

AD Policy Committee
October 21st, 2011
3110 Engineering Building II
3pm-4:30pm

Present: Dan Green, Joshua Gira, Dan Evans, Tom Farwig
Absent: Billy Beaudoin, Daniel Henninger, Wes Thibodeaux
Guests: Michael Underwood, Alan Gerber, Joe McCoy, Debbie Carraway

AGENDA:

NCSU domain policy "Domain-CWDIllegalInDIIISearch (KB2264107) Policy" (Dan G)

- causing errors in EventLog: Windows update could not be intalled because of error [2149842967](#) (Command line ""C:\Windows\system32\wusa.exe" C:\Windows\Windows6.1-KB2264107-x86.msu /quiet /norestart")
- Appears to be caused by the fact that the patches in the policy are now being pushed via WSUS and yet we continue to try and push them via this policy.
- **Committee says proceed w/ fix.**

Google ADMX (Michael U.)

- Found an adm template from Google that lets you manage some of the settings for their products.
- Apps, Chrome, Earth, Talk, Toolbar, O3D, Language Inputs, Analytics
- Request: Add to the central ADMX store. Will affect all OU Admins as they'll see in GroupPolicy MMC. **Committee approves; Derek will be asked to add it to the central ADMX share.**
- Clarification -- will not affect existing settings unless you choose to utilize the policies -- we are not going to be settings anything centrally; merely making the GPs available.

Open Seat

- With Joey Jenkins departure, we have an open AITD seat.
- **AITD will be asked to select a new member of the committee.**

Trend Micro Forced Upgrade (Michael U.)

"We've still got a ton of computers in the old Trend Micro group. It requires at least 3 reboots to be fully up to date and once in a while just freaks out. I'd like to request for a forced upgrade from the old package to the new one similarly to how we did from SAV to TM."

- Specifically -- move the **7857** computers in "SW-Trend Micro-OfficeScan-10.0.1068-20090929" to "SW-TrendMicro-Officescan-10SP1"
- Recent SCCM inventories have shown that many PCs don't have Trend installed, and a few hundred that do have old definitions.
- Old/Current package was made incorrectly -- bounces between AV servers. PRIMARY GOAL is to make sure that all computers have the newer / correct settings on them.
- Process to do this move will take a long time.
 - Wish to uncheck the "uninstall when out of scope" flag on the old policy.
 - Wait a while. Michael was originally proposing 6 months.
 - Then allow folks to move individually.
 - Finally, force the rest over.
- Debbie -- there's a new Trend client coming by end of Nov -- v10.6.

- Will this require installations or will it autoupdate?
- What's the timing of when 10.6 is available vs when Joe will push it out via updates. Need to talk to him about delaying the force to coincide w/ this effort.
- Dan -- need to tie to this new version process
 - Will require that we have the new 10.6 package force a cleanup/uninstall before attempting to install new version.
- Alan -- concern -- have to make sure that testing is done across all flavors of Windows OSes.
- Committee -- approves the removal of the "remove when falls out of scope" flag. Requests that Michael return to the committee in 4+ months once he's had time to test the upgrade path to the new package and computers have had a chance to detect the change in the policy. At that point in time, we'll discuss forcing the new version across the board.

Reporting and Monitoring

- Disabling .admin accounts associated with KRB_DISABLED unityIDs. No objection from the Committee.
 - Results from the above request:

The ones that would be disabled. It's all the accounts that have a non-admin account that's disabled or don't have a non-admin account BUT meet unity ID naming conventions:

Unity ID will be disabled: jlwagner.admin
 Unity ID will be disabled: cnrlab.admin
 Unity ID will be disabled: wpslab.admin
 Unity ID will be disabled: Wasilla.admin (Josh will correct these three)
 Unity ID will be disabled: bgerikse.admin
 Unity ID will be disabled: nso.admin (Dan will contact)
 Unity ID will be disabled: mmgainey.admin
 Unity ID will be disabled: sfatmi.admin
 Unity ID will be disabled: rlgreen2.admin
 Unity ID will be disabled: sjbarker.admin

These are the invalid ones (obviously are not unityIDs):

No Matching Unity ID: oit.ftp.admin
 No Matching Unity ID: autoinstall.admin
 No Matching Unity ID: techsmith.admin (Josh will deal with)
 No Matching Unity ID: FER-Research Labs.admin
 No Matching Unity ID: PRTM-Labs.admin
 No Matching Unity ID: PRTM-Graduate Students.admin
 No Matching Unity ID: Bio-Zeiss.admin
 No Matching Unity ID: Bio-Agilent.admin
 No Matching Unity ID: dlevans-test.admin
 No Matching Unity ID: tex.forensics.admin
 No Matching Unity ID: tex.gallery.admin
 No Matching Unity ID: tex.nwimss.admin
 No Matching Unity ID: tex.lectra.admin
 No Matching Unity ID: tex.mona.admin

How does the committee wish to proceed?

If could be a unityID, enforce.

Any length, not using . or - => disable, then send email below.

Will ignore for now, anything using the .admin convention but also using . / -

Whenever you disable, must email the OU Admins for the OU it exists in. So they're aware.

Email needs to point to naming convention and inform the recipient exactly what they need to rename if they wish to keep the account.

New Business:

Need to revisit the idea of putting another DC over with Campus Police. Dan will restart the email conversation.