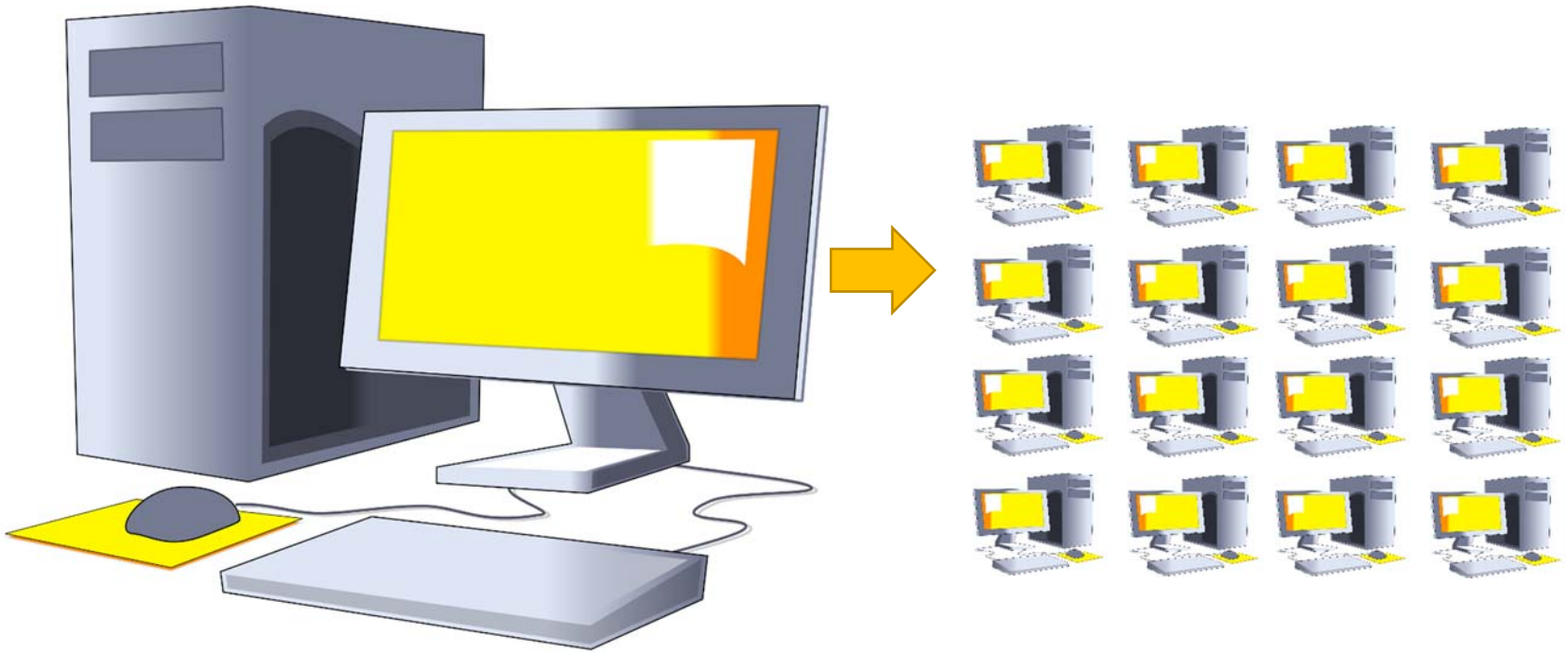
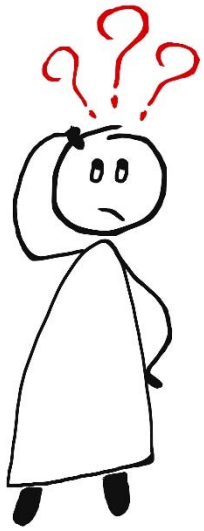
Designing a Reasonably Secure Computer Lab





Background information:
Preventing files from being saved to a disk is an important security consideration when viewing confidential or sensitive information.

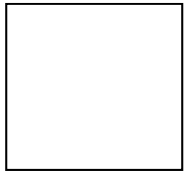
One such tool is Unified Write Filter (UWF) which we use in campus labs to keep student information secure. The main benefit of UWF over Deep Freeze is that it is simple to configure, and it is already built-into Microsoft Windows.

