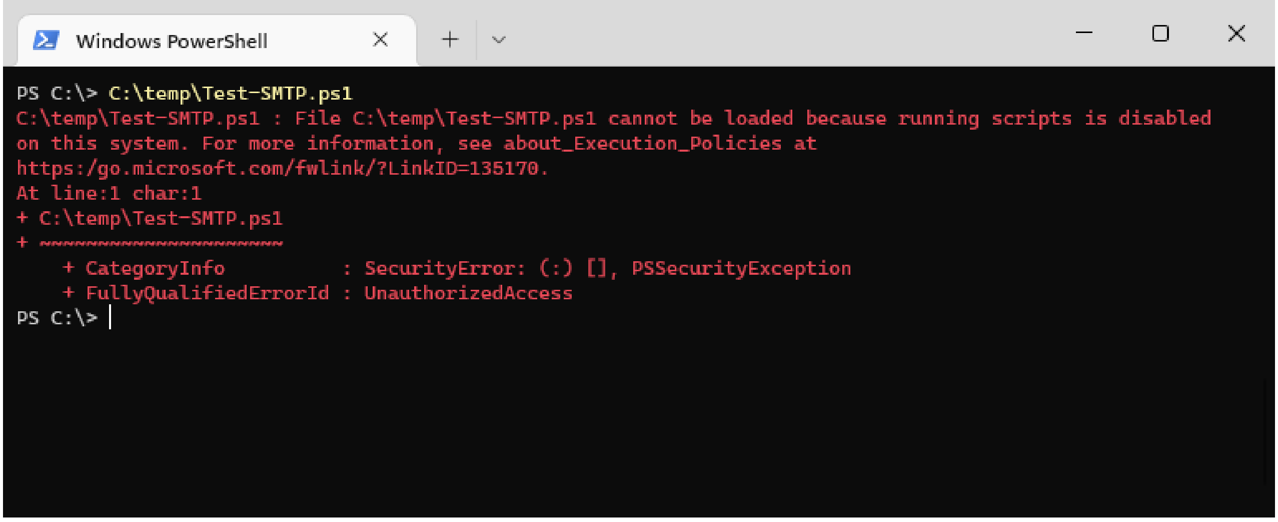
How to fix “Running Scripts is Disabled on this System”

lazyadmin.nl/powershell/running-scripts-is-disabled-on-this-system

October 11, 2022

Trying to run a PowerShell script, and do you get the error **“Cannot be loaded because running scripts is disabled on this system”**? Then we need to change the execution policy in PowerShell. To protect your computer from malicious scripts, the execution policy of PowerShell is set to restricted by default.



```
PS C:\> C:\temp\Test-SMTP.ps1
C:\temp\Test-SMTP.ps1 : File C:\temp\Test-SMTP.ps1 cannot be loaded because running scripts is disabled
on this system. For more information, see about_Execution_Policies at
https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ C:\temp\Test-SMTP.ps1
+ ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\> 
```

Cannot be loaded because running scripts is disabled on this System

This default setting will prevent you from running any PowerShell script on your computer, even scripts that you have written yourself. Luckily we can easily change the policy with a single command in PowerShell.

In this article, I will explain how you can quickly fix the error running scripts are disabled on this system, what the different policies are and how to change it on all computers with a Group Policy.

