How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

Applies to: Windows 10 Pro released in July 2015, Windows 10 Enterprise released in July 2015, Windows Vista Enterprise, More

Summary

This article describes how to enable and disable Server Message Block (SMB) version 1 (SMBv1), SMB version 2 (SMBv2), and SMB version 3 (SMBv3) on the SMB client and server components.

Warning: We do not recommend that you disable SMBv2 or SMBv3. Disable SMBv2 or SMBv3 only as a *temporary* troubleshooting measure. Do not leave SMBv2 or SMBv3 disabled.

In Windows 7 and Windows Server 2008 R2, disabling SMBv2 *deactivates* the following functionality:

- Request compounding - allows for sending multiple SMB 2 requests as a single network request
- Larger reads and writes - better use of faster networks
- Caching of folder and file properties - clients keep local copies of folders and files
- Durable handles - allow for connection to transparently reconnect to the server if there is a temporary disconnection
- Improved message signing - HMAC SHA-256 replaces MD5 as hashing algorithm
- Improved scalability for file sharing - number of users, shares, and open files per server greatly increased
- Support for symbolic links
- Client oplock leasing model - limits the data transferred between the client and server, improving performance on high-latency networks and increasing SMB server scalability
- Large MTU support - for full use of 10-gigabye (GB) Ethernet

- Improved energy efficiency - clients that have open files to a server can sleep

In Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2016, disabling SMBv3 *deactivates* the following functionality (and also the SMBv2 functionality that's described in the previous list):

- Transparent Failover - clients reconnect without interruption to cluster nodes during maintenance or failover
- Scale Out – concurrent access to shared data on all file cluster nodes
- Multichannel - aggregation of network bandwidth and fault tolerance if multiple paths are available between client and server
- SMB Direct – adds RDMA networking support for very high performance, with low latency and low CPU utilization
- Encryption – Provides end-to-end encryption and protects from eavesdropping on untrustworthy networks
- Directory Leasing - Improves application response times in branch offices through caching
- Performance Optimizations - optimizations for small random read/write I/O

More Information

The SMBv2 protocol was introduced in Windows Vista and Windows Server 2008.

The SMBv3 protocol was introduced in Windows 8 and Windows Server 2012.

For more information about the capabilities of SMBv2 and SMBv3 capabilities, go to the following Microsoft TechNet websites:

Server Message Block overview

What's New in SMB

How to gracefully remove SMB v1 in Windows 8.1, Windows 10, Windows 2012 R2, and Windows Server 2016

