

XP Service Pack 2: threat to civilization or great boon?

Presented by Mark Minasi
A7 level computer expert
help@minasi.com
www.minasi.com
copyright 2004 Mark Minasi

What is it

- Long-overdue SP2 for XP
- SP is mostly “SECURITY pack 2”
- *Lots* of cool new fixes also
- It's almost XP version 1.2
- But it *may* break a few apps, so let's get this over with:

FOR BETTER OR WORSE, MS HAS CHANGED THE DEFAULT SECURITY STANCE OF XP. THAT MEANS THAT SOME APPS WRITTEN BACK BEFORE CODERS CARED ABOUT SECURITY MIGHT NOT WORK ANY MORE.

IF YOU USE CUSTOM APPS OR REALLY OLD APPS THEN DO NOT ROLL OUT SP2 UNTIL YOU HAVE TESTED THEM ALL.

(Yes, I *am* shouting.)

Outline

what we're gonna do

- Where to get SP2
- Security Center
- Data Execution Prevention
- TCP stack changes
- RPC, DTC, COM, WebDAV changes
- Bluetooth
- Wireless
- Outlook Express / Messenger
- Internet Explorer
- Windows Firewall
- USB Storage
- New group policies
- Installing and deploying SP2, future patches and Windows Update
- Miscellaneous new stuff
- Finding out more

Slide 4

Where to get it

- Easiest way is SUS – if you have a SUS server then it's already on there
- You *can* download it, but it's big (266 MB, 332 MB expanded)
- <http://www.microsoft.com/technet/winxpsp2/>
- Includes all patches up to MS04-25 (August security releases)
- MS has released an SP2 disk and encourages people to share it with friends and family

Slide 5

The Security Center

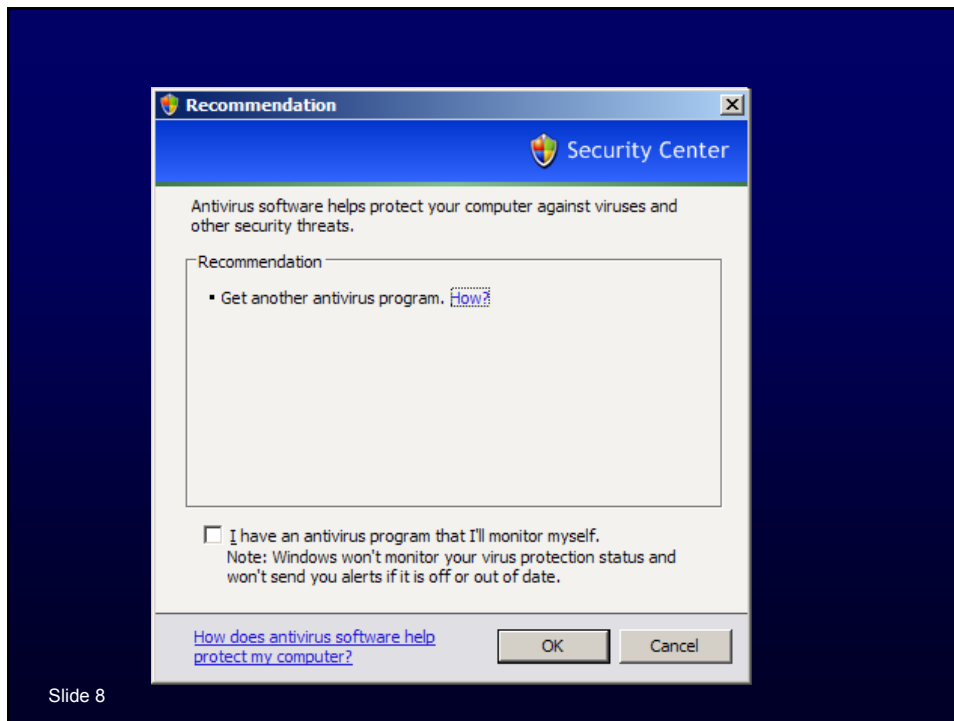
the first thing you (might) see

- The “Security Center”
- Basically it just notes whether you've got Automatic Updates on, an antivirus program installed, and the Windows Firewall on
- Tracks whether you're getting recent virus pattern files
- AV programs must be “Security Center aware”

Slide 6



Slide 7



Slide 8

The Security Center

“Waitaminute...”

- What’s that you say, you didn’t see the Security Center after SP2 installed?
- It’s because you’re a member of a domain
- You can turn it on with a group policy at Computer / Admin Templates / Windows Components / Security Center, “Turn on Security Center (Domain PCs only)
- No GP setting to turn it off for non-domain PCs

Slide 9

Data Execution Prevention

what it is

- The really bad worms crawl in when a programmer creates an area in a program that’s supposed to receive some kind of data, *but* the programmer forgets to check the amount of data
- If an attacker can insert an arbitrary amount of “data” – containing code! – into this buffer then the attacker can do really bad stuff
- DEP tries to make Windows see this and stop it
- How it does it is different on 32 and 64 bit systems
- THIS is the feature that made SP2 so big!

Slide 10

Data Execution Prevention

the 64-bit story

- 64 bitters (K8/Opteron and Itanium) have the ability to mark memory pages as “NX” or non-executable
- When someone does a buffer overflow attack, the pages are modified... but they can't run, so the worm stops!
- MAY involve some custom code changes
- Protects stack, paged pool, session pool

Slide 11

Data Execution Prevention

the 32-bit story

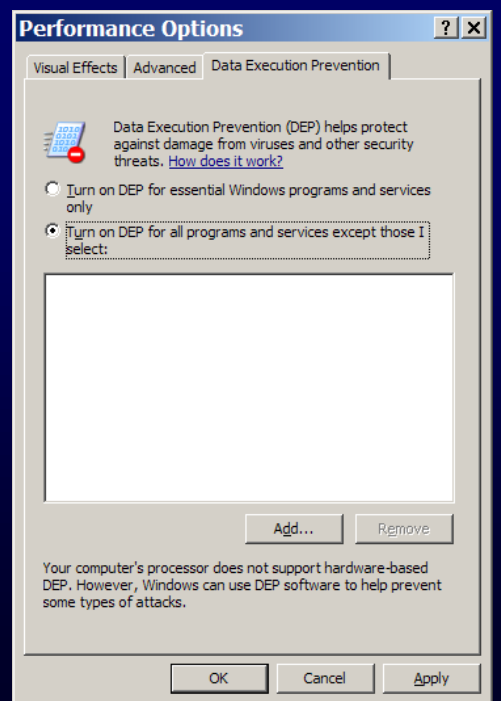
- Standard 32 bit processors lack NX support
- Instead, MS added code to the part of XP that executes code
- Anything trying to run out of the stack wakes up Data Execution Prevention
- Only works on OS apps by default, you can change that

