Frequently Asked Questions

Scan to an SMB Share

Abstract

Image Access scanners are not only a peripheral, like other scanners and printers, they also include a Linux PC which can actively send data to various network resources. If this functionality is not needed, the installation process is as simple as installing any other network peripheral. The scanner needs a valid IP address and a correct subnet mask. In some cases, it might be required to also define the IP address of the gateway to connect to other subnets. If the scanner and the host are in the same subnet, the gateway should have the same IP as the scanner or it should be left blank.

To leverage the full functionality including the capability to scan to remote resources like SMB shares, the scanner and the host(s) must be configured correctly. There are many network architectures and many operating systems existing and this FAQ will guide you through the typical setup procedures necessary to accomplish this task. The screen shots are only examples and the descriptions might not exactly match what you find in your current system environment, but we believe that this FAQ can give answers to most questions. The intended target audience is the administrator of the target network, who would also have all the necessary access right to include a new PC into the network.

Title	Scan to an SMB Share
Revision	2.0
Date:	28.07.2017
Category	FAQ
Owner	Image Access GmbH, Germany
Authors	AKU, ERI, JKN, JMO, TI

1. Confidentiality

Status	Interested Party	Source	PDF
Public Information	Image Access Support	Yes	Yes
	Authorized Service Providers	No	Yes
	Image Access Customers	No	Yes

2. Revision History

Date	Rev.	Name	Description of Change	Reason of Change
03.12.2015	1.0	ERI	Initial Version	
03.12.2015	1.1	JKN	Updated Version	
17.05.2016	1.2	TI	Update and formatting changes	
02.06.2016	1.3	DI, JMO	Scanner hosted SMB share added	Was missing
15.06.2016	1.4	TI	Formatting & Typos	
15.09.2016	1.5	JKN	MAC OS X SMB Share	Was missing
21.09.2016	1.6	AKU, JKN	Updated Version: Windows 10	Was missing
05.01.2017	1.7	ERI	Wording changes and amendments	Publishing
03.03.2017	1.8	ERI	Former chapter *10. Appendix* moved to new chapter *8.2, Add a user name or group* Update: Numbering of Figures Update: Table of Figures	Revision
28.07.2017	2.0	TI	Minor formatting changes	Formatting

3. Table of Contents

3.1. Table of Figures

4. Purpose

The purpose of this document is to answer frequently asked questions about how to open and configure an SMB share on a windows PC and how to configure a Scan2Net scanner to be able to scan directly into an SMB share.

5. Scope

The scope of the document includes all Scan2Net, Bookeye or WideTEK scanners as well as OEM versions of these scanners. The firmware versions covered by this document are 6.xx and higher. The Windows versions covered in the documentation are Windows 7 and higher.

6. Terms and Definitions

Term	Description, Meaning
Scan2Net	Technology from Image Access implemented in many scanners. More at: www.imageaccess.de/?page=SoftwareScan2Net
SMB	SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports and other resources between computers.
Bookeye	Book scanners. More at: www.imageaccess.de/?page=ScannersBookscanner
WideTEK	Wide format scanner. More at: www.imageaccess.de/?page=ScannersWideformat

7. Introduction

The target audience for this FAQ document is the administrator of a Scan2Net scanner and the administrator of the customer PCs. The administrator should have experience setting up and configuring Windows PCs, network, firewalls and virus checkers.

The document will provide a guideline to:

- Share a folder on a workstation or server.
- Make this folder accessible for the scanner.
- Setup the scanner to transfer images to the shared folder.
- Store the scanner configuration in a template.
- Troubleshoot issues if images are transferred from a Scan2Net scanner to an SMB

Depending on the location of the shared folder (standalone workstation, workstation or server in a network) and considering different security requirements, this FAQ addresses some typical scenarios.

This FAQ does not cover issues that occur due to access restrictions caused by firewalls, virus, spam, or spyware protection software. The most common problems are caused by virus protection software when "browser protection" is enabled.

In general, the IP address of the Scan2Net scanner should be explicitly excluded from the above-mentioned software tools.

7.1. Description of the SMB Concept

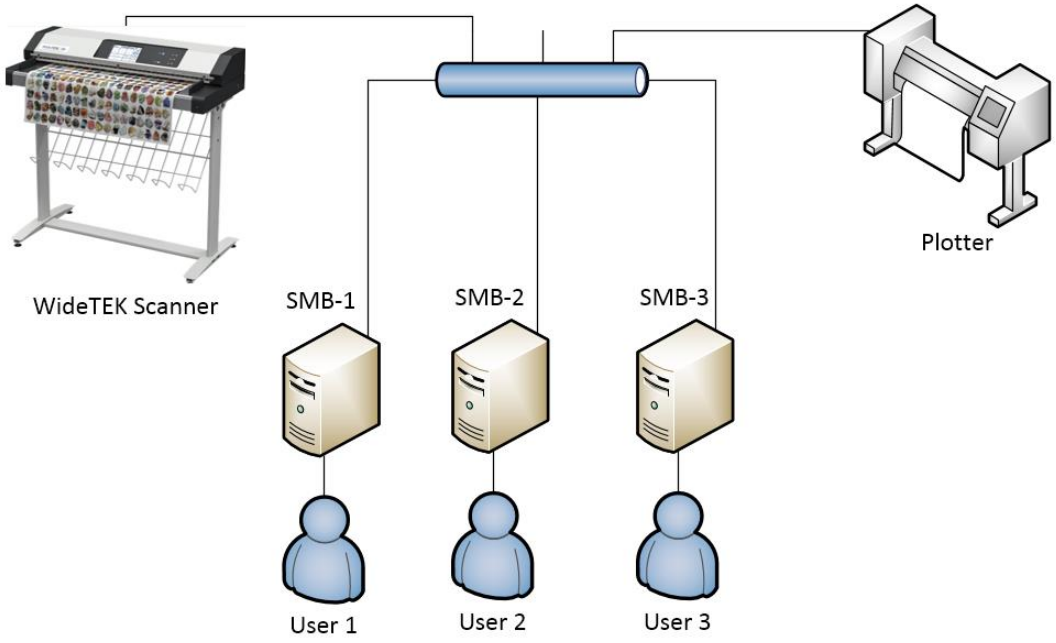

Figure 1 Typical network configuration

Scan2Net scanners are network scanners. In the above scenario, the WideTEK 36 scanner will directly copy to the plotter through the network. Several users on the local network want to scan to their local computers and to achieve this, they each have created an inbox called SMB-1, -2, -3 in the above diagram.

This document will guide the user through typical setup processes which must be executed on each host in case that a scanner accessible SMB share needs to be created and free or protected access to this SMB share is necessary.

As an alternative, the scanner hosts its own SMB share like what many MFPs do. This internal SMB share is not protected and can only be switched on or off. If the system administrator is not available or protection software inhibits the generation of a scanner accessible SMB share, the scanner's internal SMB is always available.

8. Local Scanner SMB Share

The scanner offers a SMB shared folder without any access restrictions on the device itself.

To enable an SMB local share folder, log in to the scanner as **Poweruser**, go to **Base Settings** and select **Network Configuration** from that menu. Then select **SMB settings** and set the value for Enable Local Share to Yes or No.

This SMB shared folder is not enabled by default. To enable the local shared folder, you have to switch the setting **Enable Local Share** in the SMB Settings to Yes.

Figure 2 SMB Settings (Local Share enabled)

If the local share is enabled, you can access this SMB share from any network workstation by addressing **\\SMB-hostname\scans**. The SMB hostname of the scanner is configured in the SMB Settings.

8.1. Allow Everyone to Access the Shared Folder on a Workstation or Server

The easiest way to share a folder is to allow **Everyone** to read and write into this folder. In this context, **Everyone** does not literally mean everybody. **Everyone** includes all user accounts that are allowed to access the server or workstation where the shared folder is located. Allowing **Guest** to read and write to a folder includes users who do not own an account on a workstation or server.

8.2. Add a user name or group

If **Everyone** is not present in the list of groups and user names, click **Add**.

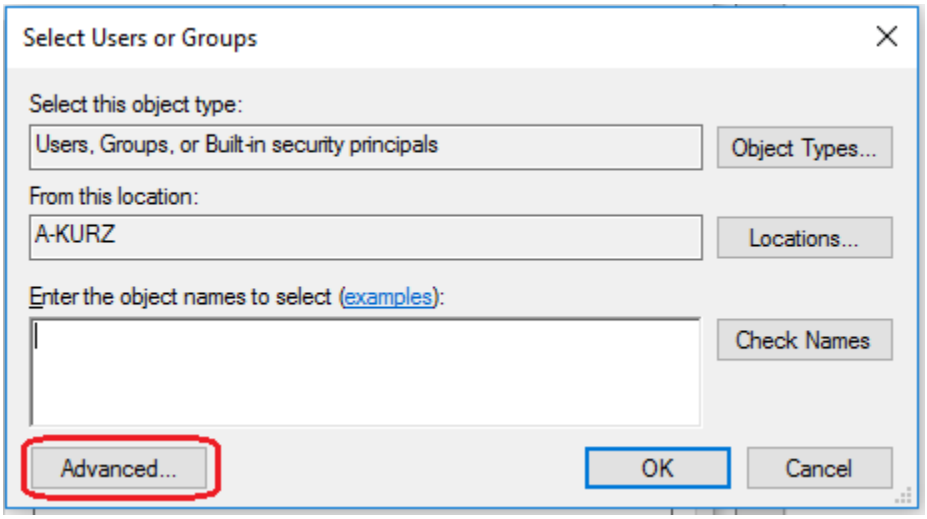

Figure 3 Find a user or group on a workstation

Either enter the user or group name or press the **Advanced** button.

Click **Find now** to see the list of all groups and user names.

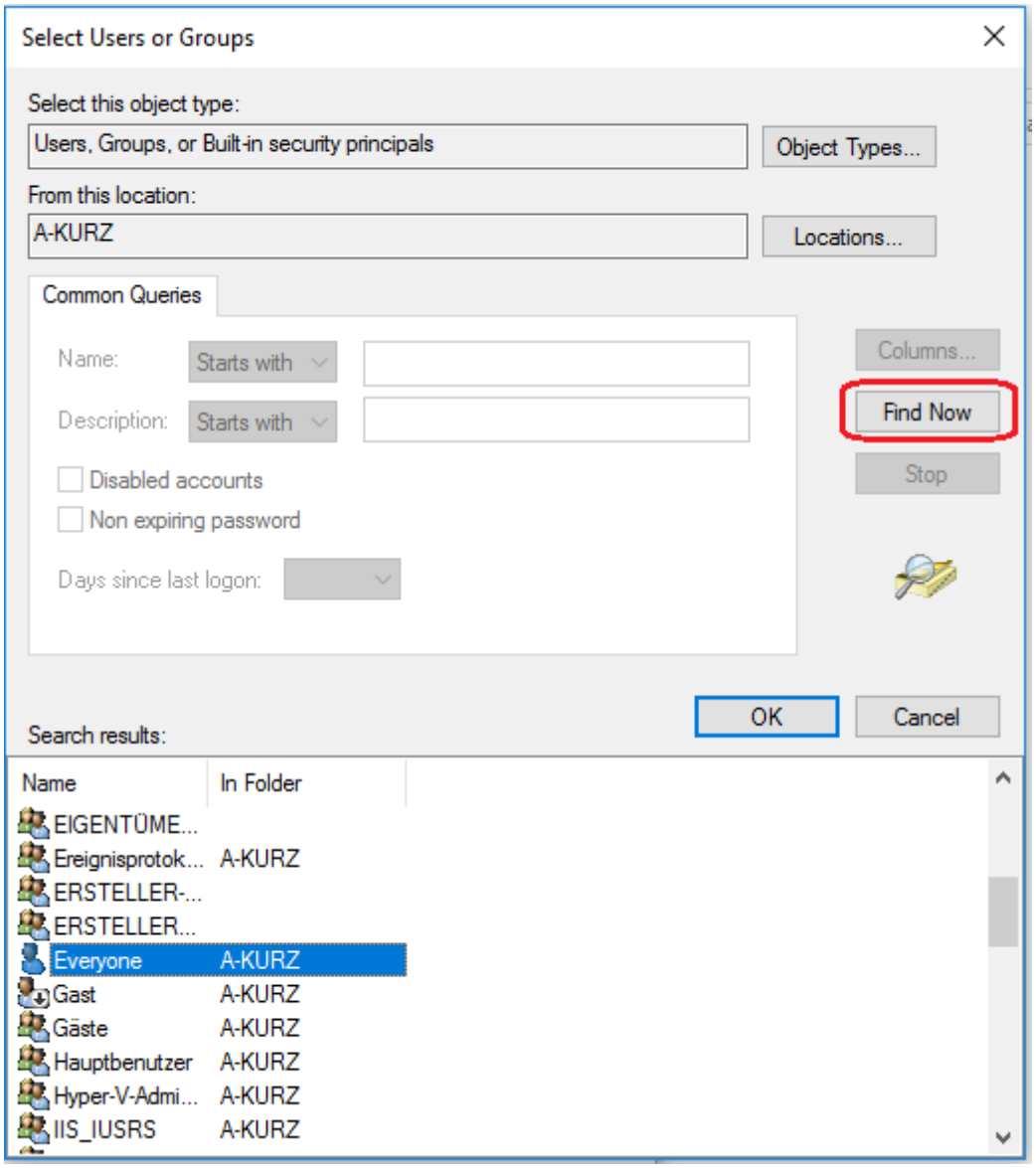

Figure 4 Select the user name or group, e.g. Everyone

Select **Everyone** and click OK.

Click OK again to confirm.

8.3. Share the Folder

8.3.1. Identify the folder to be shared

On the Windows workstation, identify the folder to be shared. Open the context menu with a right mouse click.

It is not recommended to use **Share with** because this will share not only the selected folder but the entire network path including all subfolders. Select **Properties** to use the advanced sharing function instead.

In this sample, the folder to be shared is **WideTEK36_Scans**, a subfolder of **C:\IAC-Images**.

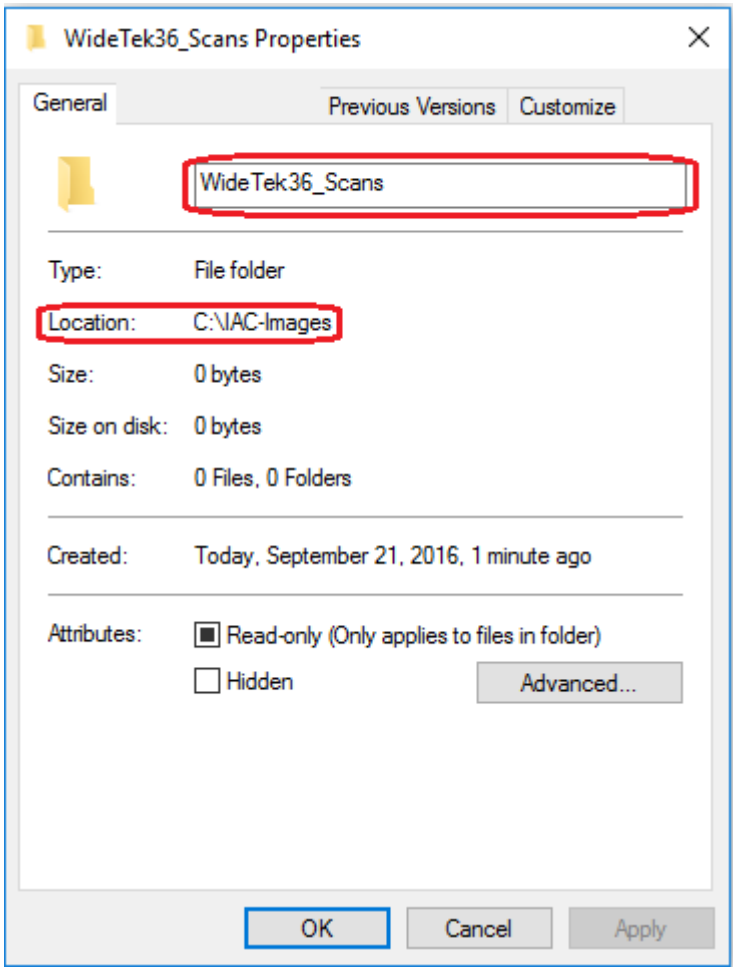

Figure 5 Properties of the folder to be shared: *General* tab

8.3.2. Advanced Sharing

Select the **Sharing** tab. This tab shows you whether this folder is currently shared and if a user name and password is required to access it.

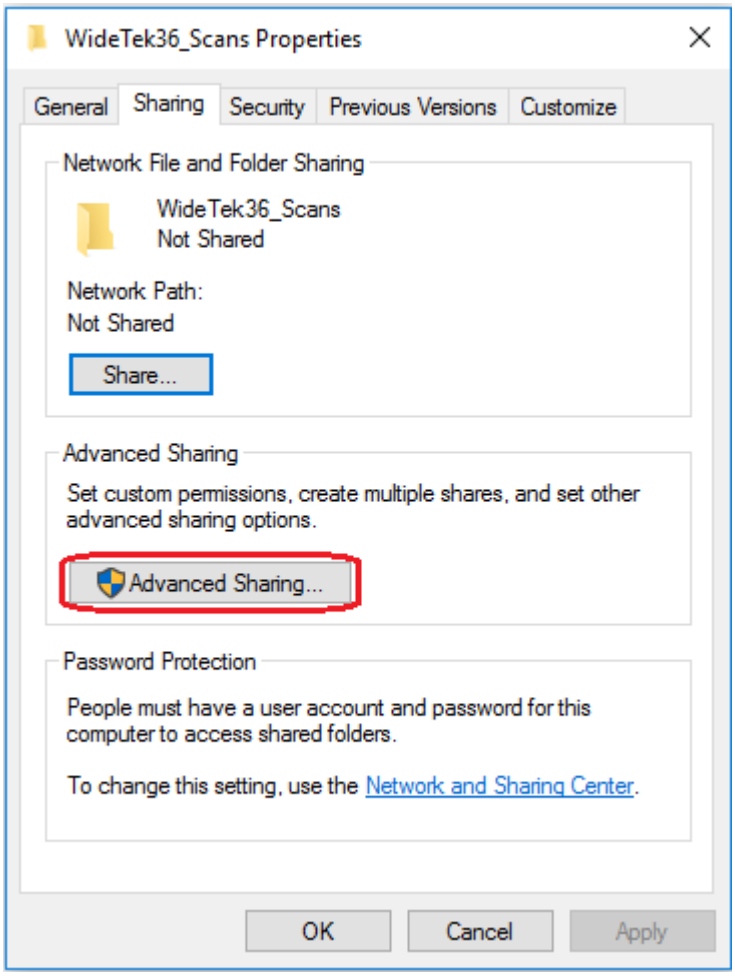

Figure 6 *Sharing* tab: Select *Advanced Sharing* to set permissions

Click **Advanced Sharing**.

Now share this folder and define a name for this share. Once this folder is shared, you can give it additional names. In this case, be sure to know the proper share name.

Limit the number of simultaneous users, if required. This can help maintain acceptable access speeds.

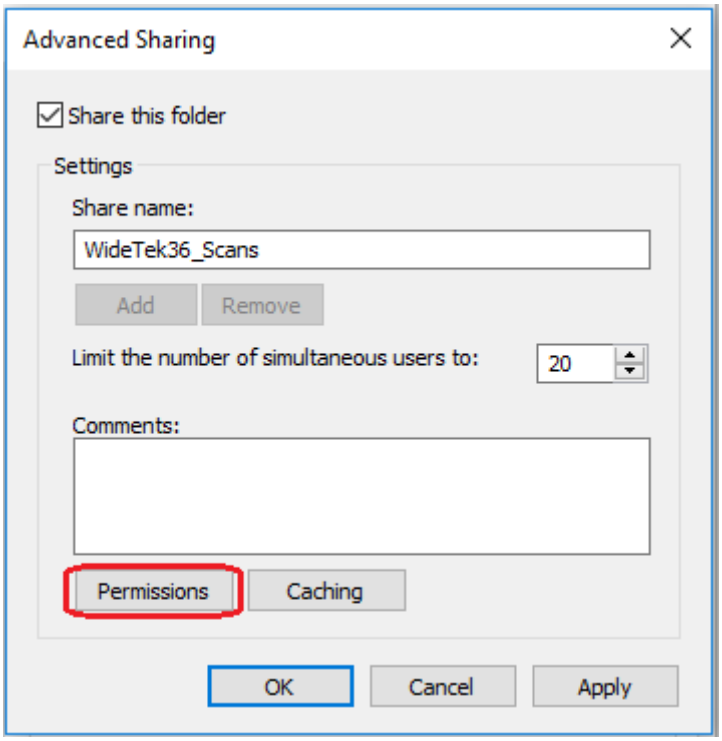

Figure 7 Advanced sharing: Share name and number of users

8.3.3. Permissions and Security

The next action is to define **permissions**.

The actual permission to access a shared folder depends on the proper combination of permissions given to the **user/group** in the network **(Permissions tab = SMB level)** and in the file system **(Security tab = NTFS level)**. Please be aware that NTFS permissions can restrict SMB permissions.

8.3.3.1. Set SMB permissions

Go to the **Permissions** tab and set SMB permissions for the user or group.

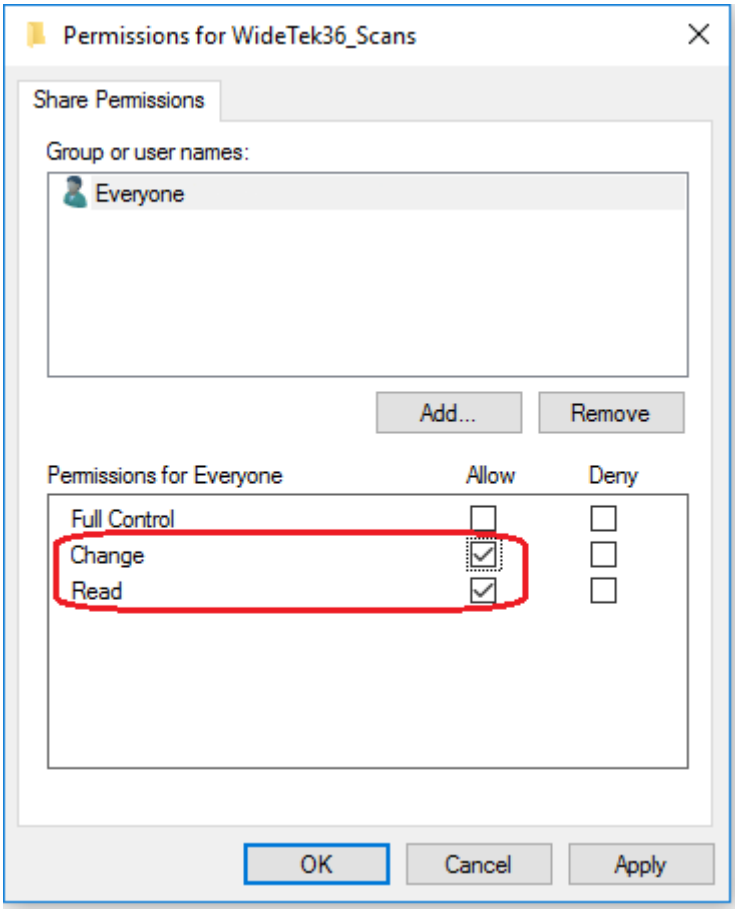

Figure 8 Set access permissions for users and/or groups

Everyone includes all users whose user name and password allows them to access the workstation or server where the shared folder is located. Therefore, **Everyone** is the default user group on the **Permissions** tab.

Now you can set share permissions for **Everyone** as shown in Figure 8.

It is neither required nor recommended to give full control to **Everyone**, just allow **Everyone** to read and to change.

8.3.3.2. Security (NTFS Permissions)

Check the permissions of the shared folder on the file system level.

Make sure that the permissions match the SMB permissions of the user or group.

Example: If you allow **Everyone** to change and read on the **Permissions** tab but deny **Everyone** to write on the **Security** tab, it will not be possible to store a file in this shared folder.

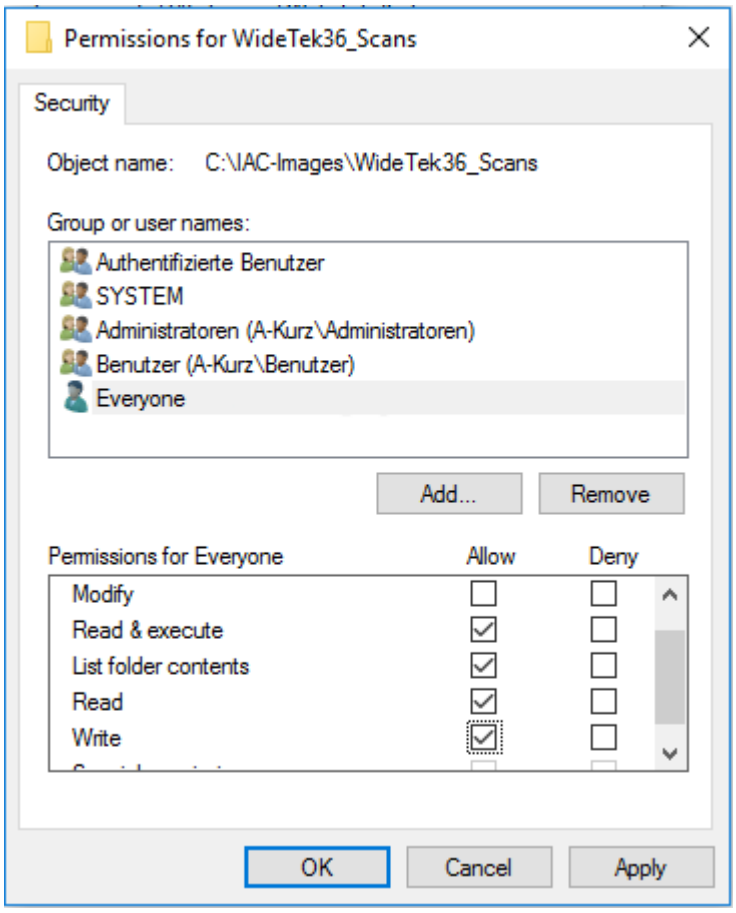

Figure 9 Check SMB permissions for users and/or groups

8.4. Select the Proper Sharing Options for your Network Profile

Open the Control Panel and go to the **Network and Sharing Center**.

Select **Change advanced sharing settings**.

The appropriate settings depend on your specific requirements and security policies, therefore only general hints can be given.

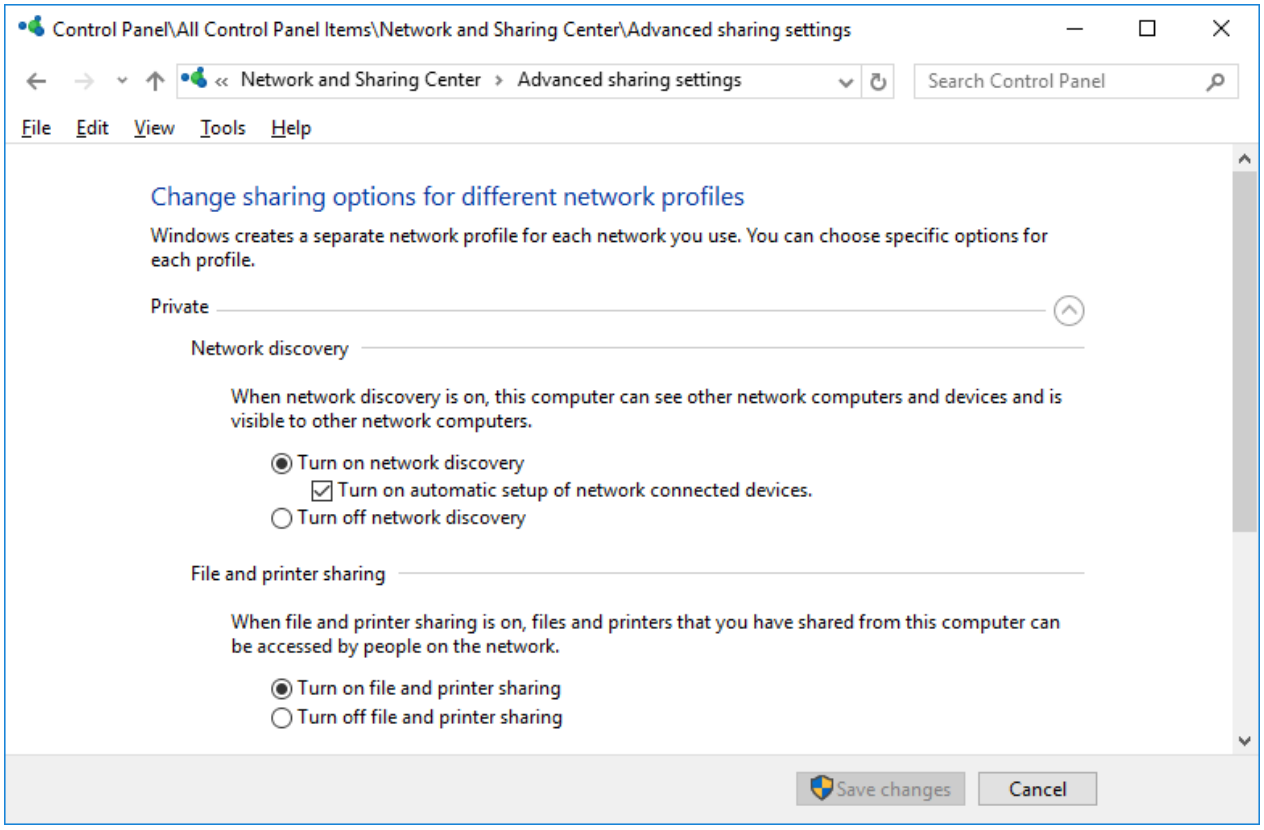

Figure 10 Sharing options 1

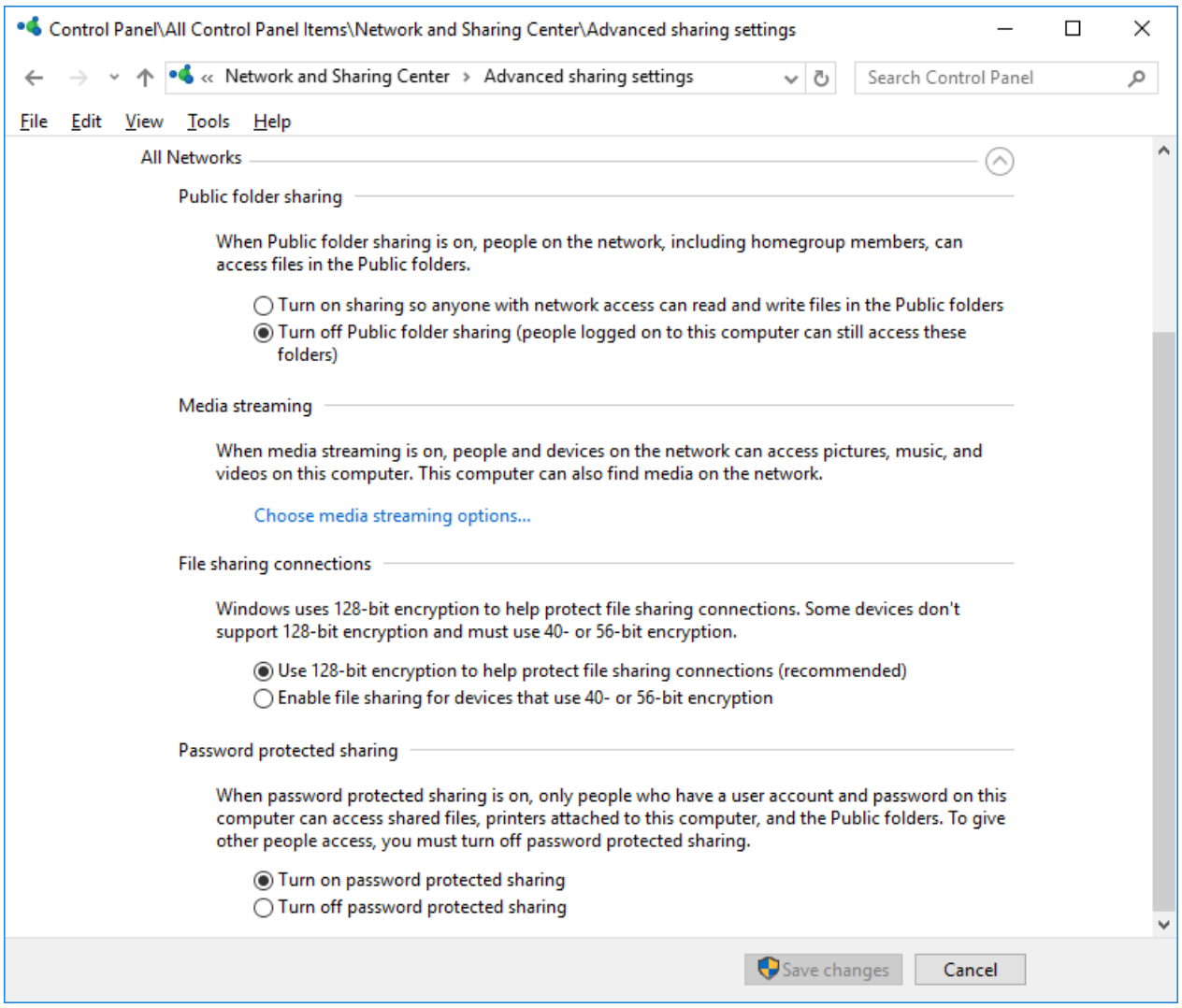

Figure 11 Sharing options 2

The sharing options shown in **Figure 10** and **Figure 11** will work in many network environments. Nevertheless, it may be required that you change some of the settings.

8.4.1. Network Discovery

If network discovery is turned on, this computer is visible in the network. This means, that also the Bookeye or WideTEK scanner can see this computer and its shares.

If turned off, the scanner cannot see the shares, i.e. the browse function will not show this computer. Still it is possible to access the share, you only must type in the entire path correctly.

8.4.2. File and Printer Sharing

Bookeye and WideTEK scanners can only access shared folders if file and printer sharing is turned on. Therefore, ensure that this is the case.

8.4.3. Public Folder Sharing

Decide whether anyone with networks access shall be allowed to access the Public folders **(turn on)** or if only users logged on to the computer shall be allowed to access the Public folders **(turn off)**.

8.4.4. Media Streaming

This option does not apply here.

8.4.5. File sharing connections

128-bit encryption is recommended and works on all Windows 7 and higher operating systems.
If outdated scanner models connect to network devices, it may be necessary to reduce encryption to 40- or 56-bit. This is only necessary if the scanner runs firmware 4.xx

8.4.6. Password Protected Sharing

The appropriate setting depends on your security requirements. If turned on, the Bookeye or WideTEK scanner needs a valid user name and password of a user account on this computer to access a shared folder. The following chapter will guide you through the setup of the scanner.

If turned off, the scanner can access a share without requiring a user name and password.

Note: **Check if the group policy allows network access by the scanner, because the group policy overrules local settings.**

In other words, the group policy can refuse to let the scanner store files in the shared folder even if its user (SMB) and file system (NTFS) permissions are properly set.

9. Set up the Scan2Net® Scanner to Access a Shared Folder

9.1. Poweruser

The setup manual of your Bookeye or WideTEK scanner tells you how to log on as **Poweruser**, how to configure the network and how to set up at least one template for accessing an SMB share.

All parts of a Scan2Net scanner network configuration should be inspected:

- **IP Configuration Method** - Manual or DHCP
- **IPv4 (Network Interface 0)** - For Ethernet networks
- **IPv4 (Network Interface 1)** - For Wireless LAN networks
- **Domain Name Server settings**
- **SMB Settings**
- **Firewall Settings** - optional

After the basic TCP/IP configuration, the following items are mandatory for accessing an SMB share from a Scan2Net scanner in a network.

9.1.1. Domain Name Server

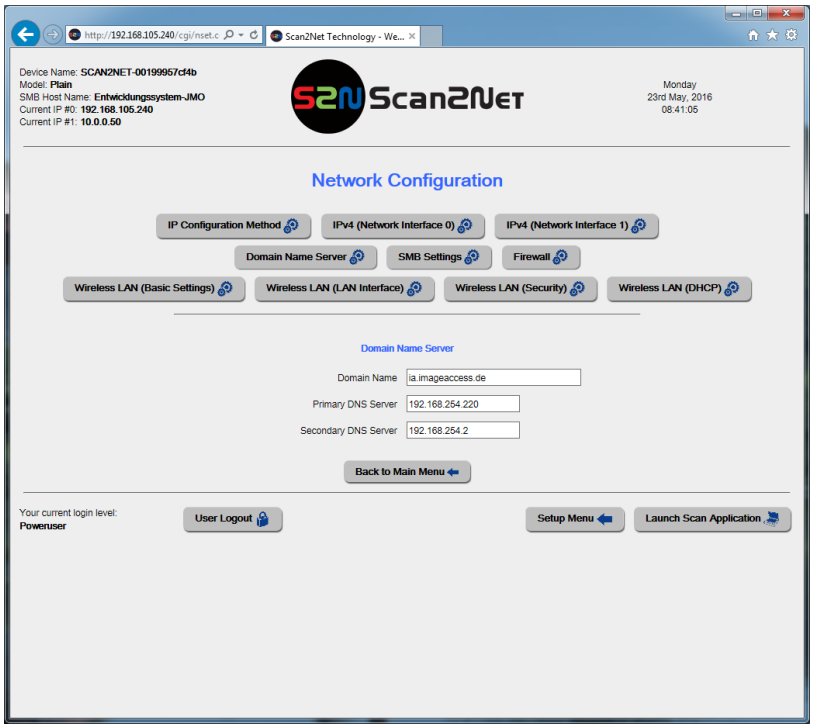

Figure 12 Domain Name Server

- **Domain Name** - Enter the domain name here.
- **Primary DNS Server** - Enter the address of the primary DNS server here.
- **Secondary DNS Server** - Enter the address of the secondary DNS server here.

9.1.2. SMB Settings

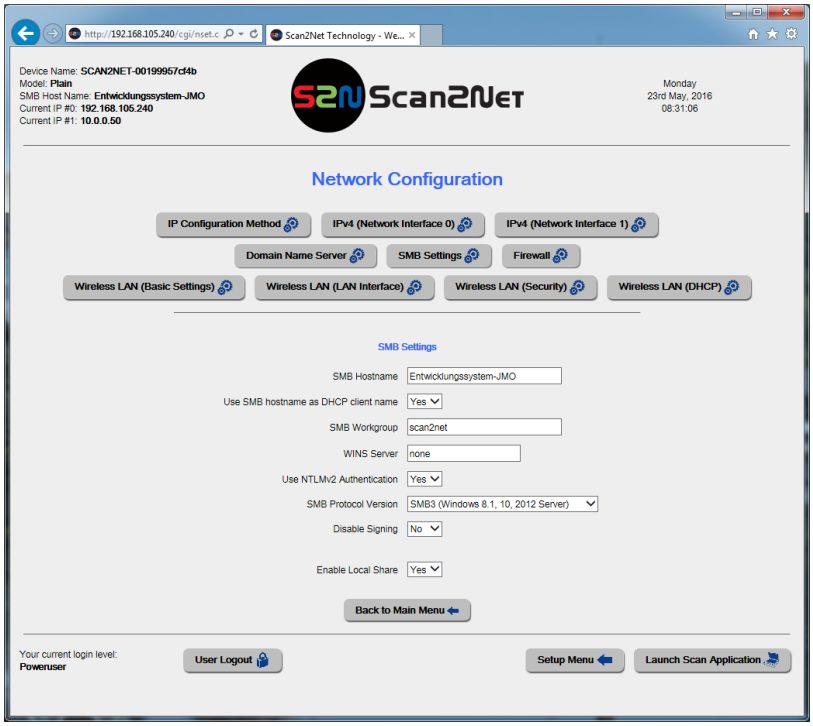

Figure 13 SMB Settings

- **SMB Hostname** — Enter an **SMB host name** to identify the scanner in the network. Default is the MAC address of the scanner.
- **Use SMB hostname as DHCP name** — Select **Yes** if the SMB host name should be used as client name for DHCP.
- **SMB Workgroup** — Enter the SMB workgroup in which the scanner is installed. In domain-controlled networks, the Domain Name Server configuration must be used.
- **WINS Server** — If a WINS server is used, enter the **IP address of the server** or **\\<Server name>** here.
- **Use NTLMv2-Authentica-tion** — Default value: **Yes**. Select **No** for Windows 2000 and earlier OS compatibility.
- **SMB Protocol Version** — Select from the settings offered in the list. The recommended operation systems for the protocol version are named in brackets. Basic SMB network functions are granted with all protocol versions, but some newer SMB features will only work with dedicated protocol versions.
- **Disable Signing** — Default value: **No**. The Apple OS-X (El Capitan and newer) implementation of SMB is slightly incompatible to Windows SMB3. Disable Signing will switch on compatibility mode.
- **Disable Signing** — Refer to chapter **8. Local Share** of this document.

Note: **As a helpful tool, you can display the local TCP/IP configuration of a network PC by the MS Windows command line entry: ipconfig /all.**

Figure 14 Display TCP/IP configuration

9.2. SMB Templates

Before you start to configure SMB templates, check if:

- the network is properly configured?
- a name server is registered in the network?
- the name server replies to the *ping* command?

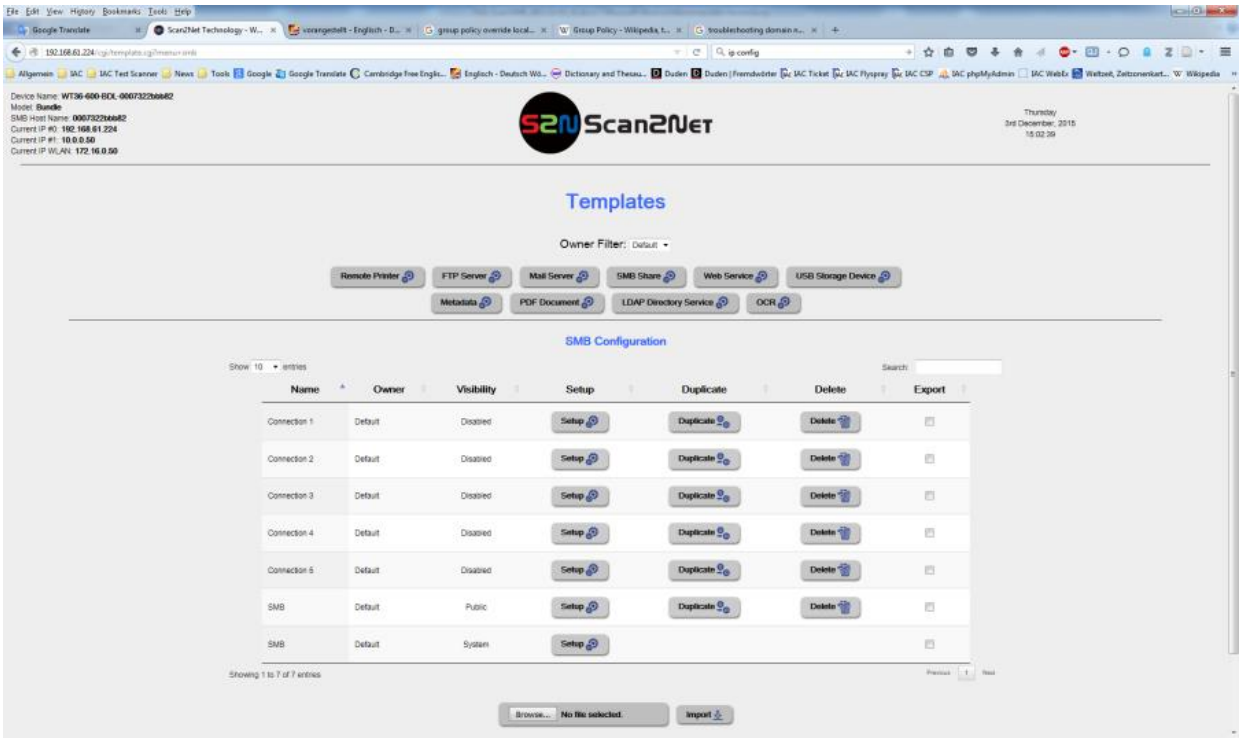

Figure 15 SMB templates

Before you set up or duplicate a template, make sure that the owner filter is set to the proper user of the template.

Owner filter: **Default** shows the configurable SMB templates of the standard operator. Select one of the templates either to set up or to duplicate before you set up the copy.

9.2.1. Setup SMB Templates

Parameter	Description
Port (139/445)	Enter the IP port for the SMB network communication. Default is port 139 for Windows workstations and port 445 for MAC workstations.
Network Type	Select between **Workgroup Network** and **Homegroup Network**. For detailed information about the correct network type ask your network administrator.
Server Authentication (only with Workgroup Network)	Select the authentication method. Set to **YES** if an authentication is required.
Login	Enter the user name on the Windows workstation/file server which you want to connect to.
Password	Enter the password associated with the user name for the login at the Windows workstation/file server which you want to connect to. The password is stored using encryption.
SMB Path	Enter the upload path on the Windows workstation. Start with a double slash (**//**) for the root directory. Click the icon to browse the workstation/server list and the directory structure of the Windows workstation/file server. **Note:** A valid login for browsing the directory structure is necessary.
Hidden Share	Select **Yes** or **No**. For further details see chapter **9.2.2, Browse the network**
File Name	Enter the file name. A time stamp will be added to this prefix to form the complete file name.

Configuration Test: Click on this link to check the settings. The scanner sends a small .txt file to the destination folder and stores it there. A separate window will open to show the test results.

Note: **Each change of an entry field is transferred to the scanner immediately.**

Note: **Export all templates that you created and/or modified yourself after they have proved to work as desired so that you can import them in case that you deleted any of them by mistake.**

9.2.2. Browse the network

If you turned on **network discovery** (see chapter 8.4.1) and network browsing is not disabled at the workstation or server, you can browse your network to find the shared folder.

Enter a valid **Login** and **Password**.

Network browsing is without function (empty SharePoint list) if the browsing itself is also allowed only to registered users. A valid user name must be set. Then network browsing is possible.

Three types of users are possible, which differ in their notation in Login: Local users, network users and domain users. Local users are listed with the username, e.g.: User. Network users have the name of the authentication server as prefix in the login name, e.g. Server/User. Domain users have the name of the domain as prefix in the login name, for example, company.local/User.

Note: **Contrary to the Windows xx notation the *slash* symbol / is the required delimiter. As of Scan2Net version 6.30A, the *backslash* symbol \ will be automatically converted to the *slash* symbol. Newer Windows networks also support the notation user@server or user@domain, e.g. User@company.local.**

If network browsing is without function, you can enter the full SMB path, e.g. **//workstation-name-or-IP address/IAC-Images/WideTEK36-scans**.

To access a hidden share, you must enter the full SMB path. The name of the hidden destination folder must be terminated with a **$** sign, e.g. **//workstation-name-or-IP address/IAC-Images/WideTEK36-hiddenscans$**.

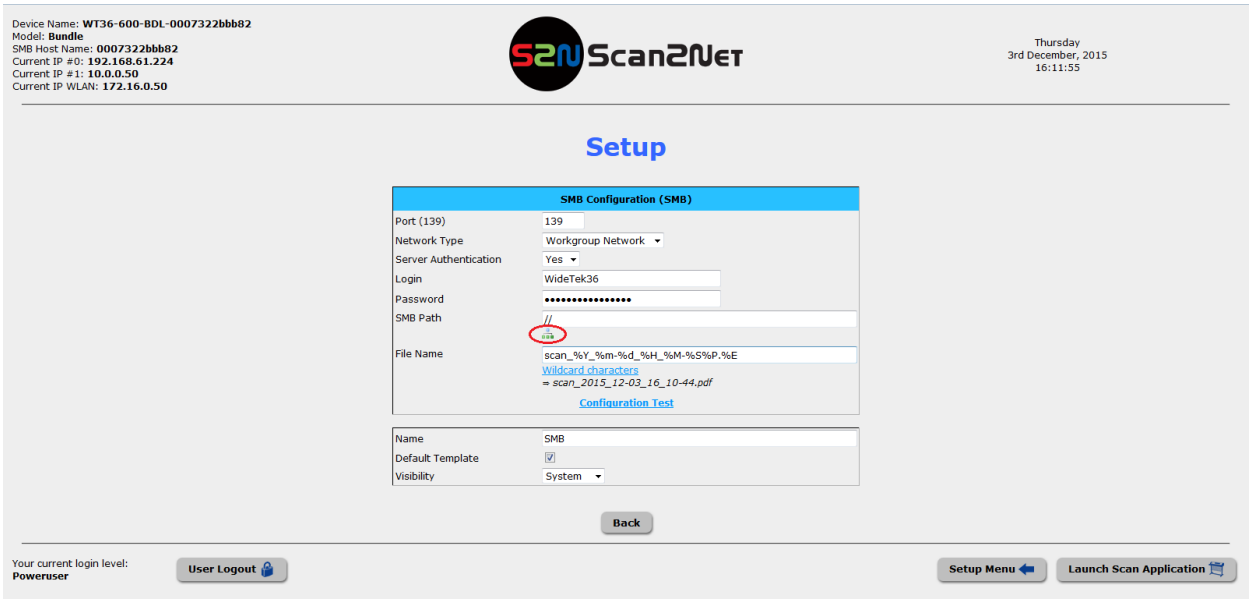

Figure 16 Hit the browse button to get a list of available Servers and workstations

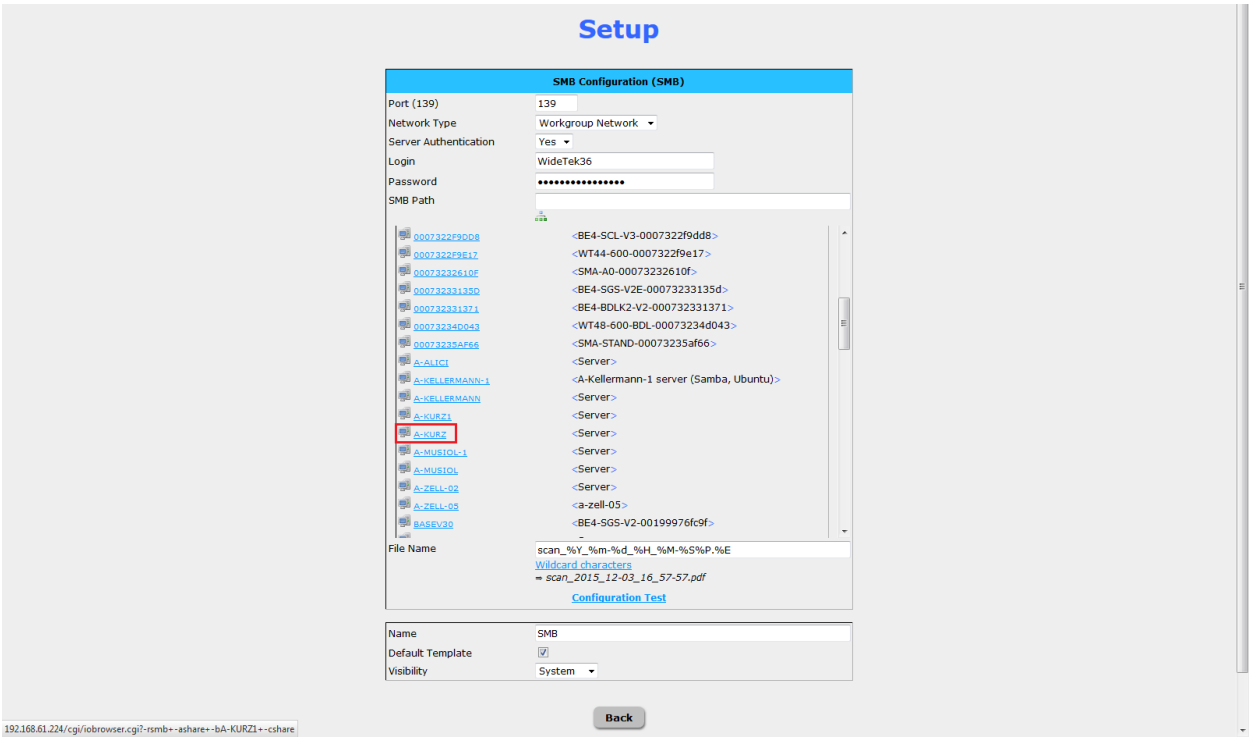

Figure 17 Select the workstation or server from the list

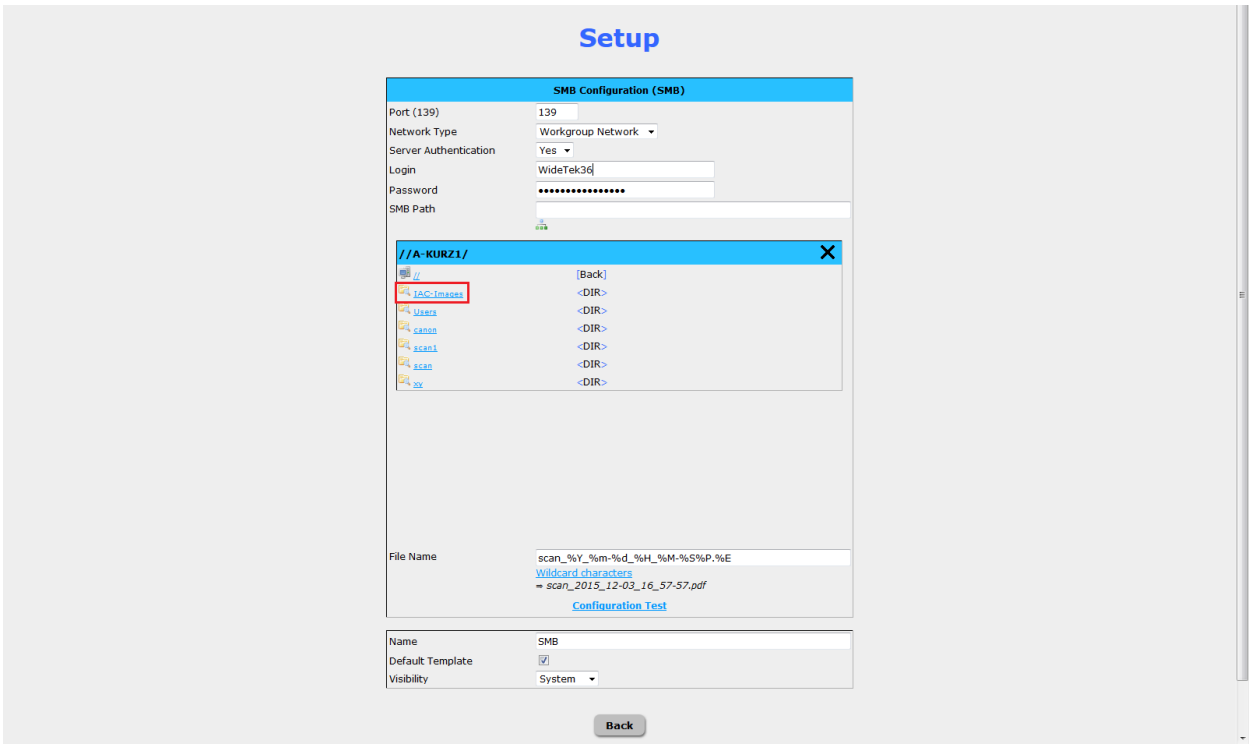

Figure 18 Select the main directory

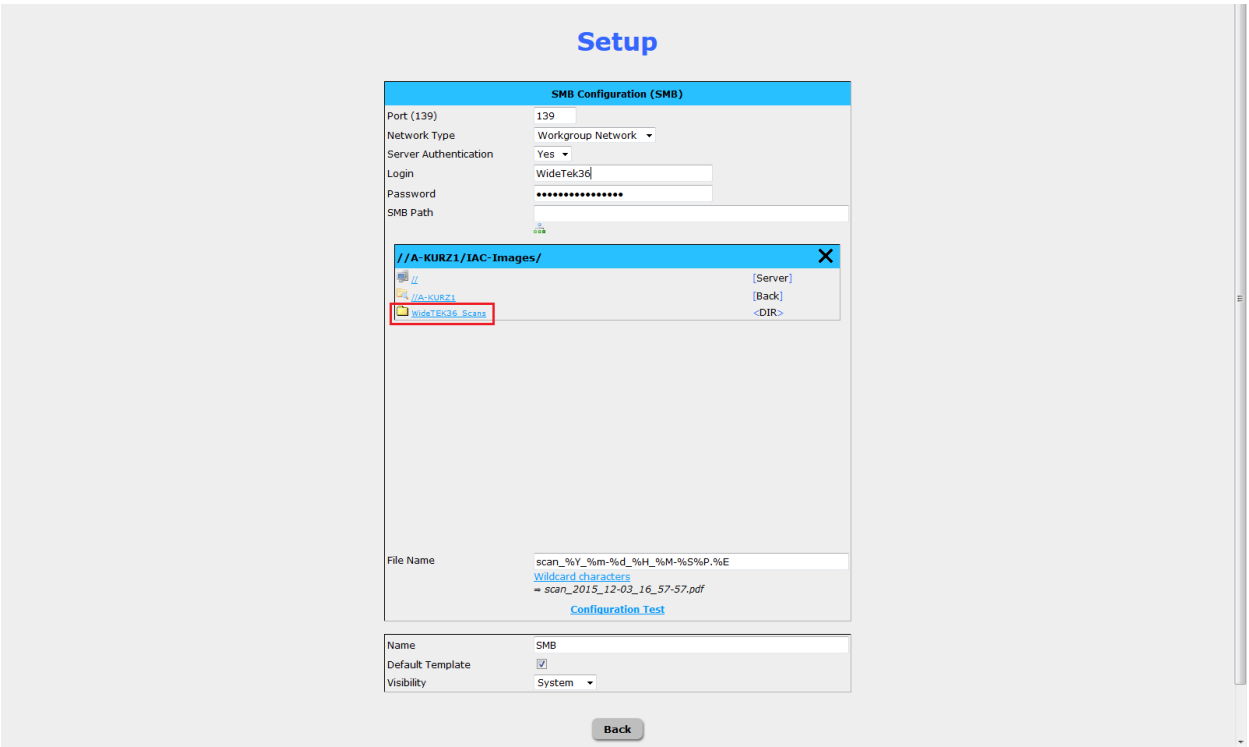

Figure 19 Select the target subdirectory

9.2.3. Select the destination folder

Select the previously shared destination folder and close the window with the X button to confirm.

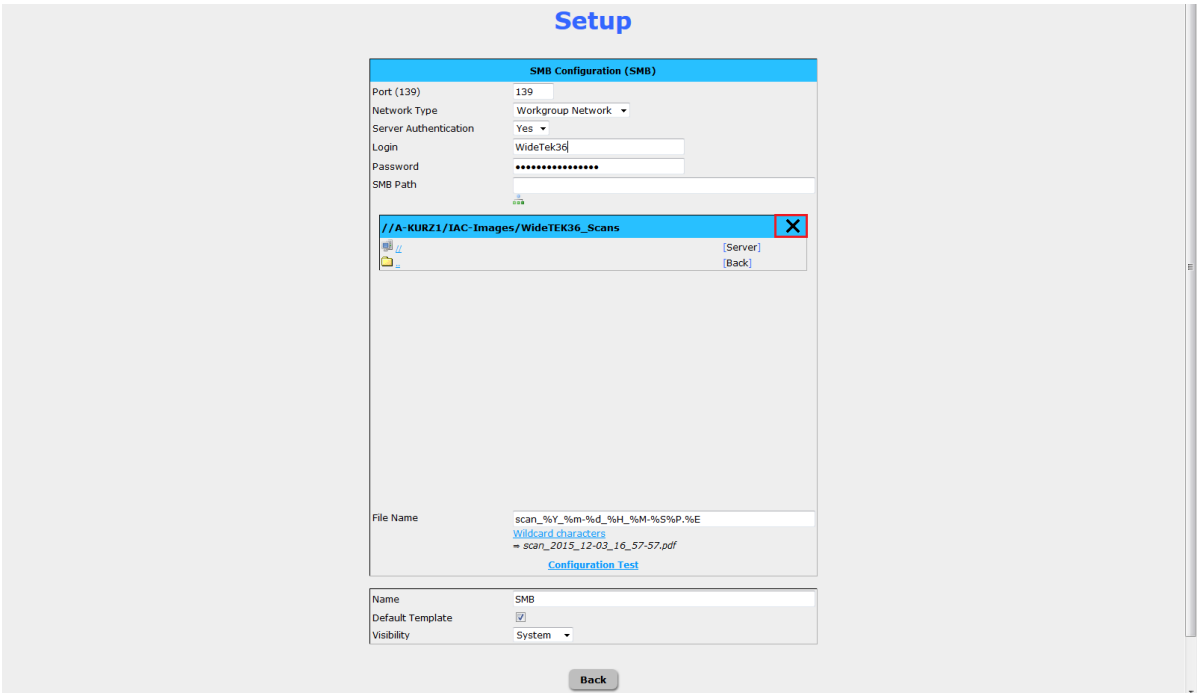

Figure 20 Finish the setup of the SMB share by closing the browse window

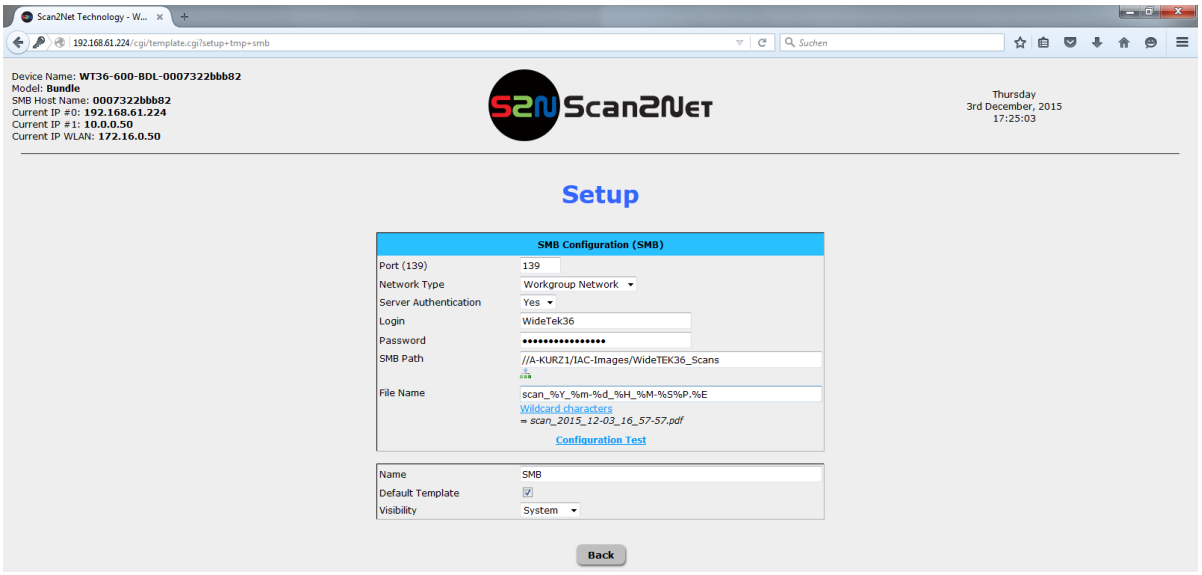

Figure 21 Example of a valid SMB Share

9.2.4. Check the settings

Perform the **Configuration Test** to check if the destination folder can be accessed.

The SMB path shows only the name of the workstation and the name you gave the share (see **Figure 21**).

