**Steps to Grant Access for PowerShell Execution**

**1. Enable PowerShell Remoting on the Target Machine**

PowerShell remoting allows users to execute commands on a remote machine. The administrator must enable it on the target machine (e.g., a server or another computer).

1. Open PowerShell as an administrator on the target machine.
2. Run the following command to enable remoting:

powershell

Enable-PSRemoting -Force

* + This starts the WinRM service and configures the firewall to allow remote connections.

**2. Add the User to the Appropriate Group**

To allow the user to execute PowerShell commands remotely, the administrator must grant them the necessary permissions.

**Option A: Add the User to the Local Administrators Group**

If the user needs full administrative access, add them to the local Administrators group on the target machine:

powershell

Add-LocalGroupMember -Group "Administrators" -Member "username"

* Replace username with the user's account name.
* This grants the user administrative privileges, allowing them to execute commands with elevated permissions

1

.

**Option B: Grant Limited Access via the Remote Management Users Group**

For more restricted access, add the user to the **Remote Management Users** group. This allows them to use PowerShell remoting without full administrative rights:

powershell

Add-LocalGroupMember -Group "Remote Management Users" -Member "username"

* This is a safer option if the user does not need full admin privileges.

**3. Configure Permissions for PowerShell Remoting**

By default, only administrators can use PowerShell remoting. To allow non-administrators (e.g., users in the Remote Management Users group) to execute commands, modify the WinRM permissions.

1. Open PowerShell as an administrator on the target machine.
2. Run the following command to view the current WinRM configuration:

powershell

Get-PSSessionConfiguration

1. Update the permissions for the default session configuration:

powershell

Set-PSSessionConfiguration -Name Microsoft.PowerShell -ShowSecurityDescriptorUI

* + A security descriptor UI will appear. Add the user or group (e.g., Remote Management Users) and grant them **Execute** and **Read** permissions.

**4. Allow PowerShell Through the Firewall**

Ensure that the firewall on the target machine allows PowerShell remoting traffic.

1. Open PowerShell as an administrator on the target machine.
2. Run the following command to allow traffic on the default WinRM port (5985 for HTTP or 5986 for HTTPS):

powershell

New-NetFirewallRule -Name "PowerShell Remoting" -DisplayName "PowerShell Remoting" -Protocol TCP -LocalPort 5985 -Action Allow

**5. User Executes PowerShell Commands from Their Local Computer**

Once the above steps are complete, the user can execute PowerShell commands remotely from their local computer.

**Example: Establishing a Remote Session**

The user can open PowerShell on their local computer and run:

powershell

Enter-PSSession -ComputerName target-machine-name -Credential (Get-Credential)

* Replace target-machine-name with the hostname or IP address of the target machine.
* The Get-Credential cmdlet prompts the user to enter their username and password.

**Example: Running a Single Command Remotely**

Alternatively, the user can run a single command on the remote machine without entering a full session:

powershell

Invoke-Command -ComputerName target-machine-name -Credential (Get-Credential) -ScriptBlock { Get-Service }

**6. Optional: Use HTTPS for Secure Connections**

For added security, configure PowerShell remoting to use HTTPS instead of HTTP. This requires setting up an SSL certificate on the target machine. Refer to the steps in my earlier response for configuring HTTPS with WinRM.

**Summary**

* Enable PowerShell remoting on the target machine.
* Add the user to the appropriate group (e.g., Administrators or Remote Management Users).
* Modify WinRM permissions to allow the user to execute commands.
* Ensure the firewall allows PowerShell remoting traffic.
* The user can then connect remotely using Enter-PSSession or Invoke-Command.