

Baseline Windows Vista Enterprise Computer Setup

Version: 0.1.0

May 5, 2008

This documents the procedure that is recommended to enhance the security of a computer running Windows Vista Enterprise. These steps are the result of scanning various best practices documents as well as other sources and guidelines on securing the Windows Vista Enterprise operating system. We will make the assumption, that the minimum level of Vista Enterprise is the RTM version.

Do NOT attach a new machine to the network until specified below:

Initial Power Up

1. Backup the initial registry. (Optional):
 1. Allows a baseline registry file to exist prior to any modifications
 2. Run->cmd regedit Registry->Export (save to administrator profile in folder named adm)
2. Set Secure Boot and Required Authentication:
Require ctr-alt-del to log on and require logon
 1. Run->"control userpasswords2":
 - i. Under Advanced tab: Check "require users to press ctrl-alt-delete before logging on"

Disable default accounts, create administrator and user accounts

1. Run->lusrmgr.msc
2. Rename the default Administrator account to make it appear as a local user account, set password to something very obscure, CUT the description (you cannot remove this account or remove it from the administrators group, it is known by a default SID which is the SAME for all systems, you can't stop hacks against the SID, but you can obscure the account name. See [KB163846](#).)
3. Create a new account named administrator, paste the copied administrator description into this new account, set the password to something random, never expires, then disable the account.
4. Check existing groups to ensure no standard user has membership in privileged groups NOTE: the users listed on the "User Accounts" control panel applet DO NOT SHOW all accounts, you MUST use lusrmgr.msc to see all the existing accounts.
5. Audit the use of elevated privileges:
 1. Run->"secpol.msc"
 - i. Chose "Security Options," set:
 1. Audit: audit the access of global system objects

2. Audit: audit the use of backup and restore
 3. Interactive Logon: Do not display last user name
 4. Interactive Logon: Message Text (whatever your policy wonks have approved)
 5. Interactive Logon: (ditto)
 6. Network Access: Do not allow anonymous enumeration of SAM accounts and Shares.
 7. Network Access: Do not allow storage of credentials or .NET passports for network authentication.
 8. Network Access: Sharing and security model for local accounts (set to classic mode).
 9. Network Security: Do not store LAN Manager hash value on next password change.
 10. Network Security: LAN manager authentication level (set to send NTLM responses).
- ii. Also look at the Audit Policies section and set auditing enabled for:
1. account logon events S/F
 2. logon events S/F
 3. policy change /F
 4. privilege use /F

Important NOTE: You should increase the size of your event log files. With the additional logging enabled above you will quickly fill up the event logs and log everyone out except administrators. Start->Run "eventvwr", Open "Windows Logs", then right click on the system, security, and application logs and increase their size to 20480kb, and set them to overwrite older events as needed. Also, these settings are a trade-off between information overload and something that might be usable in the event of an intrusion. Auditing will produce a lot of data. Grabbing the audit logs and pushing them to a central location for analysis is a good idea if you have the resources to do the analysis.

6. Remote Desktop and Remote Assistance

1. Change the windows firewall rules so that ONLY the ASU subnets (or the subnets within your control area) can access RDP.
 - i. Go to: Control-Panel, Windows firewall, Exceptions Tab. Change the "Scope" of the exception by Double-clicking on the "Remote Desktop" entry, then clicking on the "Change Scope" button.
 1. 129.219.0.0/255.255.0.0,149.169.0.0/255.255.0.0 allows all of ASU.
 2. 129.219.140.0/255.255.255.0 would allow only a specific subnet range.
2. If you are NOT allowing desktop users to be in the administrator's group, then either enter the user directly, or create an AD group that you can populate with Faculty/Staff from your area, that will be allowed to RDP to their desktops.

7. Performance Settings

1. Virtual Memory Size – Unlike XP, Vista controls this much better by default. Unless you are running an Application that requires a set amount of paging space, leave the settings along on vista. But, if you DO need to change it:

