

FDCC Technical Discussion

Kurt Dillard
kurtdillard@msn.com
fdcc@nist.gov

What Changed in June?

- ▶ Major Release 1.0:
 - 40 settings added, removed, or changed
- ▶ Java Permissions for Intranet and Trusted Sites Zones
 - Disabled → High Safety
- ▶ Screensaver Grace Period
 - 0 seconds → 5 seconds

What Else Changed...

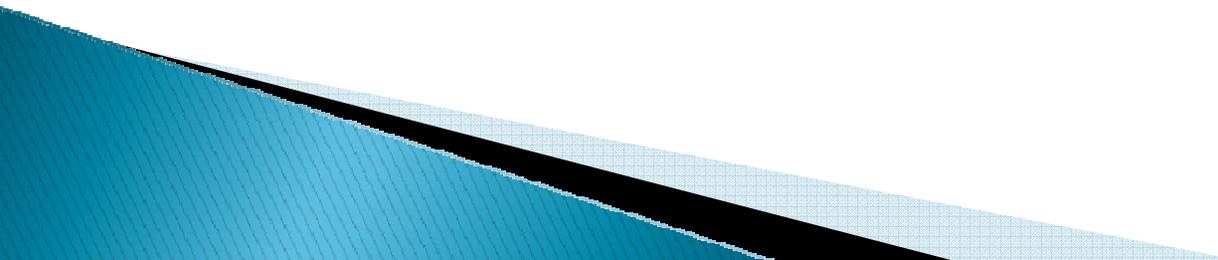
- ▶ Task Scheduler service in XP
 - Disabled → Not Configured
- ▶ Devices: Allowed to format and eject removable media
 - Administrators → Interactive Users

What Didn't Change (and Might)

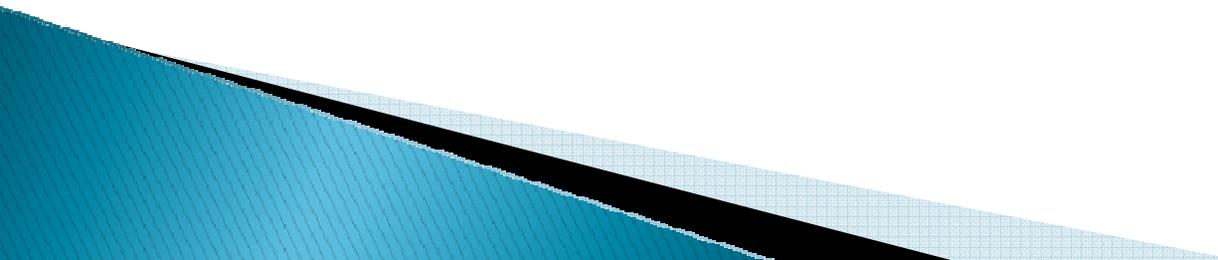
- ▶ Retain application log
- ▶ Retain security log
- ▶ Retain system log

- ▶ All set to “Enabled”

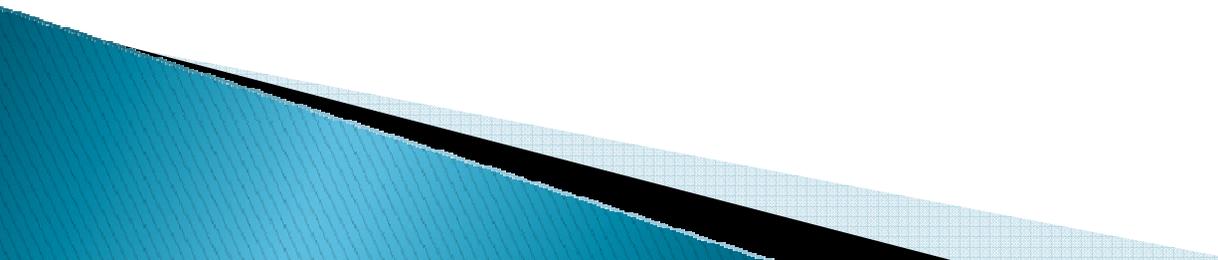
What Didn't Change (and Probably Won't)

- ▶ System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
 - ▶ NetBIOS and Secure Channel settings
 - Domain Member: Digitally encrypt or sign secure channel data
 - Network Access: Require strong (Windows 2000 or later) session key
 - Microsoft network client: Digitally sign communications (always)
- 

What Didn't Change Continued...

- ▶ Access this computer from the network
 - ▶ Apply local firewall rules set to 'No'
 - Domain, private, and public profiles
 - ▶ BITS service set to manual
 - ▶ Network access: Do not allow storage of credentials or .NET Passports for network authentication
 - ▶ Permissions on NET.EXE
- 

How Should Agencies Proceed?

