

IIS4 Directory Permissions

© Actinic Software Ltd.

Author: Shaun Sloan
Date: 22nd August 2001
Revision: 1.0

Revision History

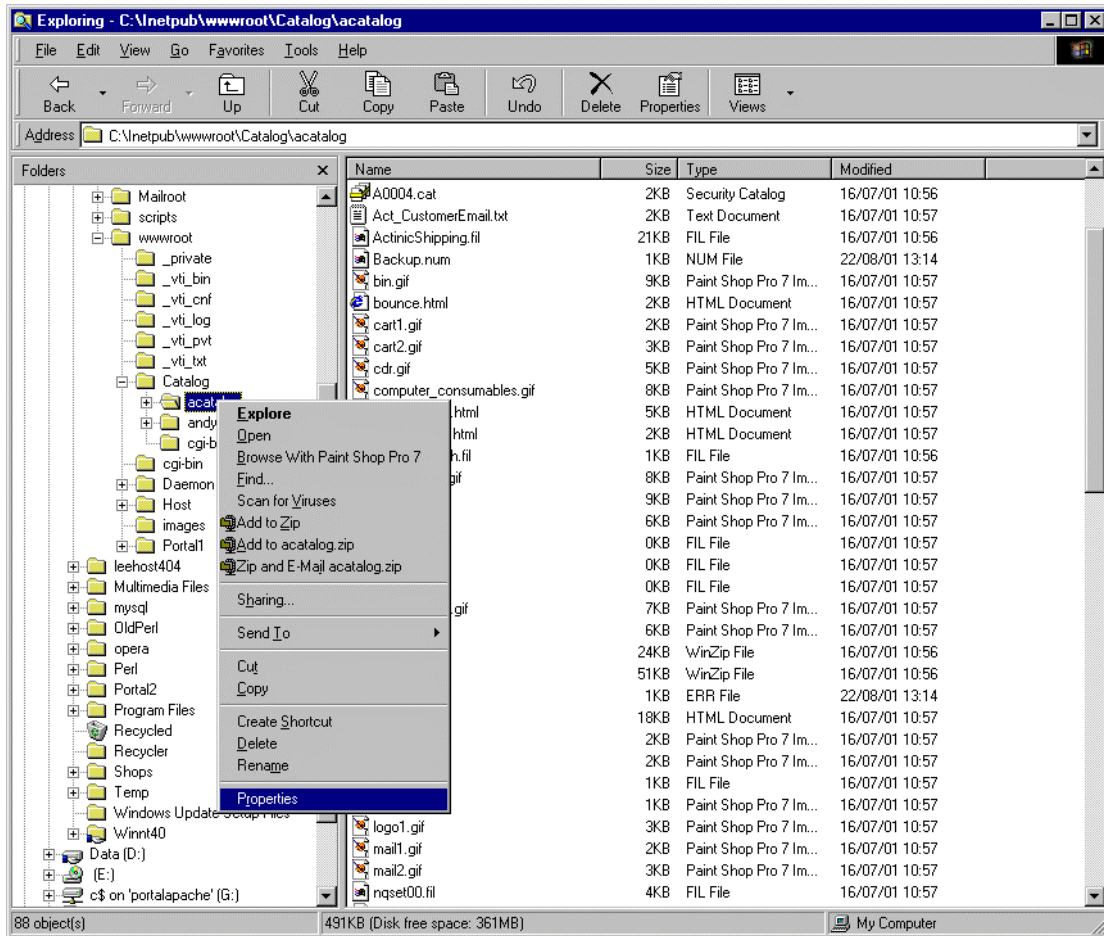
Revision	Date	Author	Comments
1.0	22 nd August 2001	Shaun Sloan	Initial

Contents

<u>1</u>	<u>Acatalog NTFS Directory Permissions</u>	4
<u>2</u>	<u>CGI-BIN NTFS Directory Permissions</u>	7
<u>3</u>	<u>Acatalog IIS Permissions</u>	10
<u>4</u>	<u>Cgi-bin IIS Permissions</u>	13