- i. Start->My Computer->Right-Click to get to system properties. Select the "Advanced" tab, then Settings on the Performance Section, then the "Advanced" tab, then "Change" on the virtual memory section. Change the current setting to 1.5 to 2 times physical memory. Note: Creating a large pagefile that does not shrink or grow will prevent page file fragmentation.
2. Change your Visual Effects. You can play with the Visual Effects settings to also improve your system's performance. If you have really new hardware its easiest to leave them alone. On older systems changing these effects can have significant effect on the usability of the system.
3. While you are in the Computer Properties dialog, you should probably turn OFF "system restore" until you have applied all your configuration changes and installed software. Yes, this prevents you from recovering many changes, but have you ever used system restore effectively to recover from some change?
4. Under the Remote Tab, change the Remote Desktop setting to the second radio button "Allow connections from computers running any version of Remote Desktop..". Until we can insure that ALL of our XP Support systems are updated, the default setting would block XP from connecting to Vista.
8. Make sure that peer-to-peer file and printer sharing is turned off (it's a security hazard).
9. Adding the LPR Windows Component.
 1. There are multiple ways to connect to networked printers. A common way is to using TCPIP connections directly to printers or to queue servers. LPR is an old standard that can be used. To get a more complete set of LPR tools to manage LPR queues, you must install print services for Unix. Windows print queues may also send print jobs to IPP style print servers, or port 9100 raw style printers. IPP and raw printers do not require additional software services to be installed.
10. Vista has the advanced Windows firewall enabled by default. Plug the system into the ASU network for the next steps.
11. Register the installed wired Ethernet card for use on the ASU DHCP service.
12. If the system REQUIRES a static IP address, then instead, do the following:
 1. Set the IP Address, Subnet mask, DNS and WINS entries.
 - i. Right-Click on the Network icon and select "Properties".
 - ii. Select the TCP/IP protocol.
 - iii. Click on "Use the following IP address", and enter the IP address, Subnet mask and Default Gateway.
 - iv. Click on "Use the following DNS server addresses".
 1. Preferred: 129.219.17.200
 2. Alternate: 129.219.17.5
 - v. Click on the Advanced Button.
 - vi. Within the DNS area, uncheck "Register this connection address in DNS".
 1. If you didn't enter the DNS server previously, enter them now.
 2. Select the radio button "Append these DNS suffixes (in order):" enter:

1. Asurite.ad.asu.edu
 2. Your college or department.asu.edu
 3. Inre.asu.edu
 4. Asu.edu
- vii. Set the DNS Servers.
- viii. Set the WINS Servers.
1. WINS1: 129.219.13.105
 2. WINS2: 129.219.17.197
- ix. Time sync. If the system will be a member of an Active Directory (AD) domain, it will receive time sync corrections from the AD NTP controller (ASUDNS3), otherwise enter 129.219.17.200 as the NPT server.
1. From a CMD prompt enter: "net time /setsntp:129.219.17.200"
 2. Control Panel->Administrative Tools->Services, set windows time service to startup automatically.

System and Driver updates

1. Update to the most current version of OS and applications.
 1. Using Windows Update (wuapp.exe) install all current critical and additionally desired recommended updates.
 2. Other updates/installs: Silverlight, Flash, Acrobat Reader, etc.
 3. Vendor Device Drivers and other miscellaneous things.

Applications

1. Install MS Office and other applications.
 1. For ease of updates, make sure that you leave a local source install location.
 2. Other "standard" applications to install include McAfee AntiVirus, Corel Suite, FireFox, Adobe Reader, QuickTime Player with I-Tunes, Flash Player, Flash Browser plug-in for FireFox, etc.
2. Revisit Microsoft's web site and apply all Operating System and Office updates. If you have NOT left the Office CAB files in C:\MSOcache, then make sure to leave your network drive install point mapped to the office install source.
3. You should setup Microsoft Update in the place in Windows update as it will grab all updates for Microsoft applications as well.

Join to ASURITE domain.

1. This MUST be done through a WIRED connection (same as when changing passwords, etc).

2. Make sure that the system has been named properly for your area (SOLS-JFINLEY1-01, UC-KARRAL-01), etc. If not, use the Systemals tool NEWSID to both set a new computer SID, and change the System name.
3. Make sure that the local elevated account password has been set to the Departmental/ASU password scheme.
4. Pre-populate the Computer Object within your Organizational Unit (OU).
5. Right-Click on “My Computer”, Click in the “Computer Name” Tab. Click on the “Change...” button.
6. Set the Domain as “ASURITE”. Authorize the change when prompted.
7. Before rebooting, Right-Click on “My Computer” select “Manage”, “Local Users and Groups”, “Groups”, then Double-Click on the “Administrators” group, and add in your Departmental Support Group from your OU area.
8. Reboot.

Why through a wired connection?

Wireless doesn't startup until the User logs on once initially. Also, to speed up the boot process, Windows Vista and XP both cache the login, unless set to act like windows 2000 did through a GPO or local Security setting.

Register the wireless connection for use with ASU.