Install Microsoft Office Via Active Directory

1. First thing's first: **we have to group together all the users that will be installing Microsoft Office Suite.** Let's create an *Organizational Unit* to hold all of them.
    a. On Active Directory Users and Computers, right-click on your host network name and select *New*.
    b. Select *Organizational Unit.*
    c. Name your Organizational Unit (OU).
2. Now that we have the place for them, **let's assemble them all together**.
    a. Find the *Users* folder on the sidebar and open it up.
    b. Highlight all of the users in your domain, and then right-click.
    c. Select *Move* from the drop-down menu.
    d. Pick the OU you just made. This will place all those users into that OU.
3. Next, **we have to make the Microsoft Office Suite installer file accessible to those users**. In order to install the program, they'll have to be able to access the file.
    a. Create a file folder on your host computer to hold the Microsoft Office installer file. (NOTE: This file has to be a .msi file – not a .exe file – in order for it to be used by Group Policy, the next program we'll be using. You can be sure you've got the right file extension by right-clicking the file, choosing *Properties,* and noting the file extension next to *Type of File).*
    b. Move that Microsoft Office Installer file into your new file folder.
4. The folder has been created and filled with the necessary file. **We now have to make sure the folder is accessible to all of our users.**
    a. Right-click on the folder and press *Properties*.
    b. From that menu, click on the *Sharing* tab.
    c. Click on the *Advanced Sharing* button.
    d. Then, check the box that says *Share this folder.*
    e. Click *Permissions.*
    f. Click on *Everyone*.
    g. Look at the boxes at the bottom of the menu to make sure only one is checked: the one box in the *read* row and the *allowed* column. If all this is set up correctly, none of your users will be able to tamper with the software, just install it!
    h. To finish up here, press *OK* on this menu.
    i. On the next menu, press *Apply* and then *OK*. You should be back on the Properties menu for your shared folder.
    j. Before you're totally done with this step, copy the network path for the folder. You'll need that later on.
5. Now, we're totally prepped and ready to get Microsoft Office Suite installed on some computers. **We'll have to force every user to open the Microsoft Office Suite file Installer upon logging in.** We can use Group Policy, a program that allows us to make changes to multiple users at once, to do this.
    a. Open up Group Policy.
    b. In the sidebar, navigate to your domain and you'll see a *Group Policy Objects* folder. A *Group Policy Object* (GPO) is basically any task you can force your set

    of users or computers to do, from installing a program to downloading a wallpaper.

    c. Right-click *Group Policy Object.*
    d. Click *New*. It’ll ask you to give your Group Policy Object (GPO) a name. Name it something straightforward, like *Microsoft Office Software Installation,* and press *OK.*

6. We’ll see that new GPO on the sidebar under your domain’s group policy objects. Now, **we’ll have to define exactly what the GPO will do to your user’s computers.**
    a. Left-click on your new GPO.
    b. Right-click and choose *Edit.*
    c. A new screen will appear, but with a similar sidebar to the last one. There, you’ll find a dropdown arrow for *User Configuration*. Click that.
    d. Click the arrow next to *Policies.*
    e. Finally, click the arrow next to *Software Settings.*
    f. You’ll see an object titled *Software Installation.* Right-click on that.
    g. Select *Properties*.
    h. You’ll see an empty task bar under *Default Package Location*. That’s where you’ll paste the network path you copied a couple steps ago.
    i. Press *Apply* and then *OK* to exit out of this menu.
7. So, we’ve created the GPO that will tell the computers what to do: install a software file. **We need to give the computers the file to install.**
    a. Back in the Group Policy Editor, right-click in the big empty space that says *There are no items to show in this view.*
    b. Highlight *New.*
    c. Click *Package.* The window that appears should automatically show the shared folder you created with the Microsoft Office Suite installer file in it.
    d. Double click on that file to select it.
    e. Now, you’ll see a menu asking which method the computer will use to deploy the software and install the program. Click the circle next to *Assigned* and then *OK.*
    f. You should see the Microsoft Office Suite Installer in the space that was previously empty.
8. We’ve successfully established what we want the users to do (install software), which file to use (the .msi Microsoft Office file), and where the file is (the shared folder we made). **We just have to link the GPO we just made with the Organizational Unit we made before that contains the big list of users in your domain**. This is selecting which users the task will run for.
    a. Close the Group Policy editor and you’ll be back on the main Group Policy Manager menu.
    b. Right click the OU and select *Link an Existing GPO.*
    c. In the menu that appears, you should find the Microsoft Office Suite Installer GPO you just made. Click on that, and then click *OK*.
9. You have officially prepared your user base to install Microsoft Office Suite! For the final step, **we’ll have to force the user computers to update their systems for your new GPO.**

   a. In the Group Policy Editor, find the OU that contains all of the users in your domain.
   b. Right click on that OU and click *Group Policy Update.* A new dialog box will appear.
   c. Click *Yes.* A new menu will appear, this time with a progress bar.
   d. Once that progress bar is full and all the computers have been force updated, click *Close*.
   e. Now, each of the users in your domain will be forced to update their computers for your GPO. After restarting, **all of your users will have Microsoft Office Suite installed!**

What are some resources available on a normal Windows workstation that should be blocked to avoid allowing end-users to damage the operating system or other critical files and how can an administrator accomplish this goal?