Unified Write Filter (UWF) is a software feature of Microsoft Windows which helps to secure computer systems. UWF prevents files on a computer from being persistently saved on any or all attached data storage.

Why do this?
By preventing data from being written to all disks it is reasonable to assume that any data which has been loaded securely through the network will be inaccessible once the computer has been turned off. In this way we can convert thick-client PCs to operate with security features of thin-clients.

Item Check List

- The most recent version of VirtualBox or VMWare Workstation
- Windows 7, 8, 10 installer disk or base image
- Any other Operating Systems (OS) which you desire
- pGina fork 3.9.9.7 or higher
- Lab computers which will load the template hard disk which we will make with VirtualBox or VMWare Workstation
- An Active Directory server or a user database that is LDAP compatible
- Disk cloning software
- Supplementary files available here: https://github.com/jaksco/Windows10_mgmt-tools



Check this big box once you have everything!

Alright! Let's go!

In this guide we will be using FOG Project server with Multicast configuration for the disk cloning software as well as Windows 10 for the base Operating System, however other alternatives exist which can be used. Please search online to find the best ones to use in your scenario.

GLOSSARY

OS	Operating System
UWF	Unified Write Filter
LDAP	Lightweight Directory Access Protocol
FOG Project	A network computer cloning and management solution

Step 1. Installing the Operating System(s)

MULTIPLE OPERATING SYSTEMS

The process of installing the Operating System will first begin with an evaluation of the needs of your computer lab.

Please ask yourself the following question: Does your computer lab have specific needs for users frequently using multiple Operating Systems?

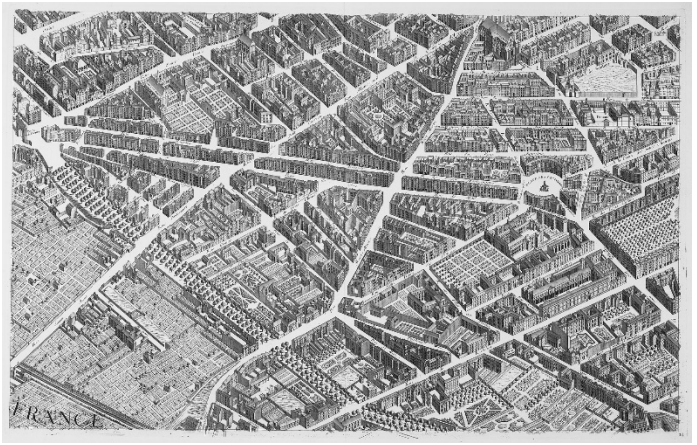
- If yes, you will need to be very careful as you complete this process in this guide.
- If no, you may want to use Microsoft Deployment Toolkit (MDT) to install and setup your Windows lab environment. It will be preferable to use MDT instead of VirtualBox or VMWare Workstation for this scenario. Please setup MDT then skip to Step 2.

! Please be sure to thoroughly evaluate the prior question as you may encounter difficulty installing another Operating System (dualboot or multiboot) once you use MDT.