Slide 12

DEP control

- Control Panel
- System
- Advanced
- Performance Options
- Top radio button is the default

Slide 13



TCP/IP Changes

restricting raw sockets

- “Raw sockets” let you hand-craft TCP, UDP and/or IP packets, letting you do things like lie about your address, or creating nonsensical flag combinations
- New restrictions: inbound raw sockets are unchanged, but *outbounds* are rejected if
 - It is TCP data
 - It is UDP data containing a return address that's not on the computer

Slide 14

TCP/IP Changes

restricted outbound connections

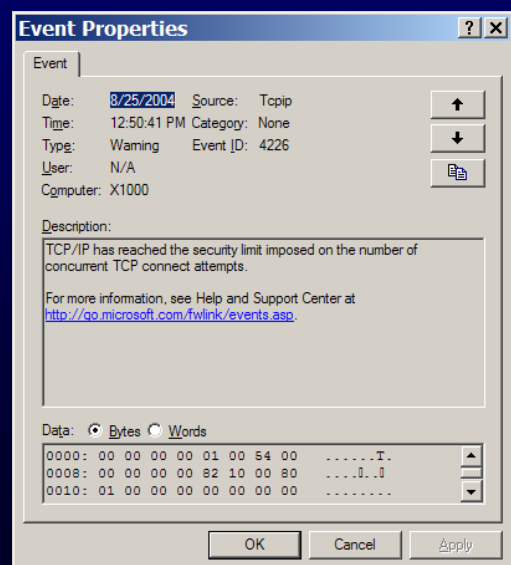
- SP2 refuses to create more than a particular number of incomplete outbound connections
- The reasoning is that the only kind of program that would try to do this is either a worm or a network scanner
- Generates a new event ID, 4226
- MS isn't telling how many, and this may cause security scanners to fail

Slide 15

TCP/IP Changes

4226 Event

- Appears to be 10 connections
- Claims of a "TcpNumConnections" Registry hack are false; this cannot be disabled



Slide 16

RPC Changes

may break an app or two

- Anonymous access to RPC disabled with new GP settings in Computer / Admin Templates / System / Remote Proc Call
 - Restrictions for Unauthenticated RPC clients
 - None = revert
 - Authenticated = default, allow exceptions
 - Authenticated no excepts. = HSP mode, no exceptions
 - RPC Endpoint Mapper Client Authentication
 - Enable (default) or Disable (like old XP)

Slide 17

DTC Changes

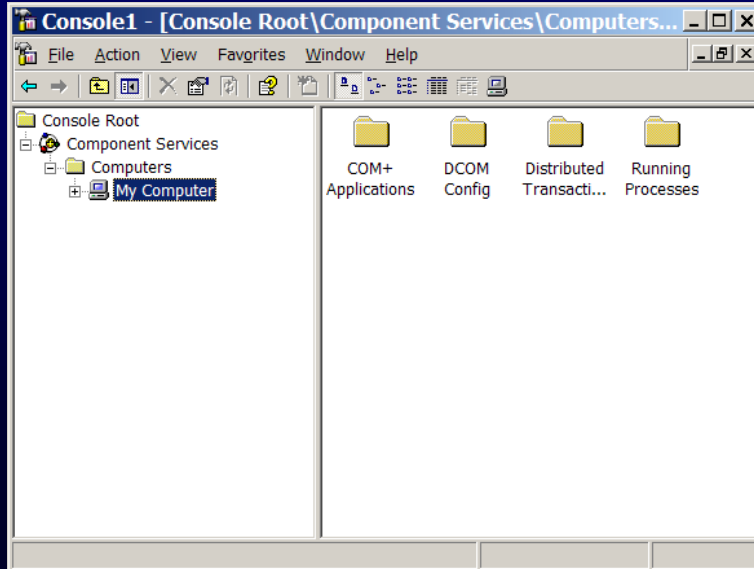
RPC's not the only one

- Distributed Transaction Coordinator blocks network transactions now by default
- SQL Server probably most common user
- To turn them back on, go to the Components snap-in, choose Properties on My Computer
- Click the MSDTC tab
- Click "Security Configuration"
- Enable "Network DTC Access"
- Enable inbound/outbound as appropriate

Slide 18

DTC Changes

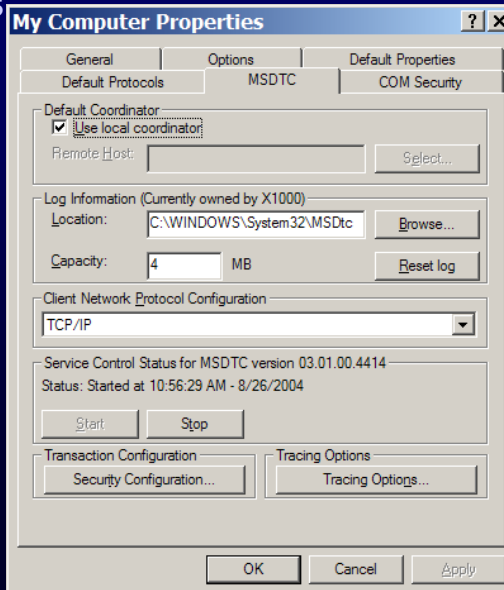
Component snap-in



DTC Changes

My Computer Properties

- Right-click Properties in My Computer, get this dialog
- Click Security Configuration to continue