It does not show the actual path from root directory through destination folder, and by that hides the directory structure of the workstation or server while the share is still accessible.

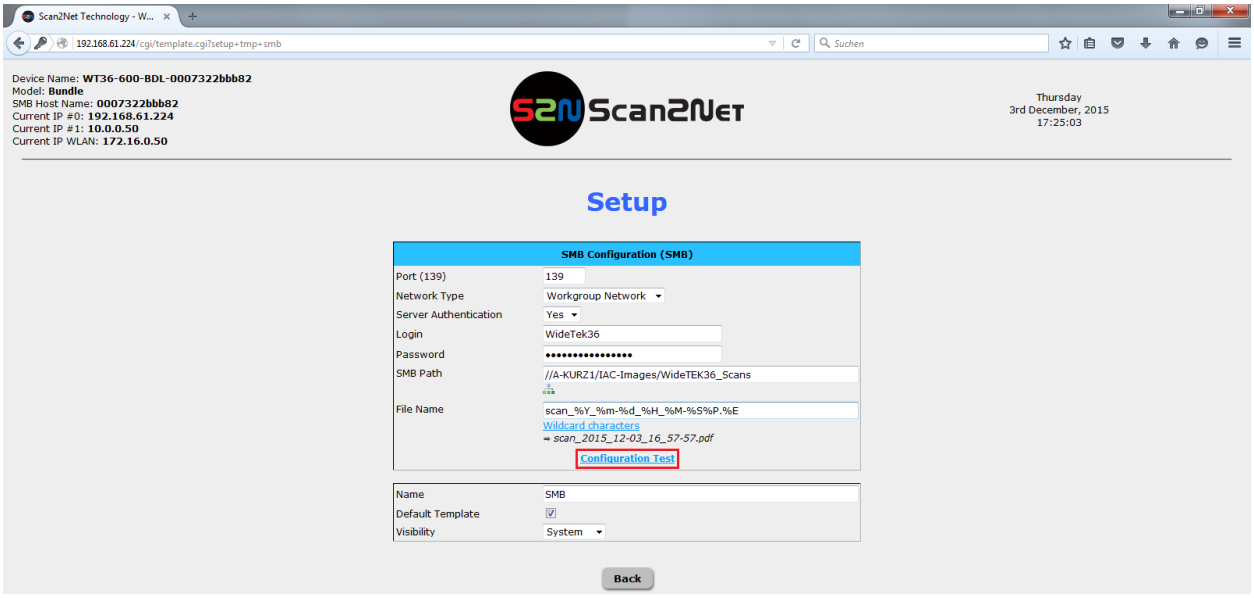

Figure 22 Configuration test

Configuration Test:
Click this link to check the settings. The scanner sends a small .txt file to the destination folder and stores it there. A separate window will open to show the test results.

Beneath you see an example of a positive test result, i.e. the .txt file could be stored in the SMB share.

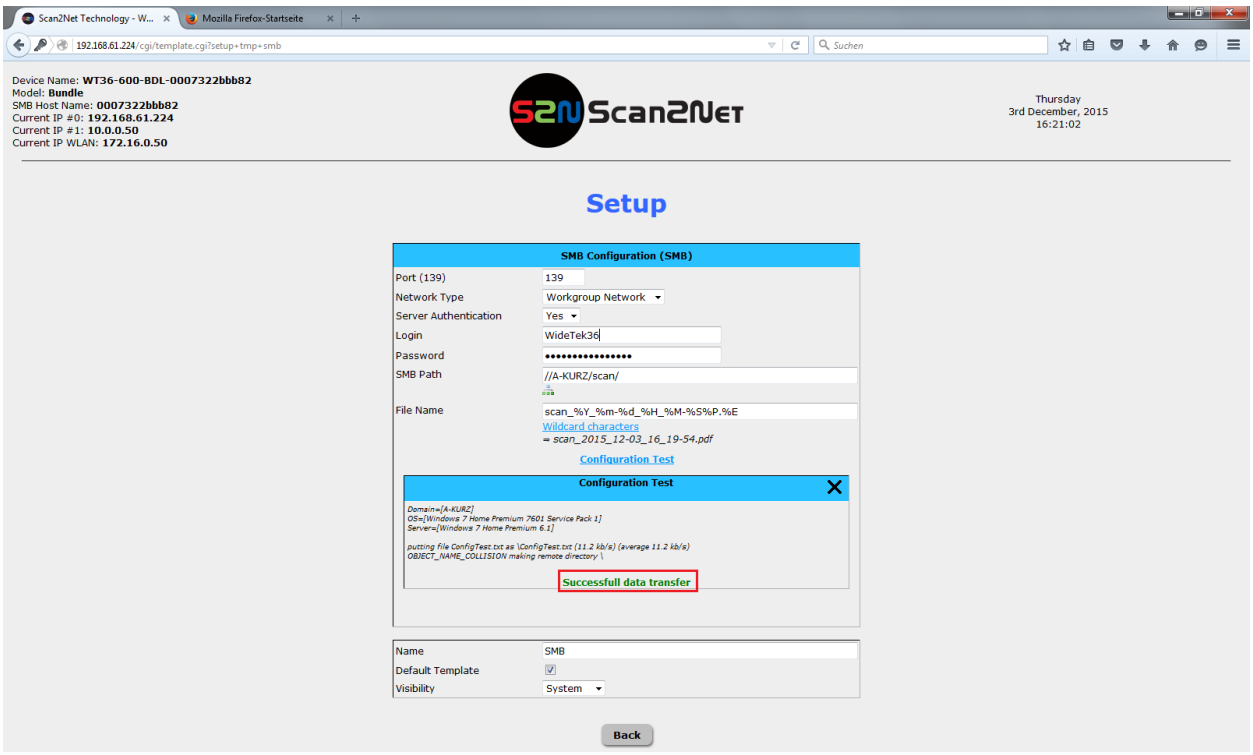

Figure 23 Successful data transfer

Close this window and click the ‘Back’ button to store this template.

The scanner is now ready to save scanned images or jobs directly in the shared folder in the network.

Beneath is an overview of the most common NT status messages: In case of failure, the status message shown would give an indication of the type of the error. **Important:** These are status messages, not error messages.

If the message **OBJECT_NAME_COLLISION** appears as in **0**, the subdirectory already exists in the share and no longer needs to be applied.

BAD_NETWORK_NAME: The specified network host or the specified share do not exist or prohibit to accessed by this user or device. If so, this may indicate the lack of appropriate permissions, i.e. to read/write in the SMB share.
Remedy: Check the network path, perform a network reachability test using ping, check the access rights and adjust accordingly.

LOGON_FAILURE: The logon to the SMB share with the specified authentication fails.
Remedy: Check login name and password and if necessary retype both, check whether the credentials match the share and if there are access restrictions of the share for specific hosts.

ACCESS_DENIED: This notice indicates that you tried to access SMB shares or browse a server directory without appropriate permissions or by using an invalid user name/password.
Remedy: Check access rights and adjust accordingly.

Note: The scanner records every status message of each SMB access in his own log file to be reviewed later. For an extended list of potential SMB relevant status messages follow this link: https://msdn.microsoft.com/en-us/library/ee441884.aspx

10. MAC OS X SMB Share

10.1. Find NetBIOS and WORKGROUP name of your MAC

To find the network name of your MAC in OS X, open the Network pane of System Preferences.

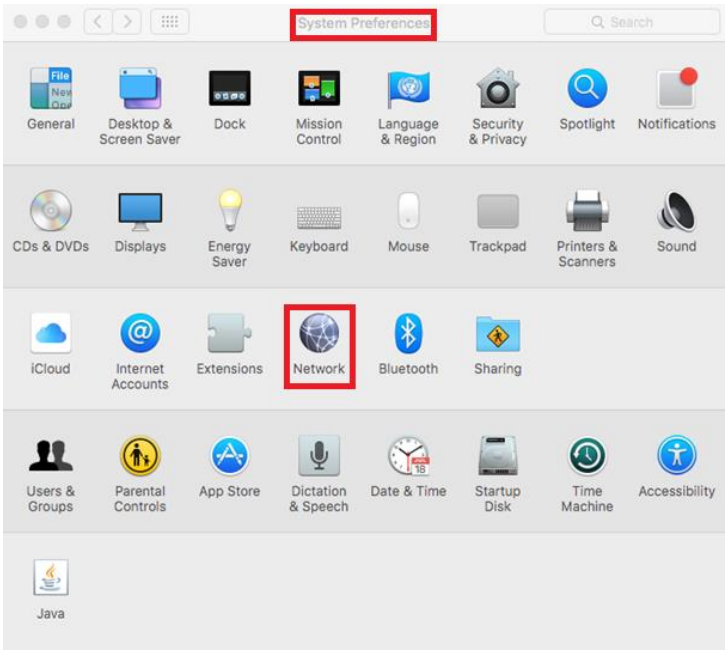

Figure 24 MAC OS X - System Preferences

Open advanced Ethernet settings.

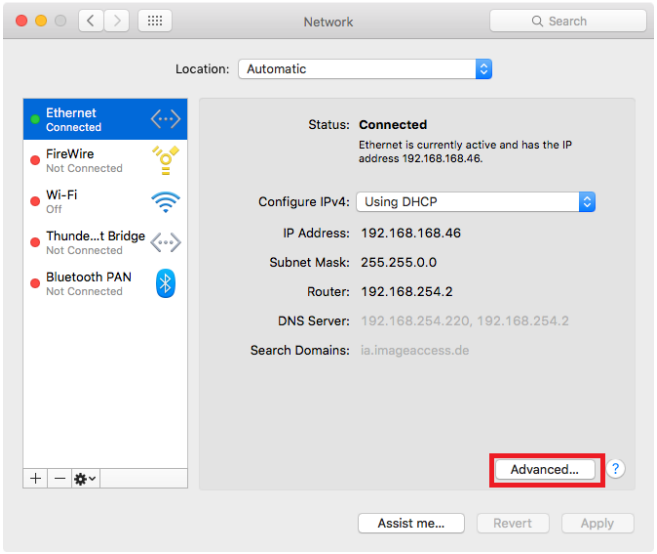

Figure 25 Network Settings

On the tab **WINS** you will find the NetBIOS and WORKGROUP name of your computer.

