Remote Support

Customer Information

Revision 1.0
March 2018

Contents

1. Overview

1.1. Introduction

Typically, customer support should be conducted by the systems reseller or systems integrator in the first instance, who are responsible for the maintenance of the complete scanning system and are most familiar with the customer setup. Often this will take place onsite. When the problem cannot be resolved by the systems reseller, it may then be escalated to Objective Imaging (OI) for further analysis.

Third-party application TeamViewer is a remote desktop application for Windows, used by OI for the purposes of technical support. This allows OI staff members to view customer computer screens as well as control customer machines where necessary. This in turn provides the capability to diagnose and resolve customer issues around the world, without the requirement of being physically onsite at the customer location.

1.2. Important Notes

OI will typically supply the host application to be used by the customer and **does not** require the customer to download and install TeamViewer client software.

Note that OI is licensed for **version 9** only.

Please consider the disclaimer at the end of this document, section 3.3.

Please close all confidential documents prior to remote support.

2. TeamViewer Information

2.1. For Customers

The customer should run the **Quick Support** tool on their machine and **not** the TeamViewer client application. The correct version of the Quick Support tool is available through the *Remote Support* button on the OI website (top right) at www.objectiveimaging.com.

If prompted, an existing TeamViewer installation may need to be stopped for the Quick Support tool to run. This **does not** require existing TeamViewer software to be uninstalled but closed instead. This is typically achieved by right-clicking the TeamViewer icon in the Taskbar and selecting option *Exit TeamViewer*.

This is a one-time-use application and does not persist in the background when closed. Therefore, no further connections will be available to OI when the customer closes the Quick Support tool or reboots the machine.

When the Quick Support tool is running, an ID number and a password will be displayed. These two items must be supplied to OI staff immediately before the support session is to begin and will allow OI to connect to the customer machine.

OI will typically require **admin level privileges** in Windows, to update software as well as access files such as log files and settings. Please consult your systems administrators to provide this access.

2.2. For Systems Administrators

Some organisations disallow remote access to their internal networks by default, and temporary exclusions may be necessary for OI staff to provide remote support to a customer installation. Details of firewall exclusions for systems administrators are available here:

https://community.teamviewer.com/t5/Knowledge-Base/Which-ports-are-used-by-TeamViewer/ta-p/4139

Please note that OI is licensed for **version 9 only** and this version of software is available for testing of network access here:

https://www.teamviewer.com/en/download/old-versions.aspx?_ga=2.87709144.1997527455.1520933701-1193999975.1502361653#version9

OI typically requires **admin level privileges** in Windows. This is required to modify files in certain system locations, for example hardware drivers in the Windows\System32 folder or applications in Program Files\Objective Imaging folder. Often it is necessary to execute software with the option **Run as Administrator** when communicating with older third-party hardware, e.g. microscope drivers. OI software installations will request **elevation to admin level** to install, and this is typically true for third-party software such as camera drivers, which may also need to be updated during support sessions. In order for the support session to be successful, please arrange admin level access for the duration of the session, which must be applied to the **customer's existing user account**, due to the fact that various settings files are stored in the user Local AppData folder.

Section *3.2 End User Recommendations* outlines various actions which OI suggests prior to the commencement of a remote support session. Some of these actions may require assistance from onsite Systems Administrators. Please ensure all appropriate measures are taken to ensure systems can be restored in event of a major problem.

3. Risks & Precautions

3.1. Overview

Objective Imaging values the safety and security of customer machines. The usage of remote desktop software is intended to provide effective resolution of customer problems only. Nevertheless, it is possible that issues may arise during modification of customer machines by OI staff and sensible precautions should be taken by the customer prior to any remote support session to ensure systems can be fully restored in event of a major problem.

3.2. End User Recommendations

The following actions are advised by OI to help ensure the smooth running of customer systems particularly in event of a problem. This is not a complete list and should be considered a starting point to implement a comprehensive safety and security plan at the customer site.

- Third-party hardware and software such as microscope, camera, filter wheels etc. should be installed and verified independently of OI wherever possible.
- The first point of contact for this should be the systems reseller, the second point of contact should be the manufacturer of these items.

- Accidental physical damage through hardware movement e.g. colliding the objective lens using the Z axis, stage travel etc, should be carefully considered by the customer and movement limits (either software or hardware) should be imposed wherever possible to prevent this. *Discuss with your systems reseller if uncertain*.
- Important slide samples should not be used during remote support sessions, to ensure valued samples do not suffer accidental physical damage or prolonged light intensity bleaching.
- Private patient samples should not be used during remote support sessions.
- Installations for all hardware and software should be retained by the customer.
- Software versions should be retained by the customer.
- Software settings should be retained by the customer for all important applications. OI provides further details on this: https://objectiveimaging.freshdesk.com/solution/articles/9000071917-settings-backup-restore
- All system data and applications should be backed up prior to any remote support session. *Discuss with your onsite systems administrators if uncertain.*
- Customer should remain present during the remote support session and supervise all activities.
- For security and privacy, any open applications or personal or confidential documents should be closed prior to the remote support session.

3.3. Disclaimer

Objective Imaging accepts no liability for damage to customer systems including hardware, software, security or other associated items such as patient tissue slides, computer files etc. OI does not disclose your ID and password to third-parties without your permission. OI is not responsible for unauthorised access to your network using TeamViewer software.

Responsibility for damage or unintended consequences of remote access resides solely with the customer, and the customer understands that by requesting such assistance you are providing OI staff with access to and control of your complete system for the duration of the remote support session.