E-BOOK SERIES 02
TIPS & TRIK REGISTRY

Kenapa e-Book ini ada?

Untuk menambah pemahaman Anda dalam mempelajari *registry*, maka untuk melanjutkan bab sebelumnya, penulis menyusun tips dan trik ini dengan harapan mampu memberi ide-ide baru dalam pembuatan suatu aplikasi, khususnya dalam pemrograman worm komputer atau pembuatan program *removal*-nya.

Pada kenyataannya banyak sekali kemampuan yang masih tersembunyi pada *registry*, dan perlu kita "gali" sendiri. Berikut ini akan dipaparkan beberapa tips dan trik yang akan membantu menambah pengetahuan Anda tentang *registry*.

2.1 HARDWARE

Sub bab ini akan memuat beberapa tips dan trik yang berhubungan dengan konfigurasi perangkat keras (*hardware*) pada komputer.

2.1.1 MENYEMBUNYIKAN DRIVE

Dengan konfigurasi ini, kita bisa menentukan *drive* apa saja yang bisa terlihat pada aplikasi Windows Explorer, dan *drive* mana yang ingin disembunyikan, caranya adalah sebagai berikut:

1. Buka aplikasi Registry Editor
2. Buka *key* berikut jika sudah tersedia, atau buat apabila belum tersedia

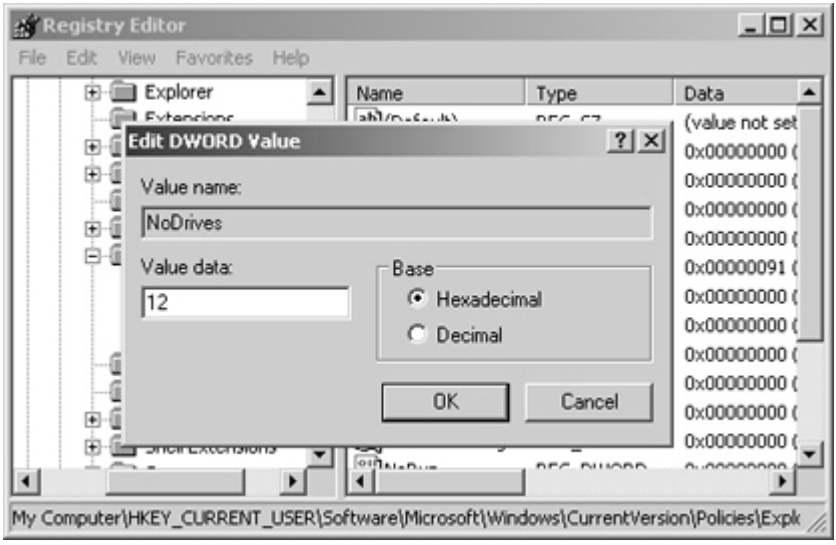
   User Key:
   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

   System Key:
   [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

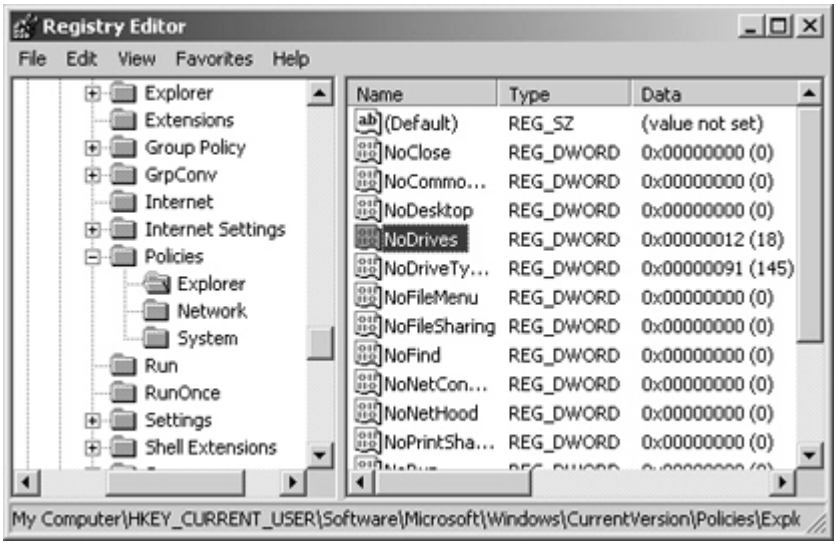
3. Buat sebuah DWORD Value baru, beri nama NoDrives, dan tambahkan data dengan bilangan yang mewakili suatu *drive* berikut ini:

A : 1	J : 512	S : 262144
B : 2	K : 1024	T : 524288
C : 4	L : 2048	U : 1048576
D : 8	M : 4096	V : 2097152
E : 16	N : 8192	W : 4194304
F : 32	O : 16384	X : 8388608
G : 64	P : 32768	Y : 16777216
H : 128	Q : 65536	Z : 33554432
I : 256	R : 131072	Semua : 67108863

Untuk memilih lebih dari satu *drive*, tambahkan bilangan yang mewakili *drive* tersebut, misalnya *drive* yang akan dipilih adalah *drive* C (4) dan D (8) maka bilangan yang digunakan adalah 12.



Gambar berikut menunjukan, proses perubahan telah sukses dilakukan.



2.1.2 FUNGSI AUTORUN

Dengan konfigurasi ini, kita bisa menentukan apakah *system* akan mengeksekusi fungsi *autorun* saat suatu *removable storage* (seperti CD dan *USB Disk*) dihubungkan pada *system*, atau menon-aktifkan fungsi tersebut.

Windows 9X/ME

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	Binary Value
Value	NoDriveTypeAutoRun
Data	0000 95 00 00 00

Windows NT/2000/XP

System Key	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom]
Type	DWORD Value
Value	Autorun
Data	(0=disable, 1=enable)

2.1.3 MANIPULASI ICON DAN LABEL DRIVE

Untuk mengubah *icon* atau nama dari suatu *drive* tertentu dapat menggunakan konfigurasi sebagai berikut:

Manipulasi Icon

System Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons]
Drive Key	Drive letter, contohnya drive yang akan dirubah adalah drive C
Icon Key	DefaultIcon
Contoh Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons\C\DefaultIcon]
Type	String Value
Value	Default
Data	Path atau lokasi Icon, contoh: C:\windows\fileicon.ico

Manipulasi Label

System Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons]
Drive Key	Drive letter, contohnya drive yang akan dirubah adalah drive D
Icon Key	DefaultLabel
Contoh Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons\D\ DefaultLabel]
Type	String Value
Value	Default
Data	Nama label, contoh: PRIVATE DRIVE

2.2 SECURITY

Sub bab ini akan memuat beberapa tips dan trik yang berhubungan dengan konfigurasi pengaman berupa *restriction* (limitasi/ pembatasan) tertentu pada *system* komputer.

2.2.1 ACTIVE DESKTOP

Konfigurasi berikut berguna untuk membatasi *user* melakukan perubahan pada *desktop* aktif.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop]
Type	DWORD Value
Value	NoChangingWallpaper
	NoComponents
	NoAddingComponents
	NoDeletingComponents
	NoEditingComponents
Data	0 = disable restriction 1 = enable restriction

Konfigurasi berikut berguna untuk menyembunyikan opsi Active Desktop yang terdapat pada menu Settings di *Startmenu*.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoSetActiveDesktop
Data	0 = disable restriction 1 = enable restriction

Konfigurasi berikut berguna untuk tetap mengaktifkan fasilitas *Active Desktop* tetapi tidak membenarkan *user* untuk melakukan perubahan secara permanen.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoActiveDesktopChanges
Data	0 = disable restriction 1 = enable restriction

Konfigurasi berikut berguna untuk menon-aktifkan fasilitas Active Desktop.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoActiveDesktop
Data	0 = disable restriction 1 = enable restriction

2.2.2 FUNGSI KLIK KANAN

Konfigurasi berikut berguna untuk menon-aktifkan menu *dropdown* yang biasanya tampil saat *user* melakukan klik kanan pada *desktop* atau pada Windows Explorer.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoViewContextMenu
Data	0 = disable restriction 1 = enable restriction

