Connect to OMV with Windows 10

In most cases, where Windows 10 PC's are connected to the internet and are regularly updated, basic network settings (Set **Private Network**, Set **Workgroup name**, and **Advanced Sharing** settings) should allow Windows 10 users to map drives to OMV's network shares.

Additional measures, beginning with **Domain Connected Windows 10 Clients / Server**, are intended for businesses and off-line Windows 10 users where clients may not be up-to-date or for OEM (non-retail) installations that have been altered by Microsoft Partners.

((This document contains external links. It's intended to be used with an internet connected PC.))

Update: "Browsing" for your OMV server under Windows Explorer, Network, now works in OMV4. If your installation hasn't been updated recently, install the update wsdd 0.3-2 (or newer) and upgrade OMV to 4-1-21 (or higher) as found under System, Update Management.

Special Cases

- **To connect to Samba shares from Domain connected Windows 10 clients or Servers, scroll to the section titled "Domain Connected Windows 10 Clients / Servers"**

- **For users of Windows 10 Enterprise and Education editions, who lost access to SMB shares in the fall of 2018, scroll to the section titled "Loss of SMB shares with Guest access" near the bottom.**

- **For users of OMV3, using Remote Mount to connect OMV to Windows 10 client shares, scroll to the bottom.**

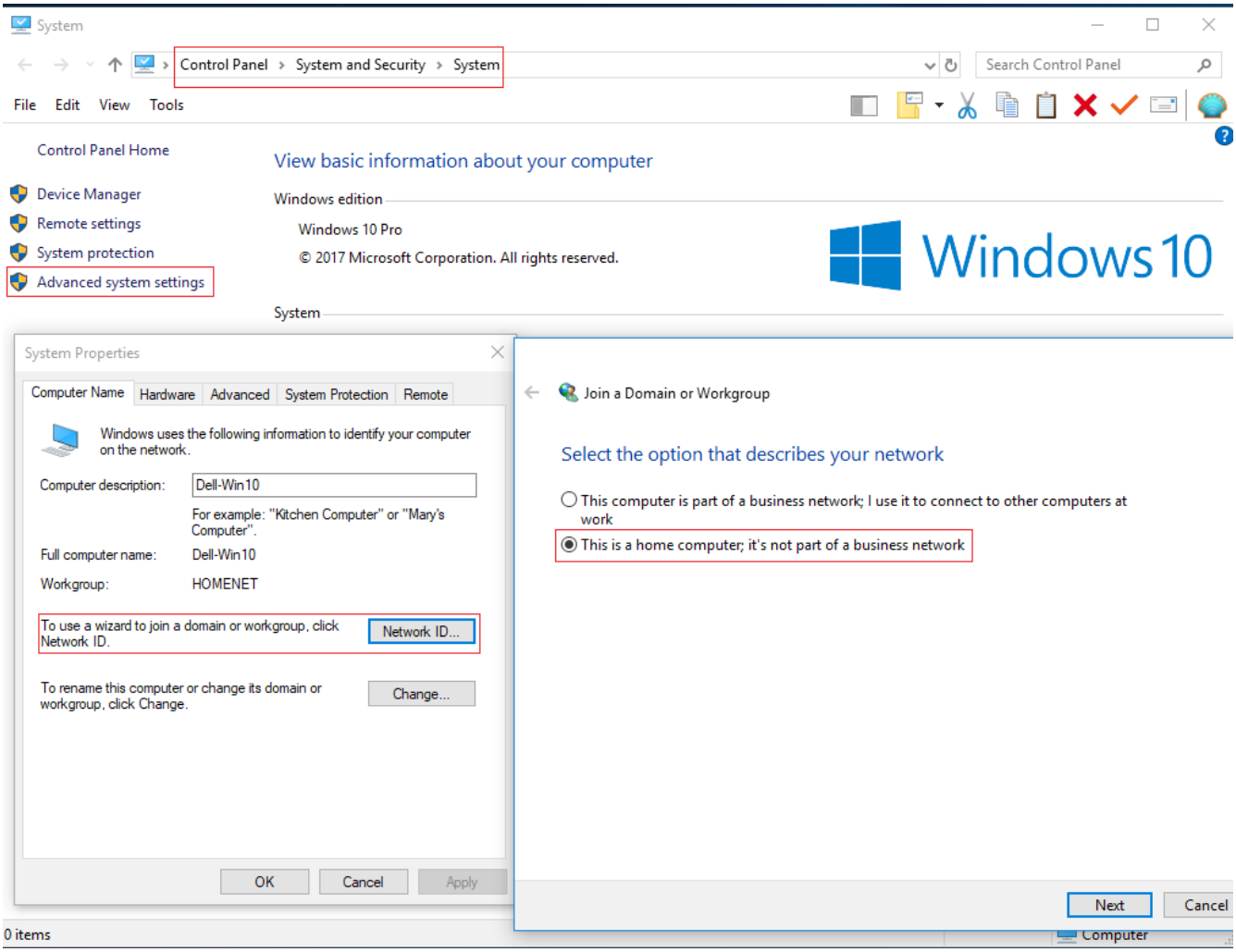
- **For businesses and users who have older peripherals that require SMB1. (scanners, photo equipment, etc.)** While Microsoft has depreciated it, SMB1 was patched on updated Windows PC's, with update 4013389, against the wanna cry vulnerability. With this update in place, reactivating SMB1, if needed, would be relatively safe for local LAN use.

- **For external users who are searching for a way to make Linux servers visible to Windows 10 clients, under Network, see the scripts for -> wsdd on github.**

Win10 Network Settings

Set Private Network

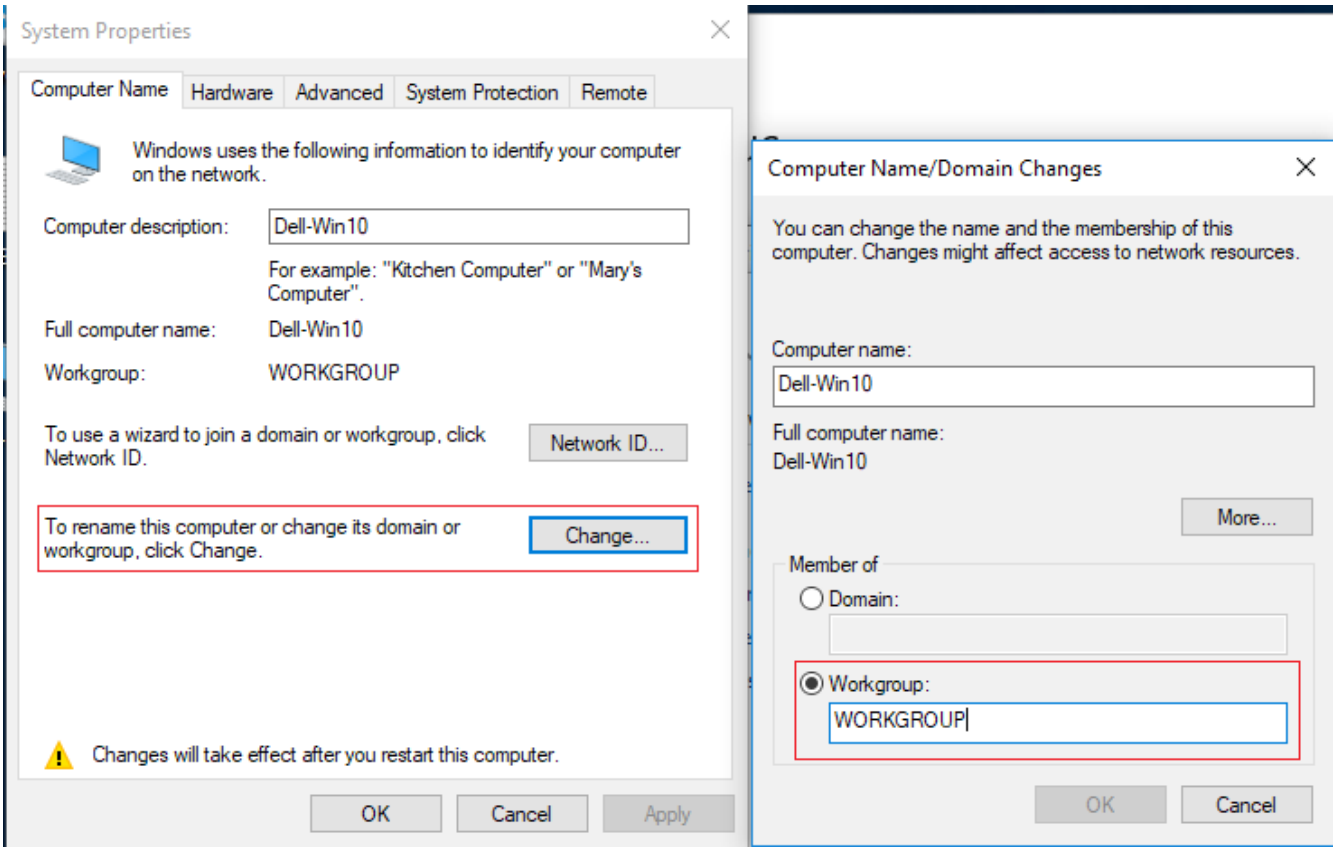
Make the selections shown.



Click “Next”.
A reboot is required.

Set WORKGROUP name

(In the same location as above:)

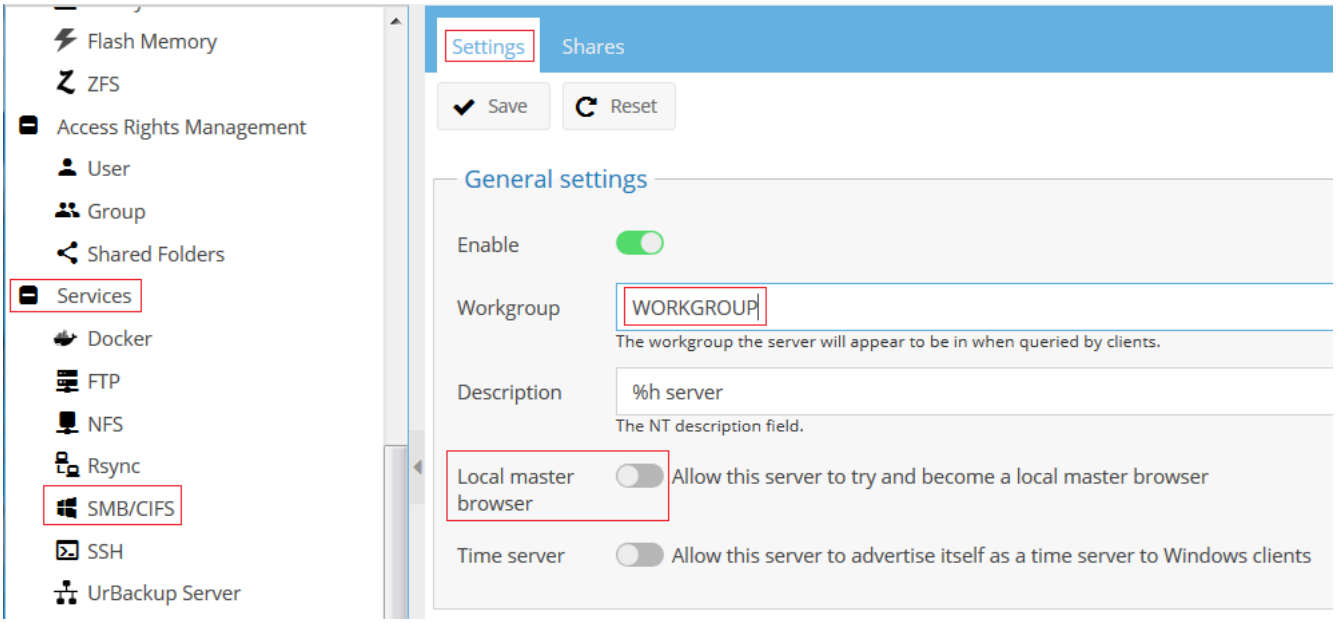


Click "OK".
A reboot is required.

(For more information, see Note 3.)

Set WORKGROUP name in OMV

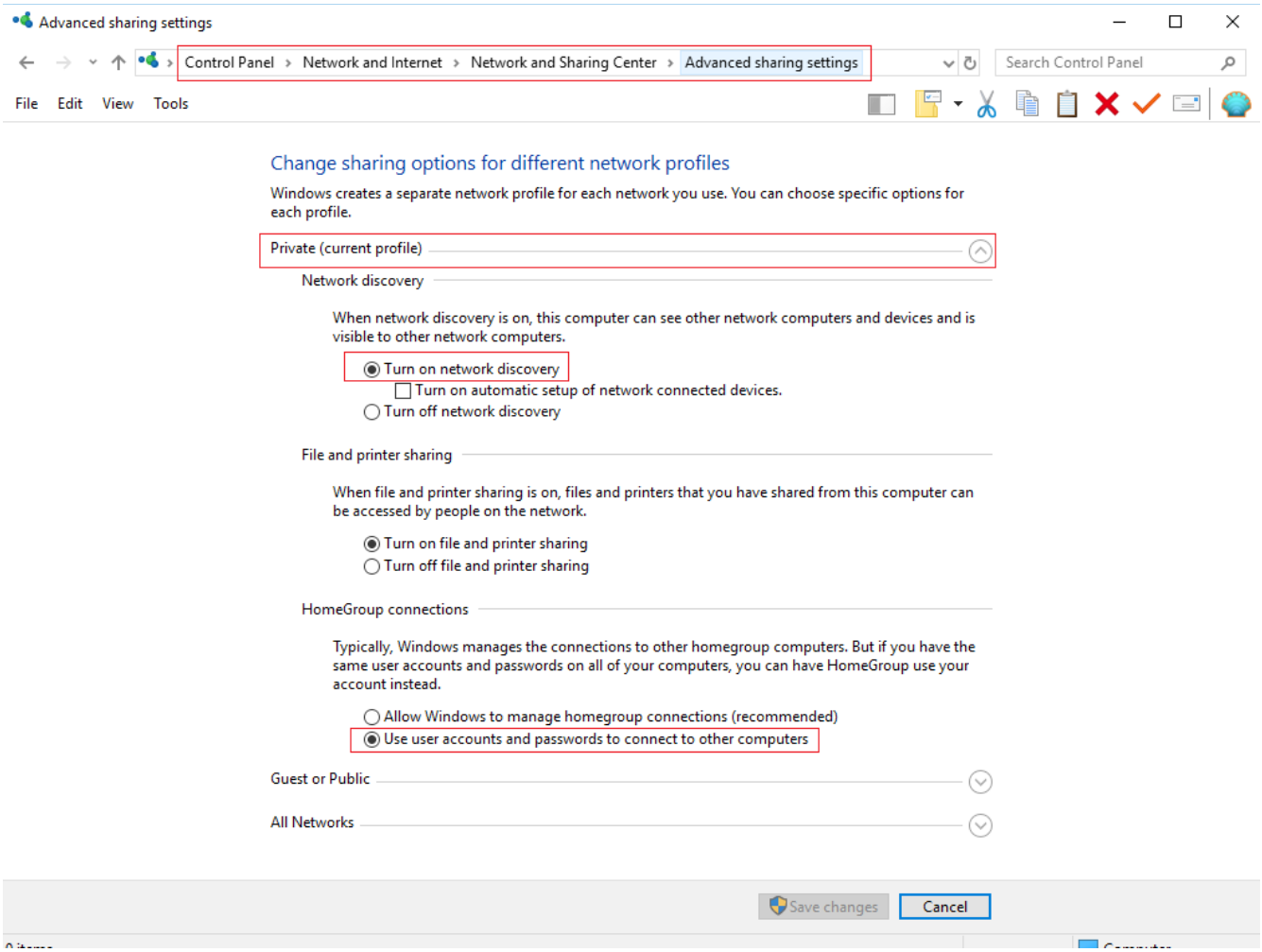
- Setting the identical workgroup name in OMV is recommended.
  - Turn **Local master browser** OFF



Local Master Browser While **LMB** is in OMV4 and earlier versions, it was depreciated in OMV5. If users are using OMV5, the Local Master Browser setting is not available.

Advanced Sharing Settings

Make the following changes to the **Private Profile**. Leave the **Guest or Public** and **All Networks** as they are.



Save Changes

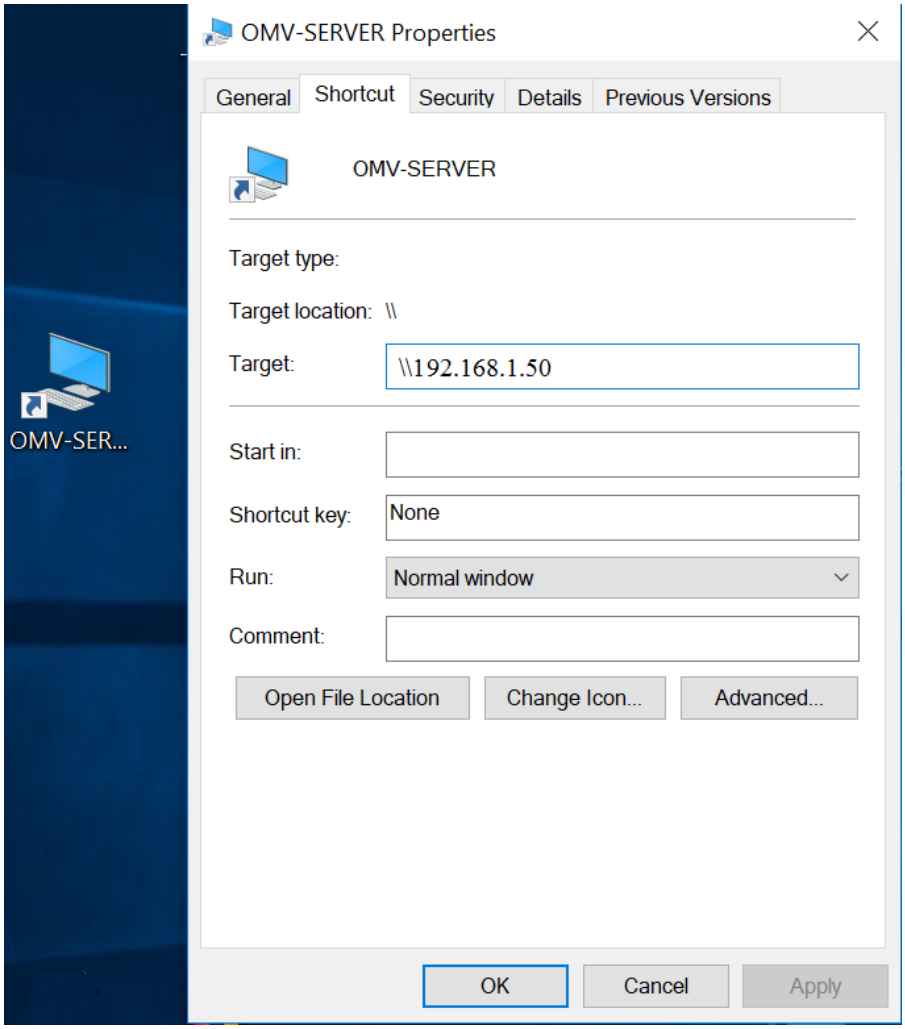
A reboot is required.

For most cases, the network setting changes made should allow an OMV servers shares to be mapped as network drives, and for the creation of a Server short cut as follows.

Create an OMV Server Shortcut

Right click on the Windows 10 Desktop. Select New, Shortcut. The location will be \\OMVSERVERIPADDR (substitute in your servers IP address similar to this -> \\192.168.1.50).
Click **Next**.
Name the Shortcut. (I used the server's name for this shortcut name).

When finished, the properties of the short cut should be similar to the following (with your server's IP address in the Target: field).



** For convenience, right click the completed Shortcut icon and pin it to **Quick Access** and **Start**. **

If the changes previously made do not resolve the the connection issue, proceed to the following.

Domain Connected Windows 10 Clients / Servers

(and, potentially, other difficult cases)

Thanks to @macom for this contribution.

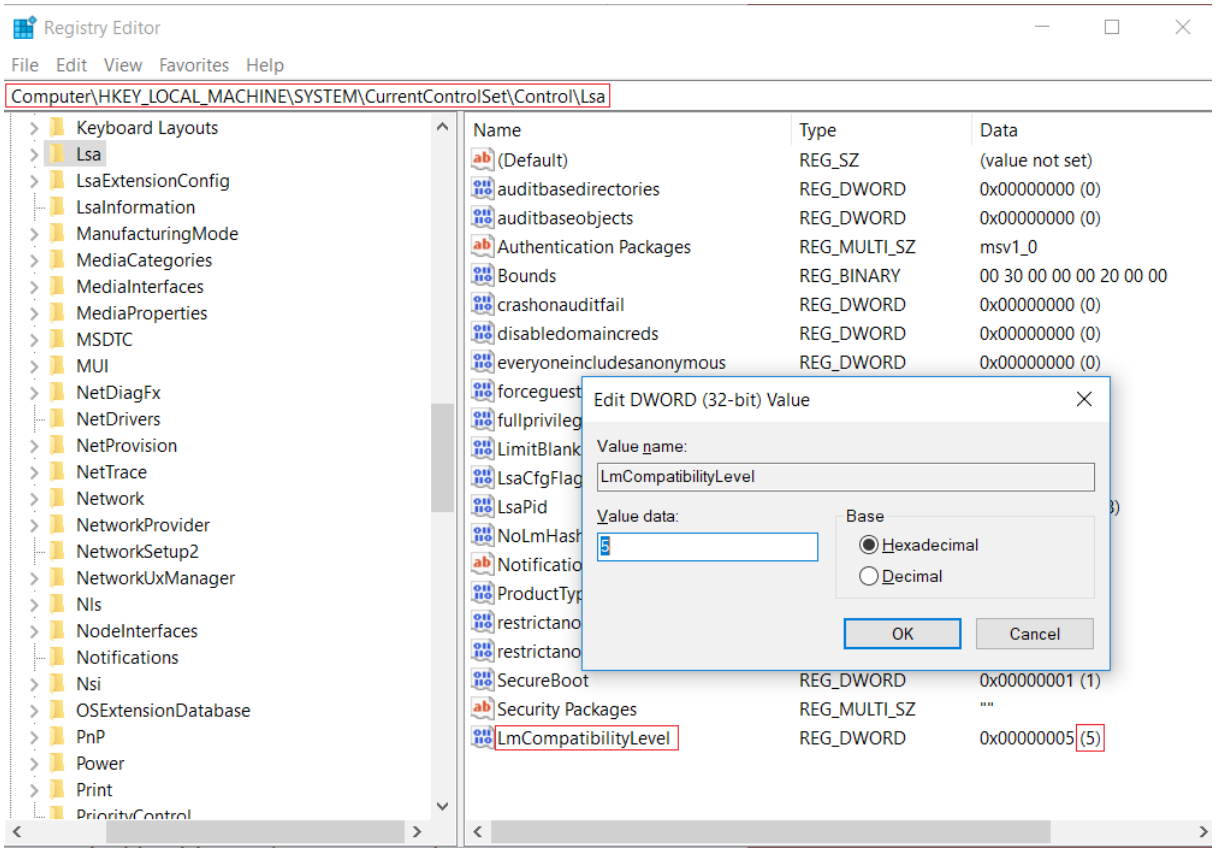
This modification allows admin's to change security policy, on a per-client basis, to allow connections to non-domain servers hosting network shares. It will also “break out” standard Microsoft servers and **Domain controllers**.

On the Windows 10 client:

At the Start Button, in the search box, Type: **regedit.exe** and start the registry editor.
Navigate to **Computer\HKLM\SYSTEM\CurrentControlSet\Control\Lsa**
In the right hand window right click and select **New, DWORD (32bit) Value**

When created, rename **New Value #1** to **LmCompatibilityLevel**
Double click on LmCompatibilityLevel and set the value data to **5**

Level 5 is the highest authentication level and it should work for connections to an OMV server. For other use cases, see the explanation and -> **guide to the levels 1 through 5.** Due to security risks, level 3 is the recommended minimum.



For Windows 10 Clients on closed networks, or that are not fully up-to-date for other reasons; the following may help with OMV - Windows 10 connectivity.

Windows 10 Client: Enable SMB2 - DisableSMB3

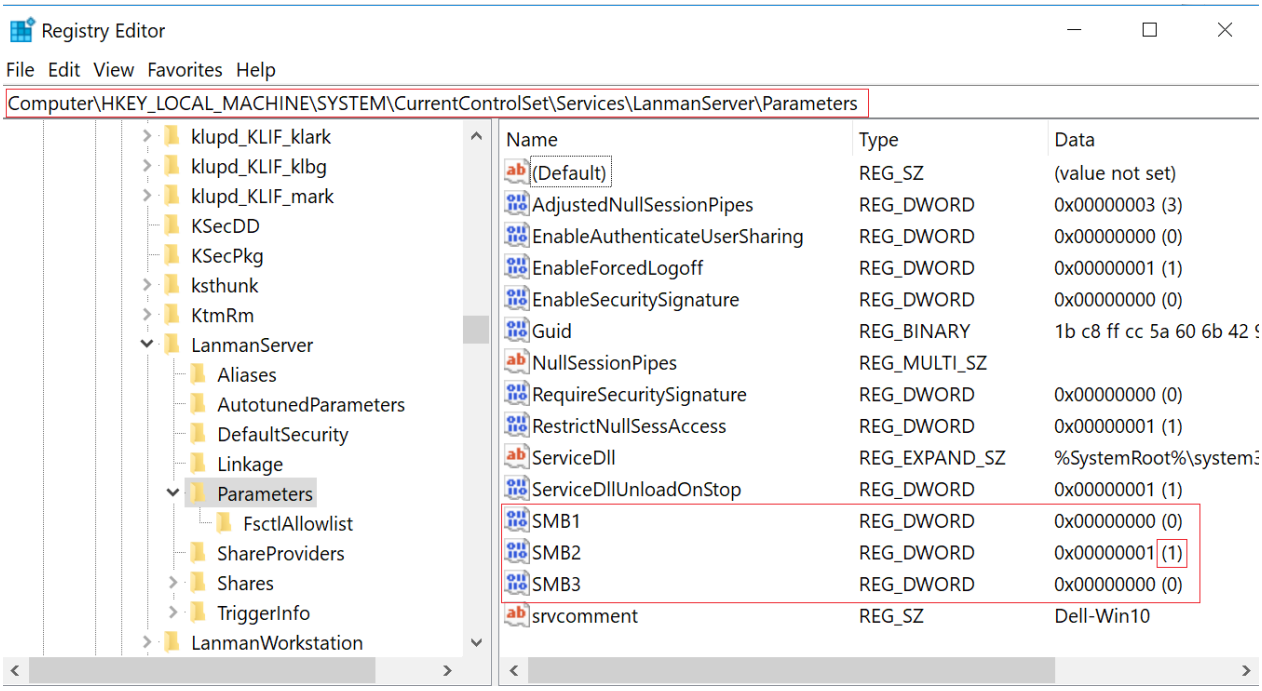
Adding items to the Windows registry entails some risk from “Fat Finger” errors. Use caution.

Run Windows Power Shell as Administrator (Right click to run as administrator)
Copy and paste the following lines into the Power Shell window.
(Do this CLEANLY, ensuring that the entire line is copied and pasted in before hitting Enter.)

1. Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Paramters" SMB1 -Type DWORD -Value 0 –Force
2. Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 1 –Force
3. Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB3 -Type DWORD -Value 0 –Force

   These commands create 3 registry keys and set SMB2 as the operational SMB protocol. With these items added to the registry users can, selectively, turn SMB levels on or off with the registry editor.

   Optional:
   To verify the Power Shell cmdlet made the additions to the Registry, regedit.exe can be used. Browse to the location shown below and check the parameters for SMB1 through 3.



For more information see Note 2

Edit Windows 10 hosts file

Prerequisite:
This change requires that the OMV server has a static IP address or a permanent/static DHCP lease.

-Right click on Notepad and run it as administrator.
-Set the **Text Documents (*.txt)** drop down to **All Files (*.*)**
-Navigate to C:\Windows\System32\drivers\etc. Open the file “hosts”.

The following is an excerpt from the default file.
Add the two lines of text to the hosts file, according to the example below, shown in **bold black**.
Enter the IP address of your OMV server. The host name will be the OMV Hostname as it appears in OMV under **System**, **Network**, the **General** tab, in the **Hostname** field.

#
102.54.94.97 rhino.acme.com # source server
38.25.63.10 x.acme.com # x client host
#
 # --Server IP---- Hostname
192.168.1.50 OMV-SERVER
#
localhost name resolution is handled within DNS itself.
127.0.0.1 localhost
::1 localhost

If the hosts file is busy with another process, saving the file may fail. Use Windows 10 safe mode, as explained here, to be able to save the file.

See Note 4.

** Update 11/26/18 - Windows 10 Enterprise and Education editions - SMB Guest access **

Microsoft pushed out a change to a Windows 10 Enterprise and Education editions security policy settings that stops "**Guest**" access to SMB shares, due to their determination that unsecured Guest access is a security risk. Since **Guest** access makes sense in some Home LAN use cases and is easy to configure; for those affected, the following fix should restore access to lost SMB Guest shares.

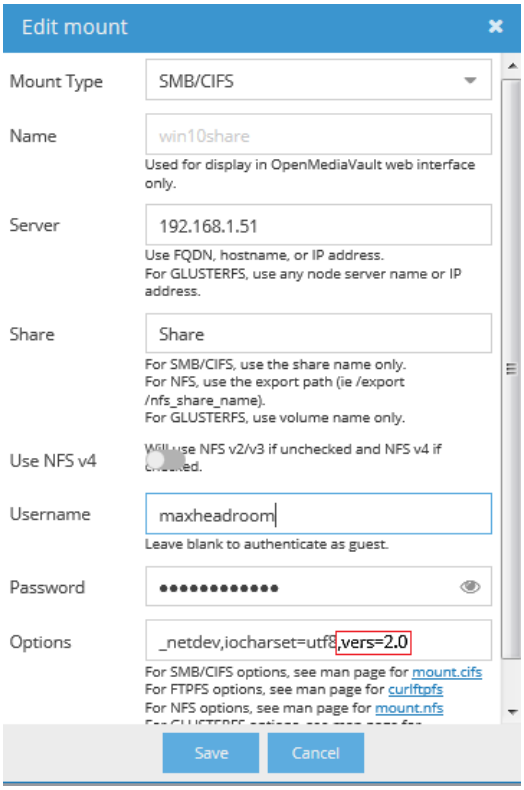
At the Windows 10 client:
Start the **CMD** prompt in Windows 10, as Administrator. (Right click on the CMD prompt icon, and select run as....)
Type: **gpedit.msc** to start the policy editor.
Go to **Computer Configuration** -> **Administrative Templates** -> **Network** -> **Lanman Workstation**
Set the value "**Enable insecure guest logons**".
Note set the value to "Enabled**" from "Not Configured"
Reboot

If the setting does not save properly make the change again and run **gpedit /force from the CMD prompt and **Reboot**.**

Configuring Remote Mount

(Applies only to OMV 3.X and earlier versions)

For users who are using Remote Mount to connect OMV to Windows 10 Shares, add **,vers=2.0** at the end of the Options box as shown. (For more info, see Note 5.)



Notes

Note 1.
Add-on client firewalls should be set to “trust” the local network with Medium or Low security settings. Using High security settings, for the local network, can result in clients becoming isolated on the network.

Note 2. (**For early versions of Windows 10, that have not been updated.**)
The issues with Windows 10 being able to map OMV SMB network shares seem to be related to Microsoft's version of SMB 3.1.1 and later variants. Setting Windows 10 to SMB2 protocols only, in registry keys, avoids surprises where shares may disappear after a newer version of SMB3 is pushed out or when an update changes Windows settings.

It should be noted that these settings already exist. Nothing new is being added. The creation of these registry keys simply make SMB parameters more accessible to users.

More information on M$'s implementation of SMB levels is available at:
https://blogs.technet.microsoft.com/josebda/2015/05/05/whats-new-in-smb-3-1-1-in-the-windows-server-2016-technical-preview-2 ** See Para 4. **

The change made, turning SMB3 off, can be undone with regedit.exe - Navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Set the data value for SMB3 to "1".
Value 1 = ON
Value 0 = OFF

Due to legitimate security concerns, SMB1 should be off. The Wcry [WannaCry] ransomware virus exploits a weakness in SMB1. This weakness still exists. While Wcry has been functionally neutralized, a day zero virus could be written to exploit SMB1.

Note 3.
The default Windows workgroup name is, (drum roll,,,) WORKGROUP. This default name will be in use in the majority of home PC systems. Regardless of the name used, all Windows clients and the OMV server should be set to the same workgroup name. If the workgroup name has been changed and is not configured in Windows 10, network connections to the OMV server may work but network discovery's detection of the OMV server may be significantly delayed.

Note 4.
The change to the host file is not required. However, some applications use host names or server names by default. (This is the case with most Web browsers.) Editing the Windows 10 host file, permanently associates the OMV server's IP address with its' hostname and speeds network connections, without reliance on local DNS or extended discovery processes.

Note 5.
The Remote Mount change reflects a security update that causes Windows 10 to reject a negotiation for an SMB1 connection, initiated from a remote host. The addition of ,vers-2.0 in Remote Mount Options, forces SMB2.