

# Services|CIFS/SMB|Shares

**Services | CIFS/SMB | Share | Edit**

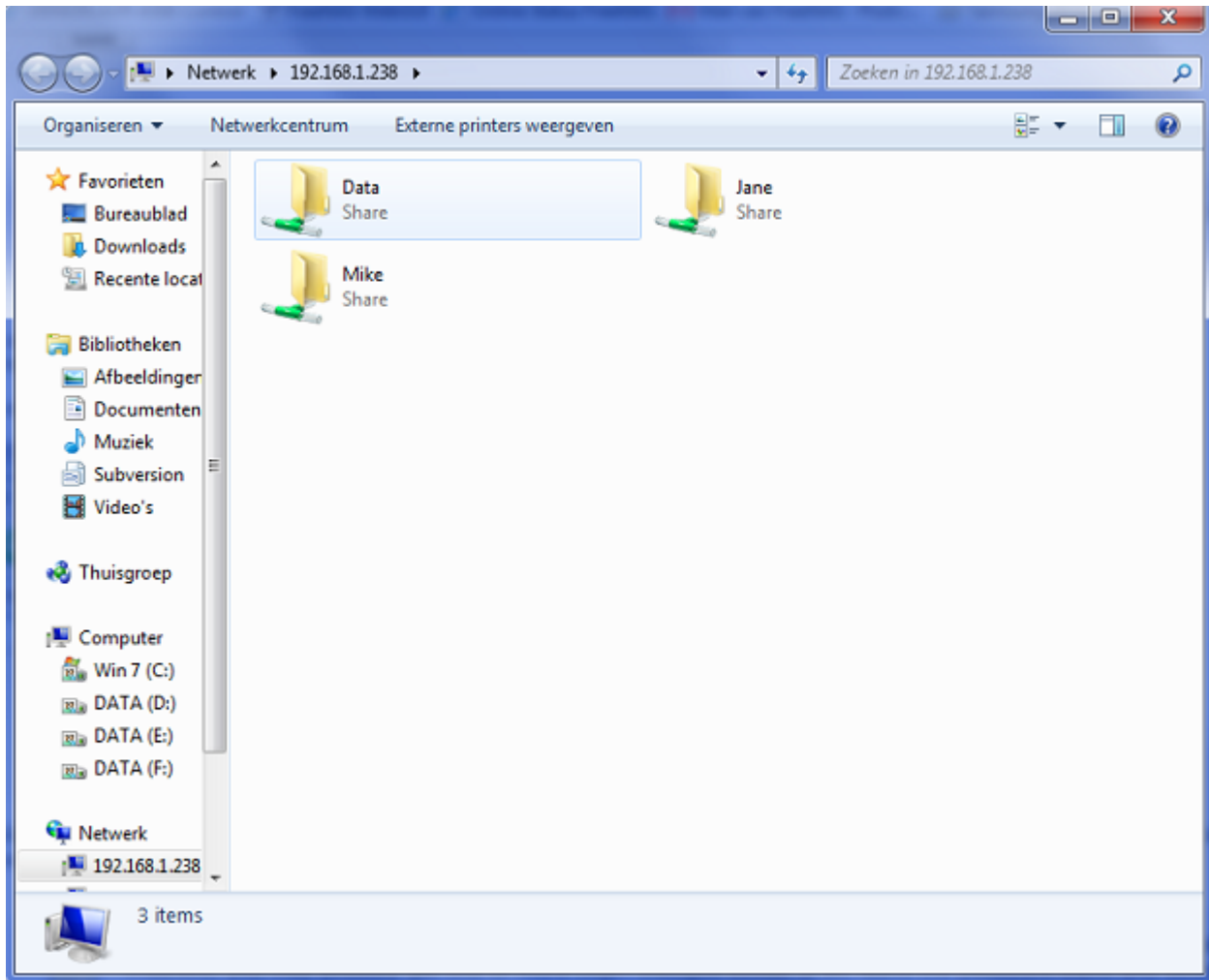
**Settings Shares**

<b>Name</b>	Data
<b>Comment</b>	Data
<b>Path</b>	/mnt/Data/ <input type="button" value="..."/> Path to be shared.
<b>Read only</b>	<input type="checkbox"/> Set read only If this parameter is set, then users may not create or modify files in the share.
<b>Browseable</b>	<input checked="" type="checkbox"/> Set browseable This controls whether this share is seen in the list of available shares in a net view and in the browse list.
<b>Guest</b>	<input checked="" type="checkbox"/> Enable guest access This controls whether this share is accessible by guest account.
<b>Inherit permissions</b>	<input checked="" type="checkbox"/> Enable permission inheritance The permissions on new files and directories are normally governed by create mask and directory mask but the inherit permissions parameter overrides this. This can be particularly useful on systems with many users to allow a single share to be used flexibly by each user.
<b>Recycle bin</b>	<input checked="" type="checkbox"/> Enable recycle bin This will create a recycle bin on the share.
<b>Hide dot files</b>	<input checked="" type="checkbox"/> This parameter controls whether files starting with a dot appear as hidden files.
<b>Shadow Copy</b>	<input type="checkbox"/> Enable shadow copy This will provide shadow copy created by auto snapshot. (ZFS only)
<b>Shadow Copy format</b>	auto-%Y%m%d-%H%M%S The custom format of the snapshot for shadow copy service can be specified. The default format is auto-%Y%m%d-%H%M%S used for ZFS auto snapshot.
<b>ZFS ACL</b>	<input type="checkbox"/> Enable ZFS ACL This will provide ZFS ACL support. (ZFS only)
<b>Hosts allow</b>	<input type="text"/> This option is a comma, space, or tab delimited set of hosts which are permitted to access this share. You can specify the hosts by name or IP number. Leave this field empty to use default settings.
<b>Hosts deny</b>	<input type="text"/> This option is a comma, space, or tab delimited set of host which are NOT permitted to access this share. Where the lists conflict, the allow list takes precedence. In the event that it is necessary to deny all by default, use the keyword ALL (or the netmask 0.0.0.0/0) and then explicitly specify to the hosts allow parameter those hosts that should be permitted access. Leave this field empty to use default settings.
<b>Auxiliary parameters</b>	<input type="text"/>

DO NOT select a Security setting of User at this stage, Refer to the User Authentication section for more information's on this feature

From another PC on the NAS4Free subnet (in this example I am using Microsoft Windows 7 Ultimate Edition). Select Start and Run and enter followed by the NAS4Free PC IP Address (\\192.168.1.238 in my example).

Click OK and the mounted Share should appear complete with the Share name you entered in the Mount process.



This Share is available to the network for Read/Write access and you can map a local drive to the share. Test it by copying some data to it. If you have 'show hidden files and folders' enabled in your Explorer settings, you will see a hidden and read only folder in there called .snap - ignore it.

If you are using a PC which normally logs into a Domain that is different from the WORKGROUP name configured in NAS4Free, you may possibly get one or more Login dialogue boxes. If so, leave the password blank and select OK.

by default Recycle Bin is enabled on the shares, when you do not see your space gets freed, clear the Recycle Bin first

From: <https://www.xigmanas.com/wiki/> - XigmaNAS

Permanent link: [https://www.xigmanas.com/wiki/doku.php?id=documentation:setup\\_and\\_user\\_guide:services\\_cifs:smb\\_shares](https://www.xigmanas.com/wiki/doku.php?id=documentation:setup_and_user_guide:services_cifs:smb_shares)

Last update: 2018/07/08 17:01

