

Kofax eCopy ShareScan

Troubleshooter User Guide

Version: 6.4.0

Date: 2021-02-12

The KOFAX logo is displayed in a bold, blue, sans-serif font. The letters are thick and closely spaced, with a modern, clean design.

© 2021 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface.....	4
Training.....	4
Getting help with Kofax products.....	4
Chapter 1: About the ShareScan Troubleshooter.....	6
Prerequisites.....	6
Start the tool.....	6
Chapter 2: Pre-installation check.....	8
Chapter 3: Full check.....	10
Chapter 4: Device check.....	12
Chapter 5: Advanced options.....	14
Network tests.....	14
Confirm device.....	17
Authentication test.....	18
Chapter 6: Database option.....	20
Testing or setting connection.....	20
Credential cache.....	21
Installed software versions.....	22
Remove unused ShareScan Manager data.....	23
Backup database.....	24
Chapter 7: Verify and troubleshoot the high availability setups.....	27

Preface

The Kofax eCopy ShareScan software extends the capabilities of digital copiers and scanners. When installing and setting up a ShareScan system, you must be familiar with the scanning device that you will use with ShareScan, the ShareScan software components, and the basic installation and configuration workflow.

This guide is intended for administrators responsible for the initial installation, configuration, and licensing of eCopy ShareScan. For the device-specific Pre-Installation Checklist (PICL), see the applicable vendor-specific Pre-Installation Checklist and Sizing Guide. For information pertaining to the ShareScan pre-installation, see this guide. For configuration and Administration Console usage, see the Administration Console Help (accessible via pressing F1 on the Administration Console).

This document is written under the assumption that readers are familiar with working within a server-client architecture and environment.

Training

Kofax offers both classroom and computer-based training to help you make the most of your eCopy ShareScan solution. Visit the Kofax website at www.kofax.com for details about the available training options and schedules.

Getting help with Kofax products

The [Kofax Knowledge Base](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the [Kofax website](#) and select Support on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

Type your search terms or phrase into the **Search** box, and then click the search icon.

- Product information, configuration details and documentation, including release news.

Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

- Access to the Kofax Customer Portal (for eligible customers).
Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Kofax Partner Portal (for eligible partners).
Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

About the ShareScan Troubleshooter

The ShareScan Troubleshooter is an integrated application of ShareScan, which allows you to pinpoint potential and existing issues you may encounter when using ShareScan.

The information provided by the tool is useful when consulting Technical Support if you encounter an issue that you cannot solve based on the information received from the tool.

Note When using a remote SQL server with Windows database authentication, the Windows user who runs the Troubleshooter (typically the currently logged in user) must be:

- The same as the user who runs the ShareScan Agent Windows service or
- Added to SQL server's users, the User Mapping has to be set to the ShareScan database, and the user's Database role membership has to be set to db_owner. The user cannot be member of the sysadmin role.

Prerequisites

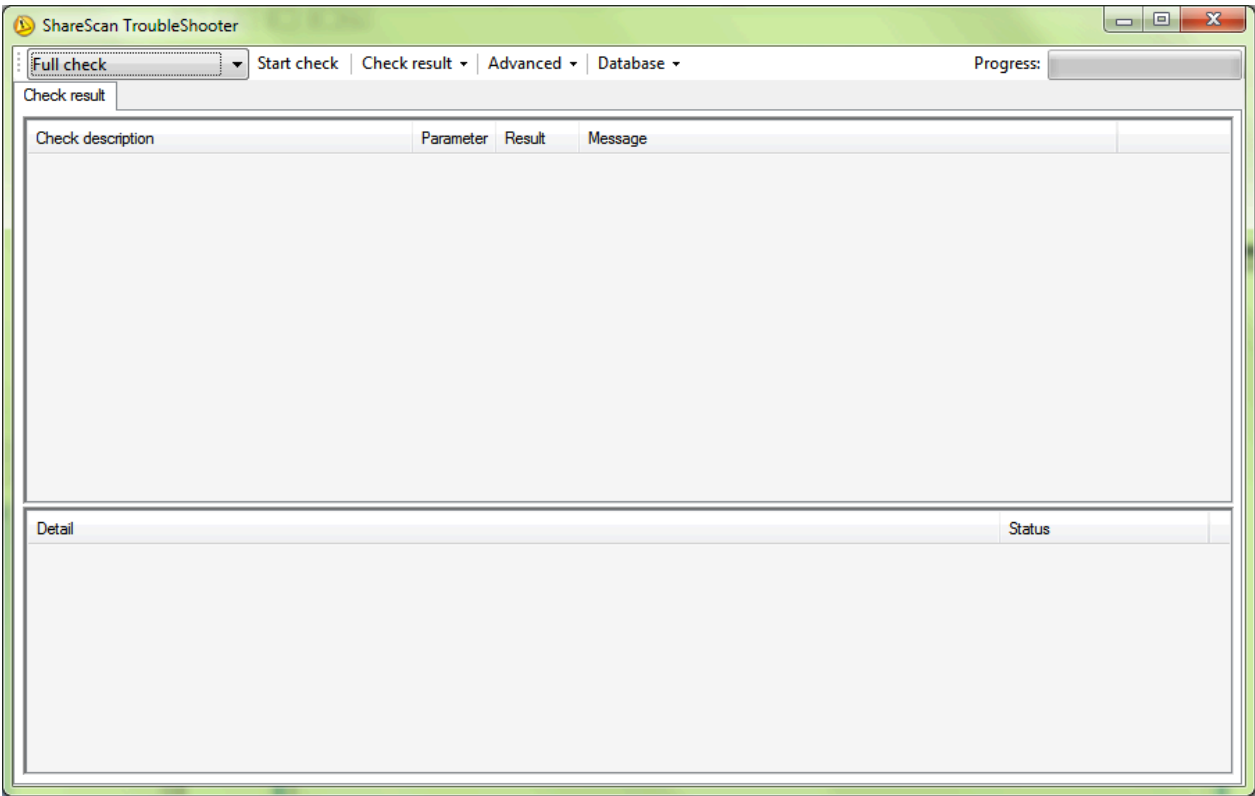
ShareScan Troubleshooter requires .NET Framework 4.8 to function properly.

Start the tool

The ShareScan Troubleshooter is located in the Tools subfolder of your ShareScan installation folder: `c:\%programfiles%\Kofax\ShareScan6.4\Server\Tools\`.

To launch the Troubleshooter:

- Start `ShareScanTroubleshooter.exe`, or
- From the Windows start menu, go to **All Programs > eCopy Applications > ShareScan 6.4 > ShareScan Troubleshooter**.



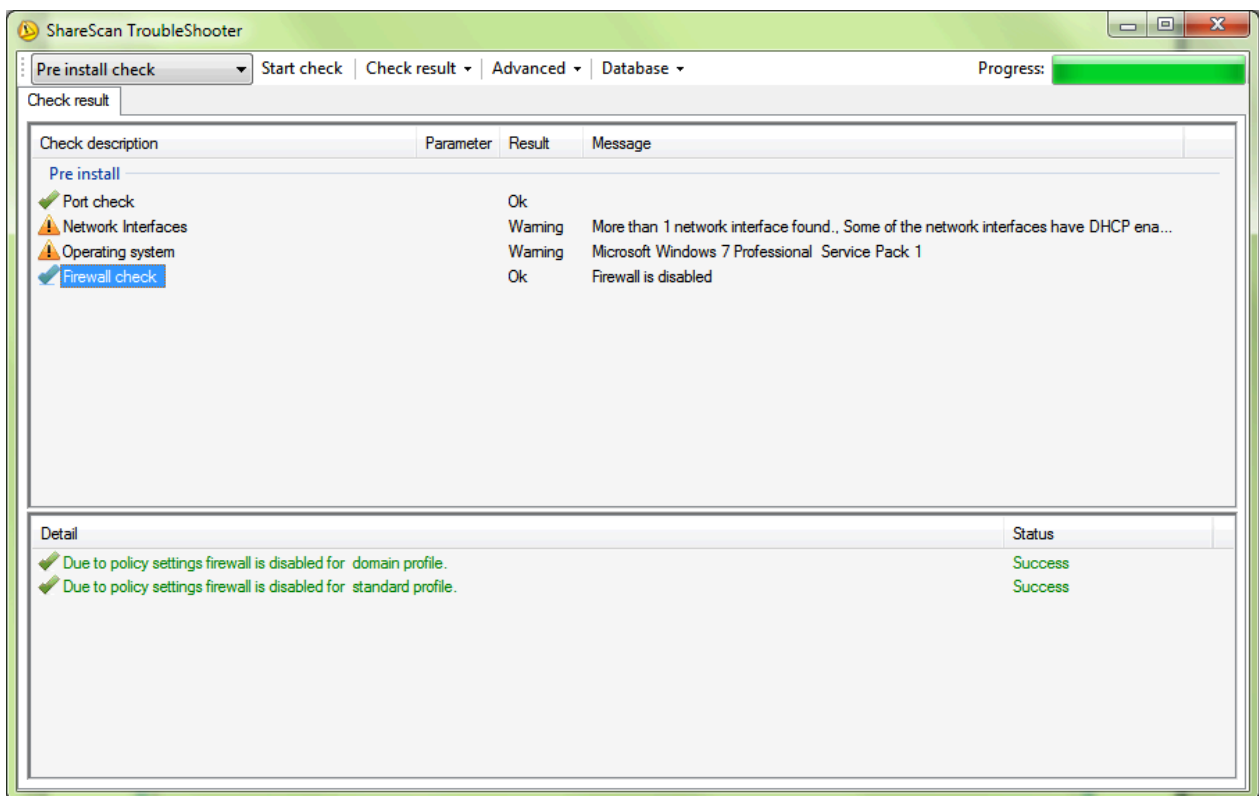
You can use the menu to select between **Preinstall**, **Full**, or **Device** checks, you can **Save** or **Load** your check results in .xml format, and you can perform a number of advanced tests.

Note When reporting issues, attaching a saved check result can be a valuable asset for Technical Support.

Chapter 2

Pre-installation check

Running a pre-installation check allows you to establish whether your system meets all the prerequisites for running ShareScan. To run this check, select the **Pre install check** option from the menu and click **Start check**:



The tool checks the following:

- Ports used by ShareScan (for a comprehensive list of used ports, see the *ShareScan Installation Guide*)
- Network interfaces (status and DHCP enablement)
- Operation system (for a list of supported operating systems, see the *ShareScan Installation Guide*)

Note Windows 10 limits the maximum number of concurrent connections to 20. Windows Server does not have this limitation.

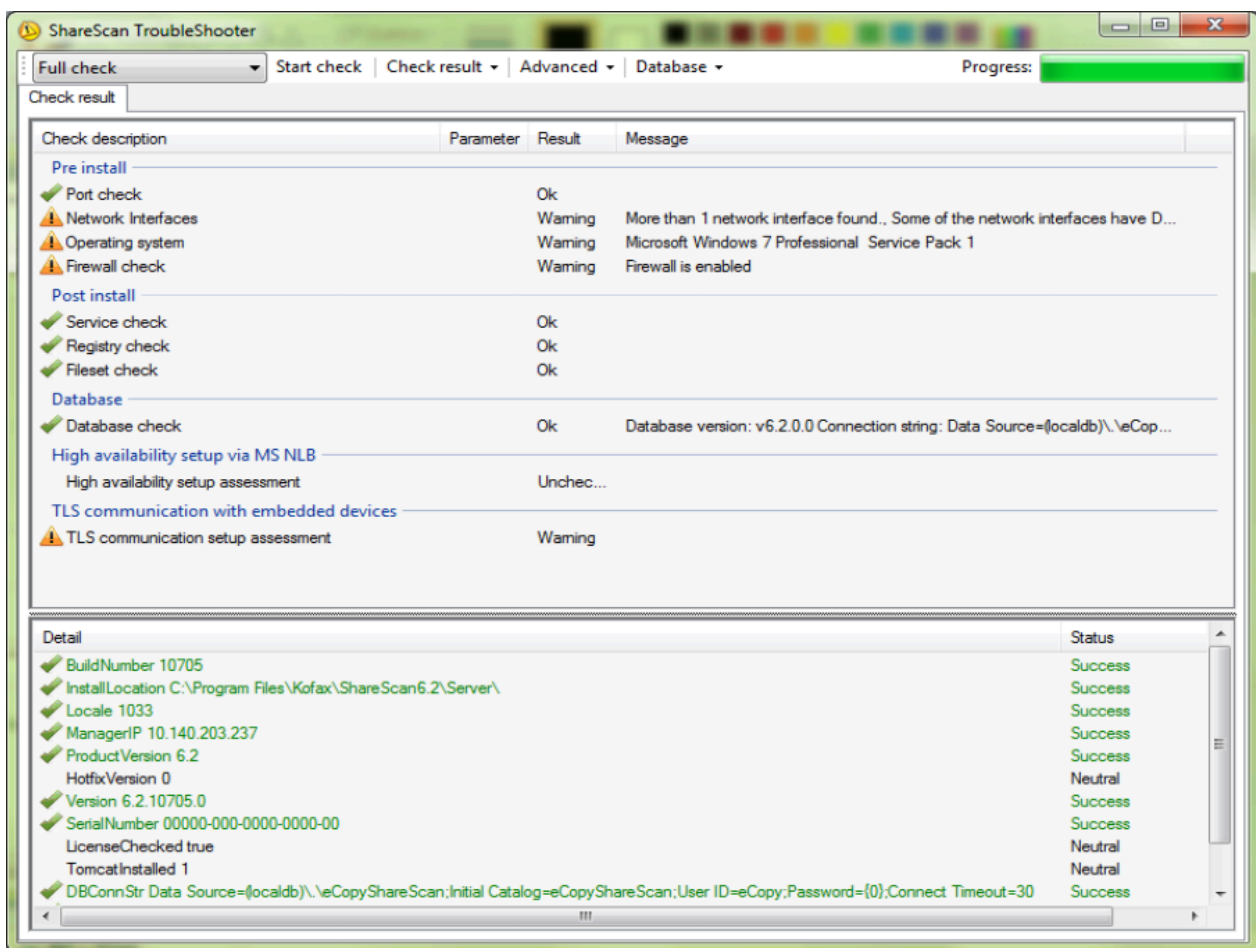
- Firewall (whether it is turned on or ShareScan is added to the firewall exceptions)

Clicking on the description names provides more details on the **Detail** pane at the bottom of the screen.

Chapter 3

Full check

A full check includes checking the preinstallation options, as well as installation, runtime, and database checks. To run this check, select the **Full check** option from the menu and click **Start check**:



The tool checks the following:

- Preinstall options (same as the preinstall check).
- Status and location of the installation log files.
- Status and availability of the ShareScan services.
- Status and availability of the registry entries.
- Status and availability of the ShareScan fileset, including full version information.

- Database version and trustworthiness (for a list of supported databases, see the *ShareScan Installation Guide*).
- Status of "Desktop Experience" OS feature (when ScanStation is installed).

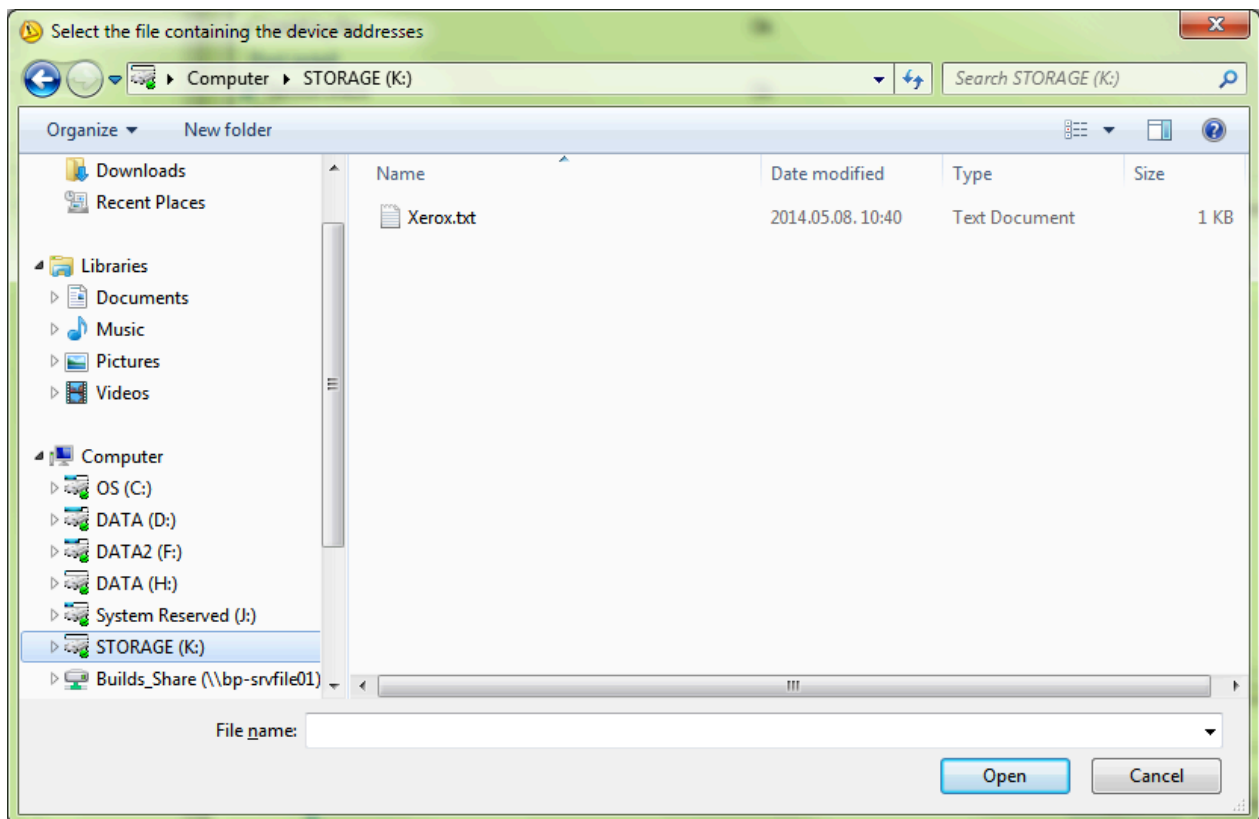
Clicking on the description names provides more details on the **Detail** pane at the bottom of the screen.

Chapter 4

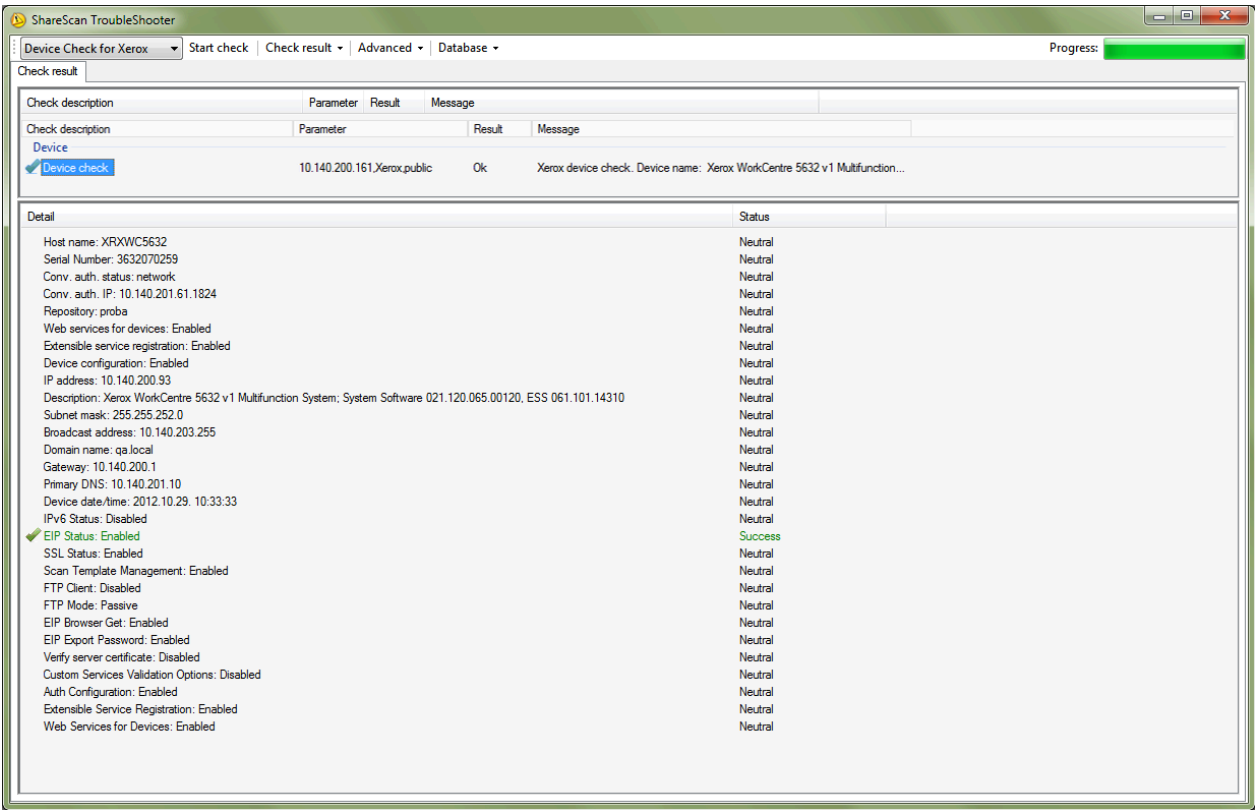
Device check

Note Currently available for Xerox devices only.

