AD Policy Working Group
April 15th, 2016
3110 Engineering Building II
3pm-4:30pm

Voting Members: Donna Barrett, Charles Cline, Dan Green, Julie Tilley, Dan Evans, Daniel Henninger, Tom Farwig, Joshua Gira, Daniel Sink

Ex Officio Members: Jeremy Brown, Michael Underwood, Gene Morse, Rob Blanke

Guests: Billy Beaudoin, Debbie Carraway, Matt Pollard, Ken Taitingfong

---

Business handled outside of meetings:

SCCM Site Server OS Upgrade
I wanted to confirm that the Policy committee approved the upgrade of the OS on the Site Server for Wednesday March 9th. If you look at your calendar Patch Tuesday is March 8th. If the Site Server upgrade is to happen it will disrupt the patching schedule, and we cannot guarantee patches will be deployed on time to any of the patching groups.

Pushed by Committee vote to March 16th to avoid patching conflict.

=====

Agenda:

Quicktime for Windows [Michael Underwood]
Apple has announced that they're not supporting QuickTime for Windows anymore and not to expect more patches. Two vulnerability in the wild have been found. S&C wants the app removed from across campus. How to handle?

Julie: Would be a problem for us as we have apps that require it. Ex: Simulation lab for animal anatomy skills.
Billy: Announce a future removal (90 day) and see who wants to request an exception from S&C? (based on the campus patching policy)

If OIT S&C is going to allow exceptions, we'll need to create a DN group for whatever script / process we'll use to remove the software.

[This process wasn't nailed down during the meeting and would likely need to be run by AD Tech. However, as the removal is being proposed for a few months from now, we have time to nail down the specifics.]

Committee: S&C [Dan Sink] needs to make a Sysnews post announcing that S&C requires the removal. Once this is announced, AD Policy can send a 2nd followup to this which will note the specifics for machines within the AD.

SCCM Core team Update/Discussion [Gene Morse]
We want to discuss upgrading SCCM to v1602, upgrade of client, and changing the way the client is maintained/upgraded.

Currently behind on the client pushed out to the machines. Want to make the upgrade of the client a part of the standard operations --- want to reduce the amount of pre-approval form the committees (as the upgrades will be happening every 3 months or so now) --- and change the installation of the client from VB to GPO.

Billy: Add SCCM upgrades to the autoapproval list (which we've never finalized). Plan to move forward on your timeline, pick a date, and inform the comms. Give them a chance to object, but if nothing heard, move forward.

Julie: Do you always test on wolftest first? *Yes.* What will be the time between WolfTest and WolfTech installation? *Normally about a week -- just checking to make sure nothing blows up during the upgrade itself.*

Committee: SCCM core team will test and then select a date for the server and client upgrades. They will announce these dates and give the committees at least 1 week notice. Should no objections be raised regarding the dates, they should proceed.

Client installation change from vbs -> GPO --- they're not clear on how this would work…

Committee: Yes, but not sure we, as the Policy Comm, really care about the specifics of this technological question… make sure whatever you switch to works, and have the AD Tech comm sign off on it.

Update on Special Configurations OU [Jeremy]
I have finished configuring the Special Configurations OU and LAPS build out.

The "Special Configurations" OU is now deployed throughout the NCSU OU and nested appropriately. I have moved groups that should be in there over and began changing the the names. I do not intend on changing the names of the SUP groups till after the late patches get deployed. There may be other groups that were missed. If you find other groups that need to be moved please let me know. I also added a folder to SCCM and moved collections into a "Special Configurations Collection" as well. That way the two environments mirror as best they can.

The intent for this OU is to hold all the unique things for devices that would not be software that a user would interact with. Other things that I expect to move into this OU would be the NIST compliance settings filtered on the upcoming GPO or possibly moving Tripwire and Identity Finder into this OU as well.
Special Configurations was discussed in 2013:
https://docs.google.com/document/d/1Tr5-miBHGdbpMXPipGml-ZfRat6zLgkiSyiy6HnLMV4/edit

May need to fix ADToolkit to show these -- Dan Green requested that an error report be submitted to wolftech-webmaster@ncsu.edu with details.

Update on LAPS [Jeremy Brown]

LAPS (Local Admin Password Slayer) is ready for deployment, I believe. There are two collections. Once is filtered on a NCSU-SC-Microsoft-LAPS-OptOut group. The other is filtered on the NCSU collection while excluding any devices in the NCSU-SC-Microsoft-LAPS-OptOut group. The plan is to deploy the software to the latter collection. The software requires two reboots for full effect. The first reboot completes the installation of the agent and registration of the .dll's. The second reboot is when the password of the builtin administrator account is changed. You can see the password on the computer object under the ms-Mcs-AdmPwd attribute. The LAPS policy GPO (NCSU-SC-Microsoft-LAPS) is currently setting the password to:

Complexity: Enabled
Length: 16
Age: 90 days

This is an opt-out feature. If you don't opt-out, you'll be in.
AD Tech has already reviewed and approved the deployment.