2.2.3 MENU FOLDER OPTIONS

Konfigurasi berikut berguna untuk menyembunyikan Folder Options dari menu Tools pada Windows Explorer.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoFolderOptions
Data	0 = disable restriction 1 = enable restriction

Konfigurasi berikut berguna untuk menyembunyikan beberapa opsi pada kotak dialog Folder Options.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Advanced\Folder]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Advanced\Folder]
SubKey	Hidden HideFileExt ShowFullPath ShowFullPathAddress SuperHidden

Type	String Value
Value	Type
Data	Data default adalah checkbox dan group, untuk menyembunyikannya cukup menghapus value atau data tersebut, atau lebih cerdik lagi dengan cara menambahkan spasi dibelakang nilai value atau data ☺.

2.2.4 MENYEMBUNYIKAN FUNGSI ENTIRE NETWORK

Konfigurasi berikut berguna untuk menyembunyikan fungsi Entire Network dari Network Neighborhood.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
Type	DWORD Value
Value	NoEntireNetwork
Data	0 = disable restriction 1 = enable restriction

2.2.5 MENYEMBUNYIKAN FUNGSI WORKGROUP

Dengan mengaktifkan konfigurasi berikut, akan menyembunyikan semua *workgroup* dari Network Neighborhood.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
Type	DWORD Value
Value	NoWorkgroupContents
Data	0 = disable restriction 1 = enable restriction

2.2.6 MENON-AKTIFKAN REGISTRY EDITOR

Dengan mengaktifkan konfigurasi berikut, *system* akan menolak untuk menjalankan aplikasi Registry Editor.

User Key	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
Type	DWORD Value

Value	DisableRegistryTools
Data	0 = disable restriction 1 = enable restriction

2.2.7 MENON-AKTIFKAN TASK MANAGER

Konfigurasi ini akan mengatur hak *user* untuk mengakses aplikasi Task Manager pada Windows NT/2000/XP dan melihat proses-proses yang sedang aktif.

User Key	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
Type	DWORD Value
Value	DisableTaskMgr
Data	0 = disable restriction 1 = enable restriction

2.2.8 MENON-AKTIFKAN FUNGSI SHUT DOWN

Dengan mengaktifkan konfigurasi berikut, *system* akan menolak untuk menjalankan fungsi Shut Down.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoClose
Data	0 = disable restriction 1 = enable restriction

2.2.9 MENON-AKTIFKAN HOT-KEYS

Dengan mengaktifkan konfigurasi berikut, *system* akan menolak untuk menjalankan fungsi Hot-Keys pada Windows.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoWinKeys
Data	0 = disable restriction 1 = enable restriction

2.2.10 MENCEGAH USER MENJALANKAN APLIKASI

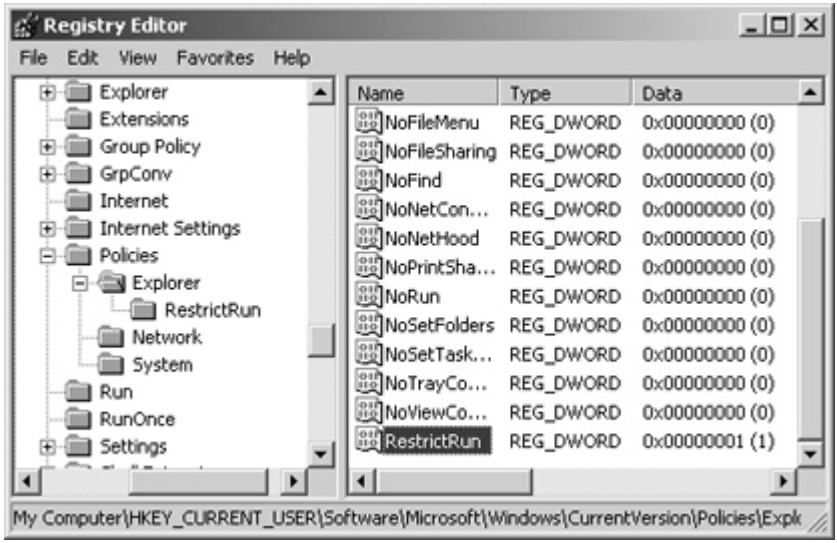
Dengan mengaktifkan konfigurasi berikut, *system* akan menolak jika *user* berusaha untuk mengeksekusi suatu aplikasi tertentu.