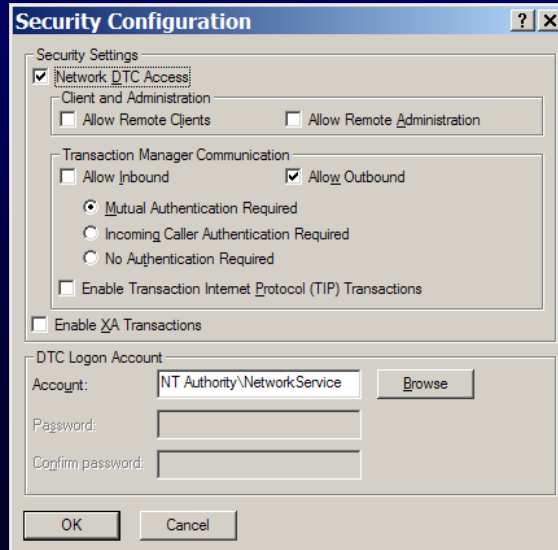


DTC Changes

where to turn on network access if needed

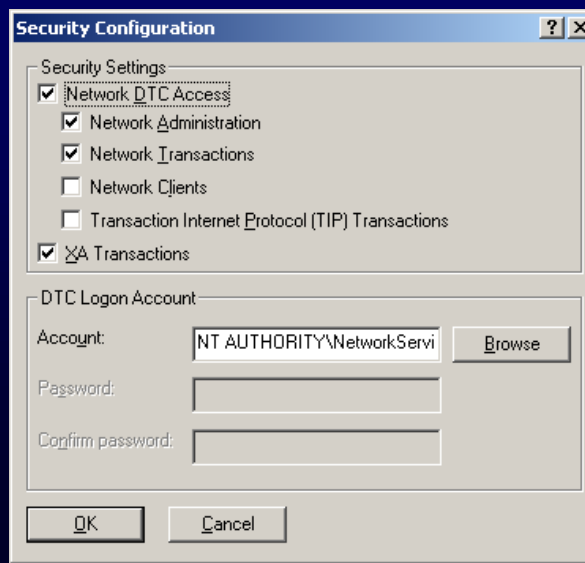
- (Network DTC Access is NOT enabled by default; it's on here just so you can see the options)

Slide 21



DTC Changes

Pre-SP2 dialog for comparison

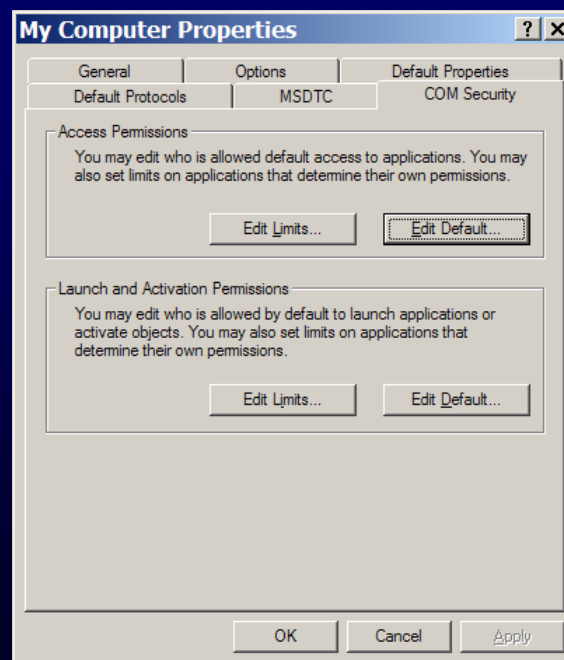


Slide 22

COM Changes

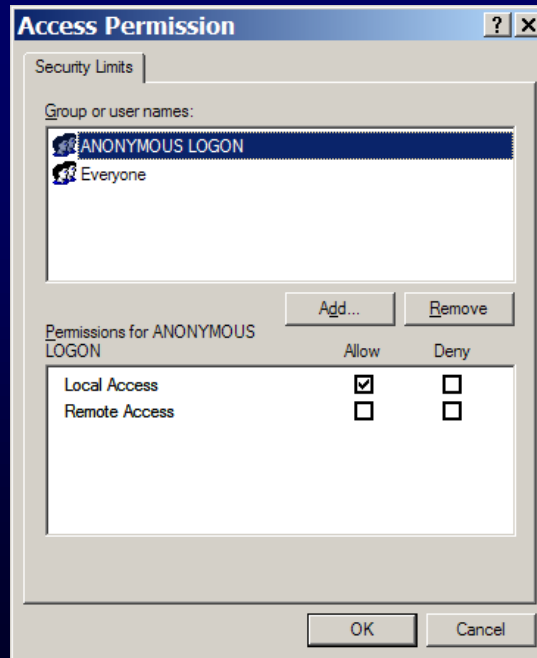
- Same story, although the permissions look a mite different
- Go to Component Services and get Properties on My Computer again, but this time click “COM Security”
- A few dialogs...

Slide 23



Slide 24

- The four dialogs look like this – you now see local versus remote access split up. Do NOT loosen these permissions unless you need to, though!



Slide 25

WebDAV gets pickier

- WebDAV lets you treat Web folders and similar tools (Exchange HTTP, SharePoint, others) as a file sharing system over port 80
- SP2 disallows basic authentication over WebDAV
- HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\WebClient\Parameters\UseBasicAuth (DWORD), set to 1 to revert to pre-SP2

Slide 26

Bluetooth Support

- XP incorporates BT support as vendor code did previously:
 - Personal Area Network (PAN) via My Bluetooth Places, creates IP stacks on BT
 - Bluetooth printer, keyboard, mouse
 - Sync BT PDAs
 - IP connectivity via BT phone or BT access point
- Somewhat better power management with USB BT adapters
- You will *not* get this support if you've got OEM drivers and support progs for your BT installed when you install SP2; you must have an SP2 BT driver

Slide 27

802.1x Changes

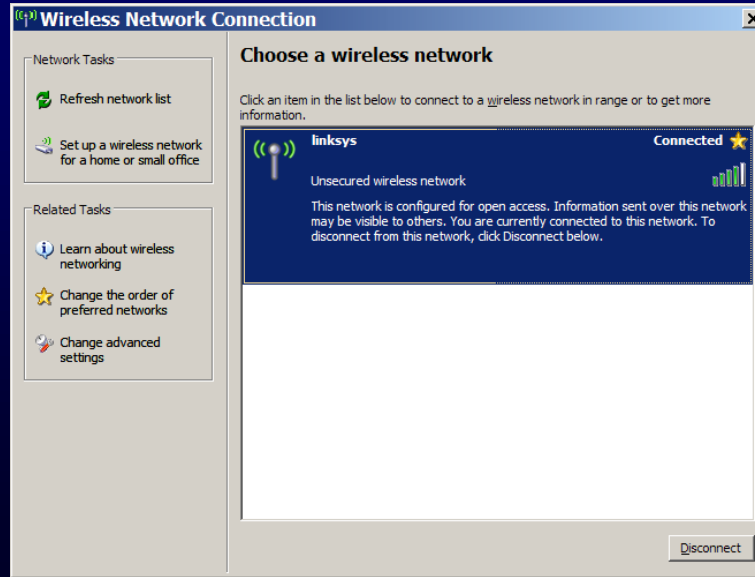
general new stuff



- A new icon in the System Tray!
- Browsing for wireless nets is far easier
- You can choose a “favorite” SSID
- WPA patches now built in, client-side stuff for Wireless Provisioning Services (which won't work until 2003 SP1)
- Wireless Network Setup Wizard is a pretty neat way to easily configure WEP/WPA for clients in a small net