- ▶ Test
 - ▶ Deploy
 - ▶ Report
 - ▶ Get Informed
- 

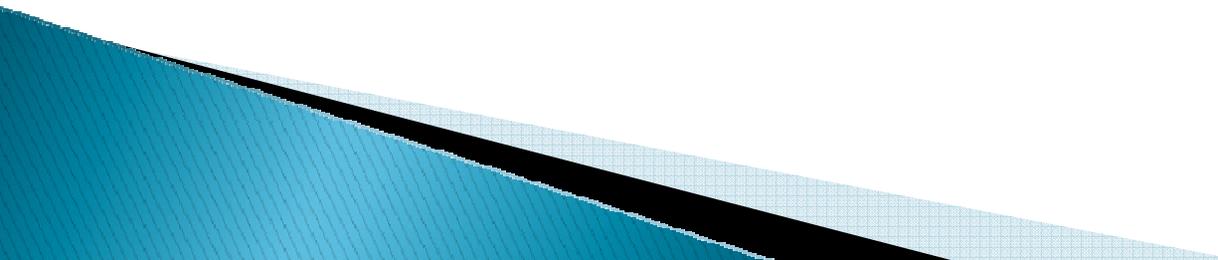
Test

- ▶ Use Active Directory group policies
- ▶ Use Aaron Margosis' tool to configure the local GPO
 - <http://blogs.technet.com/fdcc/archive/2007/12/24/set-fdcc-lgpo-utility-to-apply-fdcc-settings-to-local-group-policy.aspx>
- ▶ Deploy onto physical or virtual machines
- ▶ Download issues:
 - We can send a DVD or you can download evaluation VMs from Microsoft and configure yourself

Deploy

- ▶ Active Directory, local GPO, scripts, whatever you prefer
- ▶ Viewing or editing IE 7 and Vista GPOs on 2003 & XP
 - <http://blogs.technet.com/fdcc/archive/2008/01/29/why-don-t-all-of-the-fdcc-settings-appear-in-the-group-policy-editor.aspx>
- ▶ Administering Group Policy
 - <http://go.microsoft.com/fwlink/?LinkId=14320>.
- ▶ Enterprise Management with GPMC
 - <http://www.microsoft.com/windowsserver2003/gpmc/default.aspx>.
- ▶ Migrating GPOs Across Domains with GPMC
 - <http://www.microsoft.com/windowsserver2003/gpmc/migrpo.aspx>

Report

- ▶ Refer to OMB directives
 - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf>
 - ▶ FISMA reporting is straightforward (wrt FDCC)
 - ▶ Will additional SCAP reporting be required?
- 

Other Resources

- ▶ Policy:
 - fisma@omb.eop.gov
- ▶ Technical
 - fdcc@nist.gov
 - <http://blogs.technet.com/fdcc>
- ▶ Great guidance available from NIST & Microsoft on the security settings:
 - NIST SP 800-68
http://csrc.nist.gov/itsec/guidance_WinXP.html
 - Windows XP:
<http://go.microsoft.com/fwlink/?LinkId=14839>
 - Windows Vista:
<http://www.microsoft.com/technet/windowsvista/security/guide.aspx>

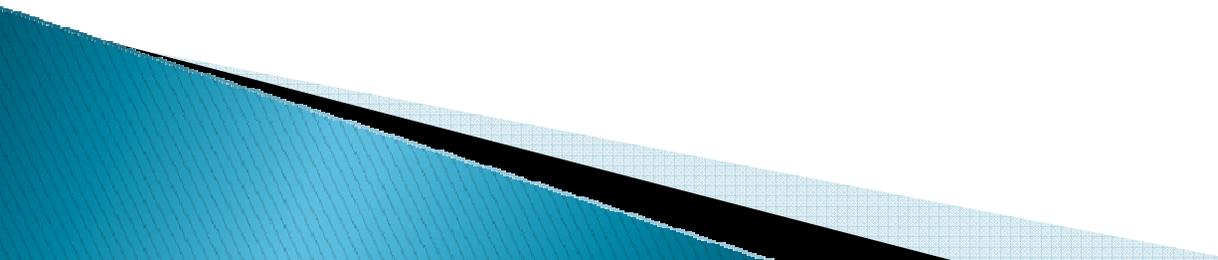
How Do Vendors Get Started?

- ▶ How do I test? How do I start?
 - <http://fdcc.nist.gov>
 - Download the settings etc:
http://nvd.nist.gov/fdcc/download_fdcc.cfm.
- ▶ Take a look at the suggested acquisition language in these OMB memos:
 - <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf>
 - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf>

Vendors Continued...

- ▶ What is required?
 - Runs on XP SP2 & Vista SP1 with latest patches
 - Does not change FDCC settings
 - Does not require admin (except IT tools)
 - Works correctly
- ▶ How do we get certified?
 - Test with SCAP scanners

Favorite Questions

- ▶ Do we really have to FDCC *all* of them?
 - ▶ Do we need to use IE7?
 - ▶ Not configured vs Not defined
 - ▶ Reactivation: slmgr.vbs -rearm
 - ▶ Why do you want me to cry?
- 

Other Frequent Questions

- ▶ Changing settings:
 - Its ok to go more secure
 - Its ok to change those that are not specified
 - Its ok to change warning banner & text
 - Its ok to ignore settings for the browser or firewall if using another vendor's
- ▶ Spreadsheet takes precedence when contradictions in GPOs, SCAP data, or VHDs.
- ▶ What if a vendor isn't compliant and won't get compliant, talk to OMB