We can use Group Policy – the program we used for the previous set of instructions – to apply administrator preferences and lock down user devices to prevent any kind of tampering or damage.

1. The first thing we can do is **prevent users from accessing the Control Panel.** The Control Panel allows users to change certain hardware and software settings.
   a. Open Group Policy Editor.
   b. Under *User Configuration* in the sidebar menu, click the arrow next to the folder labeled *Administrative Templates*.
   c. Click the folder labeled *Control Panel.* You'll see a list of policies you can apply to the computers in your domain.
   d. Click the one titled *Prohibit access to Control Panel and PC settings.* A new menu will appear.
   e. Check the bubble labeled *Enabled.*
   f. Click *Apply* in the bottom-right corner of the menu.
   g. After exiting out of this menu, you should see *Enabled* under the *State* column in the Control Panel settings folder next to *Prohibit access to Control Panel and PC settings*. After your user computers are updated, they will no longer have access to any computer's Control Panel.
2. Another step we can take is **preventing users from accessing the command prompt.** Every Windows operating system is equipped with a command prompt application that allows users to run tasks and execute commands.
   a. Under *User Configuration* in the sidebar menu on Group Policy, click the arrow next to the folder labeled *Administrative Templates*.
   b. Click the folder labeled *System*. You'll again see a list of policies you can apply to the computers in your domain.
   c. Click the one titled *Prevent access to the command prompt.*
   d. Check the bubble labeled *Enabled*.

e. Under *Options*, you'll see a dropdown menu under a question which asks *Disable the command prompt script processing also?* Make sure it says *Yes*.
f. Click *Apply* in the bottom-right corner of the menu.
g. After exiting out of this menu, you should see *Enabled* under the *State* column in the System Settings folder next to *Prevent access to the command prompt*. Now, your users won't have access to the command prompt, either.

3. There's another thing we can do in the System settings folder: **we should prevent users from accessing the computer's registry.** The registry contains sensitive information the computer will use while it's operating.
   a. Under the System settings menu in Group Policy, click the policy labeled *Prevent access to registry editing tools.*
   b. In the menu that appears, check the bubble labeled *Enabled*.
   c. Under *Options*, you'll see a question asking *Disable regedit from running silently?* Make sure it says *Yes* in the dropdown menu below it.
   d. Click *Apply* in the bottom-right corner of the menu.
   e. After exiting out of this menu, you should see *Enabled* under the *State* column in the System Settings folder next to *Prevent access to registry editing tools*. Now, your users won't have access to the command prompt, either.
4. Lastly, **we want to prevent users from running any kind of software available on a standard windows operating system that could potentially damage the computer.** One of such programs is Microsoft Powershell, a sort of advanced version of the command prompt.
   a. Open Group Policy Editor.
   b. Click the arrow next to *Computer Configuration.*
   c. Click the arrow next to *Windows Settings*.
   d. Click the arrow next to *Security Settings.*
   e. Find the folder labeled *Software Restriction Policies.* Right-click that and press *New Software Restriction Policies*.
   f. Right-click the folder that appears on the sidebar labeled *Additional Rules* and click *New Hash Rule*.
   g. On the new dialog box that appears, make sure the dropdown menu next to *Security Level* reads *Disallowed*.
   h. Now, we'll have to find Powershell. Click *Browse*.
   i. Navigate through the file explorer. The folder for Powershell should be under **Local Disk (C:) > Windows > System32.**
   j. Find the file labeled *powershell.exe*. Select it and press *Open*.
   k. Click *Apply* in the bottom-right corner of the menu and then *OK.* Now, upon being updated for this policy, your user's computers won't have access to Powershell.

HERE'S A TIP: You can use this method to disable the use of any program you'd like! All you have to do is find the exact location of the program file in your computer via step *4-i*.

5. Once you've finished adding all the security and protection settings you need via Group Policy, **it's time to force a Group Policy Update on your domain's computers.** These

directions are the same as step 9 in the previous set of instructions, and there's no need to do this twice. However, we'll go over them again just to be sure.

a. In the Group Policy Editor, find the OU that contains all of the users in your domain.
b. Right click on that OU and click *Group Policy Update.* A new dialog box will appear.
c. Click *Yes.* A new menu will appear, this time with a progress bar.
d. Once that progress bar is full and all the computers have been force updated, click *Close*.
e. Now, each of the users in your domain will be forced to update their computers for your GPO. After restarting, **all of your users will have your security preferences enabled!**