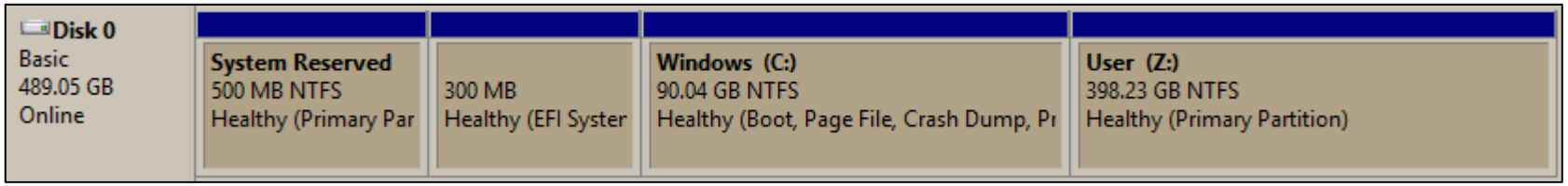
DISK PARTITIONING

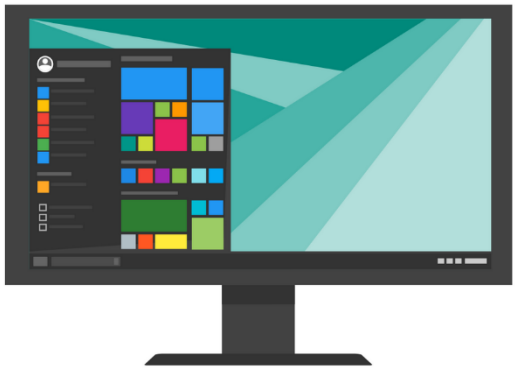
Next, you will need to determine the correct order for install the Operating Systems and the size of each hard disk partition each OS require for all your software and user data.

! Please double-check the size requirements for your scenario before you start. It will be difficult to change this later!



*TIP It may be helpful to draw out on paper a map of the partitions you plan to make before you begin installing.





INSTALLING THE OPERATING SYSTEMS

Please install the Operating Systems in the order that you determined in the prior section.

For a scenario which uses Windows and Linux, I recommend installing Windows first and then Linux. I recommend using the program grub-customizer to configure the boot menu after you have installed all Operating Systems.

> ! For a Linux OS install you will want to use a program such as ‘lethe’ to create the same environment that you will setup with UWF.

To Begin, download and install VirtualBox or VMWare Workstation. Then install the Operating System to a new virtual machine disk.

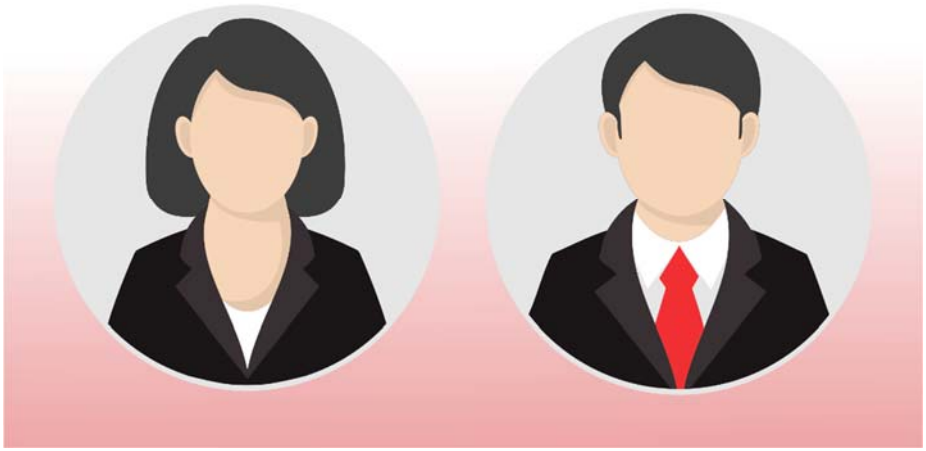
> ! This software will come in handy if we ever make a mistake while installing and configuring all of the software for the lab. Each will allow us to revert changes made from a previous snapshot, so it is important to make a snapshot after each step.

If you have any questions, refer to the installation manual of the specific Operating System or virtualization software you are installing.

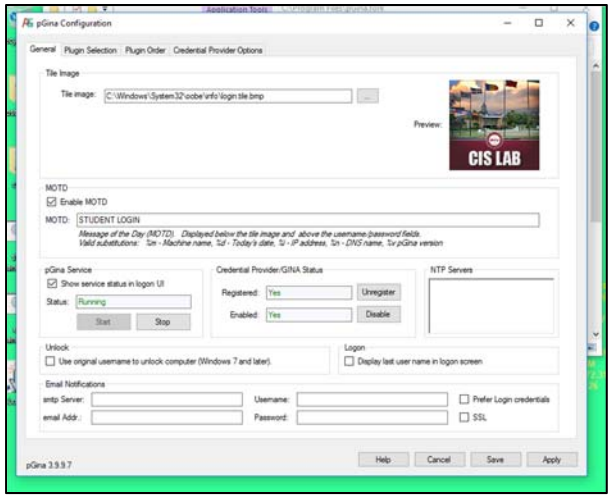
CREATE A SINGLE USER ACCOUNT FOR ALL YOUR USERS

- Use lusrmgr.msc to create a new local user that pGina will use to log users into.
- You should then setup a logoff script that restarts the computer.

