Summary:

This procedure will outline the steps to configure an autologin policy for domain-joined computers. Autologin, in this case, is defined as a service account that is used to automatically log into a computer upon the computer’s startup. This procedure is followed best while using the IT Jump server.

When to implement autologin:

* The computer is a shared computer designated for lab or kiosk use
* Manually logging into a computer may require de-gowning/de-gloving

Procedure Overview:

This procedure can be broken down into three steps.

* Step 1: Configure the group policy
* Step 2: Configure the Autologin .cmd file
* Step 3: Update the startup script properties to incorporate the .ps1 file

Setup:

* Step 1: Configure Group Policy
  + In AD navigate to the OU of where the autologin computer will exist and create/move the computer there. The autologin computer should not share the same OU as the other departmental computers since this computer will have unique group policies. In this example, we will use computer “SD-LT-EHSACT” located in: TriLinkSD > Computers > Org > G&A > Facilities > Contractor. Notice how this Facilities computer is segregated from the other Facilities computers in its own OU so it can pull individual policy without affecting other computers.

Graphical user interface, application, Word

Description automatically generated

* + Next, let’s make some policies. Pull open the Group Policy Management mmc and navigate to the OU of which we are setting up for autologin. There are three policies that need to be applied here, two of which can be directly applied without editing. However, one of the three policies will require some manual tuning for autologin to work. Go ahead and apply the two policies, “Sleep – Disable Require Password Upon Wake +0 inactivity limit” and “Start Menu – Remove Lock and Sleep Option from Start Menu”.

Text

Description automatically generated

* + “Sleep – Disable Require Password Upon Wake +0 inactivity limit” is what forces the computer to stay logged in to its session.
  + “Start Menu – Remove Lock and Sleep Option from Start Menu” removes the lock and sleep option from the windows start menu. Just because the accounts are auto logging in, does not necessarily mean that the computer cannot be locked or logged out of. These computers may still be locked/logged out of via task manager or a command in cmd.exe but this policy eliminates the chance of an accidental logout if a user is moving too quickly on the start menu. If they were to click sleep or lock, the user would need to reboot the computer at that point. Removing the sleep and lock options removes this chance of error.
  + Text

    Description automatically generatedThe third policy, and more intricate of the three, is the meat and potatoes of the process. “Autologin – Facilities Contractors” calls a powershell script at the computer’s startup that calls a .cmd file implementing the Autologin configuration on the computer. This policy should be named in the format of “Autologin - %departmentName% or %purpose%” as a way of distinguishing what the policy’s purpose is and who it is intended for. See for example the current Autologin Policies in the below image:
  + One could certainly create a new Autologin Policy from the ground up. But it is much easier to right-click > Copy an existing Autologin policy, and right-click Group Policy Objects > Paste. Then rename the duplicated policy to suit the department it is serving. Following the current example, one would copy one of the already made policies and rename it to “Autologin – Facilities Contractors”

Rename to:



* Step 2: Configure the Autologin .cmd file
  + Next, navigate to [\\trilinksd.local\SYSVOL\trilinksd.local\scripts\Autologin](file:///\\trilinksd.local\SYSVOL\trilinksd.local\scripts\Autologin). This is where the .cmd file is located for each autologin deployment. Make a folder here for the corresponding department. Following up on our example, we copied an existing folder and renamed the copy to “Facilities”. Inside the copied folder, you’ll see a autologin.cmd file. **Edit** the file and you will see the actual command that is being executed during the startup.
  + A picture containing background pattern

    Description automatically generatedThe autologin executable accepts the parameters /accepteula, username, domain, and password. For security reasons, the password has been blurred out in the picture. You can take this time to make a service account in AD under TriLinkSD > Service Accounts to the format of “al.%Department%%Purpose%%Number%”. Pictured are examples of the autologin service accounts currently used in AD.

Please include a good description when making accounts like this. The password should be randomly generated. Record of the password in the notes section of the Telephones tab in the user object. Under the account tab, click “Log On To…” and specify the computer it is allowed to login to. This ensures the account is not being abused. In this example, we would use computer “SD-LT-EHSACT” Once the account is provisioned, replace the credentials (username and password) on the autologin.cmd file opened from the previous step and save the file. That completes the .cmd step.

* Step 3: Update the startup script properties to incorporate the .ps1 file
  + Next, **edit** the policy and drill down to Computer Configuration > Windows Settings > Scripts > Startup. Double-click startup and then > show files. You will be presented with the .ps1 file that implements autologin. Rename the .ps1 file to the format of “Autologon%Department%%purpose%. Next, **edit** the renamed .ps1 file. On line 9 you will see the directory of the autologon.cmd. Change the referenced directory in the PowerShell script to call the .cmd modified in the previous step. In this example, we are calling the Autologon.cmd for Facilities Contractors under the directory: [\\trilinksd.local\SYSVOL\trilinksd.local\scripts\Autologin\Facilites\](file:///\\trilinksd.local\SYSVOL\trilinksd.local\scripts\Autologin\Facilites\)
  + The last step is to modify the startup policy parameters to reference the new .ps1 file. Since the GPO was copied, it will have the copied original GPO’s parameters. **Edit** the policy. Under the startup properties click **Edit** and under Script Parameters, replace the pre-filled .ps1 with the name of the .ps1 file renamed in the previous step. You can click on “Show Files…” a second time to view the renamed .ps1.

Graphical user interface, text, application

Description automatically generated

* + After these steps are complete, perform a gpupdate /force on the computer to ensure it pulls the new policy.
  + After a reboot or possibly two reboots, the computer will autologin as intended.