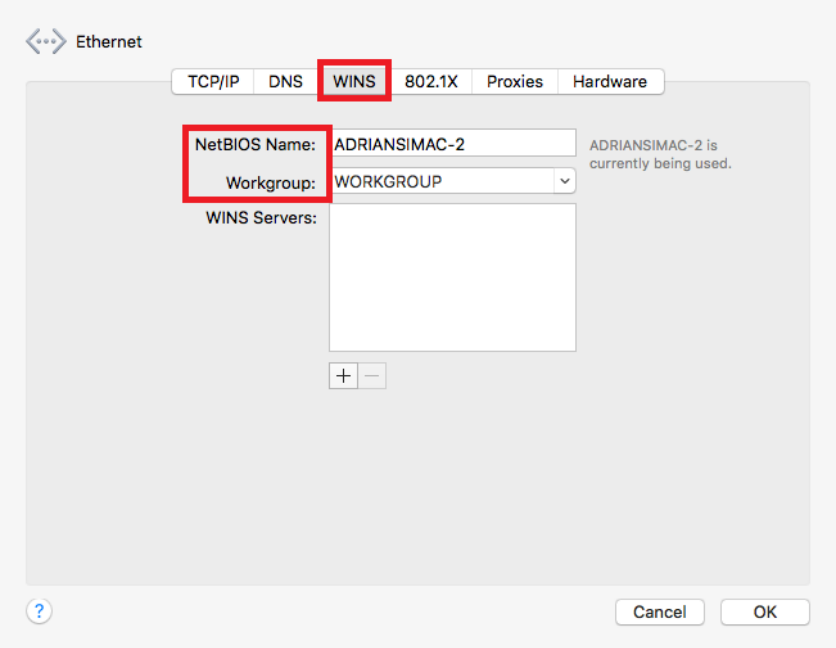

Figure 26 Advanced Ethernet Settings

10.2. Enable File Sharing

To enable File Sharing in OS X, open the Sharing pane of System Preferences.

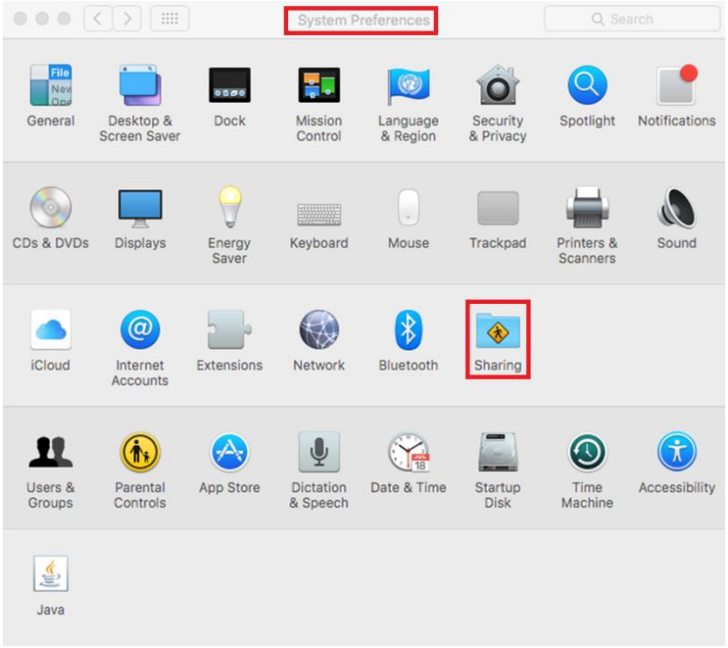

Figure 27 MAC OS X - System Preferences

First, activate the File Sharing service.

In Shared Folders select the folder you like to share.

In Users set the user permission of the shared folder to “Read and Write”.

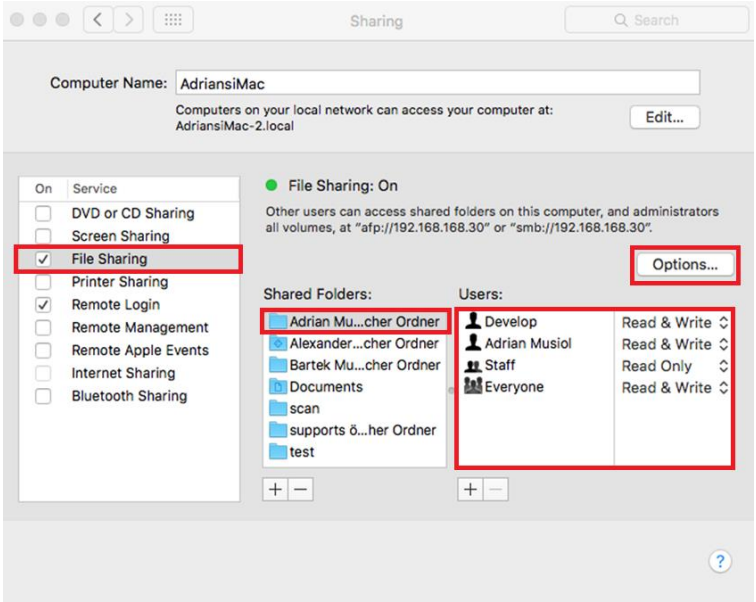

Figure 28 MAC OS X - Sharing

10.3. Advanced Options

Open “Options”.

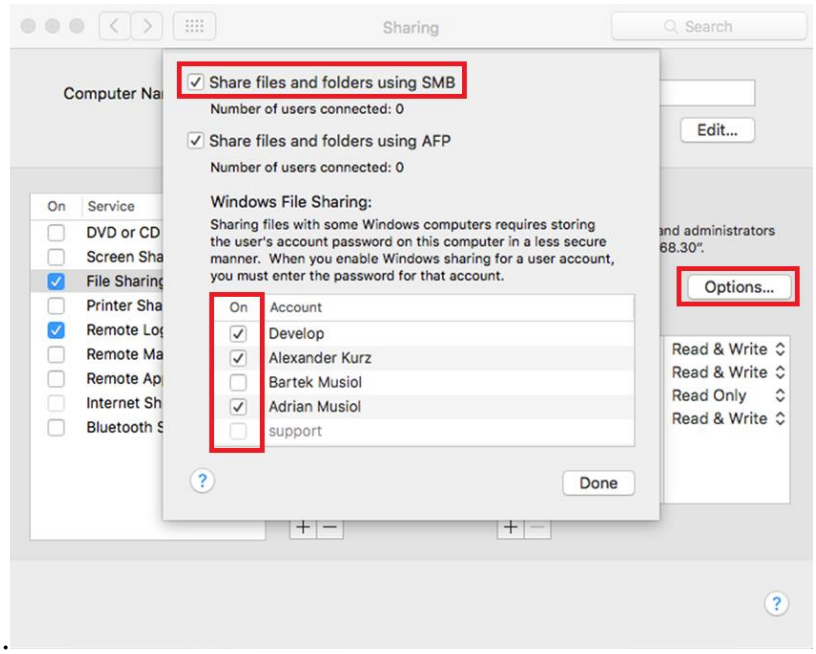

Figure 29 MAC OS X - Advanced Options

Activate “Share files and folders using SMB”.

Select the users for “Windows File Sharing” for SMB access.

10.4. Scan2Net SMB Configuration

Connect your scanner via web browser.

In Setup Device choose the login level: Poweruser and login.

In Base Settings / Network Configuration / SMB Settings set ”Disable Signing“ to YES.

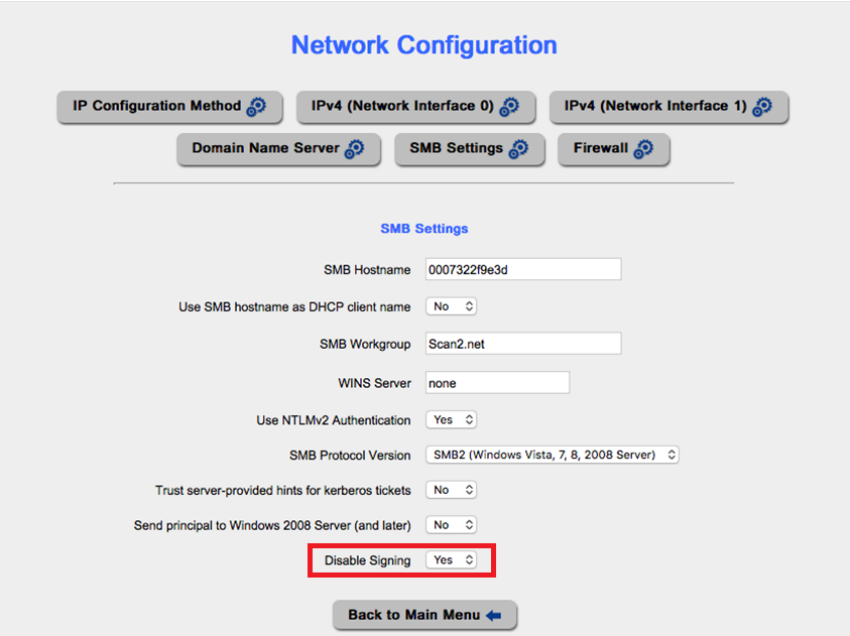

Figure 30 Scanner network configuration SMB settings

10.5. Scan2Net SMB Template Configuration

In Base Settings / Templates / SMB select SMB Share.

In SMB Configuration open the Setup of template SMB, see chapter 9.2 of this document.

Change the Port number to 445.

Set Server Authentication to Yes if required.

Enter your network login name and password if required.

In SMB Path enter the path to your shared folder using the NetBIOS name of your computer and the name of your selected shared folder like

//NetBIOS name of your computer/Name of your selected shared folder.

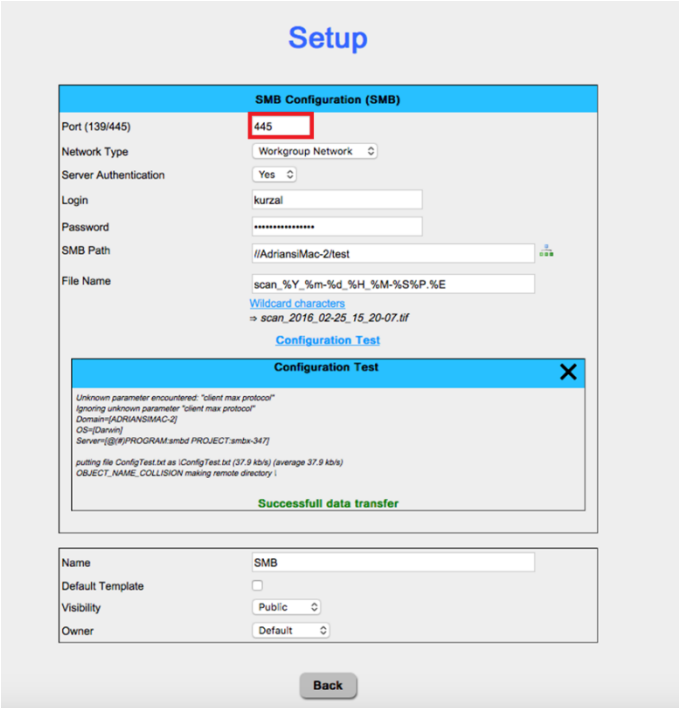

Figure 31 Scanner SMB Template configuration

Test your settings by performing the configuration test.

If the configuration test passes check Default Template to make this SMB template your main image output.

Set the visibility to public to finish the setup of your SMB template.

End of Document