Who will be able to look at computer X's LAP? Anyone in its OU Admin's group (or if you delegate that attribute to another group).
When will it go live? Can go now.
When will it be announced? Announce on Monday (April 18th) that we'll be turning it on the afternoon May 2nd.
Where's the docs on it? Jeremy will add a page to the activedirectory.ncsu.edu to explain the service.
Where has it been tested? Multiple computers managed by Jeremy Brown and M. Underwood.

Committee: Go forth and implement w/ caveats above.

Windows 10 domain defaults [Tom Farwig]

Noticing on a couple of Windows 10 machines that the last user logged in is displaying on the login screen where it did not under previous versions of Windows.

The policy setting for this is:

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options:

> Interactive logon: do not display last user name.

I have found that our current Win 10 baseline GPO, "Windows 10 Computer (SCM, v1511)" does not have this set like the previous baselines. Looking at it closer, it only has one item in the Interactive logon section that is set: the behaviour of smart card removal (set to lock workstation). The following settings are in the "Win8.1 Computer Policy" baseline GPO:

- Interactive logon: Do not display last user name
  - Enabled
- Interactive logon: Do not require CTRL+ALT+DEL
  - Disabled
- Interactive logon: Number of previous logons to cache (in case domain controller is not available)
  - 4 logons
- Interactive logon: Prompt user to change password before expiration
  - 14 days
- Interactive logon: Require Domain Controller authentication to unlock workstation
  - Disabled

None of these are overridden in the Win 8.1 Default Domain policy.

I would like to request that at least the "Do not display last user name" setting be added to the "WolfTech-Default Domain Policy - Win 10.0" since it is apparently no longer being set in the baseline. I believe the others may also be desirable but don't necessarily know the impact they would have on a Win 10 device some of them may have or if any are obsolete under Win 10. I only looked in the interactive login section for differences, I believe there may also be others.

From what I could find there was only a Win 10 Computer baseline, and no longer different configs like the Enterprise Computer baseline that we have used in the past where a lot of the above settings came from originally. I suspect this may be why there is a difference.

Julie Tilley (3/24/16): I'd like to see it set to: "Interactive logon: do not display last user name" as well. We can still override at our own OUs if we need/want to.

Derek Ballard (3/24/16): Updated the "Interactive logon: Do not display last user name" to "Enabled" in the "WolfTech-Default Domain Policy - Win 10.0" policy, since this appears to be a no-brainer FERPA thingy. If someone disagrees, please let me know and i'll change it back. Not making any other changes until further discussions and decisions made.

Dustin Duckwell (3/24/16): I would like to also recommend that the 'Show first sign-in animation' be disabled as well.

Committee: Endorses the change that Derek already made. For consistency and future NIST compliance, we'd ask that these be all added back to the Win10 policy… the only exception is the last "Req DC auth to unlock" -- we feel that the AD Tech comm needs to reinvestigate this as we recall some issues. Dustin is encouraged to set "Show first sign-in animation" at his OU.

New Chair Elections [Dan Green]

Dan is stepping down as the chair of the AD Policy Committee and as a member of the committee. While the women wept and the men beat their chests, it was acknowledged that it was time.

As a part of this process, the committee voted to clarify some rules regarding the chair and the membership of the committee:

- Does the chair need to be an existing member of the committee. Yes.
- Chair Terms -- voted to be 2yrs; no limit on how many terms a chair could serve for.
- Clarify the rules so the chair isn't separate but accounts for one of the CITD members which isn't currently clear on the website. [Dan G: website updated 4/18 to clarify this]

Josh will present these at the ITSAC-CAS for blessing.

Dan Evans volunteered, Josh Gira nominated -- both accepted.
Committee discussed and voted -- Josh Gira was named the new chair.

Stuff on the horizon… (things not quite ready to be discussed)

- **DirectAccess Demonstration [M. Underwood]**
- **Security Standard for Sensitive Data and Systems [~~Jessie Henninger~~]** https://docs.google.com/document/d/1ZdLqnHmXZLKeYsPWXwM8l4XIn3fWmuf3nLQcE-0vYyk/edit#heading=h.ik9joinausi **Rescheduling for 2016 as Jessie left S&C.**