The Device check allows you to test and confirm whether a Xerox device used by ShareScan meets the requirements for establishing communication. To run such a check, select the **Device Check for Xerox** option from the dropdown menu and click **Start check**. This test is especially useful to spot and help correct any device connection issues. The following screen is displayed:



Browse to a .txt file containing the device addresses. The file should list each device to be tested in a separate line, in **<IP address>**, **<vendor name>**, **<SNMP community name>** format. After you open a file, the Troubleshooter runs the check; the time required depends on the number of devices. When the check is finished, the following screen is displayed:

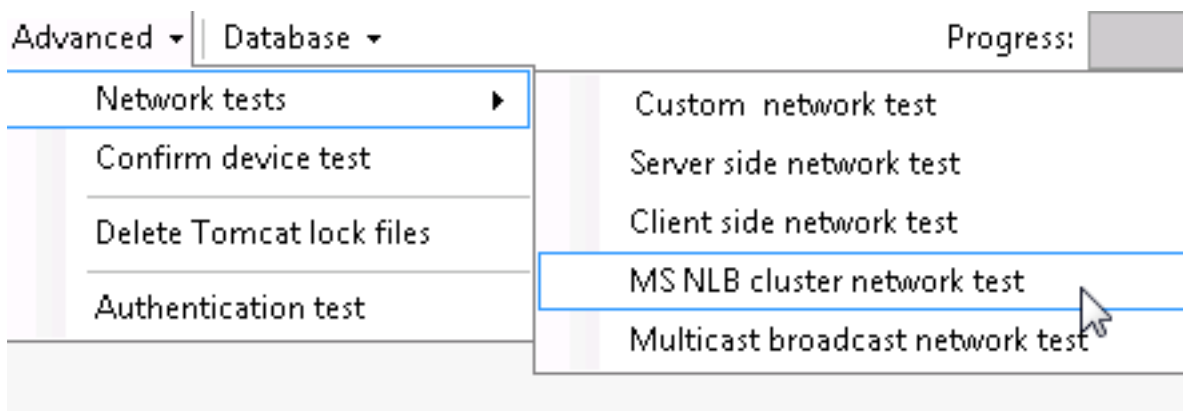


Information important for ShareScan is color-coded in the report.

Chapter 5

Advanced options

The advanced options of the ShareScan Troubleshooter are available under the **Advanced** menu. The Network test options are arranged under the Network tests category.



Network tests

As ShareScan is a client-server application, and the client (MFP) and the server (Manager) can be connected via a complicated network infrastructure, sometimes it is very hard to troubleshoot why the client and the Manager are unable to work together.

Use the ShareScan Troubleshooter tool to diagnose such issues.

The workflow of a typical network test is as follows:

1. Start the Troubleshooter on the Manager computer.
2. Click the **Advanced** menu, and select **Network tests** > **Server side network test**.
3. Connect the Manager computer to the same subnet the MFP to be tested is connecting.
4. Stop any ShareScan services running on the client computer.
5. Start the Troubleshooter.
6. Click the **Advanced** menu and select **Network tests** > **Client side network test**.
7. On the server, enter the host name (or IP) of the computer simulating the client into the Client address / hostname and some text into the **Payload** field.
8. On the computer simulating the client, enter the hostname or IP of the Manager computer, and some text into the **Payload** field.

9. Click **Connect** on both dialogs.
10. If the network connection is possible, then the **Send text** button is available; click on it to transfer the given payload test to the other end. In there is a connection problem, an error message is displayed.

Custom Network Test

Using this option, you can test the network connection between the current machine and a remote computer. Selecting **Network tests > Custom network test** item in the **Advanced** menu displays the following screen:

Source	Operation	Data	Message
Local	Start listening	Port: 8221	

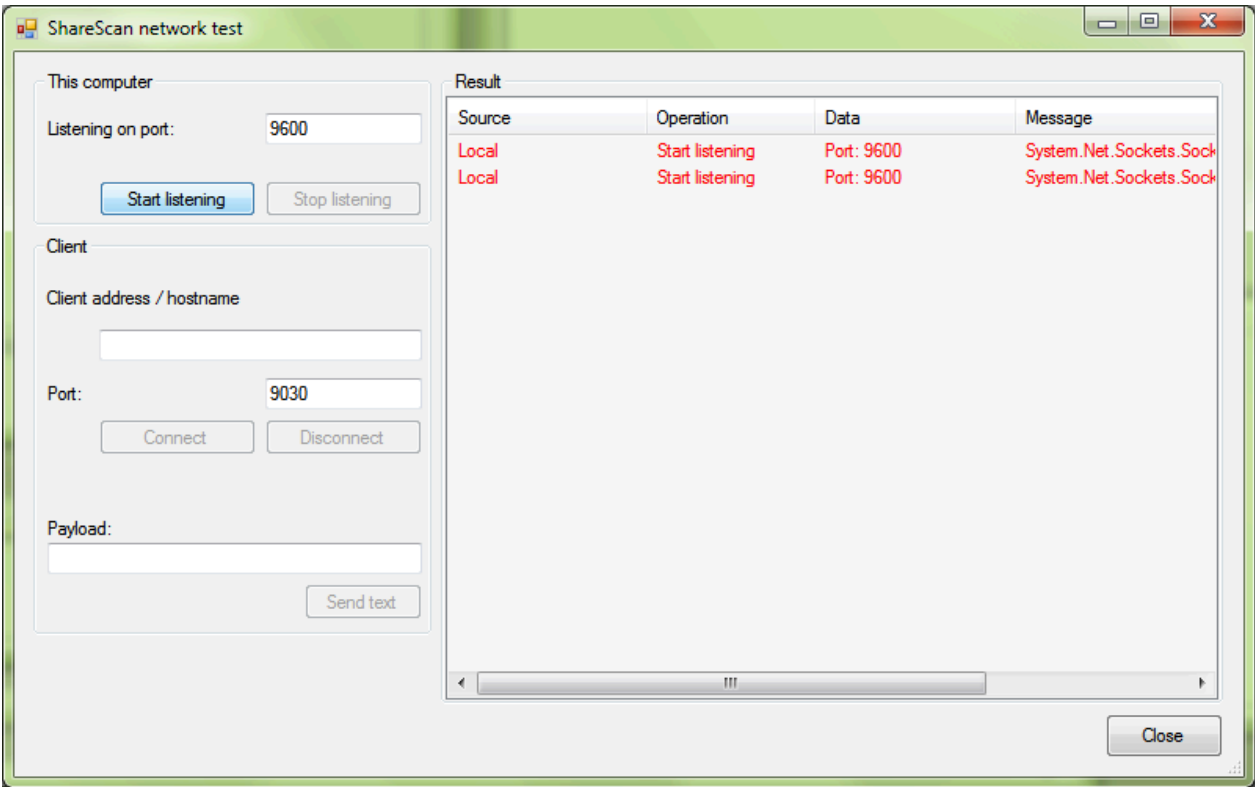
The **This computer** pane allows you to set the port number for listening, as well as **Start** and **Stop** listening.

The **Remote computer** pane allows you to set the data for the remote computer and enter a payload text to be used in the test.

Click **Close** to return to the Troubleshooter.

Server-side Network Test

Using this option, you can test the network connection from the server > client direction. Selecting **Network tests > Server side network test** item in the **Advanced** menu displays the following screen:



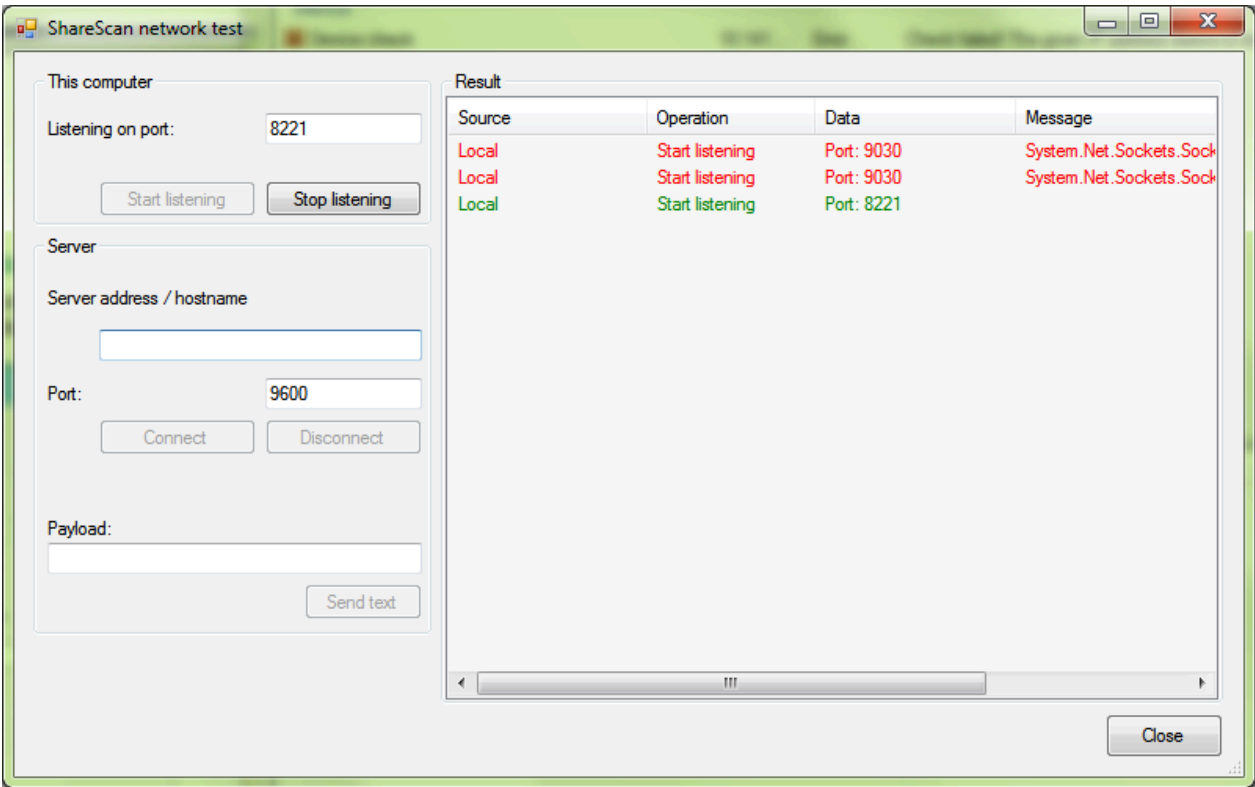
The **This computer** pane allows you to set the port number for listening, as well as **Start** and **Stop** listening.

The **Client** pane allows you to set the client-side data and enter a payload text which will be used in the test.

Click **Close** to return to the Troubleshooter.

Client-side Network Test

Using this option, you can test the network connection from the client > server direction. Selecting **Network tests > Client side network test** item in the Advanced menu displays the following screen:



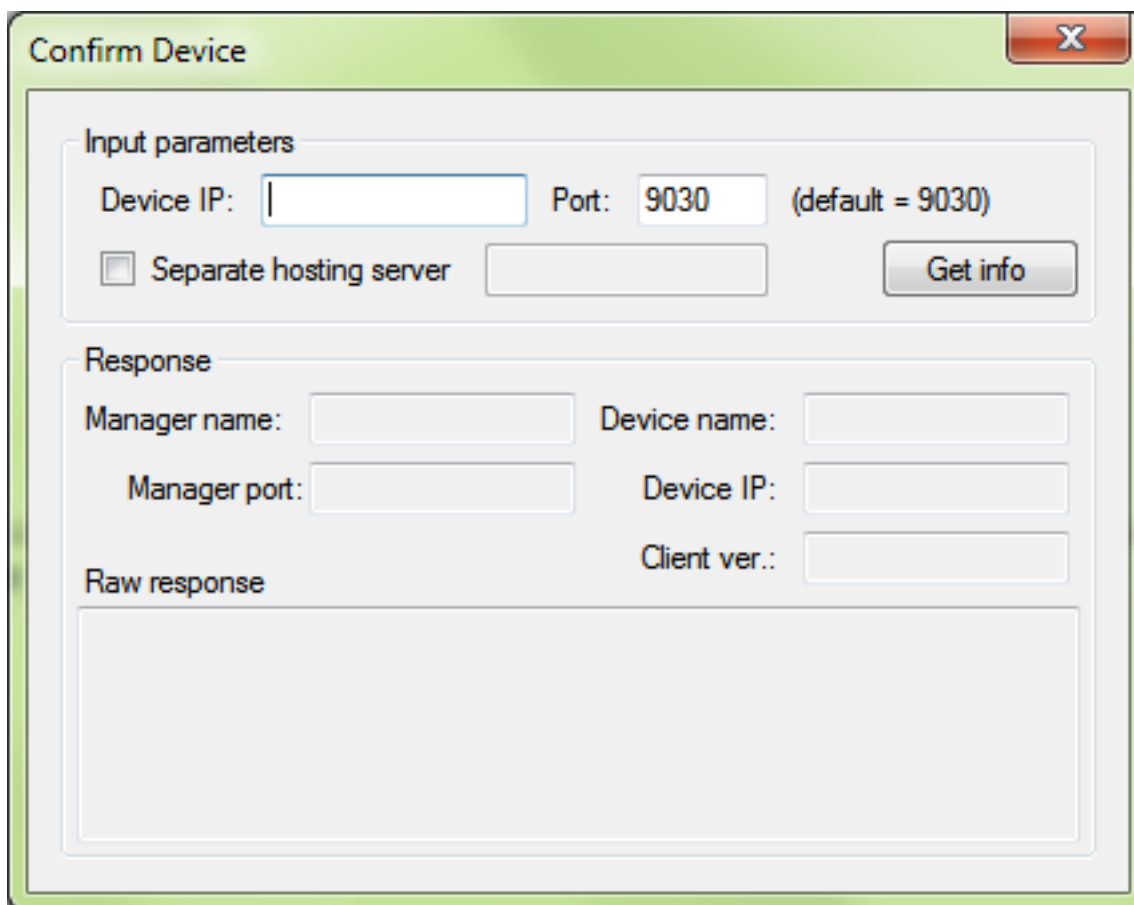
The **This computer** pane allows you to set the port number for listening, as well as **Start** and **Stop** listening.

The **Server** pane allows you to set the server-side data and enter a payload text which will be used in the test.

Click **Close** to return to the Troubleshooter.

Confirm device

You can test the connection between ShareScan and an attached device by clicking **Confirm device test** in the **Advanced** menu.

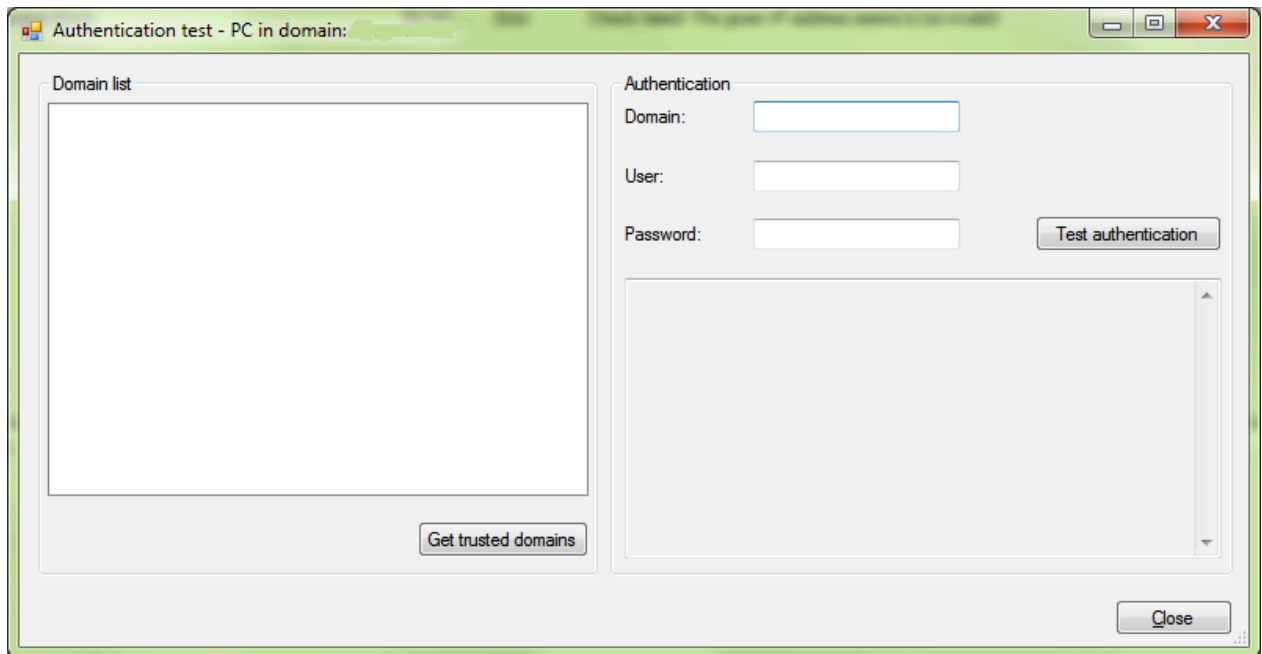


The image shows a 'Confirm Device' dialog box with a green title bar and a close button (X) in the top right corner. The dialog is divided into three main sections: 'Input parameters', 'Response', and 'Raw response'. The 'Input parameters' section contains a 'Device IP' text box, a 'Port' text box with the value '9030' and '(default = 9030)' next to it, a checkbox labeled 'Separate hosting server' which is currently unchecked, and a 'Get info' button. The 'Response' section contains four text boxes: 'Manager name:', 'Device name:', 'Manager port:', and 'Device IP:'. Below these is a 'Client ver.:' text box. The 'Raw response' section is a large, empty text area at the bottom of the dialog.

Complete the Input parameters according to your system setup, and click **Get info**. The system fills in the **Response** fields with the acquired data. The **Raw response** window provides the unfiltered data from the test.

Authentication test

This option allows you to test whether the ShareScan user whose credentials you supply is in the domain to which the ShareScan Manager computer is added. Click **Authentication test** in the Advanced menu to display the following screen:



Select the domain you want to use from the Domain list pane. Click **Get trusted domains** to list all available trusted domains.

