Windows Firewall: Allow inbound file and printer sharing exception

Back | Description | Gpedit | Regedit | CMD
VBScript | PowerShell Script

Description:

Allows inbound file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445.

If you enable this policy setting, Windows Firewall opens these ports so that this computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or subnets from which these incoming messages are allowed. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is selected and administrators cannot clear it.

If you disable this policy setting, Windows Firewall blocks these ports, which prevents this computer from sharing files and printers. If an administrator attempts to open any of these ports by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.

If you do not configure this policy setting, Windows Firewall does not open these ports. Therefore, the computer cannot share files or printers unless an administrator uses other policy settings to open the required ports. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared. Administrators can change this check box.

Note: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo requests (the message sent by the Ping utility), even if the "Windows Firewall: Allow ICMP exceptions" policy setting would block them. Policy settings that can open TCP port 445 include "Windows Firewall: Allow inbound file and printer sharing exception," "Windows Firewall: Allow inbound remote administration exception," and "Windows Firewall: Define inbound port exceptions."

Supported on: At least Windows XP Professional with SP2.

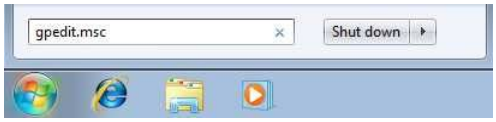
Back | Description | Gpedit | Regedit | CMD | Up
VBScript | PowerShell Script

Gpedit:

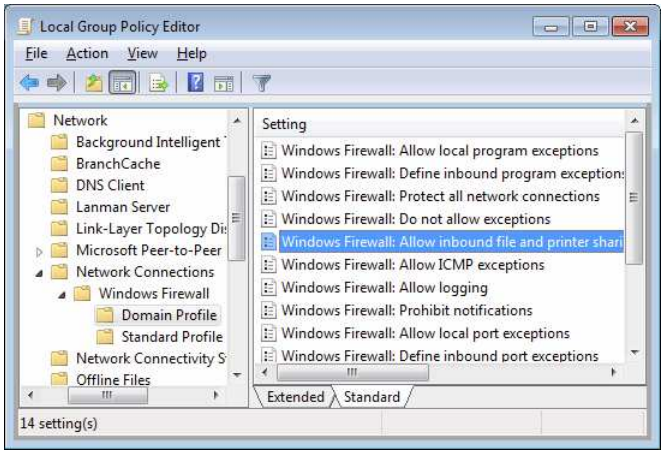
Please perform the following steps:

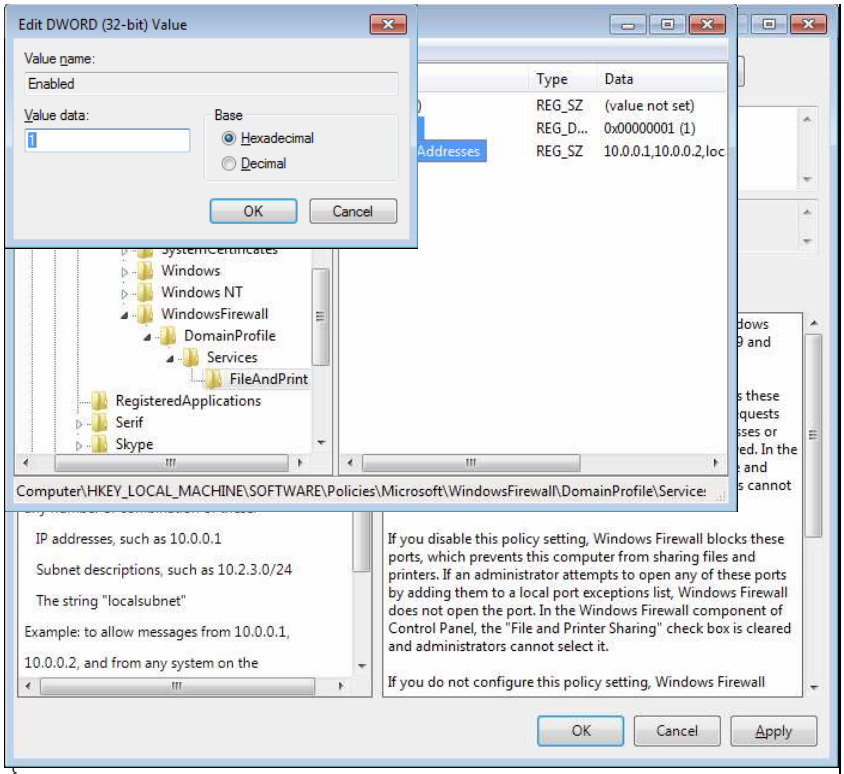
Please go to **Pearl button** (Start) and click on the **Search programs and files**
For more information about the change from Start to Pearl button click here

Type **gpedit.msc** and press **Enter**



In the **Group Policy** window please navigate to **Computer Configuration** -> **Administrative Templates** -> **Network** -> **Network Connections** -> **Windows Firewall** -> **Domain Profile** and open **Windows Firewall: Allow inbound file and printer sharing exception**.






```
}
else
{
 New-Item -path $RegKey -name DomainProfile
 $RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile"
 New-Item -path $RegKey -name Services
 $RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services"
 New-Item -path $RegKey -name FileAndPrint
 $RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint"
 ##Enabled
 New-ItemProperty -path $RegKey -name Enabled -value 1 -PropertyType DWord -Force
 New-ItemProperty -path $RegKey -name RemoteAddresses -value "10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24" -PropertyType String
 ##Disabled
 ##New-ItemProperty -path $RegKey -name Enabled -value 0 -PropertyType DWord -Force
}
}
else
{
New-Item -path $RegKey -name WindowsFirewall
$RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall"
New-Item -path $RegKey -name DomainProfile
$RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile"
New-Item -path $RegKey -name Services
$RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services"
New-Item -path $RegKey -name FileAndPrint
$RegKey = "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint"
##Enabled
New-ItemProperty -path $RegKey -name Enabled -value 1 -PropertyType DWord -Force
New-ItemProperty -path $RegKey -name RemoteAddresses -value "10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24" -PropertyType String
##Disabled
##New-ItemProperty -path $RegKey -name Enabled -value 0 -PropertyType DWord -Force
}
```

Not Configured

```
$RegKey = "HKLM:\SOFTWARE\Policies\Microsoft"
Remove-ItemProperty -Path($RegKey + "\WindowsFirewall\DomainProfile\Services\FileAndPrint") -name Enabled
Remove-ItemProperty -Path($RegKey + "\WindowsFirewall\DomainProfile\Services\FileAndPrint") -name RemoteAddresses
If( (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services\FileAndPrint")).ValueCount -eq 0 -and (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services\FileAndPrint")).SubKeyCount -eq 0)
{
Remove-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services\FileAndPrint")
If( (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services")).ValueCount -eq 0 -and (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services")).SubKeyCount -eq 0)
{
 Remove-Item -Path($RegKey + "\WindowsFirewall\DomainProfile\Services")
 If( (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile")).ValueCount -eq 0 -and (Get-Item -Path($RegKey + "\WindowsFirewall\DomainProfile")).SubKeyCount -eq 0)
 {
  Remove-Item -Path($RegKey + "\WindowsFirewall\DomainProfile")
  If( (Get-Item -Path($RegKey + "\WindowsFirewall")).ValueCount -eq 0 -and (Get-Item -Path($RegKey + "\WindowsFirewall")).SubKeyCount -eq 0)
  {
   Remove-Item -Path($RegKey + "\WindowsFirewall")
  }
 }
}
}
```