Each department <u>needs</u> to SYSPREP their image before submitting it to eBryIt for deployment to new machines. The SID, or Security Identifier, needs to be removed from the master image, or in other terms, the image needs to be 'generalized' for duplication. SYSPREP updates the SID on duplicated machines and also removes any individuality of the installed image prior to duplication. This is <u>very important for security reasons</u>, individual driver databases for each machine, and installed software on each machine.

Please keep in mind that if you do not create an answer file for your master image, the new systems will be prompted for user interaction during the SYSPREP. The SYSPREPed system will ask for the user to enter the country, language, time zone and time, rename the machine, and force the user to add a new user which may need to be deleted after SYSPREP is finished. If there is wireless setup on the machine, SYSPREP will reset all wireless passwords, which will have to be re-entered during SYSPREP.

Here is a link containing a video on SYSPREPing a Windows 7 machine. eBryIT will be doing the Imagex portion of the process, (not actually using Imagex, but using Symantec Ghost). Instead of using the Quit option, use the Shutdown option and **<u>DO NOT</u>** turn the machine back on, or the SYSPREPed machine will have to be re-SYSPREPed.

http://technet.microsoft.com/en-us/windows/ee530017.aspx

**Windows 7 SYSPREP Technical Reference:**

http://technet.microsoft.com/en-us/library/dd744263(WS.10).aspx

**Here is the command line for SYSPREP on a Windows 7 System:**

```
sysprep.exe /generalize /oobe/ shutdown
/unattend:C:\Windows\System32\sysprep\sysprep.xml
```

**Here are some explanations on why you need to SYSPREP a machine before imaging, and a brief explanation of problems that may occur with duplicate SID's.**

<u>Microsoft's System Preparation Tool (SysPrep)</u>
Microsoft provides the SysPrep utility for preparing a source computer before creating an image of that computer. SysPrep allows you to change the SID, computer name, and other configuration information.

<u>The SID Duplication Problem</u>

The problem with cloning is that it is only supported by Microsoft in a very limited sense. Microsoft has stated that cloning systems is only supported if it is done before the GUI portion of Windows Setup has been reached. When the install reaches this point the computer is assigned a name and a unique computer SID. ***If a system is cloned after this step the cloned machines will all have identical computer SIDs***. NOTE that just changing the computer name or adding the computer to a different domain does not change the computer SID. Changing the name or domain only changes the domain SID if the computer was previously associated with a domain.

To understand the problem that cloning can cause, it is first necessary to understand how individual local accounts on a computer are assigned SIDs. The SIDs of local accounts consists of the computer's SID and an appended RID (Relative Identifier). The RID starts at a fixed value, and is increased by one for each account created. This means that the second account on one computer, for example, will be given the same RID as the second account on a clone. The result is that both accounts have the same SID.

According to Microsoft Knowledge Base article Q162001, "Do Not Disk Duplicate Installed Versions of Windows NT", in a Workgroup environment security is based on local account SIDs. Thus, if two computers have users with the same SID, the Workgroup will not be able to distinguish between the users. All resources, including files and Registry keys, that one user have access to, the other will as well.

Another instance where duplicate SIDs can cause problems is where there is removable media formatted with NTFS, and local account security attributes are applied to files and directories. If such a media is moved to a different computer that has the same SID, then local accounts that otherwise would not be able to access the files might be able to if their account IDs happened to match those in the security attributes. This is not possible if computers have different SIDs.