1 Acatalog NTFS Directory Permissions

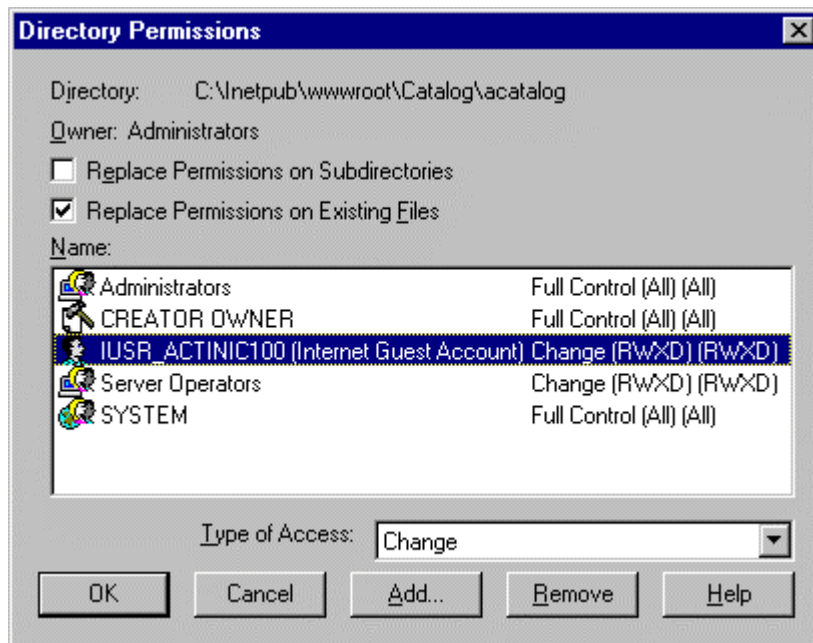
The NTFS permissions on the acatalog directory should be set via Windows Explorer and right clicking on the acatalog directory and selecting Properties from the popup menu:



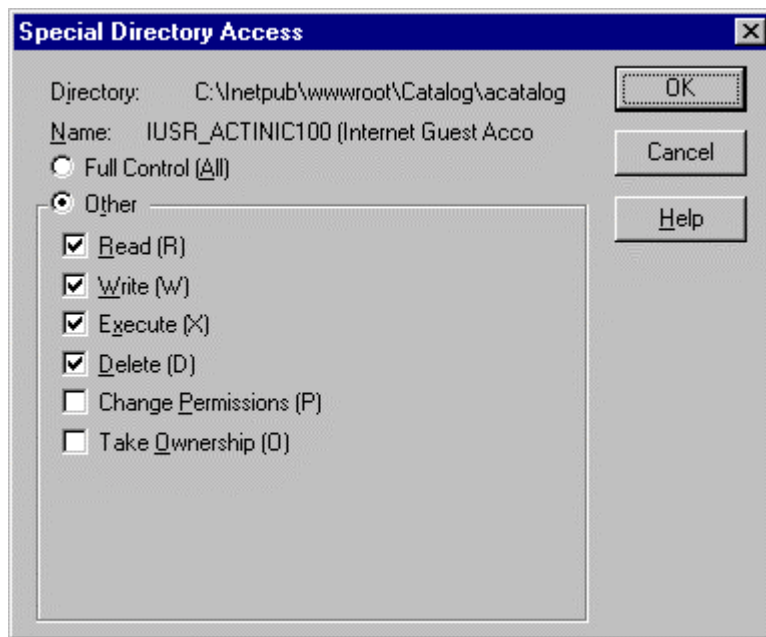
Next, select the Security tab and click on the Permissions button:



Double click on the IUSR_localhost User:



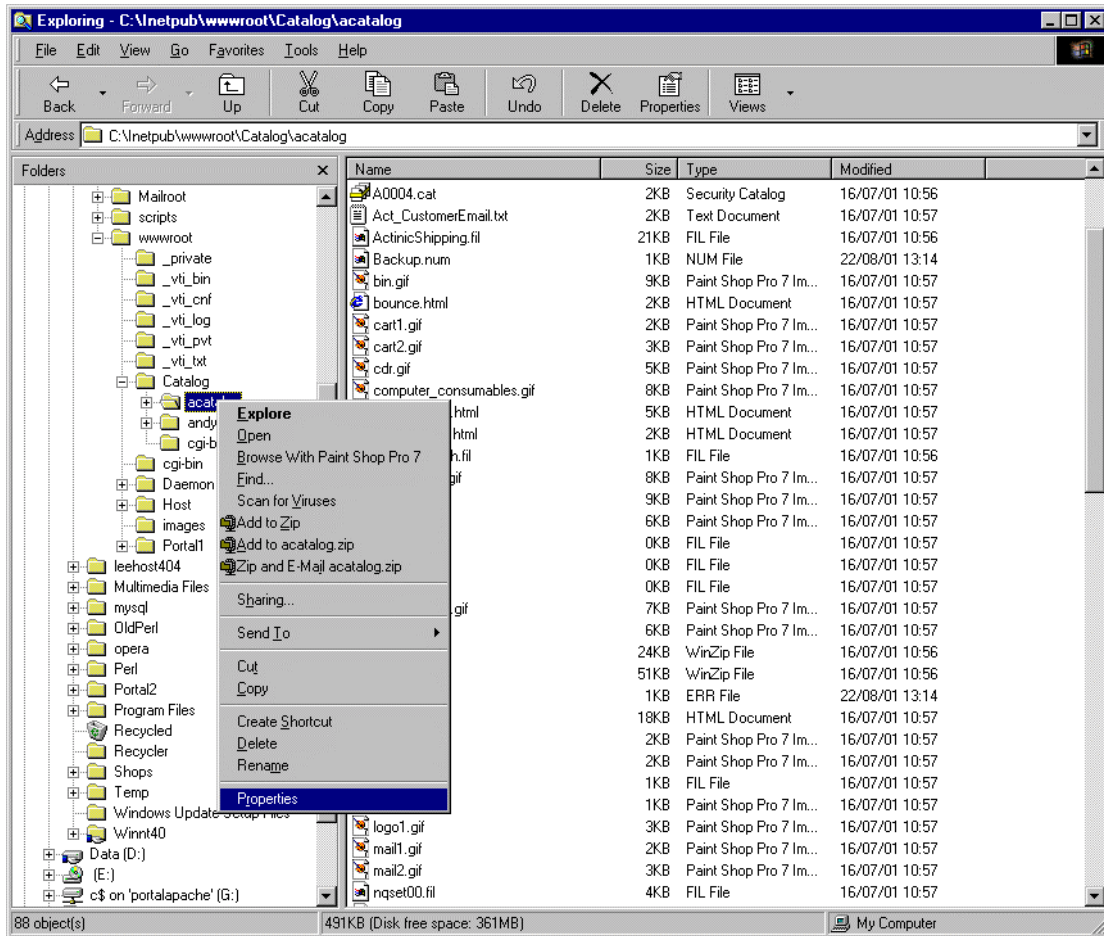
Set the permissions as follows:



Read, Write, Execute and Delete. Click OK to accept.

2 CGI-BIN NTFS Directory Permissions

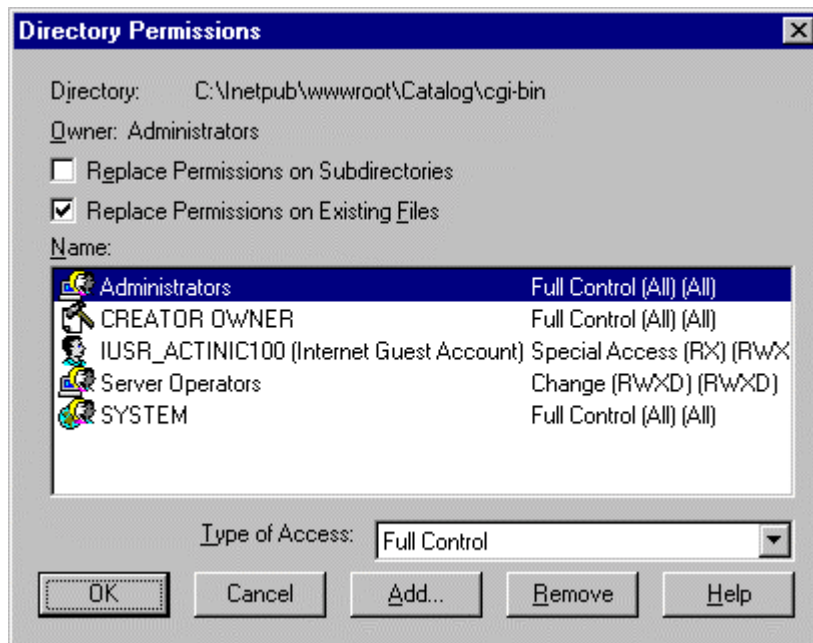
The NTFS permissions on the cgi-bin directory should be set via Windows Explorer and right clicking on the cgi-bin directory and selecting Properties from the popup menu:



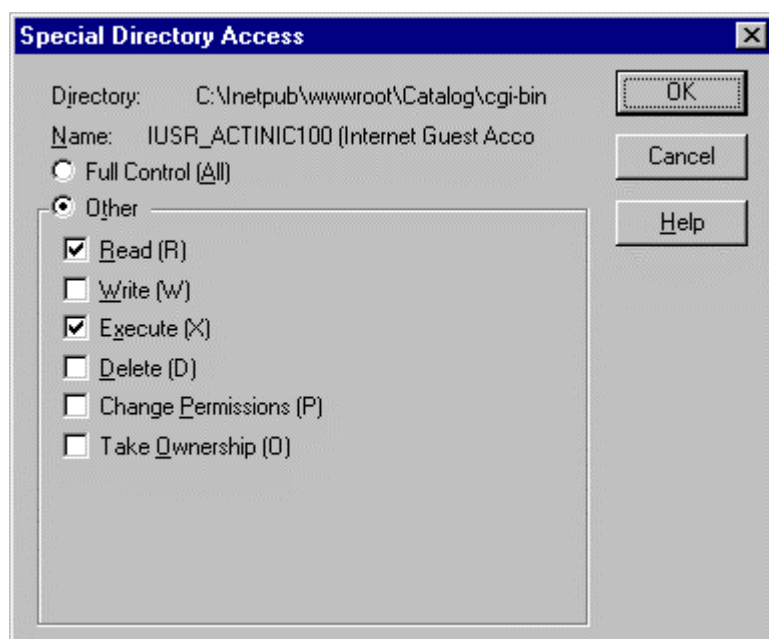
Next, select the Security tab and click on the Permissions button:



Double click on the IUSR_localhost User:



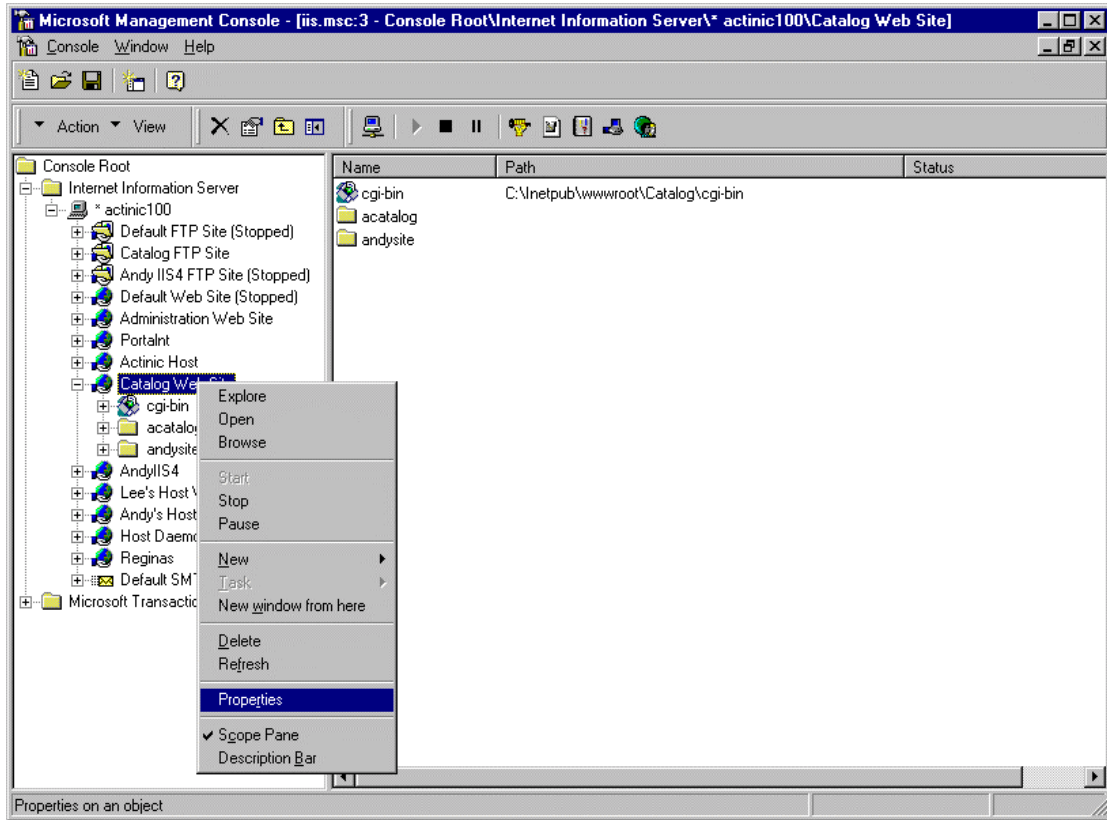
Set the permissions as follows:



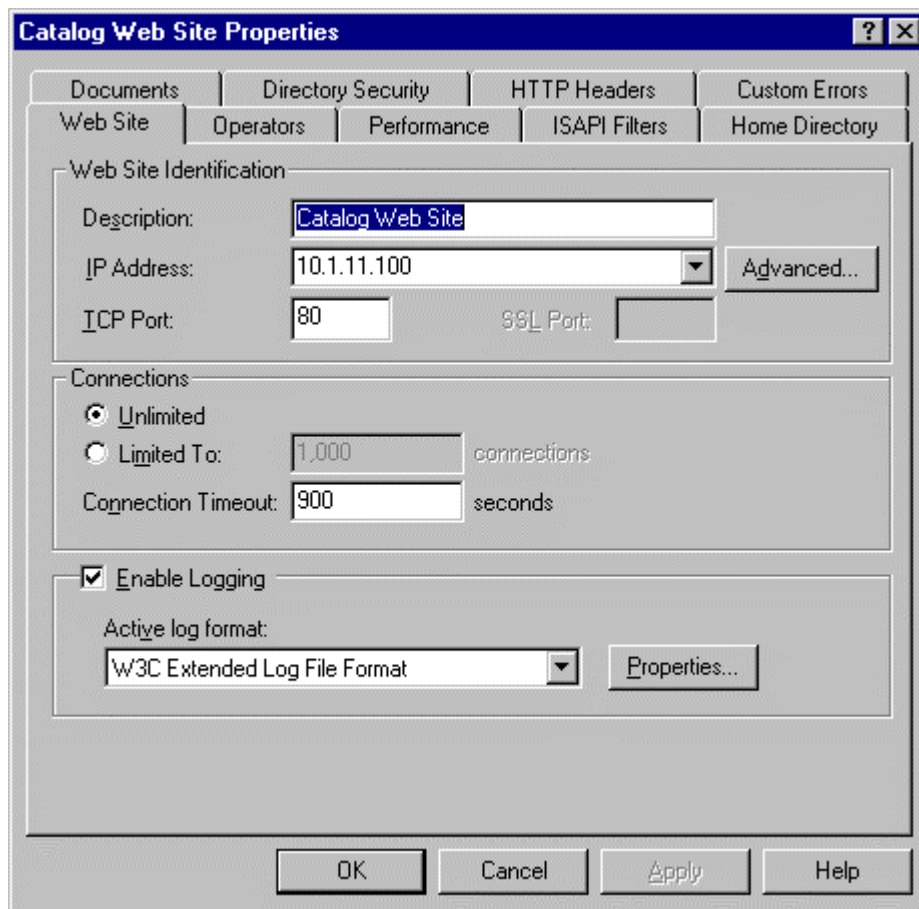
Read and Execute. Click OK to accept.