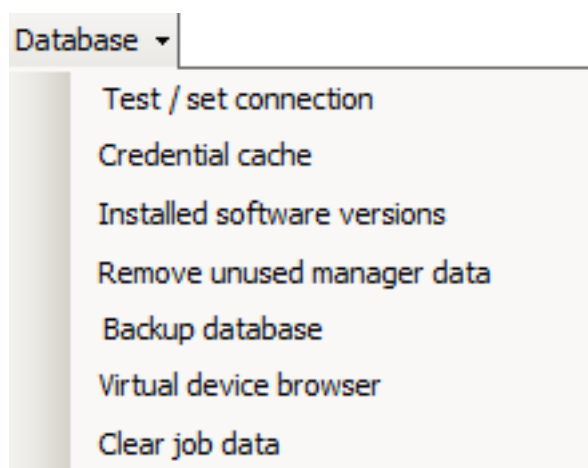
Enter the domain name and user credentials you want to test, and click **Test authentication**.

Click **Close** to return to the Troubleshooter.

Chapter 6

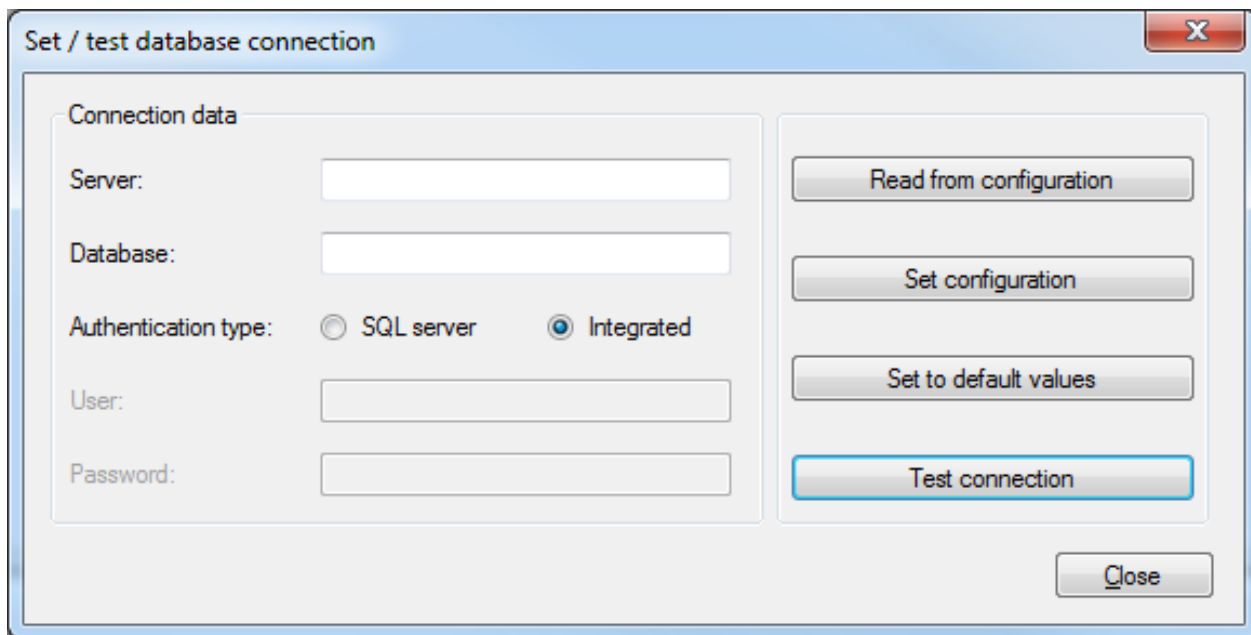
Database option

The ShareScan Troubleshooter database options (valid for the whole system) are available by clicking the **Database** menu.



Testing or setting connection

Use this option to check and optionally configure the database connection data. This test is especially useful if your database is on a remote server. Clicking the **Test / set connection** option displays the following screen:

A screenshot of a Windows-style dialog box titled "Set / test database connection". The dialog has a standard title bar with a close button (X). The main area is divided into two sections. The left section, titled "Connection data", contains five input fields: "Server:", "Database:", "Authentication type:" (with radio buttons for "SQL server" and "Integrated", where "Integrated" is selected), "User:", and "Password:". The right section contains four buttons: "Read from configuration", "Set configuration", "Set to default values", and "Test connection" (which is highlighted with a blue border). A "Close" button is located at the bottom right of the dialog.

The following options are available:

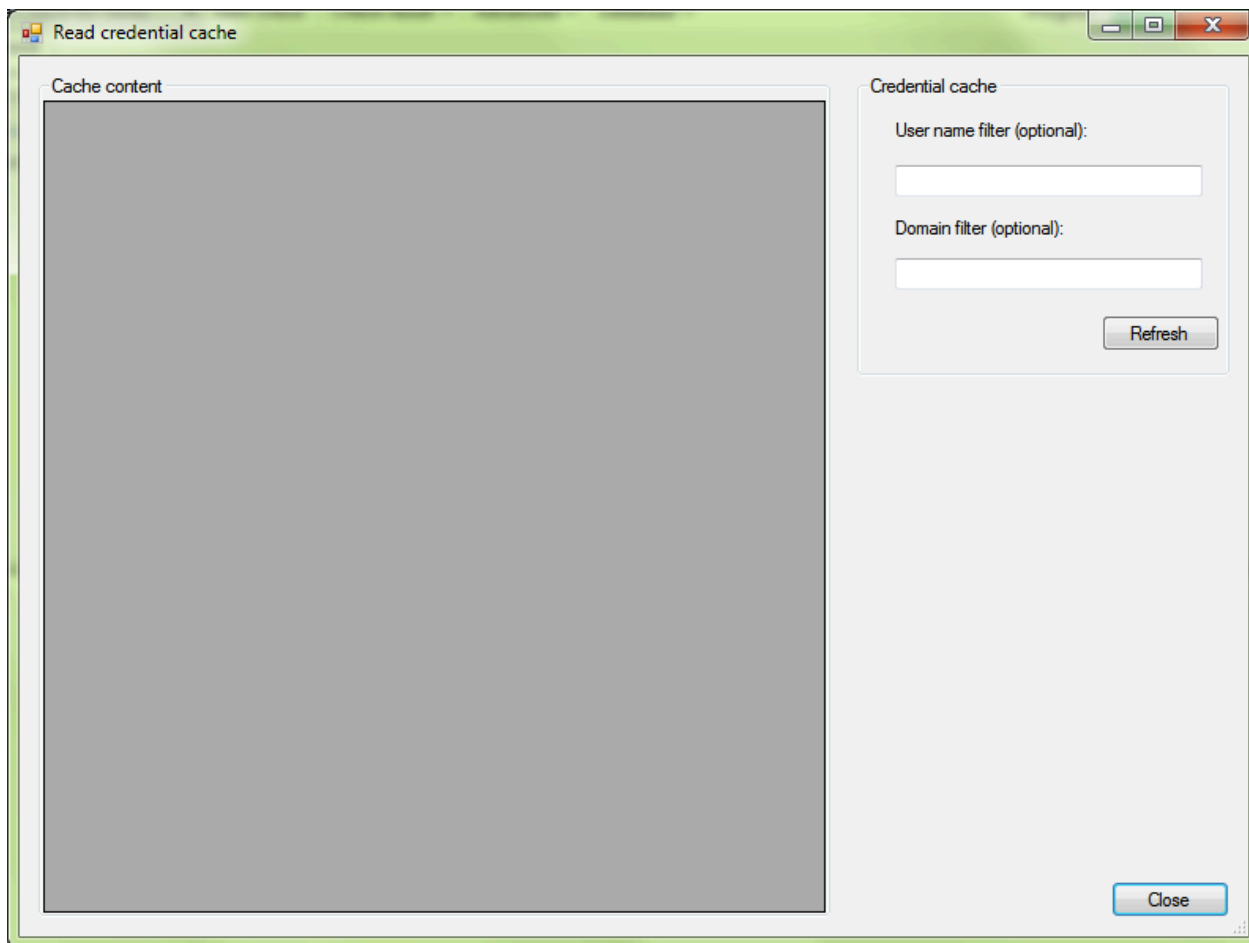
- **Read from configuration:** Populates the Connection data based on your currently installed ShareScan version.
- **Set configuration:** Allows you to enter the connection data manually.
- **Set to default values:** Allows you to discard changes and return to the default values.
- **Test connection:** Tests the database connection.

For the user running the Troubleshooter tool, the following rights must be granted: Database role membership: db_owner, default schema: ShareScan.

Click **Close** to return to the Troubleshooter.

Credential cache

This option is only useful if you have the Single Sign-On Extender installed, and enable the relevant Session Logon settings via the ShareScan Administration Console. Click **Credential cache** to display the following screen:



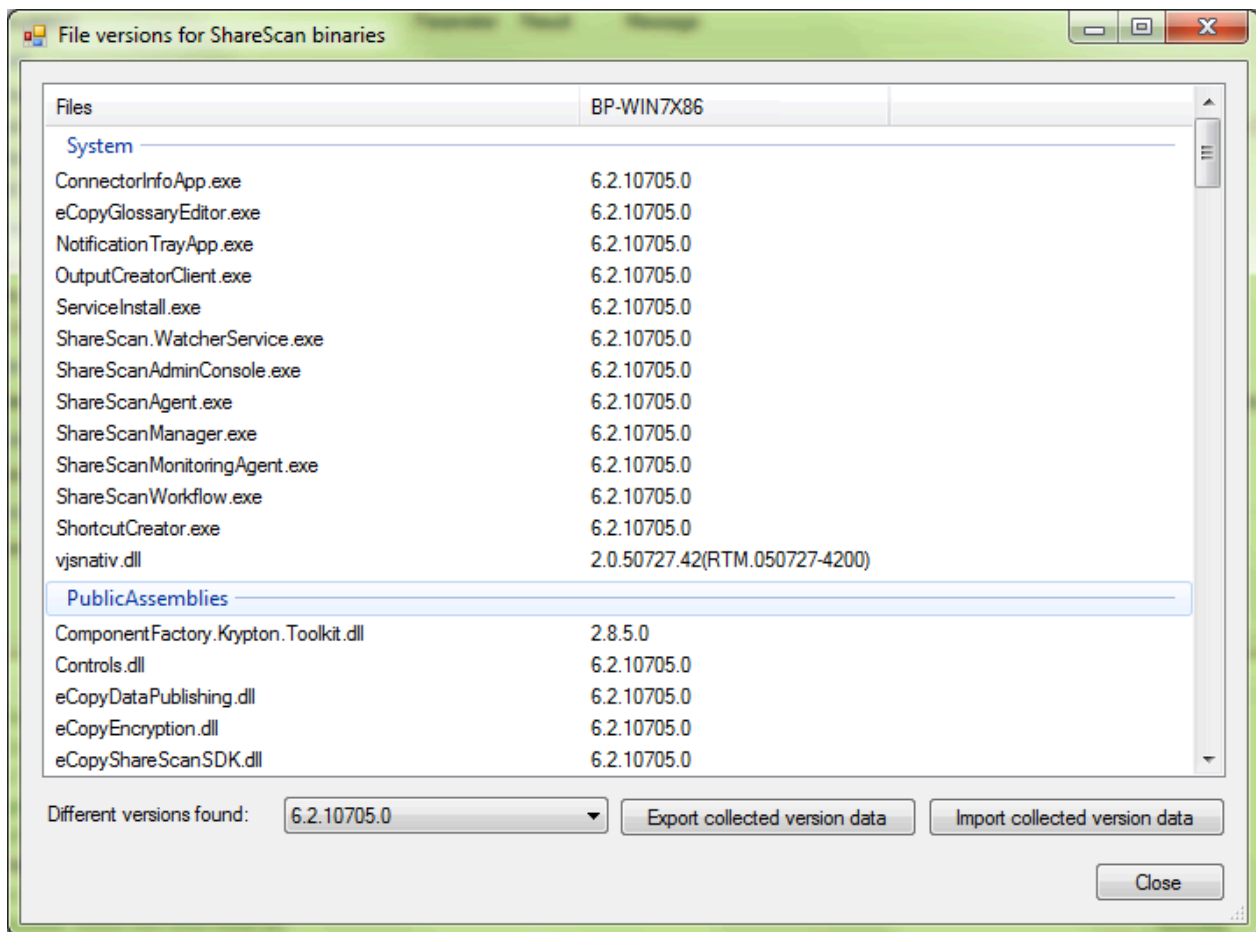
The Cache content pane displays the entries of the credential cache used by the Session Logon component of ShareScan. You can use the Credential cache pane to filter the contents if you are looking for a particular user name or domain, and you can use the Operations pane to delete the content of the credential cache.

Click **Close** to return to the Troubleshooter.

Note The credential cache contains masked passwords along with the user names.

Installed software versions

Use this option to check the version of the various ShareScan components installed on this computer. The compiled list can be a great asset when contacting eCopy technical support, as the list enables narrowing down any issues which are specific to component versions. Click **Installed software versions** to access the list:



Click **Export collected version data** to save the list into an xml file.

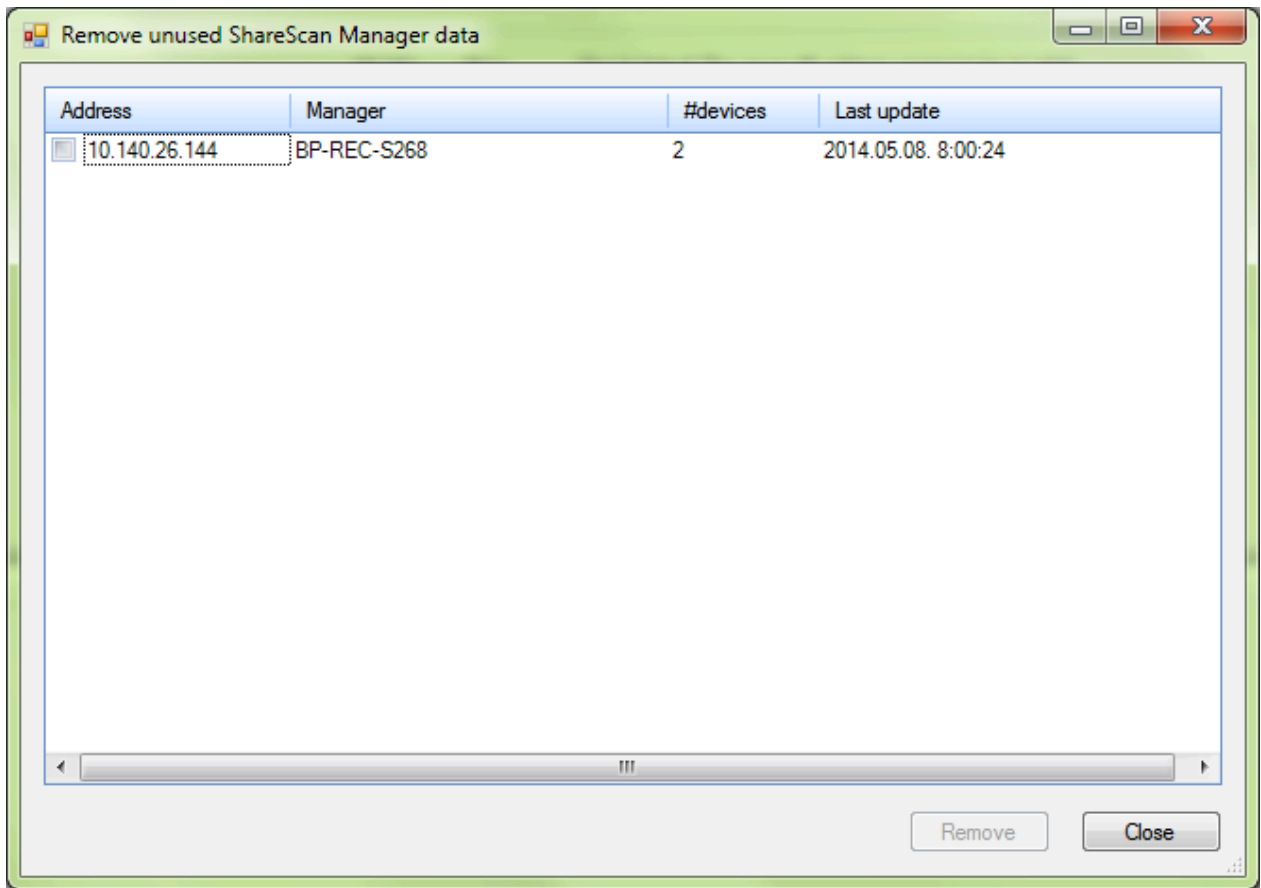
Click **Import collected version data** to import data from a previously saved xml file.

Click **Close** to return to the Troubleshooter.

Note The entries listed on the screenshot are only examples.

Remove unused ShareScan Manager data

This option allows you to remove superfluous data (obsolete logs and trace files, temporary process data, and so forth) from the selected ShareScan Managers. Click **Remove unused manager data** to display the removal screen:



Mark the check box in front of the Manager whose data you want to remove, and click **Remove**.

Click **Close** to return to the Troubleshooter.

Backup database

This option allows you to remove superfluous data (obsolete logs and trace files, temporary process data, and so forth) from the selected ShareScan Managers. Click **Remove unused manager data** to display the removal screen.

The screenshot shows a Windows-style dialog box titled "DatabaseBackup". It has a standard title bar with a close button (X). The dialog is divided into two main sections: "Connection data" and "Backup data".

Connection data section:

- Server:** A text field containing ".".
- Database:** A text field containing "eCopyShareScan".
- Authentication type:** Two radio buttons. "SQL server" is unselected, and "Integrated" is selected.
- User:** A text field containing "sa".
- Password:** An empty text field.

Backup data section:

- Destination:** A text field containing "C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER" followed by a browse button (three dots).
- Filename:** A text field containing "backup.bak".

At the bottom right of the dialog are two buttons: "Backup" and "Close".

The Connection data pane lists the credentials of the connected ShareScan database.

The Backup data pane allows you to select a Destination and a Filename for the backup data.

Click **Backup** to start the database backup process.

Click **Close** to return to the Troubleshooter.

When you perform a backup / restore in the Administration Console, all system configuration data is backed up and restored.

This includes the Tomcat configuration files: most importantly, the Tomcat web server certificate file, important whenever HTTPS connection is used for web-based devices.

If you perform the backup from the Troubleshooter tool (or via the command line scripts provided), the Tomcat web server certificate file is not stored with the backup. This is not a limitation if you do not have the ShareScan web client installed or if the Tomcat certificate file is not changed (regenerated or changed otherwise) since installation.

For successful database backup, db_owner, db_creator and db_backupoperator role memberships must be granted to the user running the Troubleshooter tool.

Chapter 7

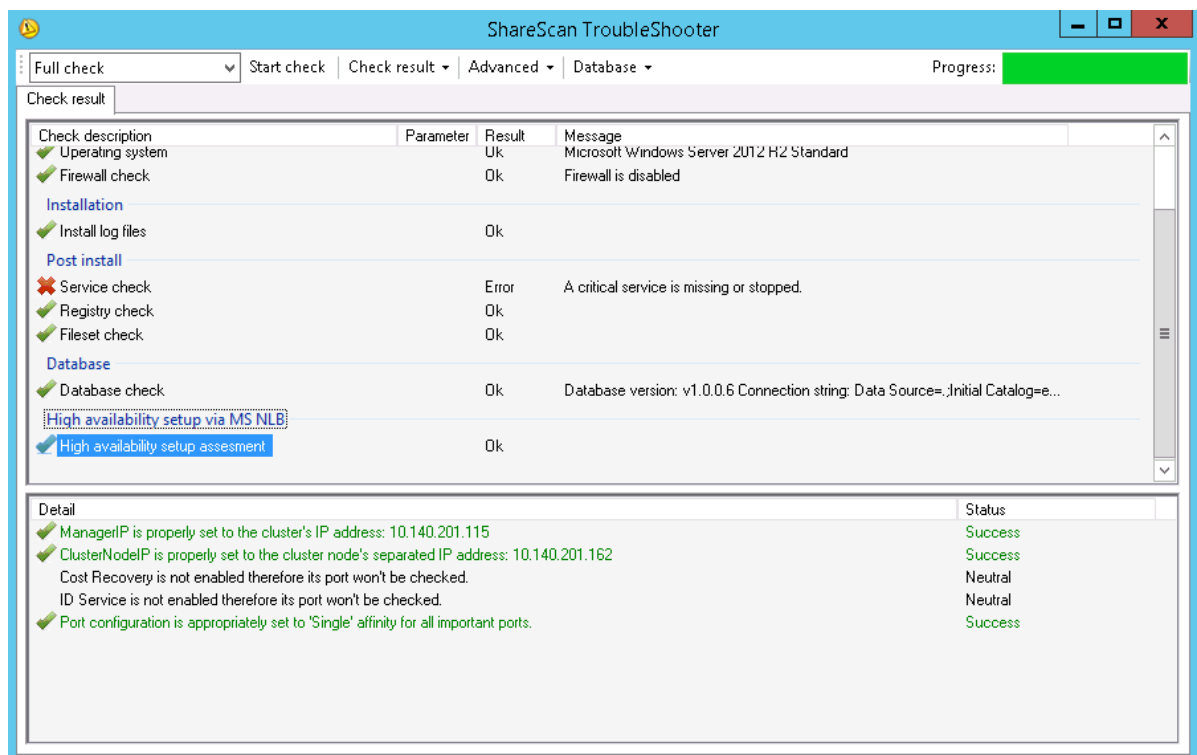
Verify and troubleshoot the high availability setups

The ShareScan Troubleshooter has the following new options to help to verify and troubleshoot the high availability setups built on the Microsoft Network Load Balancing infrastructure.