NOTE:
With UWF enabled, this account will act as a template for each of your users. All the data will be reset on restart and thus the computer will be the same state for every new logon.



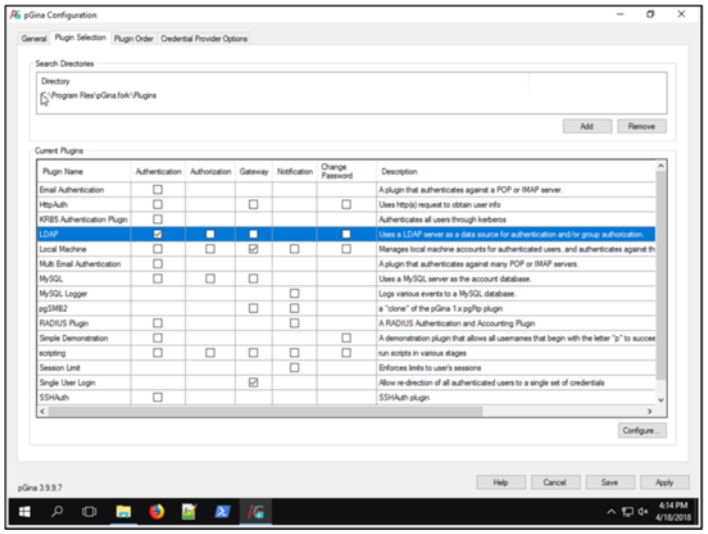
Step 2. Configuring pGina



After you have installed the Operating Systems you need to configure the software.

First, we need to install and configure pGina to connect to our LDAP database which contains username and password login information.

- Use the setup wizard to install pGina
- Register and Enable the Credential Provider
- Enable the LDAP plugin for Authentication
  - Configure the LDAP connection by typing in the LDAP host and port number of your LDAP server.
- Enable the Local Machine and Single User Login plugins for Gateway
  - In the Local Machine plugin ensure that the ‘Authorize all authenticated users’ checkbox is checked
  - In the Single User Login Plugin specify the local user account that you created in step 1.



Step 3. Configuring Unified Write Filter

The Unified Write Filter has a few options, so it is very helpful to go over the manual that Microsoft provides.

https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter

You will use UWF by running the following commands in an elevated command or PowerShell prompt.

- Specify the disks you wish to protect with ‘volume protect’
  - Example: uwfmgr volume protect c:
- Specify the overlay size. The overlay size is simply the amount of RAM UWF will use to temporarily save any files which normally are saved onto the disk.
  - Example: uwfmgr overlay set-Size 12288
- Specify file, folder, and registry exclusions. Please see supplementary files for a list of files which you should exclude by default.
  - Example: uwfmgr File add-exclusion c:_TaskSequence
  - Example: uwfmgr registry add-exclusion "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\StateSystem"
- Enable the overlay with ‘uwfmgr filter enable’

After completing this process, the configuration will always be remembered even if you disable the write filter.

Step 4. Preparing to Capture the Disk Template (disk image)

With Windows 10 and above, we will need to run a few commands before we will be able to successfully run the System Preparation Tool which Microsoft has created for preparing Windows installations to be duplicated.

These commands remove all uninstallable Universal Windows Platform (UWP) apps so that Sysprep will work correctly.

! If you need certain UWP apps for your organization, good luck! You will need to get down and dirty with the Universal Windows Platform and ensure that all user profiles' AppxPackages and AppxProvisionedPackages are all the same.