Windows Server 2012 R2 & 2016: PowerShell methods

SMB v1

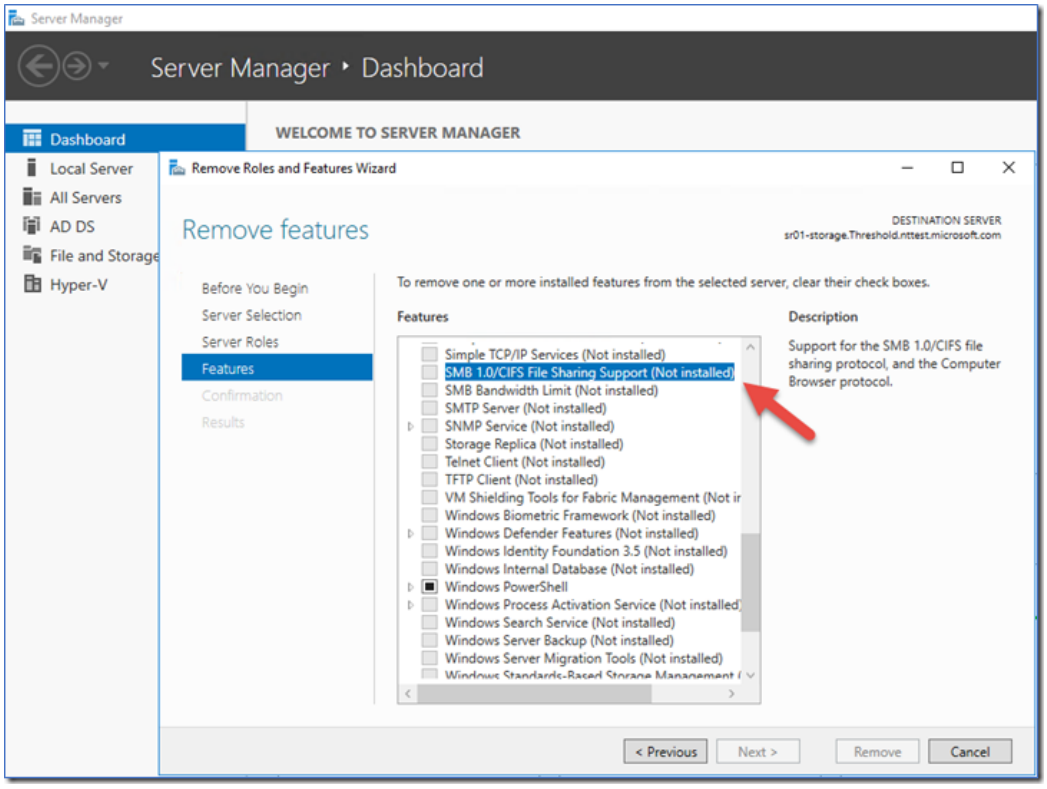
Detect:	Get-WindowsFeature FS-SMB1
Disable:	Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
Enable:	Enable-WindowsOptionalFeature -Online -FeatureName smb1protocol

SMB v2/v3

Detect:	Get-SmbServerConfiguration | Select EnableSMB2Protocol
Disable:	Set-SmbServerConfiguration -EnableSMB2Protocol $false
Enable:	Set-SmbServerConfiguration -EnableSMB2Protocol $true

Windows Server 2012 R2 and Windows Server 2016: Server Manager method for disabling SMB

SMB v1



Windows 8.1 and Windows 10: Powershell method

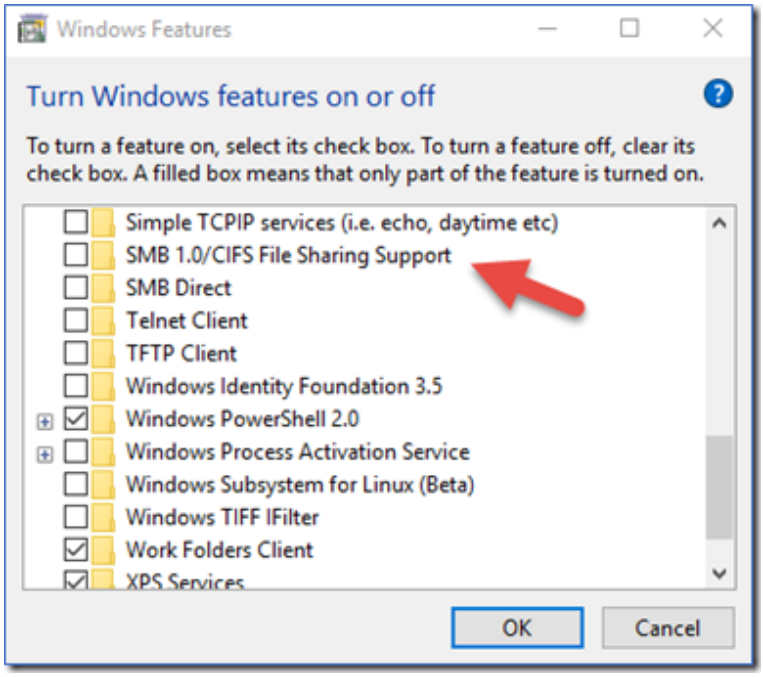
SMB v1 Protocol

Detect:	Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol
Disable:	Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
Enable:	Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

SMB v2/v3 Protocol

Detect:	Get-SmbServerConfiguration | Select EnableSMB2Protocol
Disable:	Set-SmbServerConfiguration –EnableSMB2Protocol $false
Enable:	Set-SmbServerConfiguration –EnableSMB2Protocol $true

Windows 8.1 and Windows 10: Add or Remove Programs method



How to detect status, enable, and disable SMB protocols on the SMB Server

For Windows 8 and Windows Server 2012

Windows 8 and Windows Server 2012 introduce the new Set-SMBServerConfiguration Windows PowerShell cmdlet. The cmdlet enables you to enable or disable the SMBv1, SMBv2, and SMBv3 protocols on the server component.

Notes When you enable or disable SMBv2 in Windows 8 or in Windows Server 2012, SMBv3 is also enabled or disabled. This behavior occurs because these protocols share the same stack.

You do not have to restart the computer after you run the Set-SMBServerConfiguration cmdlet.

SMB v1 on SMB Server

Detect:	Get-SmbServerConfiguration | Select EnableSMB1Protocol
Disable:	Set-SmbServerConfiguration -EnableSMB1Protocol $false
Enable:	Set-SmbServerConfiguration -EnableSMB1Protocol $true

For more information, see Server storage at Microsoft.

SMB v2/v3 on SMB Server

Detect:	Get-SmbServerConfiguration | Select EnableSMB2Protocol
Disable:	Set-SmbServerConfiguration -EnableSMB2Protocol $false
Enable:	Set-SmbServerConfiguration -EnableSMB2Protocol $true

For Windows 7, Windows Server 2008 R2, Windows Vista, and Windows Server 2008

To enable or disable SMB protocols on an SMB Server that is running Windows 7, Windows Server 2008 R2, Windows Vista, or Windows Server 2008, use Windows PowerShell or Registry Editor.

PowerShell methods

> **Note**
>
> This method requires PowerShell 2.0 or later version of PowerShell.

SMB v1 on SMB Server

Detect:

```
Get-Item HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\P
```

Default configuration = Enabled (No registry key is created), so no SMB1 value will be returned

Disable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services
```

Enable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services
```

Note You must restart the computer after you make these changes.

For more information, see Server storage at Microsoft.

SMB v2/v3 on SMB Server

Detect:

```
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Lanmar
```

Disable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services
```

Enable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services
```

Note You must restart the computer after you make these changes.

Registry Editor

Important This article contains information about how to modify the registry. Make sure that you back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756 How to back up and restore the registry in Windows

To enable or disable SMBv1 on the SMB server, configure the following registry key:

Registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Registry entry: SMB1
REG_DWORD: 0 = Disabled
REG_DWORD: 1 = Enabled
Default: 1 = Enabled (No registry key is created)

To enable or disable SMBv2 on the SMB server, configure the following registry key:

Registry subkey:**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**
Registry entry: SMB2
REG_DWORD: 0 = Disabled
REG_DWORD: 1 = Enabled
Default: 1 = Enabled (No registry key is created)

Note You must restart the computer after you make these changes

How to detect status, enable, and disable SMB protocols on the SMB Client

For Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012

Note When you enable or disable SMBv2 in Windows 8 or in Windows Server 2012, SMBv3 is also enabled or disabled. This behavior occurs because these protocols share the same stack.

SMB v1 on SMB Server

Detect:	sc.exe query lanmanworkstation
Disable:	sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi sc.exe config mrxsmb10 start= disabled
Enable:	sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi sc.exe config mrxsmb10 start= auto

For more information, see Server storage at Microsoft

SMB v2/v3 on SMB Server

Detect:	sc.exe query lanmanworkstation
Disable:	sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi sc.exe config mrxsmb20 start= disabled
Enable:	sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi sc.exe config mrxsmb20 start= auto

Notes

- You must run these commands at an elevated command prompt.
- You must restart the computer after you make these changes.

Disable SMBv1 Server with Group Policy

This will configure the following new item in the registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

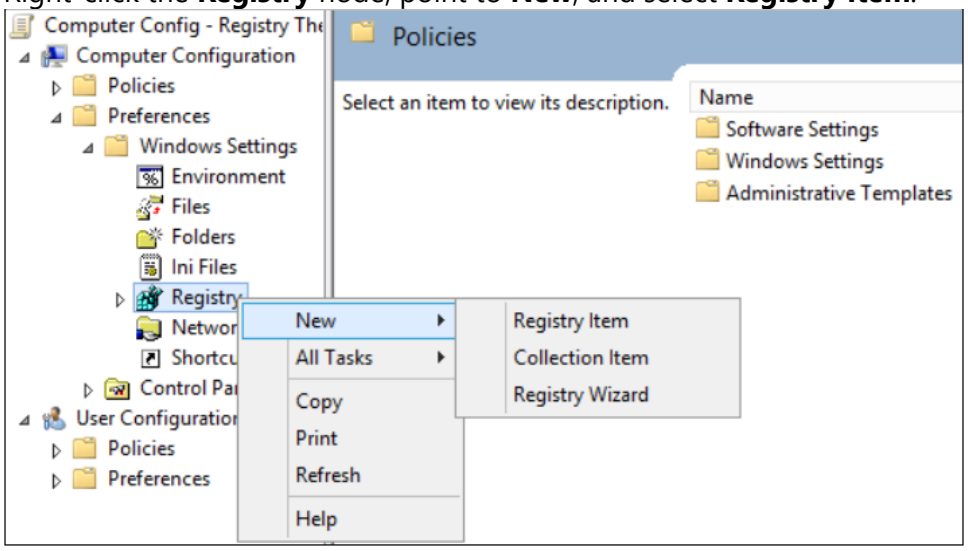
Registry entry: **SMB1** REG_DWORD: **0** = Disabled

To configure this using Group Policy:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.

2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.

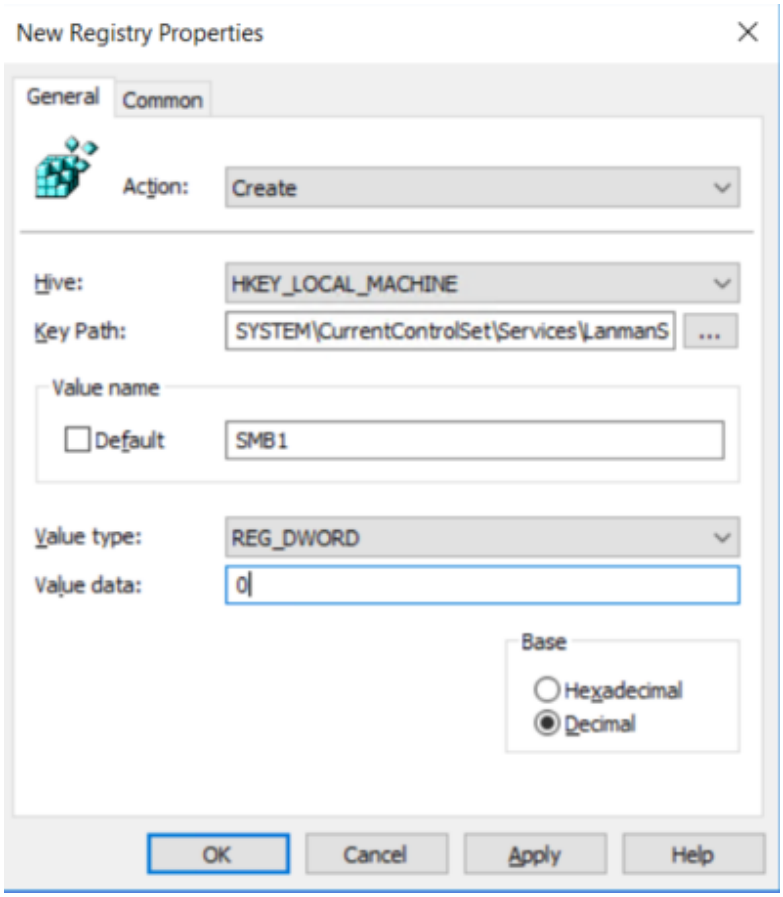
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.



In the **New Registry Properties** dialog box, select the following:

- **Action:** Create
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path:** SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- **Value name:** SMB1
- **Value type:** REG_DWORD

- **Value data:** 0



This disables the SMBv1 Server components. This Group Policy needs to be applied to all necessary workstations, servers, and domain controllers in the domain.

Note: WMI filters can also be set to exclude unsupported operating systems or selected exclusions such as Windows XP.

Caution! Be careful when making these changes on domain controllers where legacy Windows XP or older Linux and 3rd party systems (that do not support SMBv2 or SMBv3) require access to SYSVOL or other file shares where SMB v1 is being disabled.

Disable SMBv1 Client with Group Policy

To disable the SMBv1 client, the services registry key needs to be updated to disable the start of **MRxSMB10** and then the dependency on **MRxSMB10** needs to be removed from the entry for **LanmanWorkstation** so that it can start normally without requiring **MRxSMB10** to first start.

This will update and replace the default values in the following 2 items in the registry

---

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsmb10

Registry entry: **Start** REG_DWORD: **4** = Disabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation

Registry entry: **DependOnService** REG_MULTI_SZ:
"Bowser","MRxSmb20","NSI"

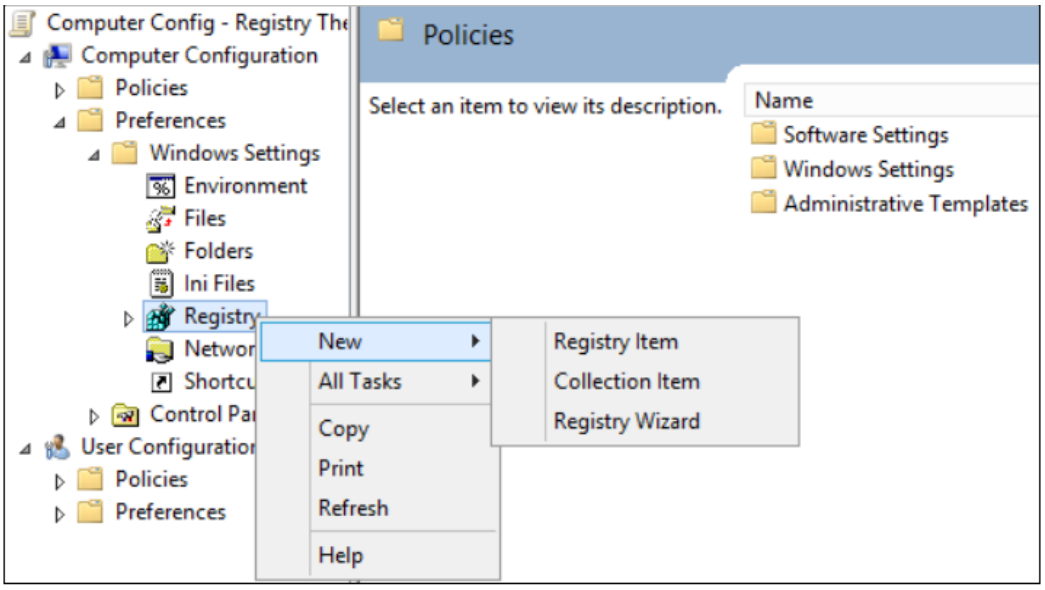
Note: The default included MRxSMB10 which is now removed as dependency

To configure this using Group Policy:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.

2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.

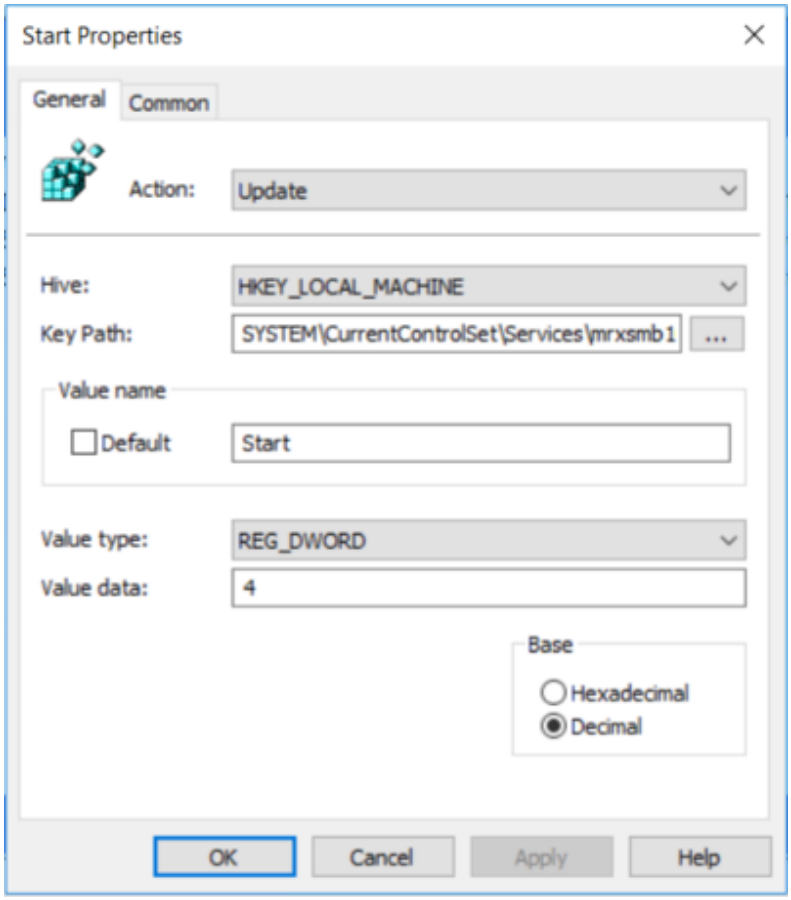
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.



In the **New Registry Properties** dialog box, select the following:

- **Action:** Update
- **Hive**: HKEY_LOCAL_MACHINE

- **Key Path:** SYSTEM\CurrentControlSet\services\mrxsmb10
- **Value name:** Start
- **Value type:** REG_DWORD
- **Value data**: 4



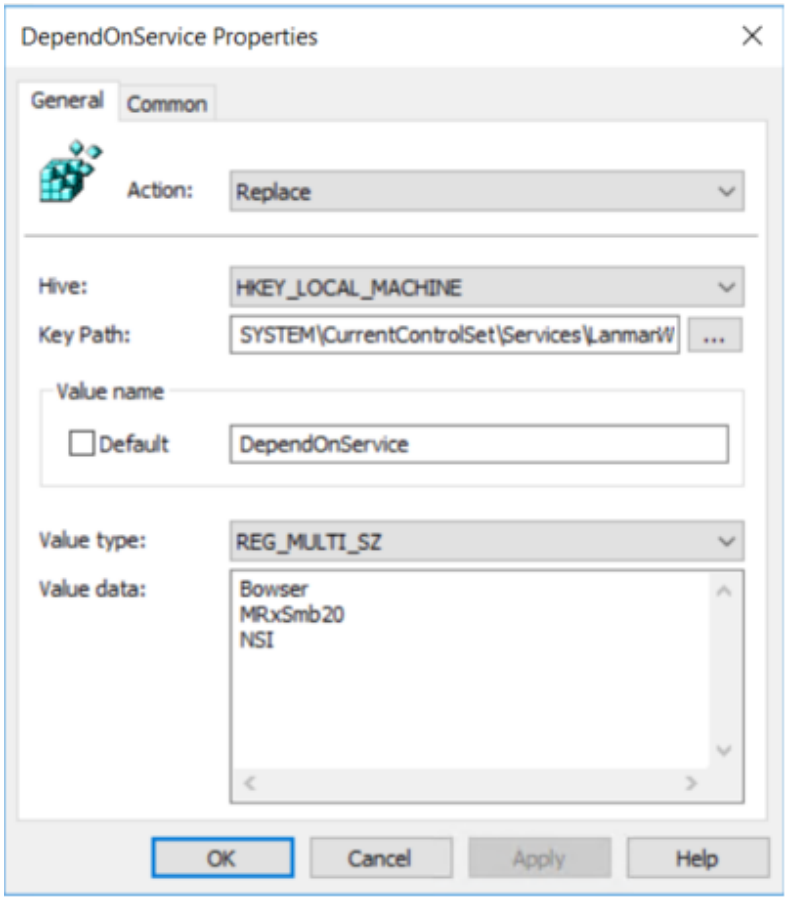
Then remove the dependency on the **MRxSMB10** that was just disabled

In the **New Registry Properties** dialog box, select the following:

- **Action:** Replace
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path:** SYSTEM\CurrentControlSet\Services\LanmanWorkstation
- **Value name:** DependOnService
- **Value type** REG_MULTI_SZ
- **Value data**:
  - Bowser

- MRxSmb20
- NSI

Note: *These 3 strings will not have bullets (see below)*



The default value includes **MRxSMB10** in many versions of Windows, so by replacing them with this multi-value string, it is in effect removing **MRxSMB10** as a dependency for **LanmanServer** and going from four default values down to just these three values above.

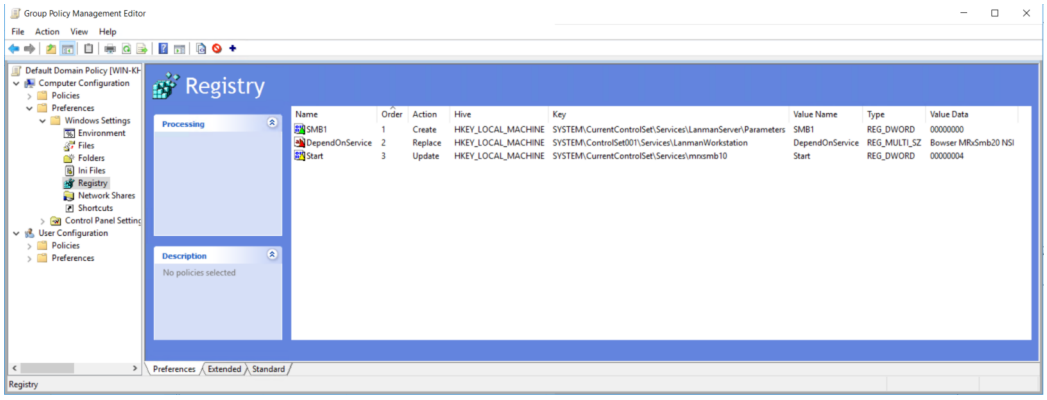
Note: When using Group Policy Management Console, there is no need to use quotation marks or commas. Just type the each entry on individual lines as shown above:

Reboot Required

After the policy has applied and the registry settings are in place, the targeted systems must be rebooted before SMB v1 is disabled.

Summary

If all the settings are in the same Group Policy Object (GPO), Group Policy Management will show the settings below.



Testing and Validation

Once these are configured, then allow the policy to replicate and update. As necessary for testing, run **gpupdate /force** from a **CMD.EXE** prompt and then review the target machines to ensure the registry settings are getting applied correctly. Make sure SMB v2 and SMB v3 is functioning for all other systems in the environment.

Caution! Don't forget to reboot the targeted systems.

Last Updated: Nov 6, 2017