Slide 28

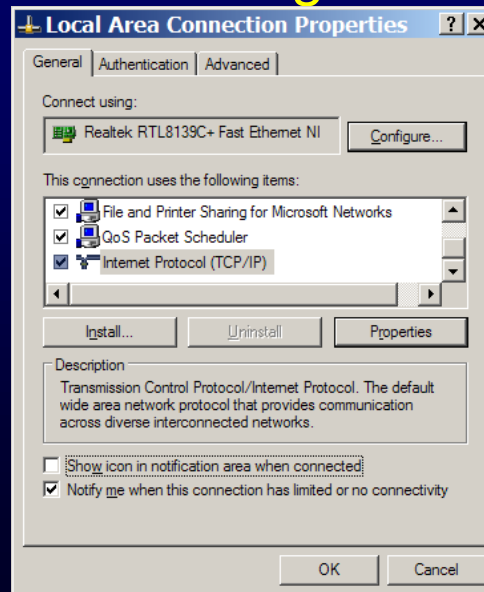
802.1x Changes



Slide 29

New Item in Connection Pages

- “Notify me when this connection...” appears first in SP2
- Unchecking it can make the wireless net cards less irritating



Slide 30

Outlook Express

- A bit more “Listerine” (anti-viral) in this edition
- Blocks bad attachments
- Offers “plain text only” mode which is on by default
- By default does not download external HTML code or images to stop “beaconing”
- Attachments opened by the Attachment Execution Service (AES) (which does not appear to be a service), which unifies the attachment processing code – in any case, it’s clearly smarter than just looking at the extension

Slide 31

Windows Messenger



- Here we’re discussing the IM tool
- File transfers are blocked if
 - The file is of a “dangerous” type (KB 291369),
 - *and* the sender is not on your Contacts list
- Users must specify a display name that is *not* their e-mail addresses
- Don’t forget to open a Messenger port in Windows Firewall, if it’s enabled

Slide 32

Internet Explorer

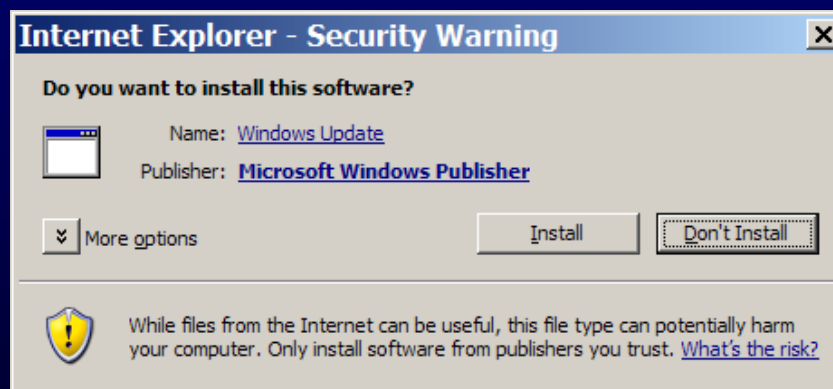
changes overview (there are lots!)

- Popup killer
- Tons of new security stuff and tighter defaults
- Zone lockdown for “local machine” zone
- File and program download prompts are consistent now
- No IE 7.x slated... need SP2 to get these!

Slide 33

Internet Explorer

new uniform “may I install/run?” dialog



Slide 34

Internet Explorer

dialog expanded with publisher blocking feature!



Slide 35

Internet Explorer

new IE security features

- Add-on control
- Binary behaviors
- Local zone lockdown
- IE object caching
- Mime sniffing
- Scripted window restrictions
- These can all be disabled with GPs if necessary

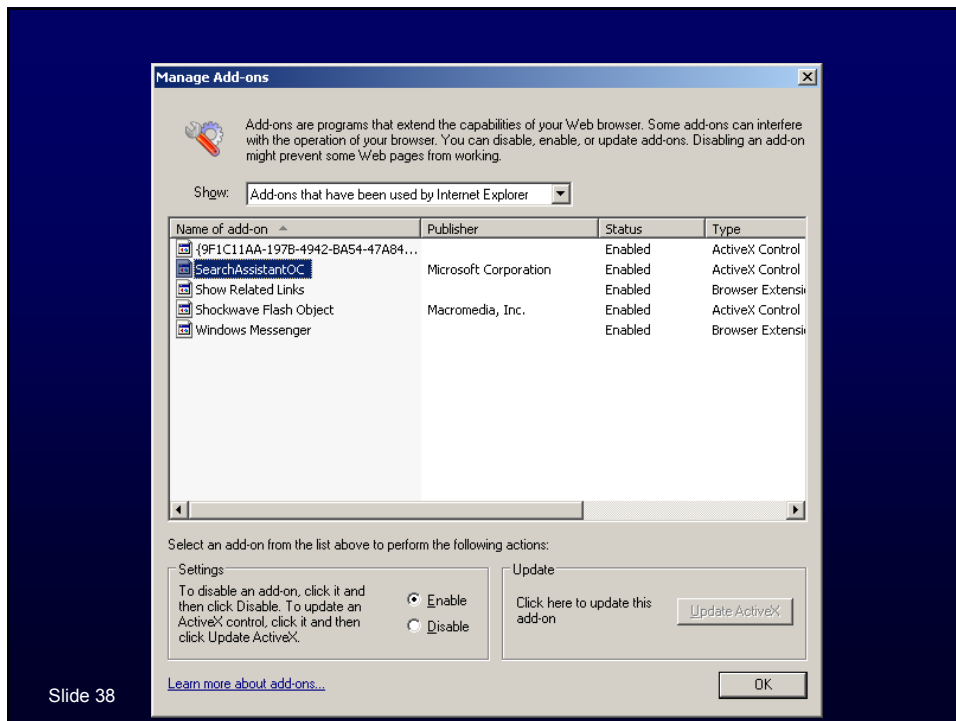
Slide 36

Internet Explorer

add-on controls

- New dialog lets you see ActiveX controls and browser helpers (“add-ons”)
- When a crash occurs, IE points to the add-on that it thinks caused it
- Shows either the currently loaded add-ons or all of the ones on the computer
- Lets you disable suspicious add-ons
- IE will not load signed objects with invalid signatures

Slide 37



Slide 38

Internet Explorer

Group Policy Control of Add-Ons

- Computer / Admin Templates / Windows Components / Internet Explorer / Security Features / Add-on Management
- “Add-on List” lets you either block or allow particular add-ons
- “Deny all add-ons unless specifically allowed in the Add-on List” makes the Add-on List an “only allowed add-ons” list