Fix Running scripts is disabled on this System

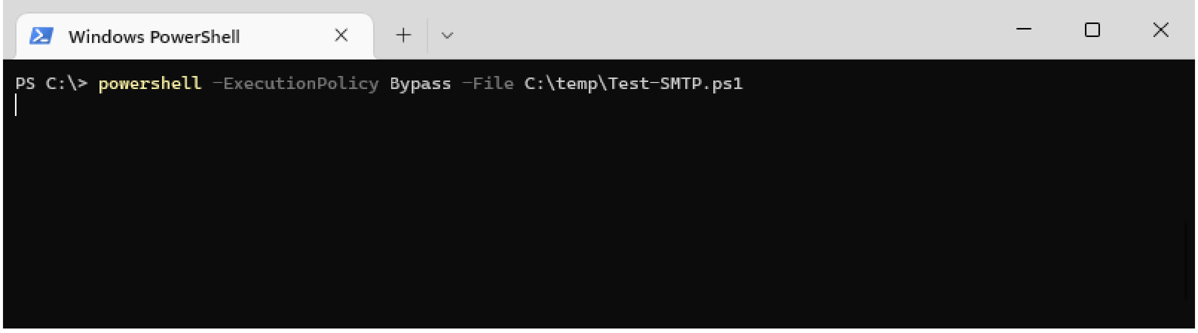
We are going to start with a quick fix. The method below only solves the issue temporarily, so you can run your script and continue. For a more sustainable solution, scroll a bit down to the next chapter.

1. **Open PowerShell or Windows Terminal**

]

2. **Enter the command below to run your script**

   powershell -ExecutionPolicy Bypass -File script.ps1



```
PS C:\> powershell -ExecutionPolicy Bypass -File C:\temp\Test-SMTP.ps1
```

The method above bypasses the execution policy only temporarily. This works great for a single file, but it requires you to use the command above every time that you want to run the file. A more sustainable solution is to change the execution policy.

Changing the Execution Policy Permanently

When you work a lot with PowerShell scripts then you probably want to change the Execution Policy permanently. But before we look into how to change the policy, let's first explain its purpose and the different policies that are available.

The execution policy isn't designed as a security system to restrict users from executing PowerShell scripts. Each user can simply bypass the policy in their current PowerShell session or even copy and paste the content of the script directly into the console. So what is the purpose of the policy then? Well, it's designed to prevent unintentional execution of PowerShell scripts.

When changing the policy we have five options to choose from:

Execution Policy	Description
Restricted	***Default option*** – Does not allow to run any PowerShell script
Unrestricted	Can run any script, shows warning for downloaded scripts
RemoteSigned	Requires a digital signature for downloaded scripts. You can run locally written scripts. You can unblock downloaded scripts to run them without signature
ByPass	You can run all scripts and no warnings are displayed
AllSigned	You can only run signed scripts from trusted publishers

PowerShell Execution Policies

Most people tend to set the policy to unrestricted, which allows you to run any PowerShell script. But a better option is to use the RemoteSigned policy. This way you can run any locally written scripts, but you will have to unblock all downloaded scripts first. The extra handling prevents users from accidentally downloading and running malicious PowerShell scripts on their system.

All users vs Current user

When changing the policy we can also determine the scope of the change. The following scopes are available for the policy:

Scope	Description
CurrentUser	The policy is only set for the currently logged-in user
LocalMachine	Policy is changed for all users on the machine
Process	Policy is only changed for the current PowerShell session