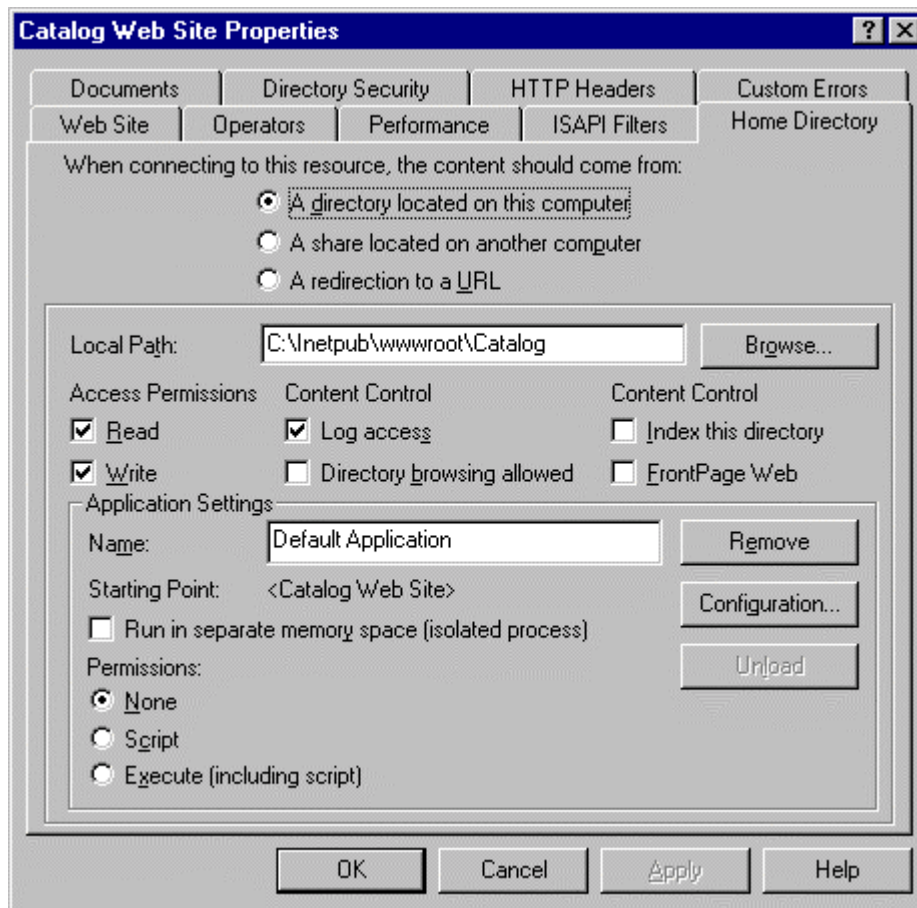
3 Acatalog IIS Permissions

In the IIS MMC select the web site and right click and select Properties:



Next, select the Home Directory tab:





The Access Permissions should be set to:

Read, Write

The Content Control to:

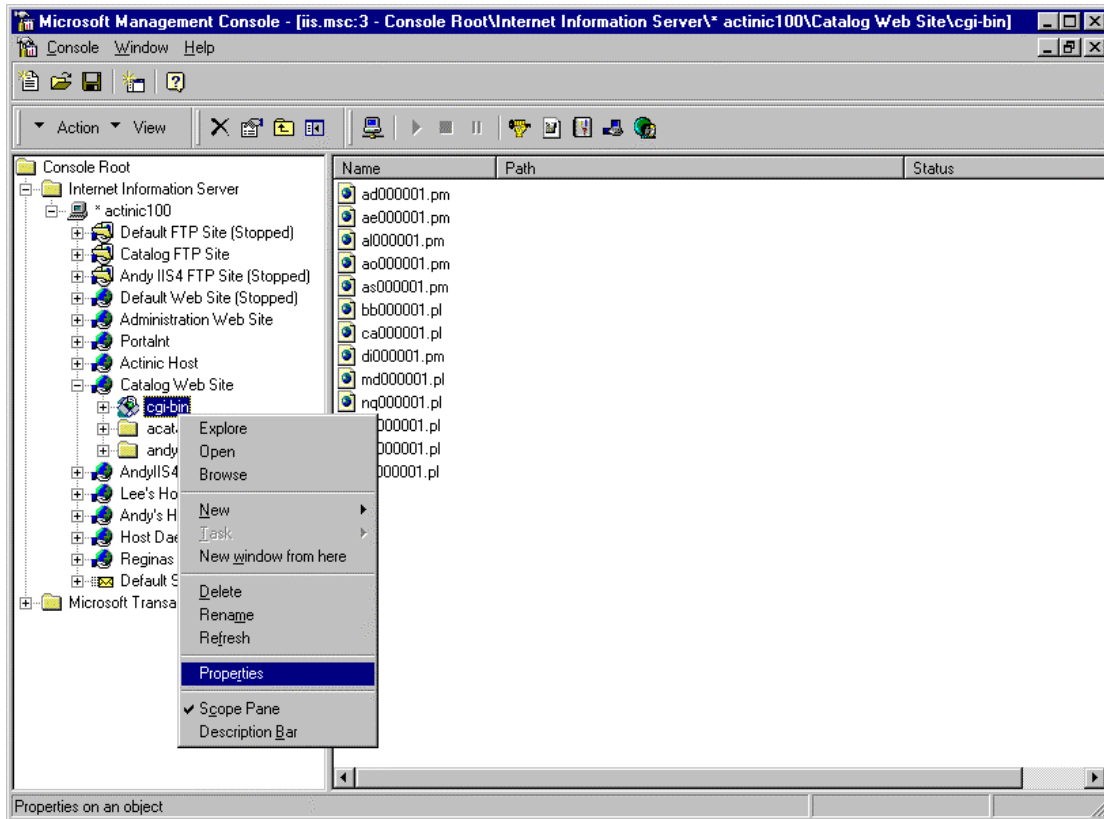
Log Access

In the Application Settings the Permissions should be set to:

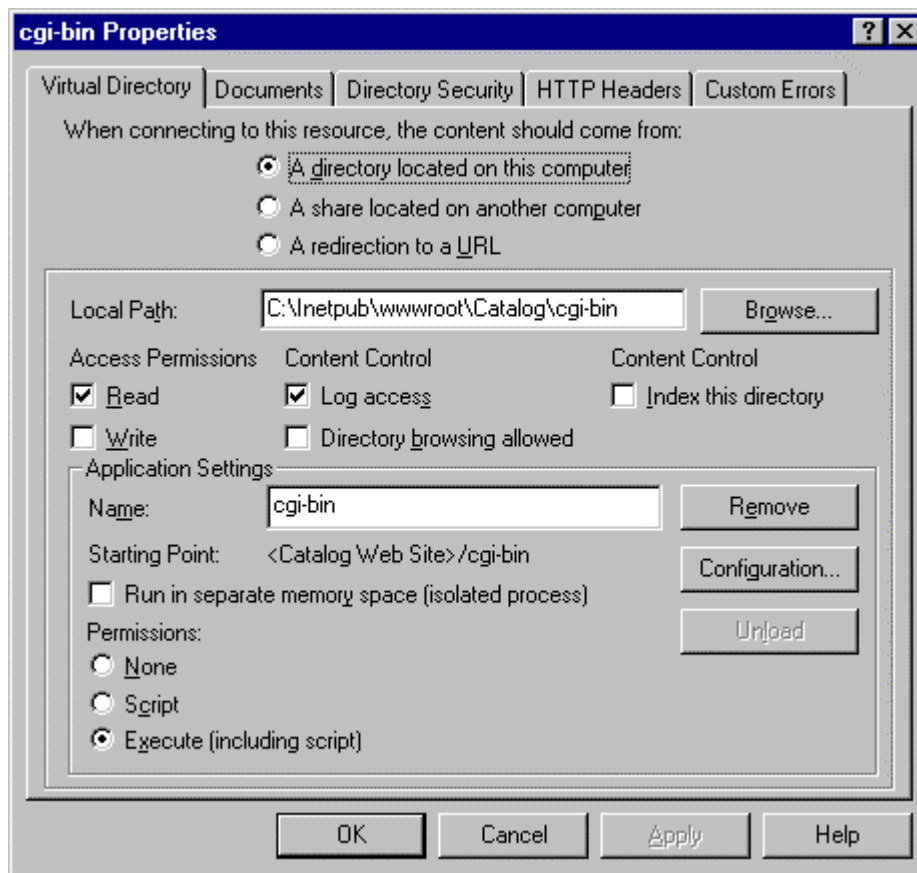
None

4 Cgi-bin IIS Permissions

In the IIS MMC in the web site select the cgi-bin directory and right click and select Properties:



The following permissions should be set:



The Access Permissions should be set to:

Read

The Content Control to:

Log Access

In the Application Settings the Permissions should be set to:

Execute (including script)