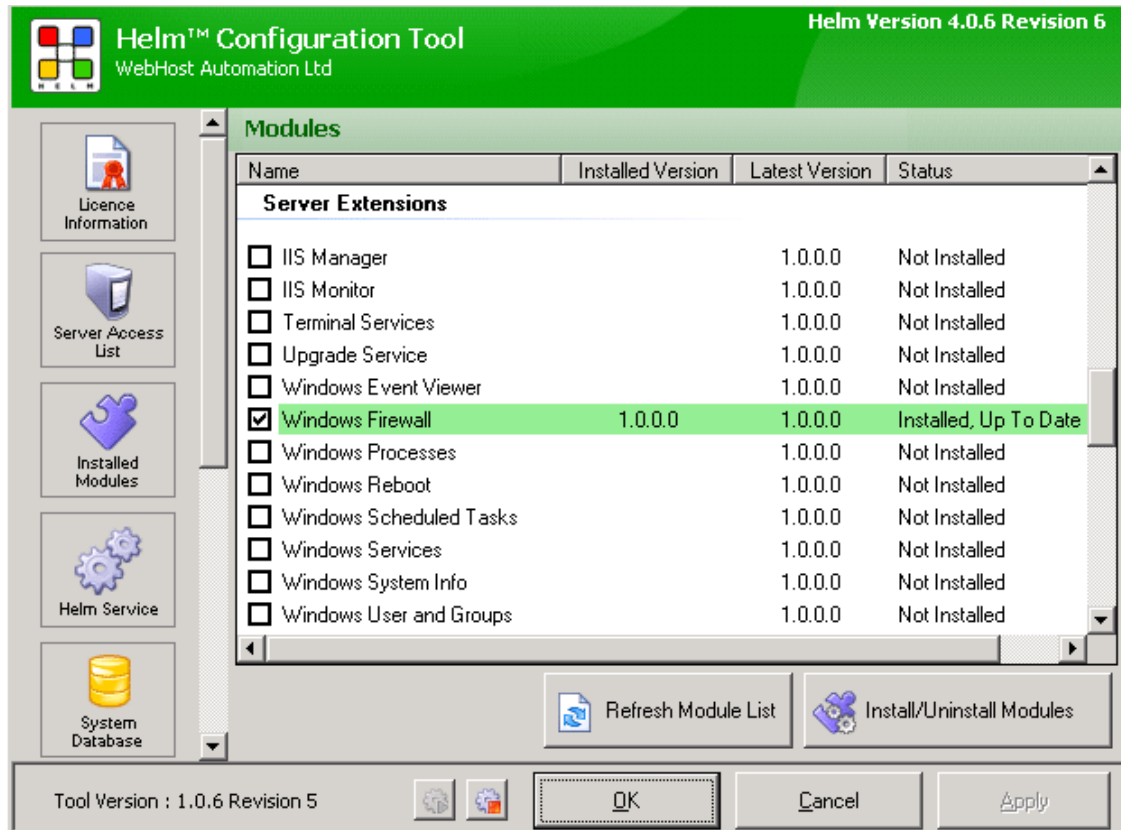
Please take some time to read over this guide. Doing so will make your experience as a user much more enjoyable and profitable. We have littered this guide with helpful screenshots and valuable step-by-step walkthroughs.

## Installing the Windows Firewall Module

To install the Windows Firewall Module, you need to open up the Helm Configuration Tool on your server. Click on the "Installed Modules" button, and you will see all of the available modules for Helm:



Find the Windows Firewall module in the list and check the box, then click the Install/Uninstall Modules button to install it:



The Windows Firewall module is now installed on your Helm build. Read on to learn how to use it in Helm.

# Windows Firewall

Helm allows you to directly manage Windows Firewall, without the need to login to the server itself. This allows you to specify port exceptions, enable and disable the firewall, and more – directly through the Helm interface. To manage the Windows Firewall for a particular server, in Helm go to:

**Home > Helm System > Servers > SERVER NAME > Windows Firewall**

Here you will see your current Windows Firewall settings. They are split into three sections:

**Windows Firewall**
Logged in as: ADMIN

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

**Windows Firewall** ↶ Back

**Windows Firewall**

Enable Windows Firewall

Save

**Service Exceptions on Local Machine**

Service Name	Port Assigned	
File and Printer Sharing	TCP-139, TCP-445, UDP-137, UDP-138	Enable
UPnP Framework	UDP-1900, TCP-2869	Enable
Remote Desktop	TCP-3389	Enable

Page 1 of 1 < 1 > Records Found: 3

**Port Exceptions on Local Machine**

+ Add New Port

Port Name	Protocol	Port	
Helm Remote	TCP	7086	Disable
RDP	TCP	4122	Disable

Page 1 of 1 < 1 > Records Found: 2

## Enable and Disable Windows Firewall

1.) To enable Windows Firewall on the server, simply check the box labeled "Enable Windows Firewall" and click Save.