Before testing, make sure the MS NLB and the ShareScan registry settings are set properly, in accordance with the *High Availability and Load Balancing Deployment Guide*.

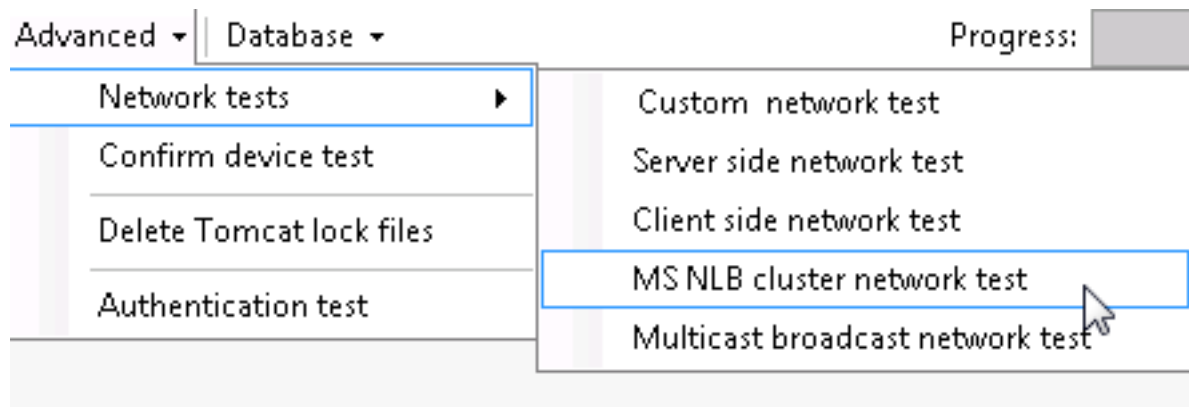
1. The **Full Check** option (started by the **Start check** button) on the menu bar performs a check to determine if the MS NLB based cluster is configured.

The checker adds a last section to the report, with a section named **High Availability setup via MS NLB**.



If there is an inconsistency or missing item in the configuration settings (ManagerIP, ClusterName and ClusterNodeIP settings in the registry) or if these are not in sync with the actual settings of the Microsoft NLB system or the network adapters, then alert lines in red appear in this section.

2. There are two new menu items.



- MS NLB cluster network test

This is a client-server communication test, to see if MS NLB is set up properly and the requests from the outside of the cluster (the part of the network where the devices exist) are dispatched to one of the server nodes in the cluster. During multiple repeated connection tests, the routing of the individual request should vary sometimes (once the response should arrive from server node

X, next time from server node Y, etc.), proving that NLB 'spreads' the requests across the server nodes.

Note This test is performed on TCP port 9599, which should be configured with Node affinity: None option in the Port Rule editor of the MS NLB Manager as it is documented in the High Availability and Load Balancing Deployment Guide, allowing the new TCP connections to assign to a server node randomly. This mode is NOT used for the normal ShareScan device-server connections, but for Cost Recovery and Identification services. However, the test is useful to prove the proper configuration of the MS NLB system.

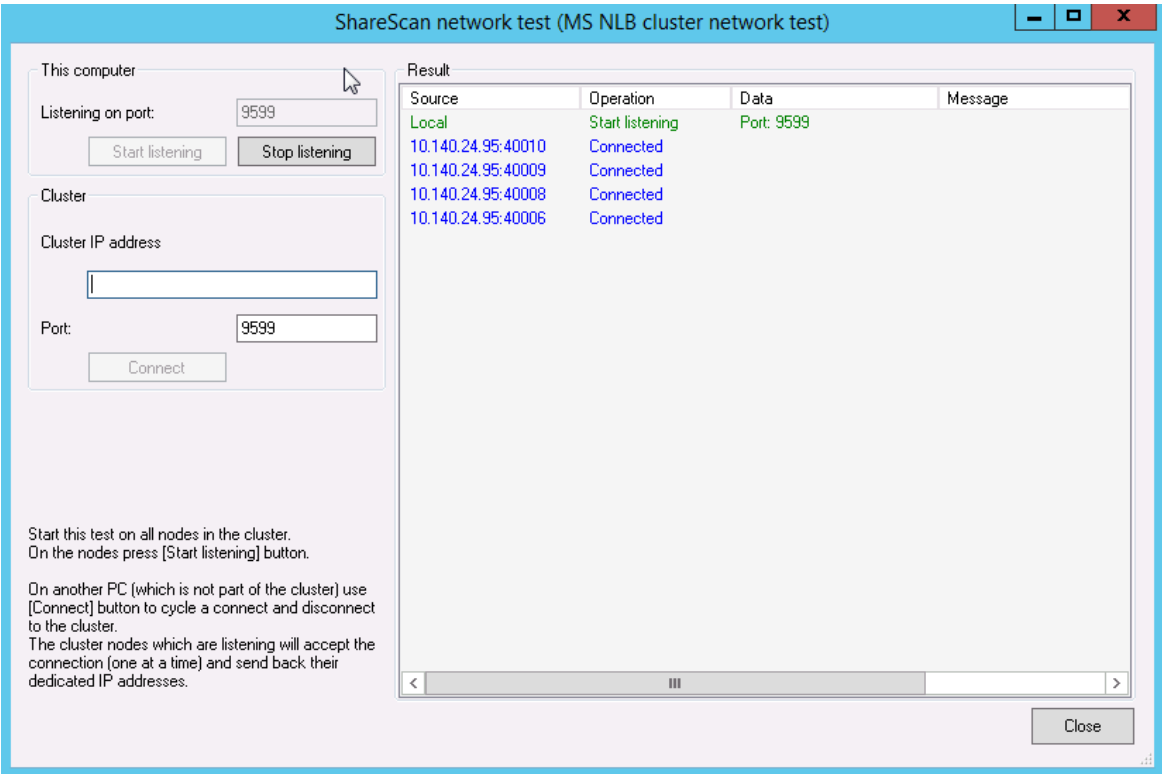
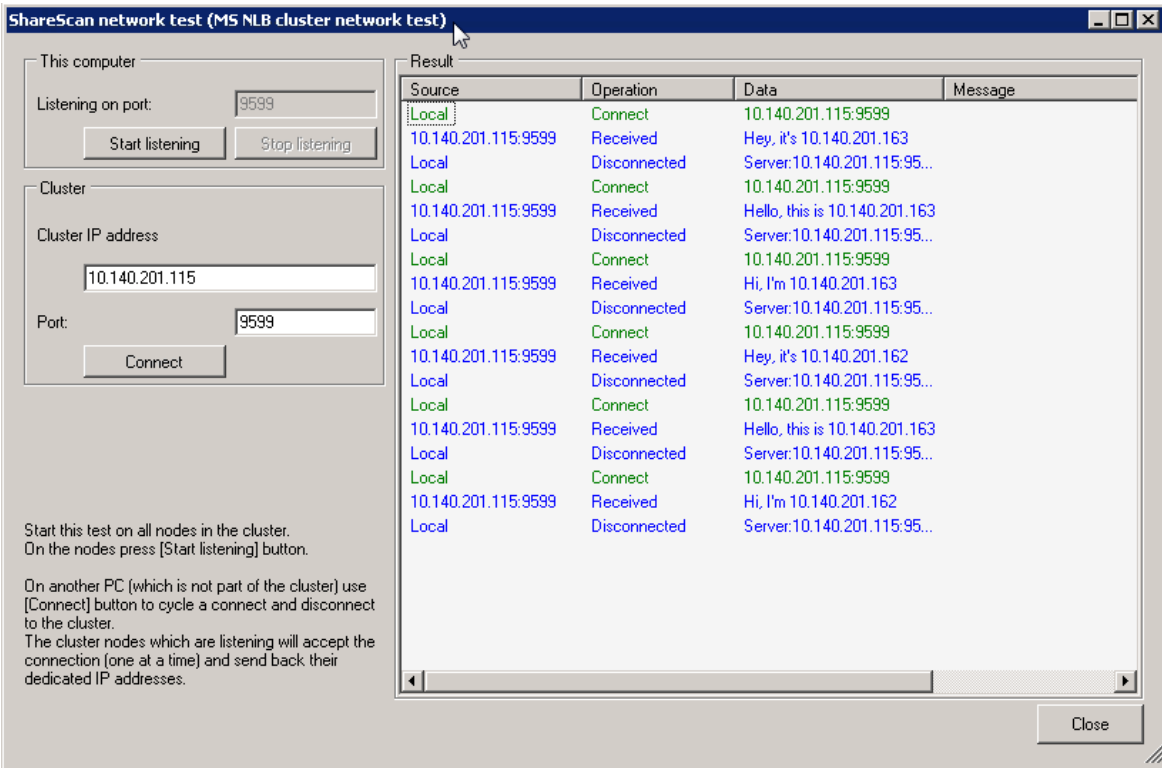
How to set up and perform a test:

- a. Start the ShareScan Troubleshooter tool on all of the tested cluster nodes – these instances of the Troubleshooter tool will be called “server agents”.
- b. Copy the following files to a folder on a computer connecting to the same network to which the MFP devices are connected (or will be connected), and launch the ShareScan Troubleshooter tool – this instance is called “client agent”.
- c. Select the MS NLB cluster network test menu option (on all nodes).
- d. A dialog appears.
- e. Click the Start listening button on the dialog on all the “server agents”.
- f. On the “client agent” instance enter the IP address of the cluster (the IP address used in the ManagerIP registry entry) into the text field.
- g. Click the Connect button on the “client agent”.
- h. If the request sending / response receiving is successful, then you should see 3 lines:
 - Local / Connect / Cluster IP:9599 (in green)
 - Cluster IP:9599 / Received / Hey, it's X or Hi, I'm X or Hello, this is X (in blue), where X is the ClusterNode IP of the responding server node
 - Local / Disconnected / ClusterIP:port
- i. In the console of the “server agents” (always only in the instance that actually gets the request) you should see lines appearing saying <IP:port> Connected in blue, where <IP:port> should correspond to the “client agent”.

