Allow domain user run batch files only from specific network folder

serverfault.com/questions/1047675/allow-domain-user-run-batch-files-only-from-specific-network-folder

You can implement Applocker policies via GPO and can use it to restrict or allow scripts/exes/apps/dlls

You need to create a new GPO in which you'll need to navigate to "Computer Configuration" > "Policies" > "Windows Settings" > "Security Settings" > "Application Control Policies" -> "Applocker"

Enforcement

First you need to "Configure rule enforcement" there you need to set the checkmark at "Script Rules" and can decide between "Enforce Rules" and "Audit only".

Enforce Rules is used to force the computer to respect the rules while "Audit only" simply generates a Windows Event which will indicate if the current rules will block or allow something to run. It is recommended to use "Audit only" until it is clear whether enabling the rules will break something important.

Rules

There you have the different categories

- Executable Rules
- Windows Installer Rules
- Script Rules
- Packaged App Rules

In your case you need to edit Script Rules. Those rules will be enforced for e.g. `ps1` or `bat` files (see here for more)

When editing a ruleset for the first time Windows should prompt if you want to add the default rules normally those rules should not break anything and can be added without worrying too much.

Applocker policies will by default fail close This means if you don't have policies defined to handle normal use cases those will be blocked!

Then you can create a new rule by right-clicking either on "Script Rules" and then clicking on "Create New Rule...".

The rule creation dialog is more or less self explanatory. What you want is a "Path Rule" which will allow scripts to run from a given path.

Be aware that `\\server` and `\\server.fqdn.com` are different paths

Enabling Applocker

For Applocker to run at all there are a few conditions which will need to be met.

1. You either need Windows 10 Education or Enterprise if you want to manage it via GPO 1.1. If you don't you can still administer Applocker via powershell.
2. You need to enable and autostart the "Application Identity service"