

Live Response and Forensics with PowerShell

Using Execution Policies to Control PowerShell



Liam Cleary

Microsoft MVP and Microsoft Certified Trainer at SharePlicity

@helloitsliam | www.helloitsliam.com



Overview

Goal: Understand Execution Policies

- Review execution policies
- Set execution policies
- Understand the impact of execution policies





Review Execution Policies



Execution Policy

PowerShell's execution policy is a safety feature that controls the conditions under which PowerShell loads configuration files and runs scripts. This feature helps prevent the execution of malicious scripts.



Execution Policies for Windows

1

Support setting an execution policy for the local computer, current user, or session.

2

Execution policies for the local computer and current user save into the registry. The session execution policy is in memory and lost after the session expires or closes.

3

Execution policies don't restrict user actions; users can bypass a policy by typing the script contents directly into the command line.



Execution Policies for Non-windows

1

The default execution policy is unrestricted and cannot be changed.

2

PowerShell displays a console message that it's not supported.

3

Unrestricted on non-Windows platforms match bypass because those platforms do not implement Windows security zones.





**Enforcement of These Policies Only Occurs on
Windows Platforms**



Execution Policies



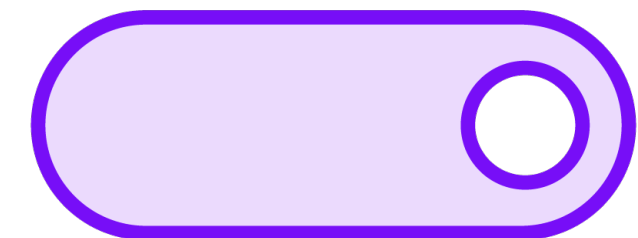
All Signed

Scripts can run; however, you must sign all scripts and configuration files, including scripts you write on the local computer.



Bypass

Nothing is blocked, and there are no warnings or prompts.

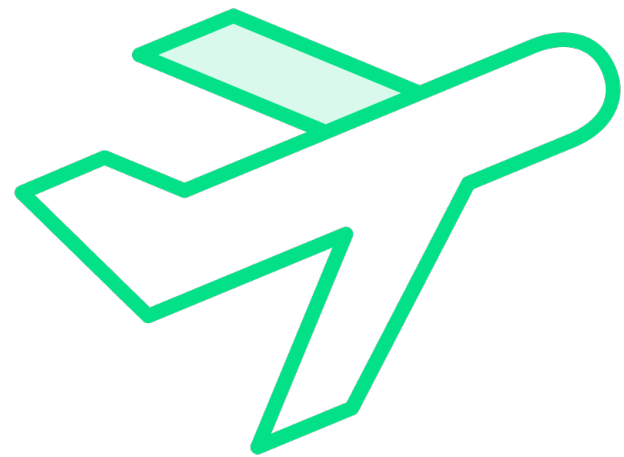


Default

Sets the default execution policy to "Restricted" for Windows clients and "RemoteSigned" for Windows servers.

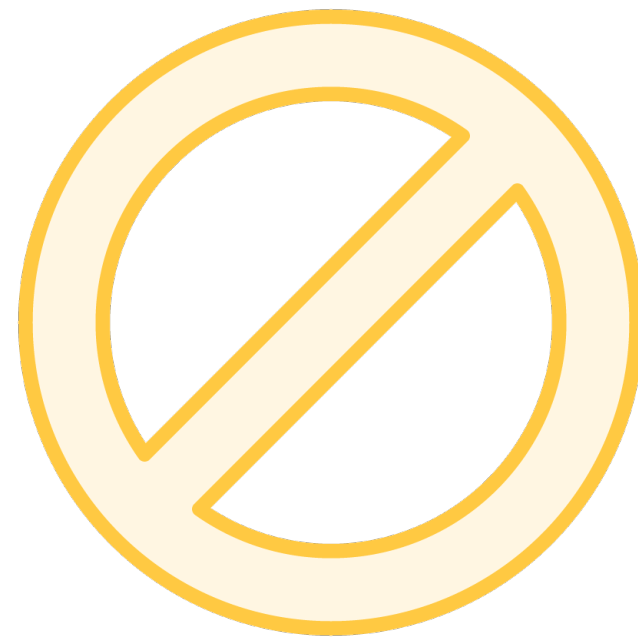


Execution Policies



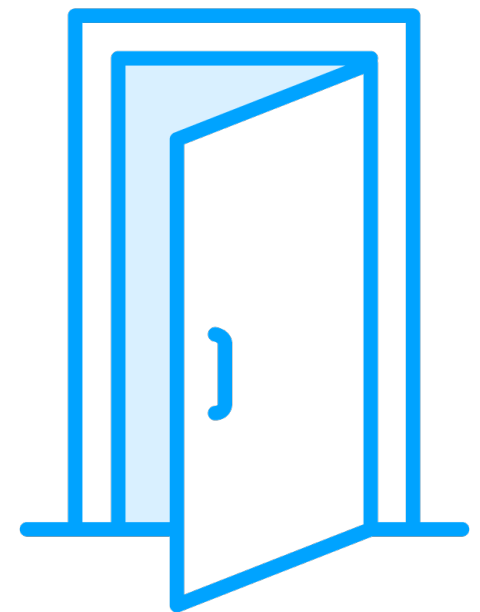
Remote Signed

It is the default PowerShell execution policy for Windows server computers.



Restricted

It is the default PowerShell execution policy for Windows client computers.



Unrestricted

It is the default execution policy for non-Windows computers and cannot be changed.



All Signed Versus Remote Signed

All Signed

Scripts can run

All scripts and configuration files need signing by a trusted publisher

Prompts before executing scripts from untrusted publishers

Risk of running signed malicious scripts

VS

Remote Signed

Scripts can run

All internet-downloaded scripts and configuration files need signing by a trusted publisher

No need to sign scripts written or downloaded locally

Risk of executing unsigned and signed malicious scripts



Restricted Versus Unrestricted

Restricted

Supports execution of individual commands, but does not allow scripts

Prevents running of all script files, including configuration (.ps1xml), modules (.psm1), and scripts (.ps1)

VS

Unrestricted

Unsigned scripts can run

Risk of running malicious scripts

Warns before executing scripts and configuration files not from the local intranet zone



Retrieving the Current Execution Policy

Retrieve the effective execution policy

```
Get-ExecutionPolicy
```

Retrieve all execution policies that affect the current session

```
Get-ExecutionPolicy -List
```

Retrieve the execution policies by scope

```
Get-ExecutionPolicy -Scope CurrentUser
```

```
Get-ExecutionPolicy -Scope LocalMachine
```

```
Get-ExecutionPolicy -Scope MachinePolicy
```

```
Get-ExecutionPolicy -Scope Process
```

```
Get-ExecutionPolicy -Scope UserPolicy
```





Execution Policies Support Scopes



Execution Policy Scopes



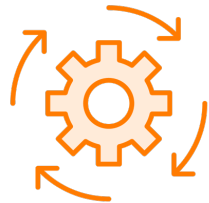
Machine Policy

Defined within a Group Policy for all users of the computer



User Policy

Defined within a Group Policy for the current user of the computer



Process

The Process scope only affects the current PowerShell session



Current User

The execution policy affects only the current user

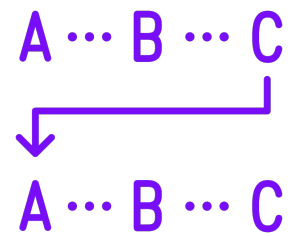


Local Machine

The execution policy affects all users on the current computer



Execution Policy Scopes



Scope values work in precedence order



If a current user policy exists, then it will take precedence over all other policies



Even with a more restrictive policy set at a lower level of importance, the higher priority will always apply

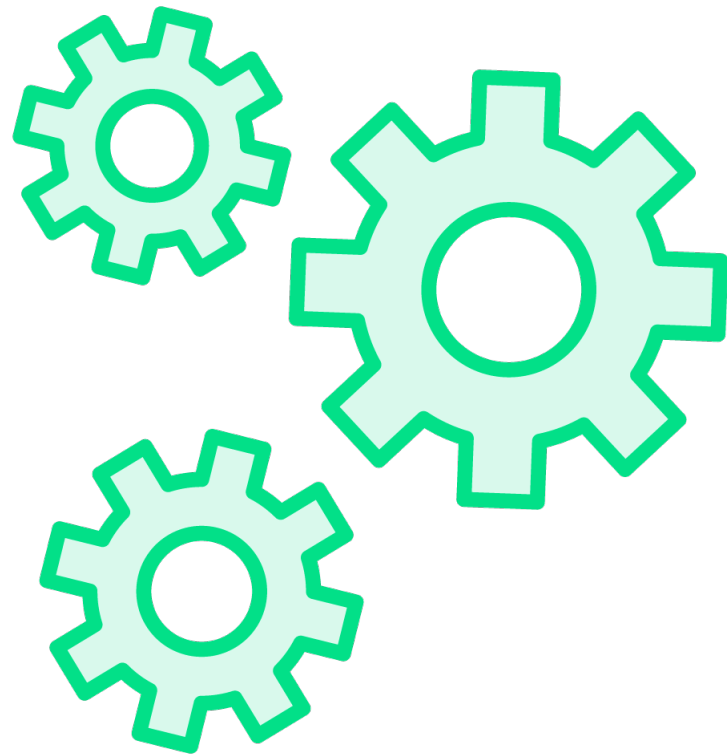




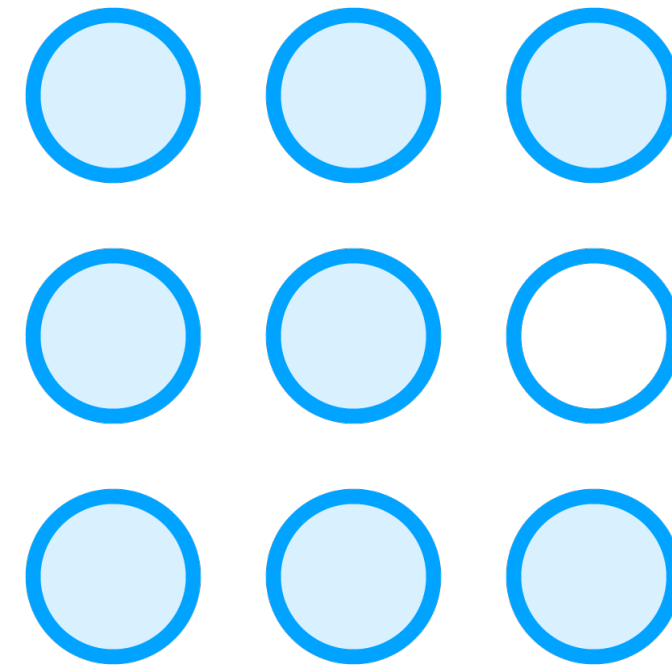
Set Execution Policies



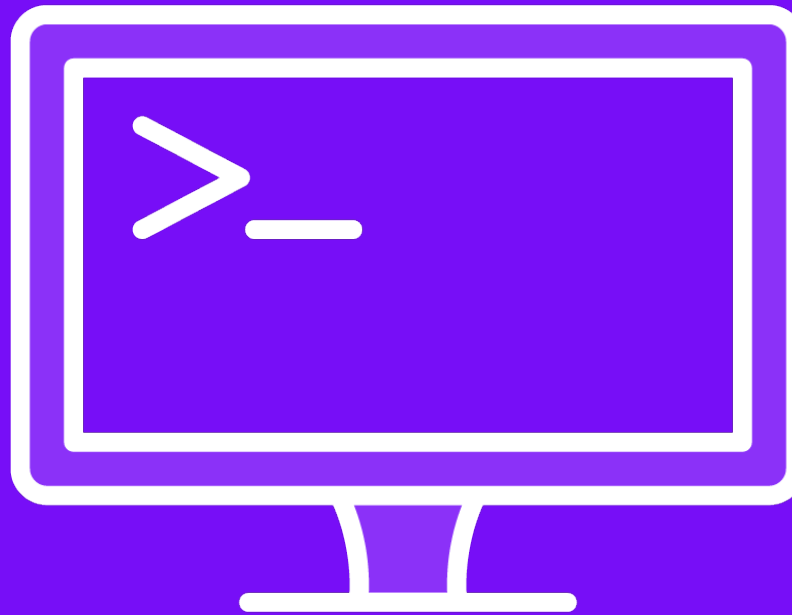
Setting Execution Policies



Set-ExecutionPolicy Cmdlet



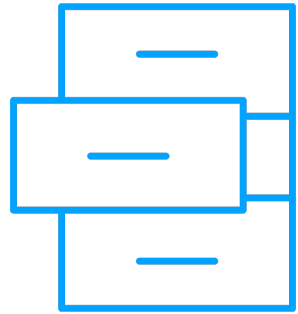
**Set the 'ExecutionPolicy' property
for single session**



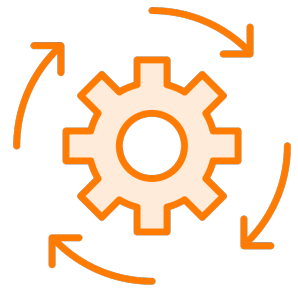
Using the 'Set-ExecutionPolicy' is effective immediately; PowerShell does not need restarting.



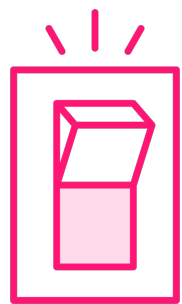
The Set-ExecutionPolicy Command



Setting the execution policy for the scopes LocalMachine or the CurrentUser, the change saves to the registry.



Setting the execution policy for the Process scope does not save to the registry.



Setting the Execution Policy may not change the current settings based on another policy assignment at the scope level.



Setting the Execution Policy and Scope

Set the execution policy

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted
```

Set the execution policy with a scope

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope LocalMachine
```

Set the execution policy for a single session

```
pwsh.exe -ExecutionPolicy Unrestricted
```



Removing the Execution Policy

Remove an execution policy

```
Set-ExecutionPolicy -ExecutionPolicy Undefined
```

Remove an execution policy for a scope

```
Set-ExecutionPolicy -ExecutionPolicy Undefined -Scope CurrentUser
```

Set no execution policy for a single session

```
pwsh.exe -ExecutionPolicy Undefined
```



Demo

Set Execution Policy Levels

Remove Execution Policy Levels





Understand the Impact of Execution Policies



Execution Policy Precedence

- 1 Group Policy: MachinePolicy
- 2 Group Policy: UserPolicy
- 3 Execution Policy: process or "pwsh.exe -ExecutionPolicy"
- 4 Execution Policy: CurrentUser
- 5 Execution Policy: LocalMachine

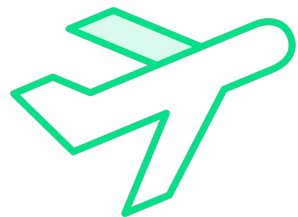


Execution Policy Impact



All Signed

Scripts can run
Must sign all scripts
Prompts before execution from untrusted



Remote Signed

Scripts can run
Must sign all downloaded scripts
No signing for locally created scripts
Supports "Unblock-File" script execution

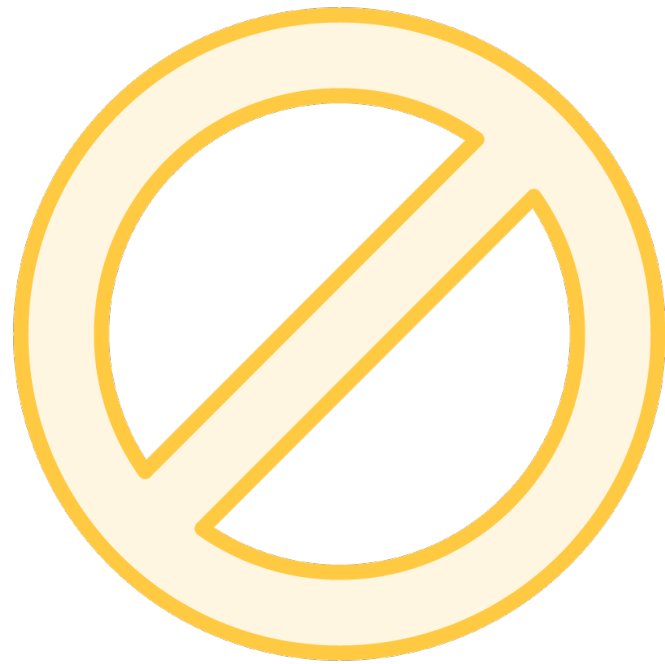


Bypass

Nothing is blocked
No warnings or prompts

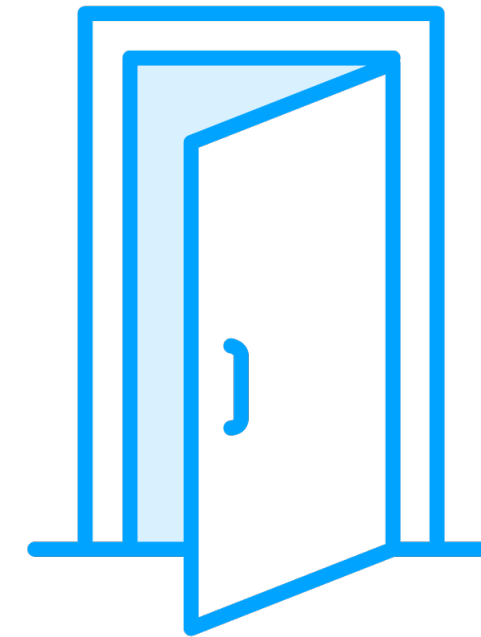


Execution Policy Impact



Restricted

Supports executing commands
Blocks script execution
Blocks ".ps1xml", ".psm1", and ".ps1" files



Unrestricted

Can execute unsigned scripts
Warns before execution of scripts not from the local intranet zone
Can execute ".ps1xml", ".psm1", and ".ps1" files



Demo

Understand the Impact of Execution Policies

- Set Execution Policy Values
- Execute PowerShell Commands
- Execute PowerShell Script



Summary

Goal: Understand Execution Policies

- Reviewed execution policy capabilities
- Set execution policies to different levels
- Executed PowerShell commands and a script with varying execution policy levels
- Learned the impact policies have on PowerShell execution



Up Next:

Using PowerShell to Collect System Information