2.) To disable Windows Firewall on the server, simply check the box labeled "Disable Windows Firewall" and click Save.

## Service Exceptions

By default in Windows Firewall there are three Services that are set by the operating system – **File and Print Sharing, Remote Desktop** and **UPnP Framework**.

If you want to **disable** any of these services in the firewall, just click the "Disable" button next to the service(s) you want to disable. This will then mean that these services are blocked by the firewall.

If you want to **enable** these services to have access through the firewall, click the "Enable" button next to the service(s) you want to enable. This will then mean these services are allowed to communicate through the firewall.

## Port Exceptions

In this section you can specify your own port exceptions to allow software to communicate through the firewall on different ports. In the screenshot above, you will see two examples that have been added – Helm Remote has been enabled on port 7086 and the Remote Desktop Protocol has been enabled on port 4122.

If you want the server to **disable** any of these port exceptions in the firewall, just click the “Disable” button next to the port exception(s) you want to disable. This will then mean that these port exceptions are blocked by the firewall.

If you want to **enable** these port exceptions to have access through the firewall, click the “Enable” button next to the port exception(s) you want to enable. This will then mean these port exceptions are allowed to communicate through the firewall.

## Adding a Port Exception

1.) Click Add New Port. You will be taken to the Port Exception screen:

**Port Name:-** Enter a friendly name for the Port Exception you are creating (e.g. SMTP).

**Port No.:-** Enter the port number you wish to allow access through the firewall to (e.g. 1234).

**Protocol:-** Select whether this port uses either the TCP or UDP protocol. Generally UDP is commonly used for streaming audio and video, and TCP is used for everything else – check the documentation of the software you are allowing through the firewall to see which protocol it uses.

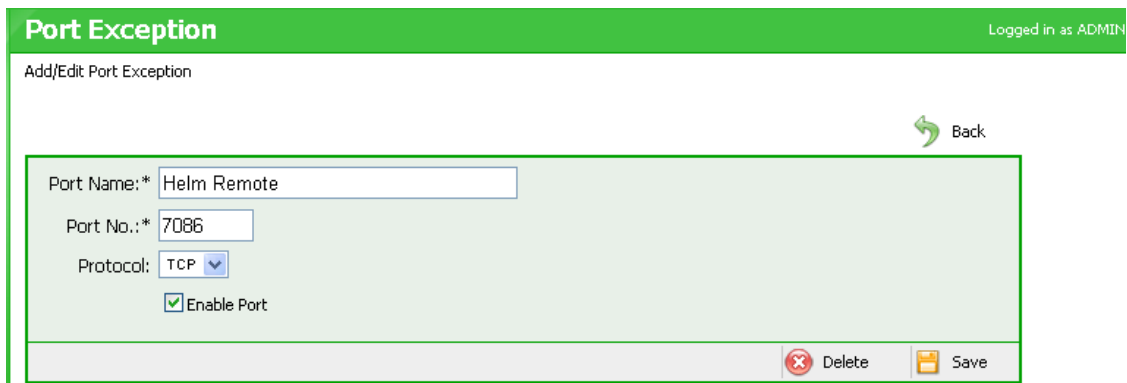
**Enable Port:-** If you want to make this port exception active straight away, check this box. If you want to add it but leave it disabled for now, uncheck this box.

2.) Choose the details of your port exception as outlined above, and click Save to save the port exception.

## Deleting a Port Exception


If you wish to delete a port exception completely:

1) Click on the port exception in the list to get taken to the Port Exception screen and then click the Delete button:



Port Exception Logged in as ADMIN

Add/Edit Port Exception



 Back

Port Name:\* Helm Remote

Port No.:\* 7086

Protocol: TCP

Enable Port

 Delete  Save

2.) On the next screen click OK to confirm the deletion.