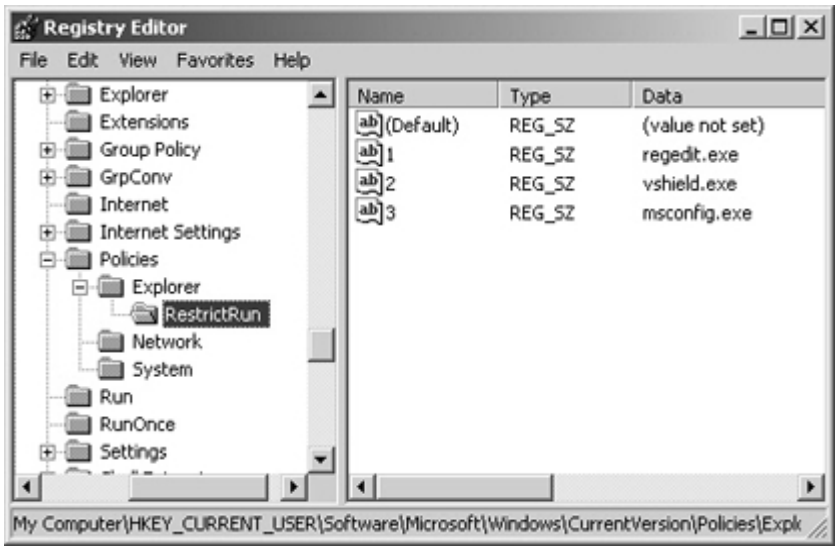
User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	RestrictRun
Data	0 = disable restriction 1 = enable restriction

Kemudian buat sebuah *key* dengan nama yang sama dengan nama *value* tersebut, dan tambahkan data yang diperlukan.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun]
Type	String Value
Value	Beri nama seperti nomor urut, contoh: 1
Data	Nama Aplikasi yang ditentukan, contoh: Regedit.exe

Untuk lebih jelasnya lihat gambar berikut:





Untuk Windows 2000/ME/XP juga bisa menggunakan konfigurasi berikut

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	DisallowRun
Data	0 = disable restriction 1 = enable restriction

Kemudian buat sebuah *key* dengan nama yang sama dengan nama *value* tersebut, dan tambahkan data yang diperlukan.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun]
Type	String Value
Value	Beri nama seperti nomor urut, contoh: 1
Data	Nama Aplikasi yang ditentukan, contoh: msconfig.exe

2.3 WINDOWS

Sub bab ini akan memuat beberapa tips dan trik yang berhubungan dengan *system* Windows.

2.3.1 REGISTERED OWNER AND ORGANIZATION

Saat pertama kali sistem operasi Windows diinstal, *system* akan menanyakan nama pemilik dan organisasi, dan sebagian besar aplikasi yang diinstal kemudian, ternyata memanfaatkan informasi ini. Windows mengijinkan kita untuk mengubah informasi tersebut tanpa harus menginstal ulang sistem operasi, dengan konfigurasi berikut Anda akan mengubah nama pemilik dan nama organisasi tersebut.