Slide 39

Internet Explorer

Binary Behaviors and Local Zone

- “Binary behaviors” is a class of script-like things that were being used maliciously
- GPOs now let you block them on particular sites
- IE used to assume that files on the local hard disk were safe and put them in “local zone”
- Now the Information Bar shows you what a local file wants to do and gets your okay

Slide 40

Internet Explorer

IE Object Caching

- Previously, one Web page could cache an object and a different Web page could access that object
- Led to some sneaky two-part attacks
- Won't work under SP2's IE

Slide 41

Internet Explorer

Mime Sniffing

- Related to Attachment Execution Service
- Doesn't necessarily believe and file's extension
- Looks in the file to see if it could be what it says it is
- Blocks the file and warns you if it seems uncertain

Slide 42

Internet Explorer

Scripted Windows Security Restriction

- Another set of security improvements
- Keep pop-up windows from
 - Positioning status bar, title bar, address bar off-screen
 - Moving themselves entirely off-screen
 - Removing the status bar, title bar, address bar to become “chromeless” windows
 - Completely covering their parent window – popups must live inside the parent’s chrome

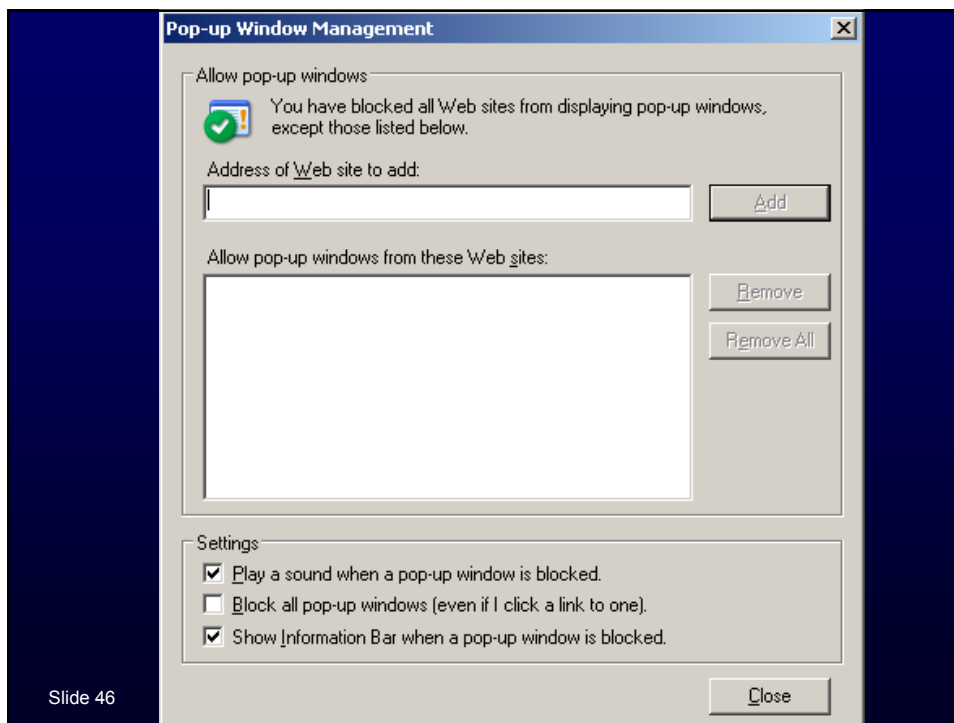
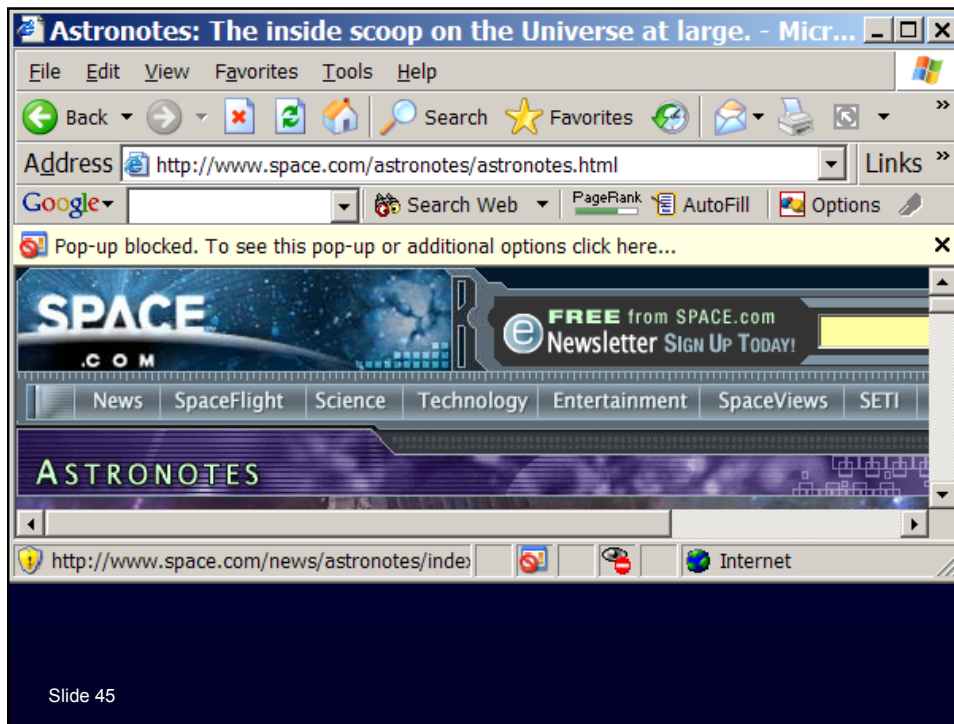
Slide 43

Internet Explorer

Pop-up Blocker

- Quite nice and much-needed
- Includes the “information bar” which lets you bring back a blocked pop-up
- Information bar also serves as the prompt for installing ActiveX controls
- Can create a “white list” of sites to allow pop-ups in
- Doesn’t block many scripted pop-ups unfortunately

Slide 44



Internet Explorer

group policies

- In SP1, IE had 9 GP settings in the Computer Configuration node
- SP2 has over 600
 - Hide items in IE
 - Pop-up control
 - Turn on/off window restrictions, mime sniffing, binary behavior, etc
 - Control security settings for each Internet zone
- Looking at your IE options will keep you pretty busy as you roll out SP2!

Slide 47

Windows Firewall

XP and 2003's Windows Firewall

- Pre-SP2 systems call it "Internet Connection Firewall; now renamed "Windows Firewall"
- Main items:
 - Now starts up *before* the TCP/IP stack
 - On by default when SP2 deployed
 - Configurable from GUI, CLI, GPO
 - No effect on being a domain member
 - Will break most remote admin tools
 - Separate inside/outside domain rules possible

Slide 48

Windows Firewall

the basics

- If you already have a personal firewall then you probably don't need this
- Only blocks incoming, uses stateful packet inspection – in other words, it only allows packets in that are responses to requests
- Permits you to open particular incoming ports
- Has been off by default... but XP SP2 enables it

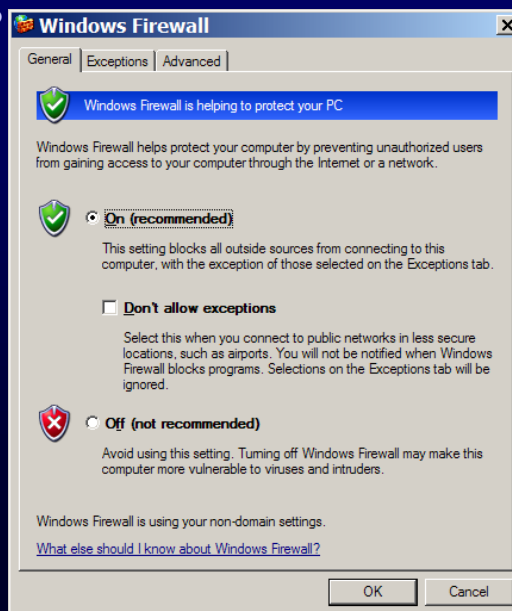
Slide 49

Windows Firewall

how do I know if it's on?

- From the GUI:
 - Control Panel / Network Connections
 - Right-click any adapter, choose Properties, then Advanced, then "Settings" under Windows Firewall

Slide 50



Windows Firewall

how do I know if it's on?

- From a command line: **netsh firewall show state**
- Add **enable** for verbose output

```
C:\>netsh firewall show state
```

```
Firewall status:
```

```
-----  
Profile                = Standard  
Operational mode      = Enable  
Exception mode        = Enable
```

Slide 51

Windows Firewall

how do I turn it on?

- From the GUI, or from the command line with **netsh firewall set opmode enabled** or **netsh firewall set opmode disabled**
- From GPs at Computer Configuration / Admin Templates / Network / Network Connections / Windows Firewall / profilename, "Windows Firewall: Protect all network connections"

Slide 52

Windows Firewall

how can I turn it on?

- One more way: netfw.inf
- Appears on an SP2 CD, a new install CD, or (once installed) in \Windows\INF
- You can change it and type **netsh firewall reset** to see the changes take effect
- See “Using the Windows Firewall INF File in Microsoft Windows XP Service Pack ” for more info

Slide 53

Windows Firewall

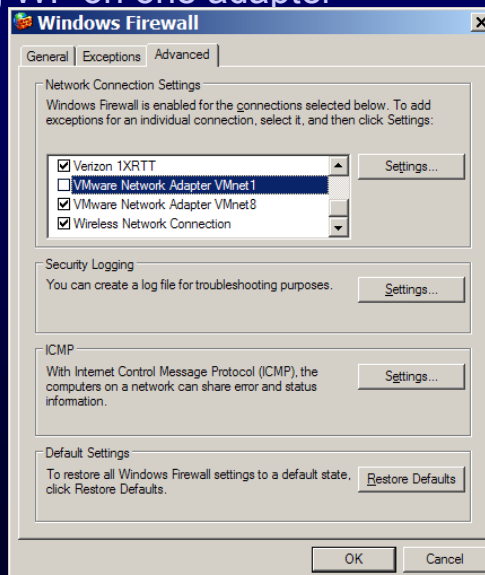
global settings – set one, you set ‘em all

- Turning on the firewall on one NIC turns it on (or off) for all NICs
- This can be annoying (e.g. with VMWare’s virtual network adapters)
- Answer: in the firewall dialog, go to Advanced and un-check boxes for whatever NICs you want to disable separately
- I don’t know of a GPO or CLI way

Slide 54

Windows Firewall

Disabling WF on one adapter



Slide 55

Windows Firewall

making WF behave differently inside and outside the office

- Wouldn't it be great if you could turn the firewall *off* when inside your intranet, but *on* when traveling?
- Answer: two "WF profiles," "domain" and "standard"
- Domain applies when your system is logged onto a domain, standard otherwise

Slide 56

Windows Firewall

how does it know which profile to use?

- Your computer remembers the DNS suffix of the NIC from which it got its last group policy info
- It looks at every active NIC's NIC-specific DNS suffix (except SLIP/PPP connections)
- If *any* match the DNS suffix from that last-GPO-receiving NIC, then you're in Domain mode; otherwise, it's Standard

Slide 57

Windows Firewall

using profiles from the command line

- To turn it on inside the firewall but off outside:
netsh firewall set opmode mode=disable profile=domain
netsh firewall set opmode enable profile=standard
- To find out what mode WF thinks it's in:
netsh firewall show state

Slide 58

Windows Firewall

do I want it on or off?

- To understand that, let's talk about how it works
- Remember, it doesn't block outgoing stuff and allows incoming stuff *as long as it's a response to something that you asked for*
- As your workstation initiates logons, no problem. Ditto for group policies, roaming profiles, etc – it's all client-initiated

Slide 59

Windows Firewall

do I want it on or off?

- If connected directly to the Internet: yes, you want it on
- If in a domain as a domain client...
 - As a client, no bad effects
 - But as a server?

Slide 60

Windows Firewall

think your XP box isn't a server? Do you...

- Want to ping it
- Control a remote PC with Manage Computer
- NET USE to C\$ or any other NET USEs
- Share your printer
- Run any "remote-able" command like systeminfo.exe or exec.vbs
- Control it with Remote Desktop or Remote Assistance or VNC or SMS etc
- Run Web, mail, news etc server software

Slide 61

Windows Firewall

MMCs that won't work w/o port 445 opened

- Certificates
- Computer Mgmt
- Device Manager
- Disk Management
- Event Viewer
- Group Policy
- RSOP
- Indexing Service
- IP Security Monitor
- IPsec policy
- Local users & groups
- Removable Storage
- Services
- Shared Folders
- WMI Control
- File sharing

Note that if you open 445, then ping echoes are enabled automatically

Slide 62

Windows Firewall

solving the remote admin problem

- Skip *all* remote control
- Turn off the firewall for domain members
 - This presents problems for mobile PCs (when to turn it back on?) and when new worms get in
- Open the ports that you'll need for remote control
 - But understand that future worms may crawl in this way
 - And it's not always clear what port #s to open

Slide 63

Windows Firewall

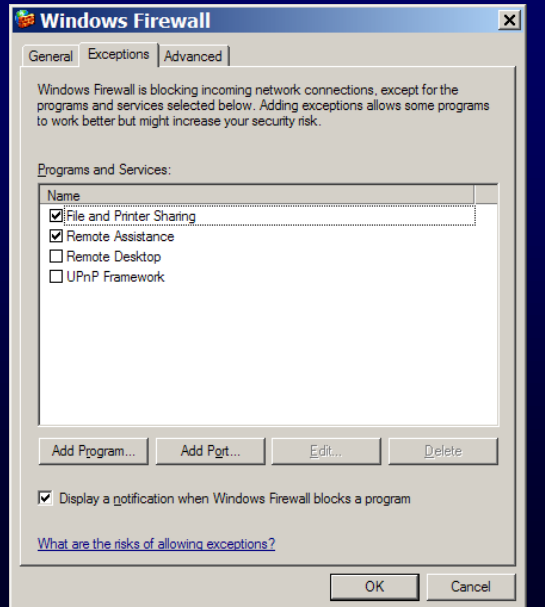
how to open ports

- Opened ports are called “exceptions”
- Create them:
 - From the GUI “Exceptions” tab
 - From the command line
 - From a group policy setting
 - Allow a particular program to open whatever ports it wants

Slide 64

Windows Firewall

Exceptions GUI-style



Slide 65

Windows Firewall

more detail on exceptions and profiles under CLI

- Controlling on/off, exceptions and profiles:
 - On/off: set opmode enable/disable – **netsh firewall set opmode enable**
 - Options: exceptions=enable/disable, profile=domain/standard; to use them either put them in order, or use mode=, exceptions=, profile=; examples:
 - **netsh firewall set opmode enable enable standard**
OR...
 - **netsh firewall set opmode mode=enable exceptions=enable profile=standard**

Slide 66

Windows Firewall

creating exceptions with the CLI

- **netsh firewall set icmpsetting type 8** enables all ICMP echoes
- **netsh firewall add portopening tcp 1433 sql enable subnet** opens 1433 just to the local subnet
- **netsh firewall add portopening tcp 1433 sql enable custom 4.0.0.0/24,10.0.0.0/255.255.0.0,subnet** opens 1433 just to the C net starting at 4.0.0.0, the B net starting at 10.0.0.0 and the local subnet

Slide 67

Windows Firewall

controlling with group policies

- All in Computer / Admin Templates / Network / Network Connections / Windows Firewall
- “Protect all network connections:” turns firewall on/off for all network connections
- “Do not allow exceptions:” close all ports
- “Define program exceptions:” specify programs which can open ports
- “Allow local program exceptions:” let local admin *add* program exceptions or not (can by default)

Slide 68

Windows Firewall

controlling with group policies

- “Allow Remote Administration Exception:” open 135 and 445, enable ping echo, enables most remote admin tools – most RPC, DCOM, WMI stuff works with this
- This is a bit scary, but consider that you can be very specific about whom to accept traffic from
- “Allow File/Print:” open UDP 137&138, TCP 139&445, allow ping echoes

Slide 69

Windows Firewall

controlling with group policies

- “Allow ICMP Exceptions:” specify what you can do with ping and other ICMP tools. Note you cannot limit this to a set of addresses
- “Allow Remote Desktop Exception:” open 3389, Remote Assistance works also
- Allow UPnP Exceptions: don’t use
- Prohibit Notifications: when you allow a program to open ports, it notifies you unless you use this policy setting

Slide 70

Windows Firewall

controlling with group policies

- “Allow Logging:” turns on an ASCII log
- “Prohibit Unicast Response...” your system does a multicast or broadcast, and another system produces a unicast response – does Firewall drop it? By default it will permit the response, as long as it occurs within 3 seconds of the broadcast. Recommend you leave it alone, as it keeps NetBIOS name conflict detection from working

Slide 71

Windows Firewall

controlling with group policies

- “Define Port Exceptions:” custom setting for rolling your own port opening
- “Allow Local Port Exceptions” lets a local admin open extra ports; they can’t by default

Slide 72

Windows Firewall

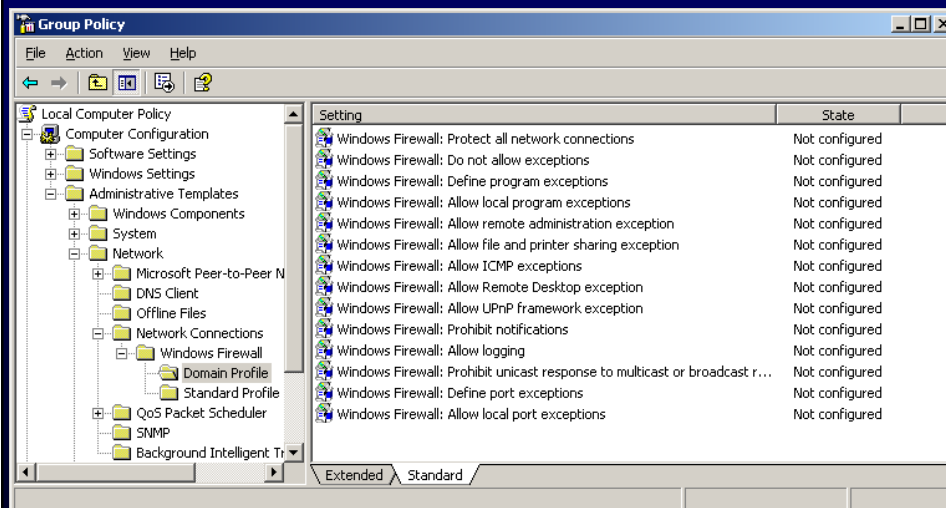
a note on using GPs

- As these new GP settings don't exist in earlier OSes, you've got to be careful how you create them
- Create and modify any WF-related GPOs from an XP workstation with SP2 on it
- Or look at KB 842933 for a patch for 2K, 2003

Slide 73

Windows Firewall

gpo settings



Slide 74

Making USB drives read-only

- You can cause an SP2 system to refuse to write to any USB drive (external drive, memory stick, thumb drive, etc)
- Good in places where you use USB storage devices but do not want people to transfer stuff from their computer to a USB device
- HKLM\System\CurrentControlSet\Control\\StorageDevicePolicies, Reg_DWORD WriteProtect = 1 to enable, =0 to disable
- Note you must create the entry *and* the key!
- No reboot necessary, read when you attach to USB