Execution Policy Scopes

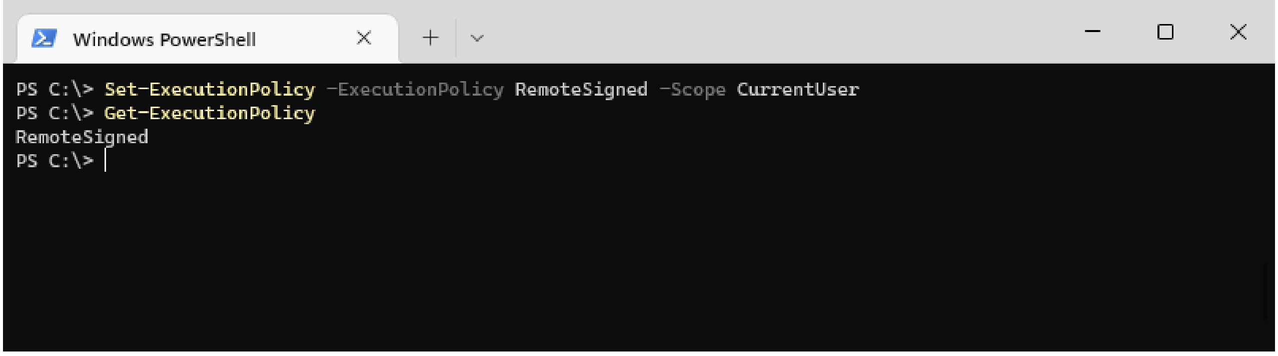
Set Execution Policy for Current user

So the most common scenario is that you want to change the PowerShell Execution policy for the current user. This will solve the error “running scripts is disabled on this system” for the logged-in user. We will set the policy to **RemoteSigned**, which means that the user still has to perform an extra step for downloaded scripts.

1. Open **PowerShell**
2. **Enter the command below** and press **enter**

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

3. Optional – Verify the setting with the command `Get-ExecutionPolicy`

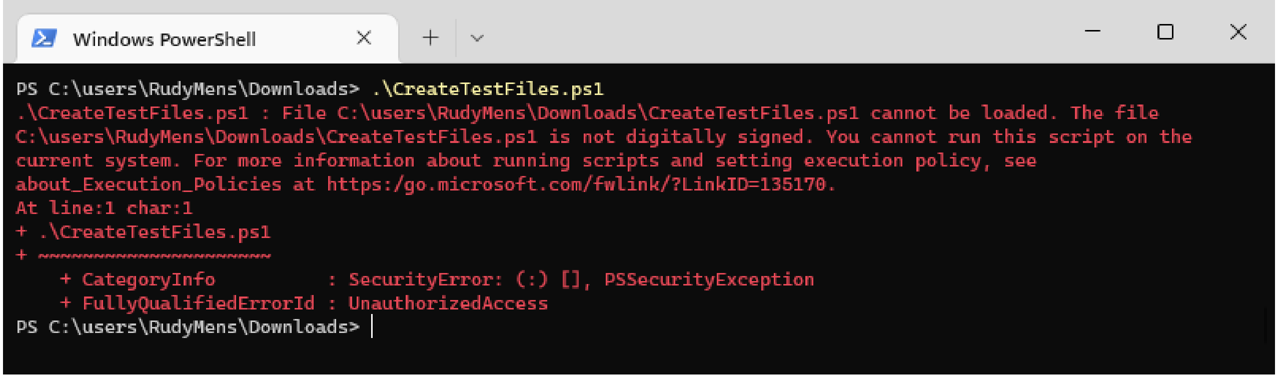


```
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
PS C:\> Get-ExecutionPolicy
RemoteSigned
PS C:\>
```

Set Execution Policy

You can now run any locally created PowerShell script without the error **running scripts is disabled on this system**.

When you try to run a downloaded PowerShell script with the execution policy RemoteSigned, then you get the error that the file cannot be loaded. The PowerShell script is not digitally signed:

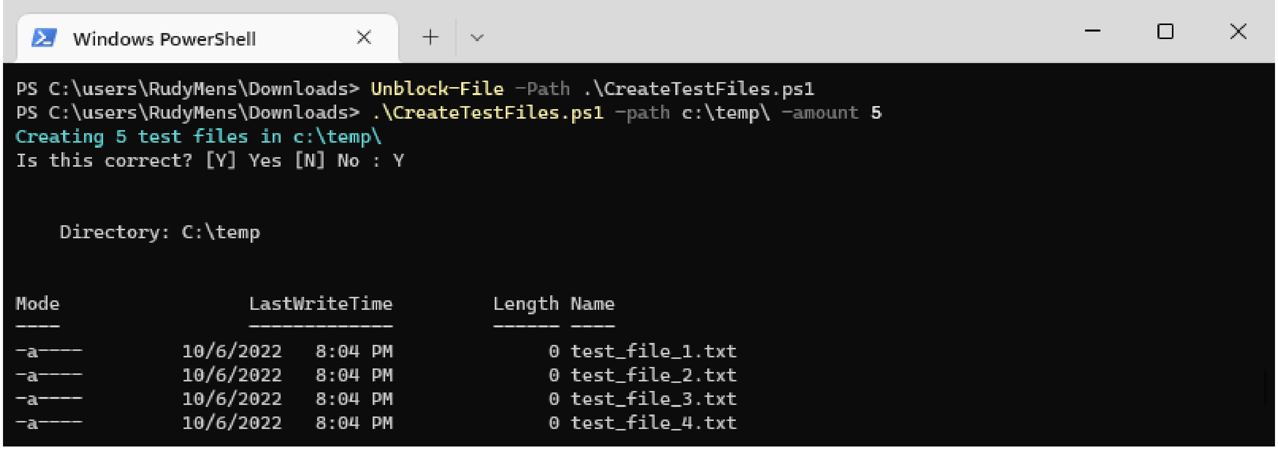


```
PS C:\users\RudyMens\Downloads> .\CreateTestFiles.ps1
.\CreateTestFiles.ps1 : File C:\users\RudyMens\Downloads\CreateTestFiles.ps1 cannot be loaded. The file
C:\users\RudyMens\Downloads\CreateTestFiles.ps1 is not digitally signed. You cannot run this script on the
current system. For more information about running scripts and setting execution policy, see
about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\CreateTestFiles.ps1
+ ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\users\RudyMens\Downloads> |
```

Not digitally signed

To solve this you will first need to unblock the file. To do this we can of course use a PowerShell cmdlet, `Unblock-File`. Simply type the cmdlet followed by the filename/path:

Unblock-File -path .\CreateTestFiles.ps1

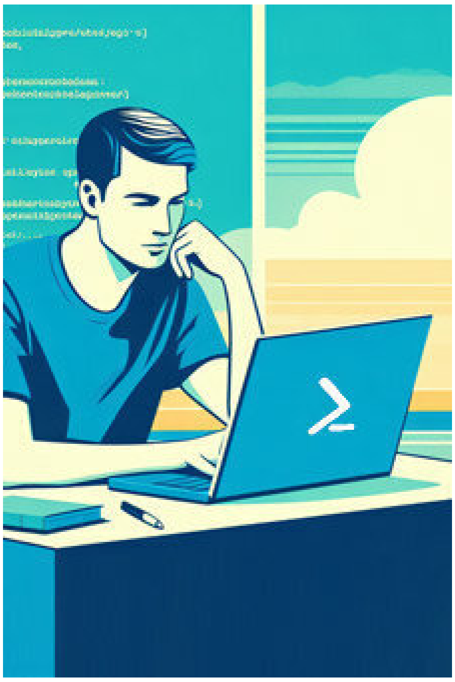


```
PS C:\users\RudyMens\Downloads> Unblock-File -Path .\CreateTestFiles.ps1
PS C:\users\RudyMens\Downloads> .\CreateTestFiles.ps1 -path c:\temp\ -amount 5
Creating 5 test files in c:\temp\
Is this correct? [Y] Yes [N] No : Y


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/6/2022   8:04 PM              0 test_file_1.txt
-a----         10/6/2022   8:04 PM              0 test_file_2.txt
-a----         10/6/2022   8:04 PM              0 test_file_3.txt
-a----         10/6/2022   8:04 PM              0 test_file_4.txt
```

Unblock remote files

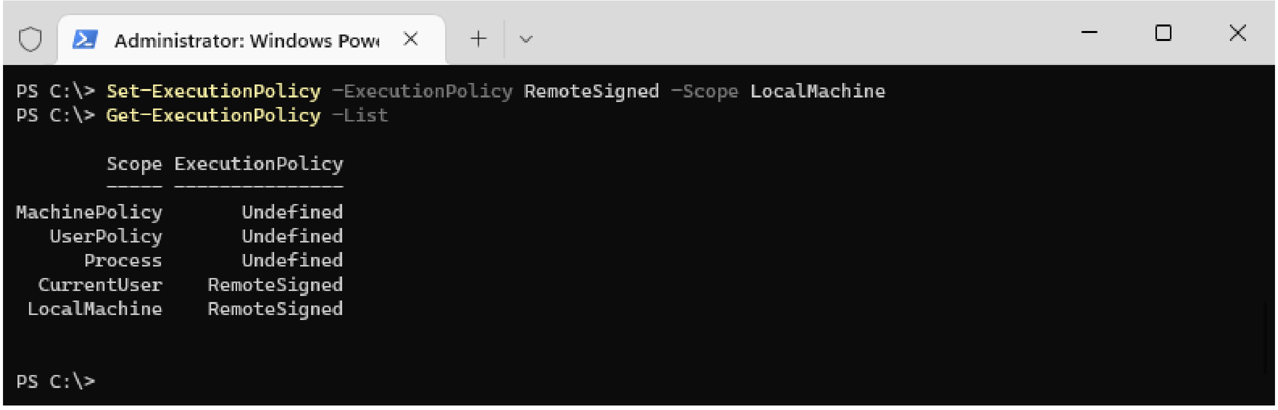


Set Execution Policy for all Users

We can also change the policy for all users on a computer. To do this, you will need to have elevated permissions (Administrator permission).

1. **Right-Click on Start** or press **Windows key + X**
2. Choose **Windows PowerShell (Admin)** or Windows Terminal (Admin)
3. Type the following command:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine



```
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine
PS C:\> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser    RemoteSigned
 LocalMachine    RemoteSigned


PS C:\>
```

Set-ExecutionPolicy

We can verify the results with the cmdlet `Get-ExecutionPolicy -List` which shows the policy for each scope. Good to know is that the CurrentUser policy takes precedence over the LocalMachine policy. So when you set the CurrentUser policy to restricted and LocalMachine to RemoteSigned, then the user still can’t execute any PowerShell script, because the policy set in the CurrentUser scope overrules the LocalMachine policy.

Change the policy only for the Current Sessions

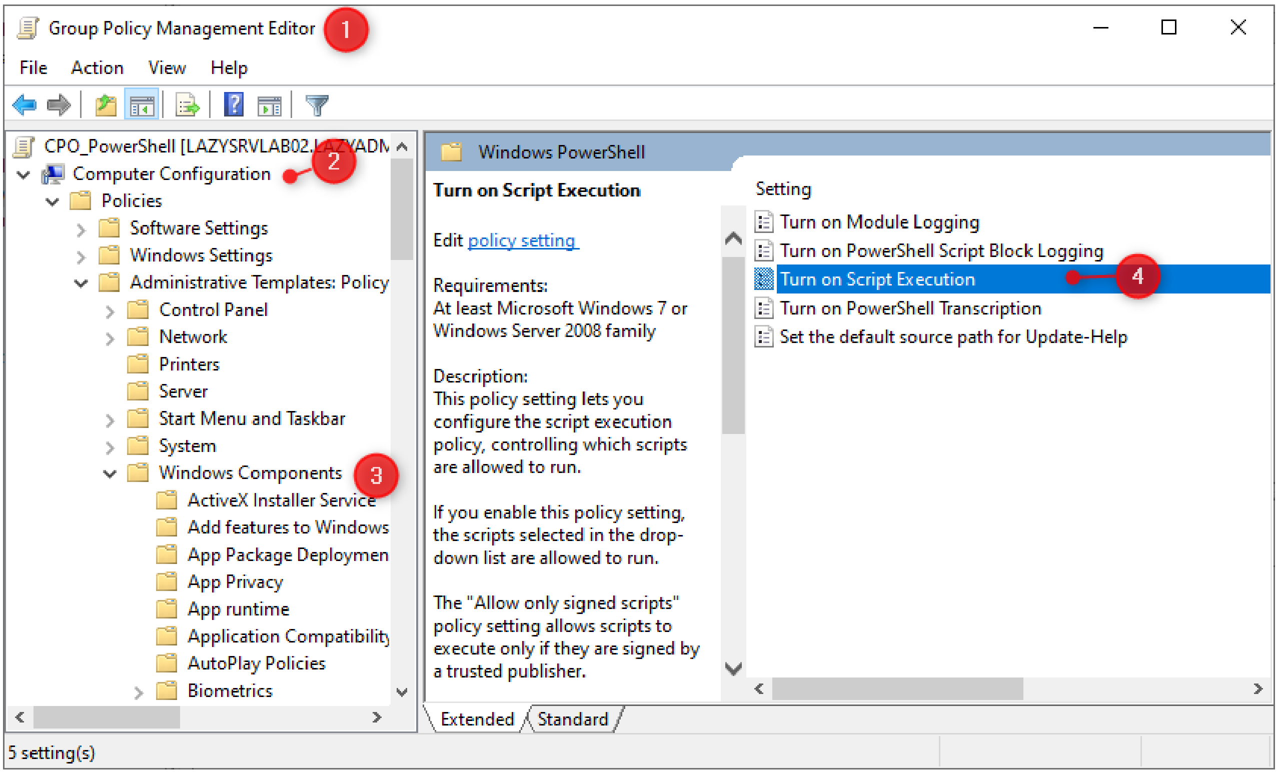
Another option is to change the policy only for the current PowerShell session. This method is useful when you need to run a couple of PowerShell scripts, but don't want to change the policy permanently. You could use the Bypass option for each script, but it's thus also possible to set change the scope for only the current PowerShell session. Use the scope `Process` for this:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process

Set Execution policy PowerShell with GPO

When you need to modify the policy on multiple computers, then it's a good idea to use a Group Policy for this. Group Policies allow you to change Windows settings on multiple computers that are members of a domain. Another advantage of the policy is that the setting can't be overwritten on the computer.

1. Open the **Group Policy Management Editor** and create a new policy.
2. Expand Computer Configuration
3. Navigate to **Policies > Administrative Templates > Windows Components > Windows PowerShell**
4. Open the setting **Turn on Script Execution**



Turn on Script Execution

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

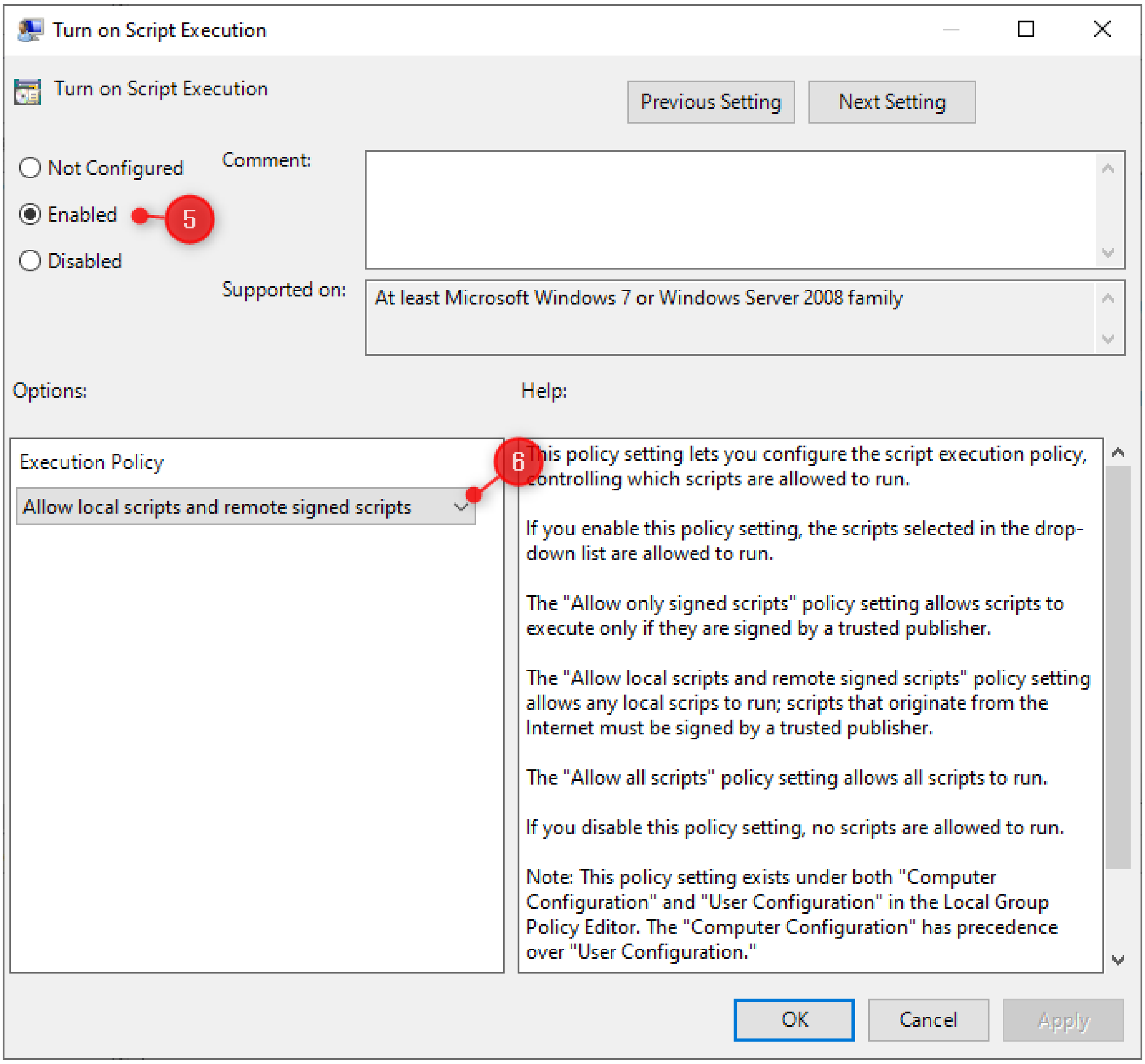
Description:
This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.

If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.

The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.

Setting
- Turn on Module Logging
- Turn on PowerShell Script Block Logging
- Turn on Script Execution
- Turn on PowerShell Transcription
- Set the default source path for Update-Help

5. Change the setting to **Enabled**
6. Select the **Execution Policy Allow local scripts and remote signed scripts**. This is the same as *RemoteSigned* that we set earlier.



Turn on Script Execution

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Execution Policy: Allow local scripts and remote signed scripts

Help:

This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.

If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.

The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.

The "Allow local scripts and remote signed scripts" policy setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.

The "Allow all scripts" policy setting allows all scripts to run.

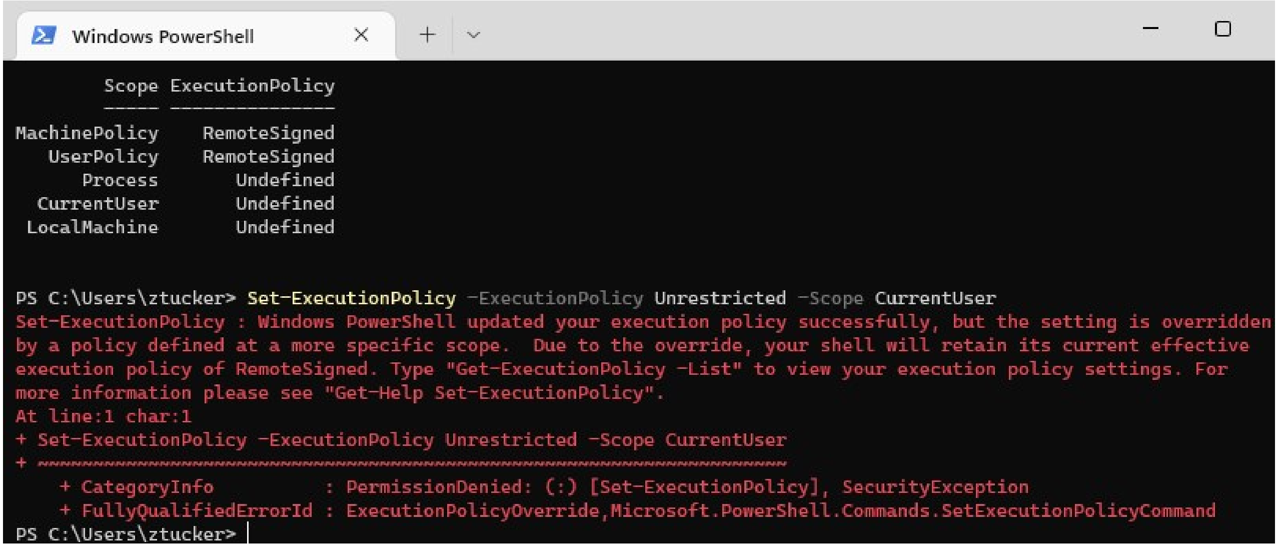
If you disable this policy setting, no scripts are allowed to run.

Note: This policy setting exists under both "Computer Configuration" and "User Configuration" in the Local Group Policy Editor. The "Computer Configuration" has precedence over "User Configuration."

We can verify the setting on one of the clients that are a member of the OU where we just applied the setting. First, make sure that the latest policy is applied on the computer using the GPUpdate command. Optionally you can use the RSOP command to verify the policy, or just check if the execution policy is set with the command:

```
Get-ExecutionPolicy -list
# Result
Scope ExecutionPolicy
----- ---------------
MachinePolicy RemoteSigned
UserPolicy RemoteSigned
Process Undefined
CurrentUser Undefined
LocalMachine Undefined
```

As mentioned, the advantage of the policies is that users can’t change the policy anymore. When you use the cmdlet **set-executionpolicy**, you will get an error that the policy is changed, but the setting is overridden by a policy defined at a more specific scope:



```
        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy    RemoteSigned
   UserPolicy    RemoteSigned
      Process       Undefined
  CurrentUser       Undefined
 LocalMachine       Undefined


PS C:\Users\ztucker> Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
Set-ExecutionPolicy : Windows PowerShell updated your execution policy successfully, but the setting is overridden
by a policy defined at a more specific scope.  Due to the override, your shell will retain its current effective
execution policy of RemoteSigned. Type "Get-ExecutionPolicy -List" to view your execution policy settings. For
more information please see "Get-Help Set-ExecutionPolicy".
At line:1 char:1
+ Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], SecurityException
    + FullyQualifiedErrorId : ExecutionPolicyOverride,Microsoft.PowerShell.Commands.SetExecutionPolicyCommand
PS C:\Users\ztucker>
```

Wrapping Up

The best way to set the Execution Policy in PowerShell is to use the Group Policy. This way all existing and new machines in your domain can be configured with the correct policy. Of course, you can create a different policy for the IT department.

I hope this article helped you to solve the error “cannot be loaded because running scripts is disabled on this system”, if you have any questions, then just drop a comment below. If you want to learn more about PowerShell, then make sure you read this getting started guide.

Did you **Liked** this **Article**?
Get the latest articles like this **in your mailbox**
or share this article

I hate spam to, so you can unsubscribe at any time.