If you click the **Connect** button several times (wait until all the 3 lines are listed) you should see different IP addresses in place of X, representing the different server nodes.

If you can see the ClusterNodeIP of all of the nodes at least once, then the entire test is successful.

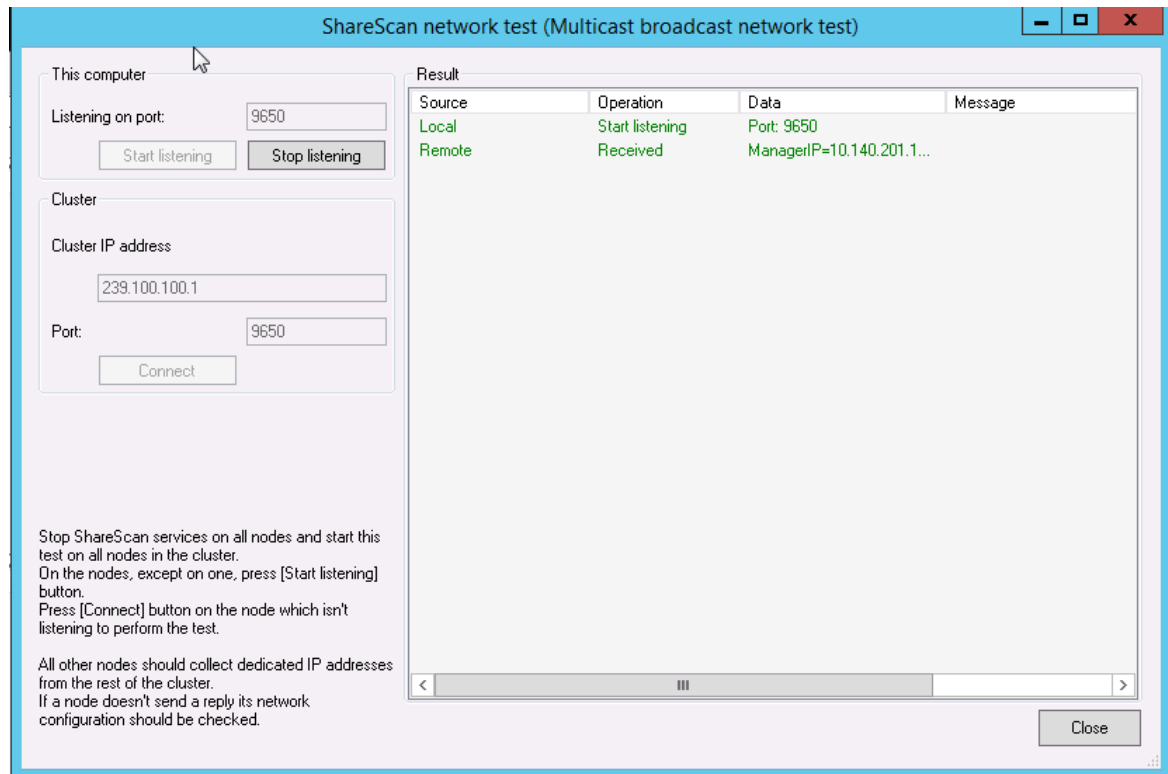
Note One should not expect that the server nodes are hit by the requests in a round-robin manner. As the TCP connection-server node assignment is decided by the MS NLB based on the client IP and the source port (which is selected randomly by the “client agent”) it is not guaranteed that the next server node is hit next, nor that the requests are spread evenly – this is out of scope for this simple test tool.



- Multicast broadcast network test

To test the Multicast broadcast functionality of the network, click the **Advanced > Network tests > Multicast broadcast network test** menu item on all ShareScan server nodes.

On the dialog that appears, click the **Start listening** button on all the server nodes (these will be the test servers), except one (which will be used as the message sender).



The dialog box is titled "ShareScan network test (Multicast broadcast network test)". It contains two main sections: "This computer" and "Cluster".

This computer section:

- Listening on port: 9650
- Buttons: Start listening, Stop listening

Cluster section:

- Cluster IP address: 239.100.100.1
- Port: 9650
- Button: Connect

Result section:

Source	Operation	Data	Message
Local	Start listening	Port: 9650	
Remote	Received	ManagerIP=10.140.201.1...	

Instructions:

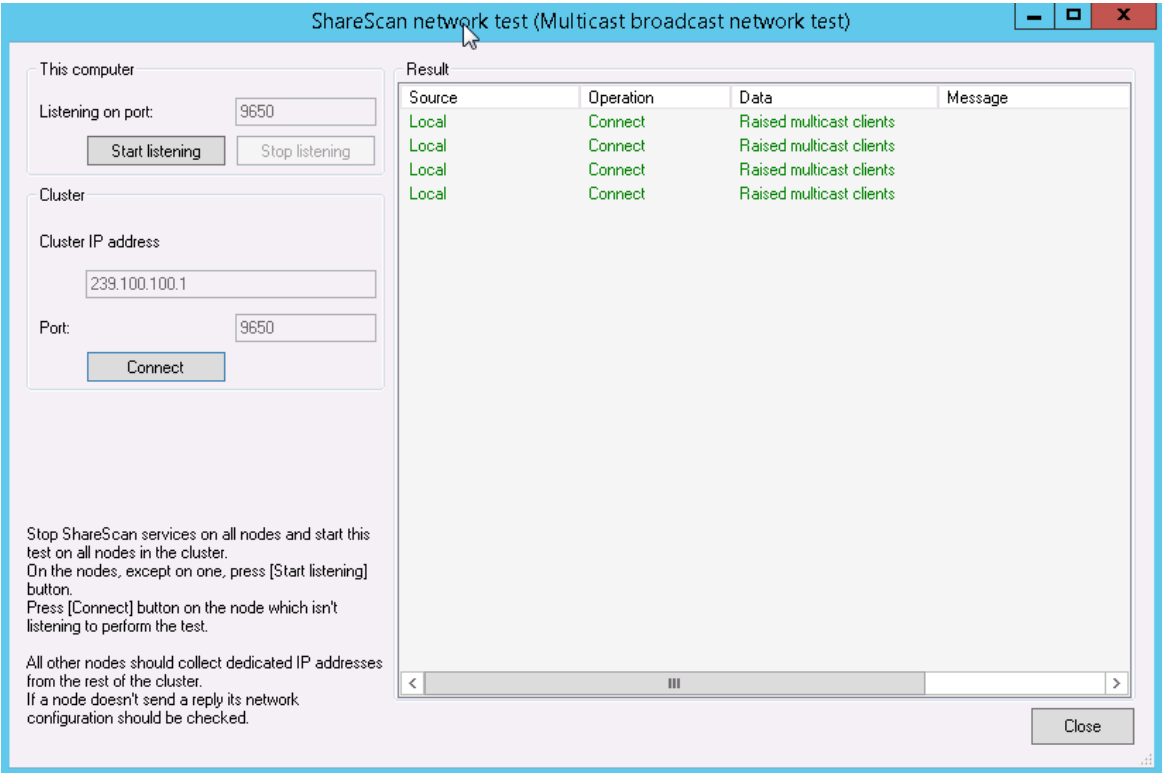
Stop ShareScan services on all nodes and start this test on all nodes in the cluster.
On the nodes, except on one, press [Start listening] button.
Press [Connect] button on the node which isn't listening to perform the test.

Additional notes:

All other nodes should collect dedicated IP addresses from the rest of the cluster.
If a node doesn't send a reply its network configuration should be checked.

Buttons: Close

On the single node you use as a message sender, click the **Connect** button.



When you click the **Connect** button, a broadcast message is sent to all the test servers, listening on UDP port 9650.

If these test servers receive the message, they write out a line into the right-hand list, with the text Receive also indicating the IP address of the sender.

This line should be shown on all the servers where the network test dialog was started with the Start listening button.

If the test was successful, it should be repeated on all nodes, so all of the nodes should act as a message sender once, while the others are listening.

To check which Manager serves the actual device request, a diagnostic feature is included:

If you create a registry setting: HKEY_LOCAL_MACHINE\SOFTWARE\Kofax\ShareScan\ShowClusterNodeIP (string value, true/false) then the ClusterNodeIP value (which can be used to uniquely identify the Manager, and is set by the registry settings at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Kofax\ShareScan\ClusterNodeIP) of the Manager serving the request will be displayed on the Main screen, in the section where usually the "Place a document

into the feeder...” instruction appears. This can be used to determine if the devices are connected to a specific Manager.

Another method to determine the MFP-Manager assignments is detailed below:

- Turn on verbose tracing on the Manager – if the High Availability system is already set up via MS NLB, then it is enough to turn on the tracing on a single Administration Console instance
- Use the devices
- Export the traces (from all server nodes)
- Open the Trace.txt file of a given Manager, and search for \xxx.yyy.zzz.www where xxx.yyy.zzz.www is the IP address of the device you need.

If the string is found, then the MFP is served by that Manager.

Note The MFP – Manager node assignment is constant only until a Manager node is removed or added to the cluster – in case of a change, the device – Manager node assignments are recalculated by MS NLB.