You will need to run the following commands in an elevated PowerShell prompt:

- Get-AppxPackage -allusers | Remove-AppxPackage
- Get-AppxProvisionedPackage -online | Remove-AppxProvisionedPackage -online

The System Preparation Tool (Sysprep) is a tool Microsoft wrote to help prepare systems for cloning. The Sysprep tool will generalize certain unique elements so that Windows will successfully reload itself onto a new system the next time it boots. When you are all done configuring the system, run the following command in an elevated command or PowerShell prompt:

- sysprep\Sysprep.exe /generalize /oobe /shutdown /unattend:C:\Users\config\Desktop\postimage\unattend.xml

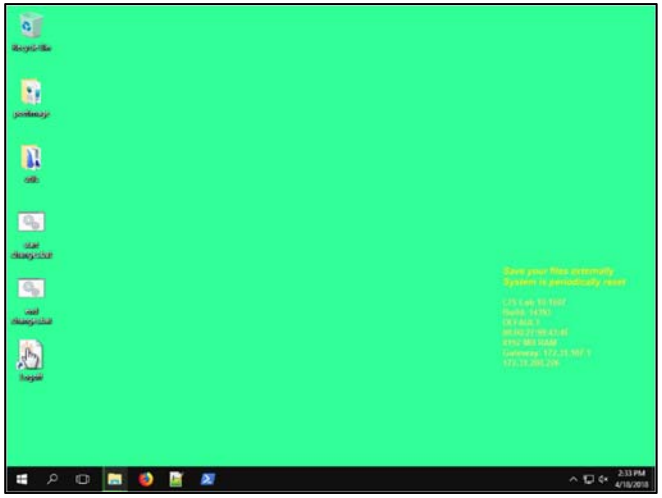
Step 5. Capturing and Deploying the Disk Template (disk image)

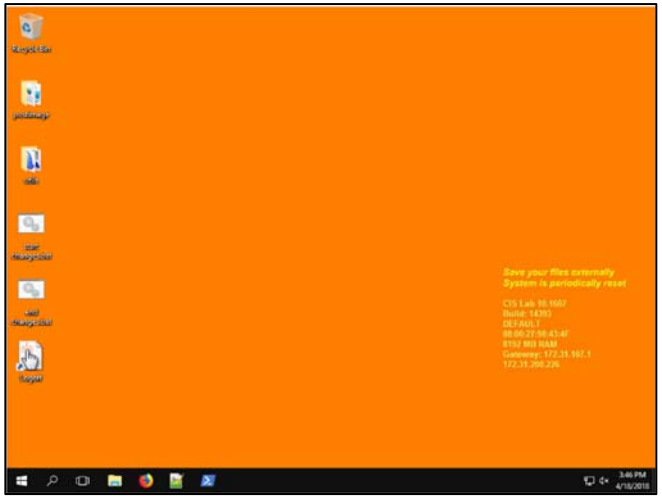
Now we finally deploy our finished disk template onto all the lab computers! It would be tedious to copy the hard disk one machine at a time, so we are going to speed things up quite a bit by using a network cloning solution which uses multicast to send the same data to all the computers at once!

There are many tools that enable us to do this, so you will need to refer to the instructions of your specific tool for your scenario. The steps are likely similar to the following:

- Transfer a copy of the disk template that we made in VirtualBox / VMWare Workstation to a multicast enabled network cloning and management solution.
- Turn on all computers and connect them to a cloning session.
- Allow the cloning to complete and the computers to reboot and run through the final stage of Sysprep.

Congratulations! You have successfully finished designing and deploying a reasonably secure computer lab!





MODIFYING THE SYSTEM AFTER DEPLOYMENT

It is very likely that you will eventually need to install a new program or update some software on a UWF enabled system. You can easily do this by creating two batch (.bat) files on the desktop of the admin account and run them when needed.

Begin_changes.bat:

```
{  start /wait uwfmgr filter disable
{  start /wait shutdown -r -t 0
{  pause
```

End_changes.bat:

```
{  start /wait uwfmgr filter enable
{  start /wait shutdown -a
{  start /wait shutdown -r -t 0
{  pause
```

It may be helpful to have the screen change colors depending on whether or not UWF is currently enabled. This way you can easily make sure that all lab computers will save the changes you are making to them. Please refer to the supplementary files to complete this task.

https://github.com/jaksco/Windows10_mgmt-tools