Untuk Windows 95, 98 dan ME

System Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]
Type	String Value
Value	RegisteredOwner RegisteredOrganization

Data	Ubah data pada RegisteredOwner dengan nama pemilik dan RegisteredOrganization dengan nama organisasi

Untuk Windows NT, 2000 dan XP

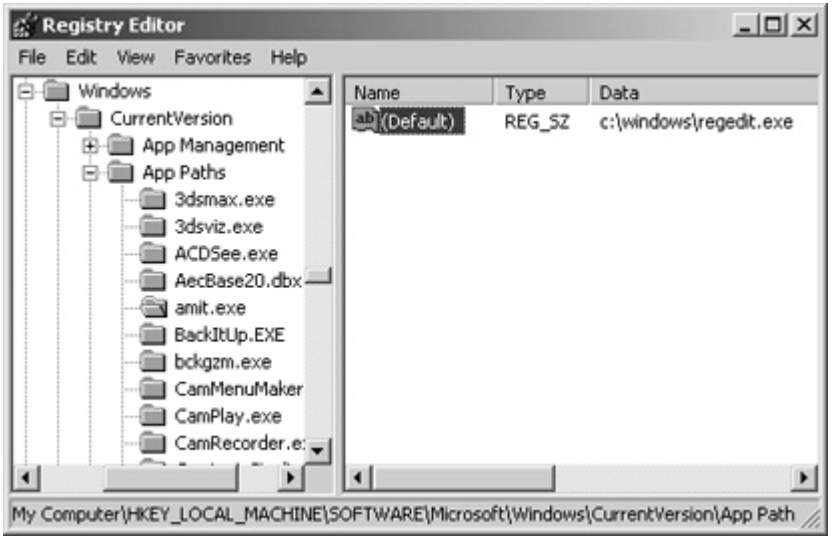
System Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]
Type	String Value
Value	RegisteredOwner RegisteredOrganization
Data	Ubah data pada RegisteredOwner dengan nama pemilik dan RegisteredOrganization dengan nama organisasi

2.3.2 PROGRAM ALIAS

Suatu fasilitas tersembunyi dari sistem operasi Windows, yang mengijinkan *user* untuk membuat suatu program *alias*, misalnya *user* ingin apabila menjalankan suatu perintah dengan nama 'amit.exe' pada menu Run dari *Startmenu* akan otomatis mengeksekusi aplikasi Registry Editor, maka bisa menggunakan konfigurasi sebagai berikut:

System Key	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths]
Alias Key	Buat suatu Key yang mewakili program alias, misalnya program alias bernama 'amit.exe' maka System Key menjadi: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\amit.exe]
Type	String Value
Value	Default
Data	Path atau lokasi file yang akan dieksekusi, contoh: C:\windows\regedit.exe

Untuk lebih jelasnya lihat gambar berikut ini:



2.3.3 MENCEGAH DOS COMMAND PROMPT PADA WINDOWS 95/98/ME

Konfigurasi ini akan mengatur hak *user* untuk mengakses aplikasi *MS-DOS* pada Windows 95/98/ME.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]
Type	DWORD Value
Value	Disabled
Data	0 = disable restriction 1 = enable restriction

2.3.4 MENCEGAH COMMAND PROMPT & FILE BAT PADA WINDOWS 2000/XP

Konfigurasi ini akan mengatur hak *user* untuk mengeksekusi Command Prompt (CMD) dan file *.bat pada Windows 2000 dan XP.

User Key	[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System]
Type	DWORD Value

Value	DisableCMD
Data	0 = enable CMD dan file batch 1 = disable CMD dan file batch 2 = disable CMD, enable file batch

2.3.5 DISABLE MANUAL SCHEDULED TASK PADA WINDOWS 2000/ME/XP

Konfigurasi ini akan mengatur hak *user* untuk secara manual memulai dan mengakhiri Task Scheduler pada Windows 2000, ME dan XP. Tugas akan tetap berjalan sesuai dengan jadwal yang telah ditentukan.

User Key	[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
System Key	[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
Type	DWORD Value
Value	Execution
Data	0 = disable restriction 1 = enable restriction

2.3.6 MENCEGAH PERUBAHAN TASK PROPERTIES PADA WINDOWS 2000/ME/XP

Konfigurasi ini akan mengatur hak *user* untuk melakukan suatu perubahan pada Task Properties yang ada pada Task Scheduler.

