

Re: Minimum NTFS Permissions – There's such a thing???

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-05/0343.html>

From: BB (*qbernard_at_hotmail.com*)

Date: 05/12/03

Date: Mon, 12 May 2003 11:52:21 +0800

This is from Terry..

Terry Harney [MSFT]

This posting is provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use. ©2001 Microsoft Corporation. All rights reserved.

HOW TO: Set Minimum NTFS Permissions Required for IIS 5.0 to Work WGID:198
ID: 271071.KB.EN-US CREATED: 2000-08-08 MODIFIED: 2003-03-06

=====

The information in this article applies to:

- Microsoft Internet Information Services 5.0 (Version: 5.0)

- #2: SUMMARY
- #3: Give Ownership and Permission to Administrators and System
- #4: Disable Inheritance in System Directories
- #5: NTFS Permissions
- #6: Policies
- #7: Grant Permissions in the Registry
- #7: Registry
- #8: Grant Rights in the Local Security Policy
- #9: Policies
- #10: Troubleshoot
- #11: Services Required
- #12: REFERENCES

SUMMARY

=====

This step-by-step article describes how to set the minimum permissions that you must have to run Internet Information Services (IIS) 5.0 in a secure and protected environment. This document does not, unless

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

otherwise

noted, outline the security that is necessary to run additional Microsoft or

third-party applications in an IIS 5.0 environment.

Note This article only applies to IIS 5.0. It does not apply to any other versions of IIS.

For

additional information about the necessary permissions for IIS 4.0, click the following article number to view the article in the Microsoft Knowledge Base:

KBLink:187506.KB.EN-US: List of NTFS Permissions Required for IIS Site to Work

Testing for this document included the following functional tests:

- Hypertext documents (HTML)
- Active Server Pages (ASP)
- FrontPage Server Extensions (connecting, editing, and saving), if FPSE is enabled while you use the Lockdown Tool
- Secure Socket Layers (SSL) Connections

Because Microsoft does not recommend that you run IIS on domain controllers, these permissions and rights were not tested. Microsoft also does

not recommend that you run IIS in any of the following environments:

- Microsoft Exchange 5.5 or Microsoft Exchange 2000 Outlook Web Access
- Microsoft Small Business Server 2000
- Microsoft SharePoint Portal or Team Services
- Microsoft Commerce Server 2000 or Microsoft Commerce Server 2002
- Microsoft BizTalk Server 2000 or Microsoft BizTalk Server 2002
- Microsoft Content Management Server 2000 or Microsoft Content Management Server 2002
- Microsoft Application Center 2000

Before you apply the permissions in this article, Microsoft recommends that you run the most current version of the IIS Lockdown Tool. For

more information about this tool, visit the following Microsoft Web site:

<http://www.microsoft.com/technet/security/tools/tools/locktool.asp>

The following programs and services are installed when you use the permissions that are outlined in this article:

- Index Services
- Terminal Services
- Script Debugger
- IIS
- Common Files
- Documentation
- FrontPage Server Extensions 2000
- Internet Services Manager (HTML)
- WWW
- FTP

To assign permissions to the system:

1. Open Windows Explorer. To do this, click "Start", click "Programs", and then click "Windows Explorer".
2. Expand "My Computer".
3. Right-click the system drive (this is typically drive C), and then click "Properties".
4. Click the "Security" tab, and then click "Advanced" to open the "Access Control Settings for Local Disk" dialog box.
5. Click the "Owner" tab, click to select the "Replace Owner on Sub containers and Objects" check box, and then click "Apply".

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

If you receive the following error message, click "Continue":

An error has occurred applying security information to %systemroot%\Pagefile.sys

6. If you receive the following error message, click "Yes":

You do not have permission to read the contents of directory %systemroot%\System Volume Information - Do you want to replace the directory permission - All permission will be replaced granting you Full Control

7. Click "OK" to close the dialog box.

8. Click "Add".

9. Add the following users, and then grant them the Full Control user right:

- Administrator
- System
- Creator Owner

10. After you have added these user rights, click "Advanced", click to select the "Reset permission on all child objects and enable propagation of inheritable permissions" check box, and then click "Apply".

11. If you receive the following error message, click "Continue":

An error has occurred applying security information to %systemroot%\Pagefile.sys

12. After you have reset user rights, click "OK".

13. Click the "Everyone" group, click "Remove", and then click "OK".

14. Open the properties for the %systemroot%\Program Files\Common Files folder, and then click the "Security" tab.

Add the account that is used for anonymous access (by default, this is the IUSR_<MachineName> account) and the Users group, and then make sure that only the following are selected:

- "Read & Execute"
- " List Folder Contents"
- "Read"

15. Open the properties for the root directory that holds your Web content (by default, this is the %systemroot%\Inetpub\Wwwroot folder).

Click the "Security" tab, add the IUSR_<MachineName> account and the Users group, and then make sure that only the following are selected:

- "Read & Execute"
- " List Folder Contents"
- "Read"

16. If you want to grant the Write user right for Inetpub\FTProot or the directory path for your FTP site or sites, repeat step 15. Note Microsoft does not recommend that you give the Write user right to the anonymous account in any directories that the FTP service uses. This can cause unnecessary data to be uploaded to your FTP site.

1. In the %systemroot%\winnt\System32 folder, select all folders except the following:

- Inetsrv
- Certsrv (if present)
- Com

2. Right-click the remaining folders, click "Properties", and then click the "Security" tab.

3. Click to clear the "Allow inheritable permissions" check box, click "Copy", and then click "OK".

4. In the %systemroot%\winnt folder, select all folders except

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

the following:

- Assembly (if present)
 - Downloaded Program Files
 - Help
 - IIS Temporary Compressed Files
 - Microsoft.NET (if present)
 - Offline Web Pages
 - System32
 - Tasks
 - Temp
 - Web
5. Right-click the remaining folders, click "Properties", and then click the "Security" tab.
 6. Click to clear the "Allow inheritable permissions" check box, click "Copy", and then click "OK".
 7. Apply permissions to the following:
 - a. Open the properties for the %systemroot%\Winnt folder, click the "Security" tab, add the "IUSR_<MachineName>" and "IWAM_<MachineName>" accounts and the "Users" group, and then make sure that only the following are selected:
 - "Read & Execute"
 - " List Folder Contents"
 - "Read"
 - b. Open the properties for the %systemroot%\Winnt\Temp folder, select the "IUSR_<MachineName>" account (this account is already present because it inherits from the Winnt folder), and then click to select the "Modify" check box. Repeat this step for the "IWAM_<MachineName>" account and the "Users" group.
 - c. If FrontPage Server Extension Clients such as FrontPage or Microsoft Visual InterDev are being used, open the properties for the %systemroot%\Inetpub\Wwwroot folder, select the "Authenticated Users" group, select the following, and then click "OK":
 - "Modify"
 - "Read & Execute"
 - "List Folder Contents"
 - "Read"
 - "Write"

The following table lists the permissions that will be applied when you follow the steps in the section. This table is for reference only.

To apply the permissions in the following table:

1. Open Windows Explorer. To do this, click "Start", click "Programs", click "Accessories", and then click "Windows Explorer".
2. Expand "My Computer".
3. Right-click "%systemroot%", and then click "Properties".
4. Click the "Security" tab, and then click "Advanced".
5. Double-click "Permission", and then select the appropriate setting from the "Apply Onto" list.

Note In the ?Apply To? column, the term Default refers to ?This folder, subfolders, and files.?

```

=====+=====
====+=====+=====+
| Directory                                     | Users\Groups
|   | Permissions           | Apply To           |
+=====+=====+=====+
=====+=====+=====+

```

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

```

| %systemroot%\ (c:\winnt) | Administrator
| Full
Control | Default |
+=====+
| | Full Control | Default | System
+=====+
| | Read, Execute | Default | Users
+=====+
| %systemroot%\system32 | Administrators
| Full
Control | Default |
+=====+
| | Full Control | Default | System
+=====+
| | Read, Execute | Default | Users
+=====+
| %systemroot%\system32\inet_srv | Administrators
| Full
Control | Default |
+=====+
| | Full Control | Default | System
+=====+
| | Read, Execute | Default | Users
+=====+
| Inetpub\adminscripts | Administrators
| Full
Control | Default |
+=====+
| Inetpub\urlscan (if present)
Default | Administrators | Full Control |
+=====+
| | Full Control | Default | System
+=====+
| %systemroot%\system32\inet_srv\metaback | Administrators
| Full
Control | Default |
+=====+
| | Full Control | Default | System

```


microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

```

=====+=====+=====+
|                                     | IWAM_<Machinename>
|   | Read,
|   Execute| This folder and files   |
+=====+=====+=====+
|                                     | Network
|   | Full Control   | This folder and
|   files |
+=====+=====+=====+
|                                     | Service
|   |                                     | This folder and files |
+=====+=====+=====+
|                                     | Users
|   | Read, Execute  | This folder and
|   files |
+=====+=====+=====+
| Inetpub\wwwroot (or content
| directories) | Administrators | Full Control |
This folder
and files |
+=====+=====+=====+
|                                     | System
|   | Full Control   | This folder and
|   files |
+=====+=====+=====+
|                                     | IWAM_<MachineName>
|   | Read,
|   Execute| This folder and files   |
+=====+=====+=====+
|                                     | Service
|   | Read, Execute  | This folder
|   and files |
+=====+=====+=====+
|                                     | Network
|   | Read, Execute  | This folder
|   and files |
+=====+=====+=====+
| Optional**: | Users
|   | Read, Execute  | This
|   folder and files |
+=====+=====+=====+

```

** If you are using FrontPage Server Extensions, the Authenticated Users or the Users group must have the Change user right to create, rename, write, or provide the functionality that a developer might need from a FrontPage type of client, such as Visual InterDev 6.0 or FrontPage 2002.

1. Click "Start", click "Run", type "regedt32" (without the quotation marks), and then click "OK". Do not use Regedit.exe because it does not permit you to change permissions in Windows 2000.

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

2. In Registry Editor, locate and select "HKEY_LOCAL_MACHINE".
3. Expand "System", expand "CurrentControlSet", and then expand "Services".
4. Select the "IISADMIN" key, click "Security" (or press ALT+S), and then select "Permissions" (or press P).
5. Click to clear the "Allow inheritable permissions from parent to propagate to this object" check box, click "Copy", and then remove all users except:
 - Administrators (Allow Read and Full Control)
 - System (Allow Read and Full Control)
6. Click "OK".
7. Perform these steps again for the "MSFTPSVC" key.
8. Select the "W3SVC" key, click "Security", and then click "Permissions".
9. Click to clear the "Allow inheritable permissions from parent to propagate to this object" check box, and then remove all entries except:
 - Administrators (Allow Read and Full Control)
 - System (Allow Read and Full Control)
 - Network (Read)
 - Service (Read)
 - IWAM_<MachineName> (Read)
10. Click "OK"

 The following table lists the permissions that will be applied when you follow the steps in the section. This table is for reference only.

Note The acronym HKLM stands for HKEY_LOCAL_MACHINE.

```

=====
+=====+=====
| Location                | Users\Groups
| Permissions            |
+=====+=====
+=====+
| HKLM\System\CurrentControlSet\Service\IISAdmin | Administrators
| Full
| Control |
+=====+=====
+=====+
|                | System
| Full Control    |
+=====+=====
+=====+
| HKLM\System\CurrentControlSet\Service\MsFtpSvc | Administrators
| Full
| Control |
+=====+=====
+=====+
|                | System
| Full Control    |
+=====+=====
+=====+
| HKLM\System\CurrentControlSet\Service\w3svc   | Administrators
| Full
| Control |
+=====+=====
+=====+
|                | System
| Full Control    |
+=====+=====
+=====+
|                | IWAM_<MachineName>
    
```

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

```
| Read |
+=====+
+=====+
```

1. Click "Start", click "Settings", and then click "Control Panel".
2. Double-click "Administrative Tools", and then double-click "Local Security Policy".
3. In the "Local Security Settings" dialog box, expand "Local Policies", and then click "User Rights Assignment".
4. Modify the appropriate policy:
 - a. Double-click the policy.
 - b. Select and then click "Remove" for any user who is not listed in the table.
 - c. Add any user who is not listed. To do this, click "Add", and then select the user in the "Select Users or Groups" dialog box.

Note that because a domain controller policy overrides the local policy, you must make sure that Effective Policy Setting matches Local Policy Setting.

The following table lists the permissions that will be applied when you follow the steps in the section.

```
-----
+=====+
+=====+
| Policy | Users
+=====+
+=====+
| Log on Locally | Administrators
+=====+
+=====+
| (Anonymous) | IUSR_<MachineName>
+=====+
+=====+
| Access this computer from the Network | Administrators
+=====+
+=====+
| | ASPNet (.NET Framework)
+=====+
+=====+
| (Anonymous) | IUSR_<MachineName>
+=====+
+=====+
| | IWAM_<MachineName>
+=====+
+=====+
| | Users
+=====+
+=====+
| Log on as a Batch Job | ASPNet
+=====+
+=====+
| | Network
+=====+
```

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

```
+=====+
=====+
|           | IUSR_<MachineName>
|           |
+-----+
=====+
|           | IWAM_<MachineName>
|           |
+-----+
=====+
|           | Service
|           |
+-----+
=====+
| Logon as a Service | ASPNet
|           |
+-----+
=====+
|           | Network
|           |
+-----+
=====+
| Bypass Transverse Checking | Administrators
|           |
+-----+
=====+
|           | IUSR_<MachineName>
(Anonymous) |
+-----+
=====+
|           | Users (Basic, Integrated,
Digest)    |
+-----+
=====+
|           | IWAM_<MachineName>
|           |
+-----+
=====+
-----
```

For additional information about the services that you need for IIS 4.0, click the following article number to view the article in the Microsoft Knowledge Base:

KBLink:189271.KB.EN-US: List of Services Needed to Run a Secure IIS Computer

For additional information about the services that you need for IIS 5.0, click the following article number to view

the article in the Microsoft Knowledge Base:

KBLink:810866.KB.EN-US: Services Required to Run a Secure IIS Server on Windows 2000

REFERENCES

=====

12

For additional information about how to restore default NTFS permissions for Windows 2000, click the following article number to view the article in the

Microsoft Knowledge Base:

KBLink:266118.KB.EN-US: How to Restore the Default NTFS Permissions for Windows 2000

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

QUERY WORDS

=====

iis 5 NTFS permission permissions security internet
information services lockdown policy template

=====

===

List of NTFS Permissions Required for IIS Site to Work WGID:198
ID: 187506.KB.EN-US CREATED: 1998-06-10 MODIFIED: 2003-03-06

=====

===

The information in this article applies to:

- Microsoft Internet Information Server 4.0 (Version: 4.0)

SUMMARY

=====

This article lists the Microsoft Windows NT File System (NTFS) access permissions that you must have for an Internet Information Server (IIS) Web site, an Internet Information Services (IIS) Web site, or a File Transfer Protocol (FTP) site to work. This article applies only to IIS 4.0. For additional information about IIS 5.0, click the following article number to view the article in the Microsoft Knowledge Base:

KBLink:271071.KB.EN-US: Minimum NTFS Permissions Required for IIS 5.0 to Work

Note When you install IIS, it creates the correct NTFS access permissions for the default Web site and for the default FTP site for the anonymous user account (IUSR_Computer_Name) and, if applicable, for the application owner user account (IWAM_Computer_Name). If you try to gain access to a Web page that you do not have access permissions for, you may receive the following error message:

HTTP Error 401 401.3 Unauthorized: Unauthorized due to ACL on resource.

MORE INFORMATION

=====

To properly access and manage IIS, the local System account and local Administrators group need FULL CONTROL permissions to all drives on the computer. These permissions can be added from a command prompt. Type the following commands on each NTFS drive:

```
cd \  
cacls * /T /E /C /P System:F Administrators:F
```

NOTE: Modifying permissions may take several minutes per drive, depending on the amount of data on that drive. If the drive has no files, you receive the following error message:

The System cannot find the file specified.

To configure the minimum required NTFS permissions for users who access IIS, grant the following directory permissions to the anonymous Internet user account (by default, this is the IUSR_computer_name account) and any other accounts or groups that need access to the Web server:

Directory	Permissions
Content	READ (RX)
Winnt	READ (RX)
Winnt\System32	READ (RX)
Winnt\System32\Inetsrv	READ (RX)
Program Files\Common Files	READ (RX)
(and all subdirectories)	

NOTE: In IIS 3.0, Active Server Pages is an add-on product and is located

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

in its own folder. For this reason, IIS 3.0 installations that are running ASP require READ (RX) permissions set on the Winnt\System32\Inetsrv\Asp folder.

Content is defined as anything (such as Web pages, images, and files) that someone can use the Web browser to access. By default, the content folder for the World Wide Web Publishing Service is \InetPub\Wwwroot, and the content folder for the FTP Service is \InetPub\Ftproot.

IIS requires both appropriate NTFS permissions and the appropriate user rights to access the Web server. The following table lists the authentication type and the corresponding user right that is required to use the specified authentication type:

Authentication Type	Required User Right
-----	-----
Anonymous Synchronization disabled)	Log on locally (Password
Anonymous (Password Synchronization enabled)	Access this computer from the network
Basic (Clear Text)	Log on locally
NT Challenge Response	Access this computer from the network
Digest (IIS 5.0 only)	Access this computer from the network
Integrated (IIS 5.0 only)	Access this computer from the network

For additional information about how to determine which authentication types can be used by which browser and in which environments, click the article number below

to view the article in the Microsoft Knowledge Base:

KBLink:229694.KB.EN-US: How to Use the IIS Security 'What If' Tool

For more information, see the "Security" topic in the Windows NT 4.0 Option Pack documentation. To view this topic, locate Microsoft Internet Information Server, locate Server Administration, and then locate Security. For more information, see the "Security" topic in the Internet Information Services 5.0 documentation. To view this topic, locate Administration, locate Server Administration, and then locate Security.

For additional information about troubleshooting permission issues with IIS, click the article numbers below

to view the articles in the Microsoft Knowledge Base:

KBLink:271071.KB.EN-US: Minimum NTFS Permissions Required for IIS 5.0 to Work

KBLink:313075.KB.EN-US: How to Configure Web Server Permissions for Web Content in IIS

KBLink:120929.KB.EN-US: How the System Account is Used in Windows

KBLink:148437.KB.EN-US: Default NTFS Permissions in Windows NT

KBLink:155253.KB.EN-US: Improper NTFS Permissions May Result in IIS Failure

KBLink:265161.KB.EN-US: FP: Errors Appear When You Attempt to Connect to Database Results Page

For additional information about how to connect to a Microsoft Access .mdb file from Active Server Pages (ASP), click the article number below

to view the article in the Microsoft Knowledge Base:

KBLink:251254.KB.EN-US: PRB: 'Disk or Network Error' or 'Unspecified Error' Returned When Using Jet

QUERY WORDS

=====

```
acl access control list manager domains IUSR_<computername>
IUSR_<machinename> IUSR_<machine_name> IWAM_<computername>
IWAM_<machinename> IWAM_<machine_name> folder folders directories akz
```

=====

--- Very difficult to read.. but better than nothing :)

--

Regards,

Bernard Cheah

<http://support.microsoft.com/>

"Ademar G. Diaz" <ademar@isqsolutions.com> wrote in message

microsoft.public.inetserver.iis.security: Re: Minimum NTFS Permissions – There's such a thing???

news:ef1Y4XlFDHA.2108@TK2MSFTNGP10.phx.gbl...

> The article "Minimum NTFS Permissions Required for IIS 5.0 to Work" seems
> like it is not available anymore.

>

> And i've been unable to find those settings clearly stated by Microsoft
> anywhere, not even in this forum.

> All i have found is references to the aforementioned article.

>

> Would be somebody there so kind as to showme the righth direction.

>

> Thanks in advance.

>

> Ademar Gonzalez

> Programmer

>

>