



IIS Password Configuration Guide

How to configure IIS Password for use with Helm

WebHost Automation Ltd
<http://www.webhostautomation.com/>
February 2007
Doc: HELM300.02.14

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

Using Helm with IIS Password

IMPORTANT:- Before installing IIS Password, make sure that your Domains folder (the folder where all of your website folders and data are stored) has the "Network Service" Windows user added to it, with "Read" permissions. This is required by IIS Password and will need to be added in order for it to work with Helm.

You can download IIS Password from the site of its developer, Troxo:

<http://www.troxo.com/>

Refer to IIS Password installation instructions in order to install IIS Password. Once installed, you will need to configure Helm to use IIS Password.

In Helm, go to the web service you have set up:

Home > System Settings > Servers > [Your Server] > Services > Web Service

At the bottom you will see Secure Folder details:

Server Name:	DEVSVR1
Friendly Name:	IIS 6.0 Service
Service Type:	Microsoft IIS 6.0
Physical Root Path:	C:\Domains
IP Address:	192.168.1.3 - (192.168.1.3) ▼
Parking Page:	_holding.htm
ASP Path:	C:\Windows\system32\inetrv\ASP.DLL
ASP.NET Library Path:	C:\Windows\Microsoft.NET\Framework\v1.0
Perl App. Path:	C:\perl\bin\perl.exe "%s" %s
PHP App. Path:	C:\php\php.exe
CFusion App. Path:	c:\cfusionmx\runtime\lib\wsconfig\1\jrun.dll
Scripts Directory:	c:\inetpub\wwwroot\cfide
Flash Remoting Dir.:	c:\cfusionmx\runtime\lib\wsconfig\1\
Shared SSL Domain:	
Shared SSL Folder:	SSL
FP Admin Username:	Administrator
FP Admin Password:	●●●●●●●●
FrontPage Port:	0
Secure Folder Type:	- None - ▼
Secure Filter Path:	
Secure Folder Realm:	
Maximum Domains:	999999999
<input type="button" value="Back"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>	

Select **IIS Password** from the Secure Folder Type dropdown box. In the Secure Filter Path, you need to type the path to IIS Password's DLL file. By default this will be:

C:\Windows\system32\inetrv\iispasswordfilter.dll (for Windows 2003 servers)

or

C:\WINNT\system32\inetrv\iispasswordfilter.dll (for Windows 2000 servers)

However, if you have installed it to a different location you will need to type in the correct path to the DLL.

NOTE:- If you are not using the latest version of IIS Password available from their website, it is recommended to download this. Otherwise, the path to the DLL will be different to the above paths:

C:\Program Files\Troxo\IISPassword\iispasswordfilter.dll

The Secure Folder Realm is simply what the top of the authentication box will say when you try to access a password protected folder. In here you can enter whatever you wish.

Below is how the web service should look if you have installed IIS Password to the default location, along with an example of a secure folder realm:

Secure Folder Type:	IIS Password
Secure Filter Path:	C:\Program Files\Troxo\IISPassword\iispass
Secure Folder Realm:	Protected by Helm!

(Those with the latest version of IIS Password do not need to follow the next step):

IMPORTANT NOTE: On **older** versions of IIS Password, the Server Administrator must ensure that the "NETWORK SERVICE" user has "read" permissions to the **domains** folder, or wherever you are storing your Helm-created domains:

- Go to the domains folder, right-click, choose properties and go to the Security tab.
- Add a new user and type "Network Service" and click Check Names. Windows should pick up this user automatically. You need to ensure this user has read permissions on the domains folder.

Click Save to update the service, and to complete IIS Password configuration.

Final Steps for setting up Password Protected Directories

Now that your password protection software of choice is set up, all you need to do is assign your plans and packages with the number of installations you wish to provide. For instance, you might want to allow your reseller to purchase 100 Secure Folder installations, which they can then sell on to their customers:

Login to Helm as **admin**, and from the Home screen select 'Reseller Plans'. Choose 'Resource Limits' then choose 'Web Resources'. You can see Secure Folders highlighted below. Change this to the number you wish to offer, and click 'Save'.

Home > Reseller Plans > Sample Reseller Plan > Plan Resources > Web Resources - [[Help](#) | [Log Off](#)]

Plan Resources

Below are the resources that have been assigned to this plan. All packages that created from this plan will inherit the values below.

Sample Reseller Plan

Enable Web Resource

System Resource:

ODBC DSNs:

Sub Domains:

ASP: domains

ASP.NET: domains

Perl: domains

PHP: domains

CGI-BIN: domains

ColdFusion 5/MX: domains

FrontPage Webs: domains

Shared SSL: domains

Secure Folders: domains

Custom Error Pages:

MIME Type Editor:

File Manager:

Now all your resellers need to do is alter their users' hosting plans to provide Secure Folders installations as and when required.