Slide 75

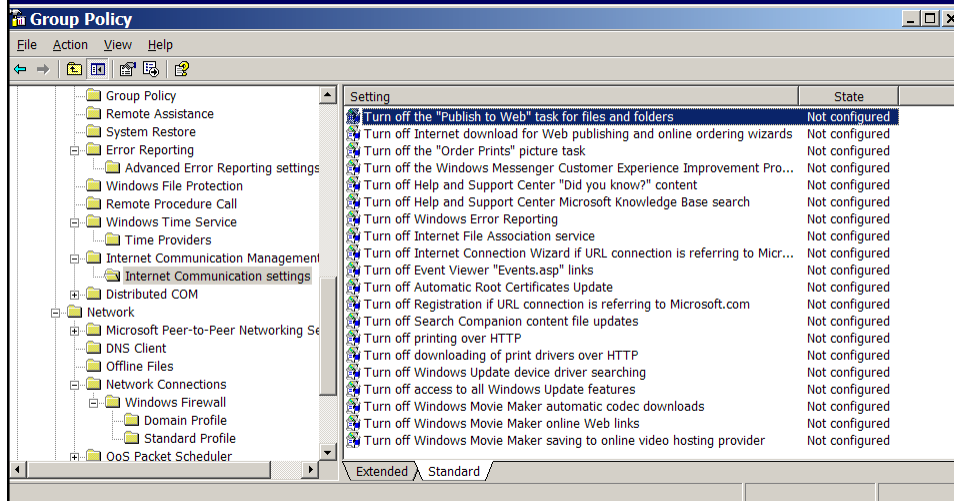
Group Policies

- MS claims 609 new policies, seems like more
- Most are modifications of existing ones or new IE settings (619 IE settings!)
- Full list at www.microsoft.com/downloads, search for "policyssettings.xls"
- Also ... big bonus ... the spreadsheet links each policy to its Registry entry!

Slide 76

Internet Comm. Settings

greatly reducing the unauthorized Net browsing



Slide 77

They Seem To Mean it...

"New Hardware" asks before it phones home



Slide 78

Installing SP2

notes

- Again, *please* test apps before a big rollout
- Remove bluetooth drivers and OEM support programs to get SP2's bluetooth tools
- Laptops must be on AC or SP2 won't load

Slide 79

Installing SP2

rollout options

- SUS or SMS are probably the best way to do it
- But you can also slipstream, as before
- Or roll out with a software installation group policy to `\\i386\update\update.msi`
- Or do unattended from the command line
- Defaults to creating backup files and waiting for you to tell it to reboot

Slide 80

Installing SP2

new command-line switches for the package

- /quiet (doesn't ask any questions, no display)
- /passive (unattended with a progress bar)
- /n (do not create backup for uninstall)
- /o (overwrite newer OEM files w/o prompt)
- /f (force apps closed when rebooting)
- /forcerestart and /norestart control reboot
- /uninstall (starts uninstalling)
- -x (extract files to a directory)
- /l (list installed updates/hotfixes)
- /integrate:*fullpath* slipstreams
- /d:*path* place to put back up files

Slide 81

Installing SP2

the new way to install patches

- New update.exe and Installer 3.0 lets you install patches out of order without problems
- If you install a patch that's older than SP2 (or whatever SP you have) then it's ignored; otherwise it's installed
- In theory *every* patch supports the same command-line options as SP2!
- That means you can now slipstream (now "integrate") patches

Slide 82

Troubleshooting SP Installs

- Once in a while, an updated driver will cause an OS to bluescreen
- Answer #1: it's always a good idea to refresh your drivers *before* installing an SP, and reboot *before* installing an SP
- Answer #2: if you retained uninstall information for your SP (or any other), then just run the "uninstall the SP" batch file

Slide 83

Where's That?

- In the Windows\%NTServicePackUninstall%\spuninst directory, which is hidden and read-only
- File's name is spuninst.txt, rename to .bat
- Run the batch file
- This will run fine from Recovery Console

Slide 84

Windows Update Client

improvements you can use now

- Can designate how often to look for patches
- Doesn't treat Admin users differently any more
- Patches that don't require a reboot can be applied immediately, optionally
- Client prioritizes downloads
- Client now scriptable
- BITS now includes more bandwidth throttling, is more efficient on restart

Slide 85

Windows Update Client

benefits that need WUS

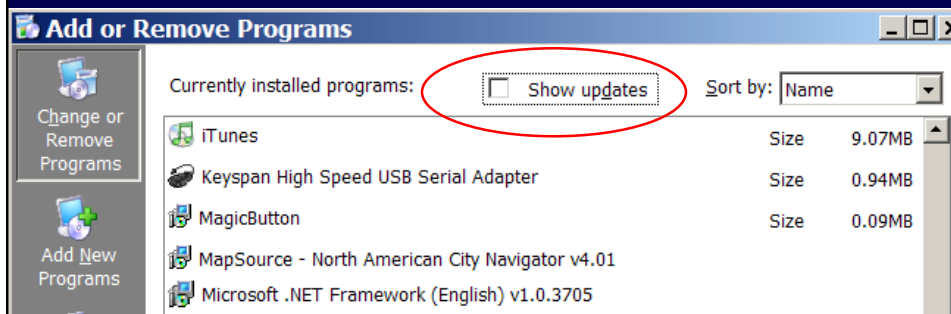
- Can designate groups that only get a subset of patches
- Includes support for patches for Office, SQL, Exchange, ISA etc (once MUS/WUS appear)
- You can filter critical/non-critical

Slide 86

Simplifying Add/Remove Programs

removing the patch clutter

- Now that patches appear in Add/Remove Programs, it can be cluttered; a new check box filters them out by default:



Slide 87

Miscellaneous

- Messenger and Alerter services are off
- If you uninstall SP2 then you lose your Media Player licenses
- DirectX 9.0 installed
- Installer includes a patch compress option
- At.exe can no longer schedule remote computers unless at.exe runs on an SP2 box
- Tablet PC non-security-related enhancements

Slide 88

Get ALL The Details

- Eight Word documents at <http://go.microsoft.com/fwlink/?LinkId=28022>
- Complete details, more Registry keys, etc
- The group policy spreadsheet is at <http://go.microsoft.com/fwlink/?LinkId=28031>

Slide 89

Thanks!

- I hope this was useful and not Too Much Information, thanks for spending some time with me!
- You can find my newsletters and seminar information at www.minasi.com; there is a free support forum there as well
- And remember, you'll like this presentation even better when Mark delivers it at your site; contact us at assistant@minasi.com to inquire

Slide 90