User Key	[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
System Key	[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
Type	DWORD Value
Value	Property Pages
Data	0 = disable restriction 1 = enable restriction

2.3.7 MENAMPILKAN DAN MENYEMBUNYIKAN FASILITAS FIND PADA STARTMENU

Konfigurasi berikut akan membuat fasilitas Find pada Startmenu yang berguna untuk melakukan pencarian suatu file

atau direktori, menjadi tampil atau tidak tampil pada menu Startmenu.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoFind
Data	0 = show 1 = hide

2.3.8 MENAMPILKAN DAN MENYEMBUNYIKAN FASILITAS RUN PADA STARTMENU

Konfigurasi berikut akan membuat fasilitas Run pada Startmenu yang berguna untuk mengeksekusi suatu file program secara instan, menjadi tampil atau tidak tampil pada menu Startmenu.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoRun
Data	0 = show 1 = hide

2.3.9 MENAMPILKAN PESAN POPUP SETIAP KALI WINDOWS STARTUP

Konfigurasi berikut akan menampilkan sebuah kotak pesan setiap kali Windows StartUp.

User Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WinLogon]
Type	String Value
Value	LegalNoticeCaption
Data	Isi dengan pesan Anda

2.3.10 MENCEGAH PENAMBAHAN DAN PENGHAPUSAN ITEM PADA TASK SCHEDULER WINDOWS 2000/ME/XP

Konfigurasi ini akan mengatur hak *user* untuk membuat atau menghapus item pada Task Scheduler.

User Key	[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
System Key	[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Task Scheduler5.0]
Type	DWORD Value
Value	Task Creation
	Task Deletion
Data	0 = disable restriction 1 = enable restriction

2.3.11 MENCEGAH WINDOWS INSTALLER

Konfigurasi ini akan mencegah *user* untuk menambah atau menghapus suatu aplikasi yang menggunakan Windows Installer.

System Key	[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer]
Type	DWORD Value
Value	DisableMSI
Data	0 = disable restriction 1 = hak akses untuk admin 2 = enable restriction

2.3.12 MENAMPILKAN DAN MENYEMBUNYIKAN FILE SYSTEM

Konfigurasi berikut akan membuat file *system* yang umumnya beratribut *Hidden* (tersembunyi) bisa terlihat pada Windows Explorer.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Type	DWORD Value
Value	ShowSuperHidden
Data	0 = Tetap sembunyikan file 1 = Tampilkan file tersembunyi

2.3.13 MENAMPILKAN DAN MENYEMBUNYIKAN FILE DAN FOLDER

Konfigurasi berikut akan membuat file dan *folder* yang beratribut *Hidden* bisa terlihat pada Windows Explorer.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Type	DWORD Value
Value	Hidden
Data	0 = Tampilkan file tersembunyi 1 = Tetap sembunyikan file tersembunyi

2.3.14 MENCEGAH KLIK KANAN PADA TASKBAR

Konfigurasi berikut akan menon-aktifkan menu yang biasanya tampil saat *user* melakukan klik kanan pada *taskbar*.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Type	DWORD Value
Value	NoTrayContextMenu
Data	0 = disable restriction 1 = enable restriction

2.3.15 MENGAKHIRI APLIKASI YANG TIDAK MERESPON

Konfigurasi berikut akan mengatur apabila suatu aplikasi menjadi *not responding* (tidak merespon), maka *system* secara otomatis akan menutup aplikasi tersebut.

User Key	[HKEY_CURRENT_USER\Control Panel\Desktop]
System Key	[HKEY_USERS\.DEFAULT\Control panel\Desktop]
Type	String Value
Value	AutoEndTasks
Data	0 = disable 1 = enable

2.3.16 OTOMASI APLIKASI SAAT WINDOWS STARTUP

Konfigurasi berikut akan mengatur untuk mengeksekusi suatu aplikasi pada saat Windows *startup*.

User Key	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
System Key	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

Type	String Value
Value	Beri sembarang nama yang mewakili dari aplikasi tersebut
Data	Path atau lokasi file yang akan dieksekusi, contoh: C:\windows\regedit.exe

Lokasi *key* lainnya yang memungkinkan untuk mengatur otomasi aplikasi saat *system* Windows diaktifkan adalah:

User Key

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]

System Key

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit]