

Re: Design Guidelines for Non-Power Users?

Source: <http://www.tech-archive.net/Archive/VB/microsoft.public.vb.general.discussion/2004-10/2548.html>

From: Randy Birch (rgb_removethis_at_mvps.org)

Date: 10/19/04

Date: Tue, 19 Oct 2004 19:52:10 -0400

This may help, from the Win 2000 Prof. Res Kit. Hope the formatting doesn't screw up to badly as these are mostly in table format...

Default Settings

The following section describes the default permissions provided to different users.

Default File System and Registry Permissions

Table 13.6 describes the default file system and registry permissions.

Table 13.6 Default Settings for User Write Access Object

Permission

Description

HKEY_Current_User

Full Control

User's portion of the registry.

%UserProfile%

Full Control

User's Profile directory.

All Users\Documents

Read, Create File

Allows Users to create files that can subsequently be read (but not modified) by other Users.

%Windir%\Temp

Synchronize, Traverse, Add File, Add Subdir

Each computer has one temporary directory for use by service–based applications that use this directory to improve performance.

\ (Root Directory)

Not Configured during setup

No permissions are applied to the root level of the directory because the Windows 2000 ACL Inheritance model would cause any root level permissions to affect all child objects, including those outside the scope of setup.

File System Permissions for Power Users and Users

Table 13.7 describes the default access control settings that are applied to file system objects for Power Users and Users during a clean installation of the Windows 2000 operating system onto an NTFS partition. For directories, unless otherwise stated (in parentheses), the permissions apply to the directory, subdirectories, and files.

- a.. %systemdir% refers to %windir%\system32.
- b.. *.* refers to the files (not directories) contained in a directory.
- c.. RX means Read and Execute.

Table 13.7 Default Access Control Settings for File System Objects

File System Object

Default Power User Permissions

c:\boot.ini

RX

None

c:\ntdetect.com

RX

None

c:\ntldr

RX

None

c:\ntbootdd.sys

RX

None

c:\autoexec.bat

Modify

RX

c:\config.sys

Modify

RX

\ProgramFiles

Modify

RX

%windir%

Modify

RX

%windir%*.*

RX

RX

%windir%\config*.*

RX

RX

%windir%\cursors*.*

RX

RX

%windir%\Temp

Modify

Synchronize, Traverse, Add File, Add Subdir

%windir%\repair

Modify

List

%windir%\addins

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\Connection Wizard

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\fonts*.*

RX

RX

%windir%\help*.*

RX

RX

%windir%\inf*.*

RX

RX

%windir%\java

microsoft.public.vb.general.discussion: Re: Design Guidelines for Non–Power Users?

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\media*.*

RX

RX

%windir%\msagent

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\security

RX

RX

%windir%\speech

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\system*.*

Read, Execute

RX

%windir%\twain_32

Modify (Dir\Subdirs) RX (Files)

RX

%windir%\Web

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%

Modify

RX

%systemdir%*.*

RX

RX

%systemdir%\config

List

List

%systemdir%\dhcp

RX

RX

%systemdir%\dllcache

None

None

%systemdir%\drivers

RX

RX

%systemdir%\CatRoot

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%\ias

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%\mui

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%\OS2*.*

RX

RX

%systemdir%\OS2
\DLL*.*

RX

RX

%systemdir%\RAS*.*

RX

RX

%systemdir%\ShellExt

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%\Viewers
.

RX

RX

%systemdir%\wbem

Modify (Dir\Subdirs) RX (Files)

RX

%systemdir%\wbem
\mof

Modify

RX

%UserProfile%

Full Control

Full Control

All Users

Modify

Read

All Users\Documents

Modify

Read, Create File

All Users\Application Data

Modify

Read

Note that a Power User can write new files into the following directories but cannot modify the files that are installed there during text–mode setup. Furthermore, all other Power Users inherit Modify permissions on files created in these directories.

- a.. %windir%
- b.. %windir%\config

- c.. %windir%\cursors
- d.. %windir%\fonts
- e.. %windir%\help
- f.. %windir%\inf
- g.. %windir%\media
- h.. %windir%\system
- i.. %systemdir%
- j.. %systemdir%\OS2
- k.. %systemdir%\OS2\DLL
- l.. %systemdir%\RAS
- m.. %systemdir%\Viewers

For directories designated as [Modify (Dir\Subdirs) RX (Files)], Power Users can write new files; however, other Power Users will only have read access to those files.

Registry Permissions for Power Users and Users

Table 13.8 describes the default access control settings that are applied to registry objects for Power Users and Users during a clean installation of the Windows 2000 operating system. For a given object, permissions apply to that object and all child objects unless the child object is also listed in the table.

Table 13.8 Registry Permissions for Power Users and Users Registry Object

Default Power User Permissions

Default User Permissions

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE \SOFTWARE

Modify

Read

HKLM\SOFTWARE\Classes\helpfile

Read

Read

HKLM\SOFTWARE\Classes\hlp

Read

Read

HKLM\SOFTWARE\Microsoft\Command Processor

Read

Read

HKLM\SOFTWARE\Microsoft\Cryptography

Read

Read

HKLM\SOFTWARE\Microsoft\Driver Signing

Read

Read

HKLM\SOFTWARE\Microsoft\EnterpriseCertificates

Read

Read

HKLM\SOFTWARE\Microsoft\Non–Driver Signing

Read

Read

HKLM\SOFTWARE\Microsoft\NetDDE

None

None

HKLM\SOFTWARE\Microsoft\Ole

Read

Read

HKLM\SOFTWARE\Microsoft\Rpc

microsoft.public.vb.general.discussion: Re: Design Guidelines for Non–Power Users?

Read

Read

HKLM\SOFTWARE\Microsoft\Secure

Read

Read

HKLM\SOFTWARE\Microsoft\SystemCertificates

Read

Read

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion
\RunOnce

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Drivers32

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Font Drivers

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\FontMapper

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\IniFileMapping

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Perflib

Read (via Interactive)

Read (via Interactive)

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\SeCEdit

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Time Zones

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Windows

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Winlogon

microsoft.public.vb.general.discussion: Re: Design Guidelines for Non–Power Users?

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\AsrCommands

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Classes

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Console

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\ProfileList

Read

Read

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Svchost

Read

Read

HKLM\SOFTWARE\Policies

Read

Read

HKLM\SYSTEM

Read

Read

HKLM\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg

None

None

HKLM\SYSTEM\CurrentControlSet\Control\
Session Manager\Executive

Modify

Read

HKLM\SYSTEM\CurrentControlSet\Control\
\TimeZoneInformation

Modify

Read

HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security

None

None

HKLM\HARDWARE

Read (via Everyone)

Read (via Everyone)

HKLM\SAM

Read (via Everyone)

Read (via Everyone)

HKLM\SECURITY

None

None

HKEY_USERS

HKEY_USERS.DEFAULT

Read

Read

HKEY_USERS.DEFAULT\SOFTWARE\
Microsoft\NetDDE

None

None

HKEY_CURRENT_CONFIG

= HKLM\System
\CurrentControlSet
\HardwareProfiles
\Current

HKEY_CURRENT_USER

Full Control

Full Control

HKEY_CLASSES_ROOT

= HKLM
\Software\Classes

= HKLM
 \Software\Classes

--

Randy Birch

MS MVP Visual Basic

<http://vbnet.mvps.org/>

"Randy Birch" <rgb_removethis@mvps.org> wrote in message news:%23dpB5XjtEHA.1464@TK2MSFTNGP15.phx...

: As I recall, user's have read/write access to the folders under their
: profile, as well as to the HKEY_CURRENT_USER registry key. They may also
: have read/write access to other non-system folders on local or shared
: (mapped) drives or network paths as determined by the network admin.

:

: --

:

:

: Randy Birch

: MS MVP Visual Basic

: <http://vbnet.mvps.org/>

:

:

: "George" <nospam@please.com> wrote in message

: news:OcoIRAgteEHA.2876@TK2MSFTNGP14.phx.gbl...

: : Hi,

: :

: : I am building a VB6 application that will need to run with limited (user)
: : privileges. I understand that non-power users only have write access to a
: : few specific directories on the system, as well as very limited registry
: : access.

: :

: : However, I cannot find a definitive guide as to exactly what resources are
: : available to limited users. Do you know of any such listing? What are the
: : guidelines to building VB6 applications that will be run in limited mode?

: :

: : Thank you very much!

: :

: : George

: :

: :

: