Title: Hardware And Software Installation And Configuration Protocol

IT Code: 44370

Purpose: All workstation (WRK), development (DEV), server (SRV), and clinical (ACS) CLASS computers are given identical base installation of software and configurations. Additional software and/or configuration changes may be mandated by the intended use of the system.

The following procedure details the base CLASS IT installation protocol.

Procedure:

**PART 1: BASIC INSTALLATION**

Note: this installation assumes that the computer being configured is connected to our local (CLASS) LAN … BEHIND A FIREWALL!

1) Unpack the computer and monitor.

2) Attach the mouse, keyboard, monitor cable, Ethernet cable, and power cords (1 for computer and 1 for monitor).

3) Turn on the monitor and computer (boot it up!).

4) Write down the model number, Service Tag (serial number), U of M tag number, and any other identifying information you think may be useful (date of installation is an example) on our CLASS Configuration Documentation Log (CDL) [see SOP 44371].

5) Go through all the normal software/operating system startup protocol that the system requires (it runs from its hard disk so you really don’t have much choice). Settings are generally not critical since we are going to replace all of this in the next step. (Testing: Internet Explore) … Computer Name:CLASS-WRK138; Local area network(LAN);IP Address: See log sheet…

6) Insert the Windows 2000 Professional Installation CD (#1) into the computer's drive and restart.
7) If the system does not give you a choice to boot from CD, Hit bios configuration key (Dell – F12 key, HP – F9) during reboot, navigate to “Boot Sequence”, and make the CD drive the first choice. Save changes and continue restart. Note: you may need to make these choices quickly while its rebooting.

8) When the “Press any key to boot from CD …” appears, hit any key immediately.

9) Accept the “Agreement” (F8 key). (a long period of computer, so you can do some other things)

10) If the HD information shows a small (31MB on Dell) partition of “unknown” type and a larger NTFS partition - leave the little partition alone (it for rebuilding the system)! But delete the large partition and then create a new partition using _ of the total size (e.g. on a 40 GB drive, make two 20 GB partitions). That is, delete big one; partition half & half; set up (enter); then point to C.

11) Set up Windows on the “selected item” … the C: New (Unformatted) partition.

12) Format the partition using the NTFS file system. And wait till it’s through (time to read something interesting – a magazine, book, whatever).

13) Always use these values for “Name and company” question: (SYS ADMIN first line, CLASS – UMICH second line)

14) The computer name should be in the form: “CLASS-tttnnn” where “ttt” is the type (SRV, DEV, WRK, ACS) and “nnn” is the last three digits of its TCP/IP address (examples: CLASS-WRK101, CLASS-DEV001). Administrator Password later, so for now just make sure it is included.

15) Set date, time, and time zone (EST), and “Automatically adjust clock for daylight …” (a lots of time here …)

16) When down, remove the CD and wait for reboot.

17) Choose the appropriate log on based on system type:

A) If this is a Win2000 Server – Log on to the system with “Administrator” account and log.  

B) If this is a Win2000 Professional – Select “Users must enter a name and password to use this computer”. Then logon with “Administrator” and “temptemp”)

2 - 16
18) Get rid of the “Getting Started with Windows 2000” pop up window by uncheck the “Show this screen at startup” and then selecting “Exit”.

19) Load our (second one) “CLASS_CONFIG” upgrade CD, navigate (My Computer) to the CD, and install Windows Service Pack 4 (W2KSP4_EN) (check “do not accept the “archive old” option”). When it’s finished, it will start to restart the computer.

20) Install updated drivers for the specific computer being used:
   
   A) If a DELL: Create a new folder called “Updates” on the C: drive. Then, copy our standard DELL Driver Update Folder into it and install hardware specific update drivers for this computer and OS (Intel Chipset [R58201]; Intel Graphics [R60084]; Analog Device Sound [R58182]; Intel NIC update [59444] - rebooting between each.

   B) If a HP/Compaq: Create a new folder called “Updates” on the C: drive. Then, copy our standard HP/Compaq Update Folder into it and install hardware specific update drivers for this computer and OS: Intel Extreme graphics driver (SP24357); Broadcom NetExtreme NIC (SP24462); ADI SoundMax Driver (SP24465 note: takes awhile to load); and, Microsoft USB 2.0 driver (SP23821) - rebooting between each.

   C) Delete the “Updates” folder from C, and remove the CD.

21) Configure the display:

   A) Go to – Start:Control Panel:Display. Select “Settings” tab. Set Screen area to “800 by 600” and “Colors” to “True Color (32 bit)”. Apply and “keep” these settings after the 15 second “trial” period.

22) Configure the Firewall/Gateway communications parameters: (Need to redo after computer is moved to the downstairs. E.g. 192.168.1.1(upstairs); or, 192.168.1.2 (downstairs)

   A) Go to – Start:Settings:Network and Dial-up Connections. Double click “Local Area Connection” and select “Properties”.

   B) Highlight “Internet Protocol (TCP/IP)” and click on “Properties”. Before proceeding, select an unassigned IP number from our table (CLASS IP
Select “Use the following IP address:”

IP address: 192.168.1.nnn (substitute real)
ACS (160-169)
WRK (130-138)

Subnet mask: 255.255.255.0

Default gateway:

Select “Use the following DNS server addresses”

Preferred DNS server: 141.211.144.17
Alternate DNS server: 141.211.125.17

C) Click “OK” and click “OK” again to the “empty WINS address” window.

D) Returning to the “Local Area Connection Status” window, click Properties, click “Install”; highlight “Protocol”; and click on “Add”. When the “Select Network Protocol” window appears – highlight “NetBEUI Protocol” and click “OK”.

E) Now do the same procedure to install the “AppleTalk Protocol”.

F) (close all) Close the “Local Area Connection Properties”, “Local Area Connection Status”, and “Network and Dial-up Connections” windows and reboot the machine.

G) Make this computer a member of the “CLASS” workgroup. Using “Start>Settings>Control Panel>System”, select the “Network Identification” tab and
23) Click on the Internet Explorer icon (IE browser) and do a quick configuration as:

A) “I want to set up my Internet connection manually”;

B) “I connect through a local area network (LAN)”;

C) “Automatic discovery of proxy server”;

D) “Do you want to set up an Internet mail account now?” – NO;

E) Click the “Finish”.

24) Using IE Navigator go to http://windowsupdate.microsoft.com ;

A) Allow installation of Microsoft update software;

B) Add to “favorites”; scan for updates;

C) Install all critical updates and service packs (may require multiple reboots and returning to this site for all the updates -that’s why we added it to “Favorites”). (until critical updates and service pack goes 0)

D) Lastly, make this page the default page (Under Tools: Internet Options…: Home Page).

25) In general, DO NOT UPDATE ANY DRIVERS it recommends and, you can probably skip the general Windows 2000 updates also.

26) Use “Start:Settings:Control Panel:Administrative Tools:Computer Management:Disk Management” tool to create a primary partition on the second half of the hard disk and format it as NTFS:

A) Highlight the “Unallocated” box; right click and select “Create Partition”.

B) With the “Create Partition Wizard”: select “Primary partition”; Maximum disk space (should already be set in the “Amount of disk space to use” box); “Assign a drive letter” as “E:”; “Format this Partition with …” NTFS, Default, and erase the “Volume Label”; then “Finish”. (take a while)
C) After it is finished formatting the new partition, Rename CD drive as “Z.” (right click on CDRom box; select “Change Drive Letter and Path”; select “Edit …”; select “Assign a drive letter:” Z; select “OK”; select “Yes” ), and then set new partition to “D:” (same technique).

D) Close windows and reboot

PART 2: SECURITY CONFIGURATION (1ST LEVEL)

27) Using the CLASS_CONFIG SUPPORT CD, install McAfee Enterprise 7.0 (virus scanner) from U of M website (Virus Busters) and configured it as per ALL DEFAULT INSTRUCTIONS. Its filename is currently “vs70um”. Note: at this point there are no “Network Files” so you do not need to disconnect from the LAN.

28) Using the CLASS_CONFIG SUPPORT CD, install the free version of ZoneAlarm firewall – use the default configuration. Its filename is currently “zaSetuo_1001”.

A) Accept default location (“C:\Program Files\Zone Labs\ZoneAlarm”).

B) Name and Organization should appear automatically (SYS ADMIN, CLASS – UNICH).

C) Enter email address as: “mpdavis@umich.edu”

D) Unclick the “I want to register …” and “Inform me about” boxes and continue.

E) Accept the License and “Install”

F) Survey: T1/LAN;Advanced;5-10;Network

G) “Do you want to start ZoneAlarm now?” – Yes

H) When the “Welcome to ZoneAlarm” window appears: click “Next”; select “Don’t alert me at all – protect my computer silently”; “Do you want ZoneAlarm to preconfigure access permission? – Yes; “Skip the tutorial (unless you are interested in it); close the ZoneAlarm window; and say “OK”.

I) Reboot
29) Install Windows Office 2003

   A) Accept default User name (SYS ADMIN) and Organization (CLASS – UMICH) and set Initials to “SYS”.
   B) Use the product key in this PC’s Configuration Documentation Log (e.g., M2D2Y CGH9R TY4W6 PYTKY R44DY).
   C) Accept License Agreement

   D) Select “or choose an install type:” Custom and the default (C:\Program Files\Microsoft Office\) location

   E) Select only: Word, Excel, PowerPoint, Publisher (ACS only Excel) [+ “Install … typical options”]

   F) Install

   G) Using IE Navigator go to http://windowsupdate.microsoft.com (it’s your home page if everything is configured properly (see step 24D)

   H) Select “Office Update” from the menu bar just above the “Welcome to Windows Update”

   I) Click on “Check for Updates” and allow installation of “Office Update Installation Engine”. You will need to do this several or many times to get them all.

   J) Apply all Office 2003 updates and patches (accept all defaults and license agreements).

   K) Reboot

30) Install Acrobat 5.0 (full install)

   A) Navigate to the “Acrobat 5” folder on the Acrobat CD and double click “Setup” program (the one with the icon of a computer and a box).

   B) Accept defaults (US English, Accept, Typical, Destination folder
A) Set Name – “SYS ADMIN”; Company – “CLASS – UMICH”

B) Select “Typical” setup, BUT change Destination directory to: “C:\Program Files\StatView” and let it create the directory.

C) Finish (skip the ReadMe file unless interested)

D) Note this serial number in the Configuration Documentation Log

E) Complete the default install

F) Launch the “Adobe Acrobat 5.0” icon on the desktop and dismiss the registration screen – Click “Do not display this dialog again”

G) Close Acrobat

31) Install StatView 5.0 (full install) [no serial number required]

A) Select “Install FileMaker Pro 6”

B) Accept License; accept default User Name (SYS ADMIN); Organization (CLASS – UMICH); and install “Anyone who uses this computer (all uses)”.

C) Accept default Destination folder “C:\Program Files\FileMaker\FileMaker Pro 6\”

D) Select setup “Complete”

E) Select Network Protocol – “TCP/IP”

F) Application Shortcuts – “Yes”

G) Enter installation code (e.g. 1-1027-0995-2822-7667) and note this serial number in the Configuration Documentation Log.

H) Click “Install”
PART 3: SECURITY CONFIGURATION (2nd LEVEL)

34) Create a new security environment


   B) Disable the Guest User account:

       - Right Click on the “Guest” user and select “Properties”.

       - Under “General” make sure that the following boxes are checked:
         “User cannot change password”; “Password never expires; “Account is disabled”

       - Select “Member Of” tab, highlight the “Group” and Remove “Guests” and then “Apply” and then “Close”

       - Right Click on the “Guest” user again and select “Set Password”.

       - Enter a complex password e.g., [e.g., TcEhK94623]

       - Reenter this password at “Confirm”

       - You DO NOT need to log this password to the CDL
INFORMATION TECHNOLOGIES (IT)
STANDARD OPERATING PROCEDURE

C) Protecting the Administrator account:

- Right Click on the “Administrator” user and select “Rename”
  - Rename account to “FakeSysAdmin”
  - Right Click on the “FakeSysAdmin” user and select “Set Password”.
  - Enter and confirm a complex password based on our special CLASS formula for passwords (see MARK) [e.g., wysys-tbf138]
  - Log this account and password in the CDL
  - Right Click on the “FakeSysAdmin” user and select “Properties”.
    - Under “General” make sure that ONLY the following box is checked “Password never expires”.
    - Change the “Description” to “HoneyPot honey trap Admin”.
    - Apply and Close

D) Creating a really fake Administrator user to keep the script kiddies busy!

- Right Click on the “User” icon and select “New User”
  - User name: “Adminstrator”
  - Full name: don’t enter anything in this box
  - Description: “Built-in account for administering the computer”
  - Enter and Confirm a complex password [e.g., TcEhK94623]
  - Uncheck the “User must change password at next logon” box
  - Check the “User cannot change password” and “Password never expires” boxes.
  - Click “Create” and “Close”
Right Click on the “Adminstrator” user and select “Member Of”.

- Remove “Users and then “Apply” and then “Close”

E) Creating User Accounts:

- Right Click on the “User” icon and select “New User”.
- User name: (from the current user list)
- Full name: don’t enter anything in this box
- Description: “CLASS User”
- Enter and Confirm a complex password from the current user list
- Uncheck the “User must change password at next logon” box

- Check the “User cannot change password” and “Password never expires” boxes.
- Click “Create” and “Close”
- Log this account and password in the CDL
- Repeat for all users in the current user list as per policy
- (close everything)
- Reboot and logon as {FakeSysAdmin e.g. wysys-tbf138}

35) Use “Start:Settings:Control Panel:Display”

- Select “Screen Saver” tab and set Screen Saver pull down to “Logon Screen Saver”
- make sure the “Password protected” box is NOT CHECKED
- Then set “Wait” to 60 minutes
- select “Apply” and “Ok”
INFORMATION TECHNOLOGIES (IT)
STANDARD OPERATING PROCEDURE

36) Use “Start:Settings:Control Panel:Power Options”
- On “Power Schemes” tab set “Power schemes” to “Always On”
  - “Turn off Monitor” - After 30 mins
  - “Turn off hard disks” - Never
  - “System standby” - Never
  - “Apply” and “Ok”

37) New Security Policy Settings
     - “Passwords must meet complexity …” - enable, “OK”
     - “Minimum password length” – 7 characters
     - “Account lockout threshold” – invalid logon attempts
     - Accept (“OK”) suggested lockout duration and resets
     - “Do not display last user name in … “ – enabled
     - “Disable CTRL-ALT-DEL logon requirement” – disabled
     - “Prevent users from installing printer drivers” – enabled
     - “Restrict CD_ROM access to locally logged user” – enabled
     - “Restrict floppy access to locally logged user” – enabled

- “Audit account logon events” – “Audit these attempts” – Failure

38) Use “Start:Settings>Control Panel>System>Advanced>Startup and Recovery”

- Set “Write Debugging Information” to “(none)”
- “OK” and allow computer to be restarted

39) Disabled CD Autorun capability: (Careful!!!)

- Use “Start>Program>Accessories>Command Prompt”
- Type “regedit” and hit the Enter key
- Use HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Services>Cdrom
- set AutoRun (Edit DWORD Value) to 0 (was 1)

- click “OK”
- Close Registry Editor
- Close Command Prompt window

40) Check that there are no modems in machine (and disable if present)

A) Use “Start:Settings>Control Panel>Administrative Tools>Computer Management>Device Manager

B) Look for a “Modem” or modem under “Network adapters”

C) if found, disable by right clicking on the icon and selecting “Disable”

41) Disable some services:

A) Use “Start:Settings>Control Panel>Administrative Tools>Services

B) Click on “NetMeeting Remote”
PART 4: REALVNC INSTALLATION

43) Install the RealVNC Server V3.3.7 and configured ZoneAlarm to work with it

   A) Using the CLASS_CONFIG CD, install the RealVNC Server V3.3.7 (file name is currently “vnc-3.3.7-x86_win32”)(VNC folder)

      - VNC Install wizard appears, accept “License Agreement”
      - Accept Destination Directory of “C:\Program Files\RealVNC”
      - Select “Full installation” with VNC Server and Viewer checked
      - Accept “Start Menu Folder” as “RealVNC”
      - Under “Select Additional Tasks”, check “Register VNC Server as a system service” and “Start the VNC Server system service”
      - Click “Install”
- ZoneAlarm should issue an Alert – check “Remember this answer …” and click on “yes”

- ZoneAlarm should issue a second Alert - check “Remember this answer …” and click on “yes”

- “Setup – VNC” continues -> click on “Next” and “Finish”

- Click “OK” at the warning “This machine has no default password …”

B) Configure ZoneAlarm to work with VNC (Part 1):

- Double click the ZoneAlarm icon in the icon tray (red and yellow ZA)

- Click on “Program Control” (left side of window) and then the “Programs” tab at the top

- Make sure that “VNC server for Windows” has three of the four options (Access: Trusted, Internet) and (Server: Trusted) set true with a green check mark (left click over each option to use selection menu)

- Make sure that “VNC server for Windows” has the last option (Server: Internet) blocked with a red X (set as above).

- (may not be there) In the same window, set “ZoneAlarm” options for (Access: Trusted, Internet) to true (green check mark)

- Close window

- Reboot the computer

C) Configure ZoneAlarm to work with VNC (Part 2):

- Open the ZoneAlarm window by double clicking on its tray icon (red and yellow ZA).

- Click on “Firewall” (left side of window) and then the “Zones” tab at the top

- Click “Add” and “Subnet”
INFORMATION TECHNOLOGIES (IT) 
STANDARD OPERATING PROCEDURE 
- Set “Zone” to “Trusted”; “IP Address” to 192.168.1.0; “Subnet Mask” to 255.255.255.0; and, “Description” to “CLASS LAN”

- Click “Apply” and close the ZoneAlarm window.

- Right click the ZoneAlarm tray icon (red and yellow ZA) and select “Shutdown ZoneAlarm” and confirm.

- Using “Start>Programs>Zone Labs>ZoneAlarm”, restart the ZoneAlarm program. The reason we do this is that ZoneAlarm will only remember certain setting (like Zones) if you shut it down and restart it … don’t ask me why.

D) Remove the VNC “viewer” application

- Using “Start>Programs>RealVNC”, delete (right click and select “delete”) the “Run VNC Viewer” icon. Confirm “short cut delete”. Note, the computer may “hang” here juts give it a couple of minutes and if it doesn’t respond, use Ctrl-Alt-Del to bring up the Task Manager and reboot.

- Using “Start>Programs>RealVNC”, delete (right click and select “delete”) the “Run VNC Viewer” folder. Clear the warning window.

- Go to the VNC folder (My Computer>Local Disk C: >Program files>RealVNC” and delete the vncviewer file. Empty the recycle bin.