CK SYSTEMS OPERA CONFIGURATION GUIDE

Table of Contents

Please note that Virus Exclusions, User rights and permissions and DEP settings should be implemented for any Opera install - however CK Systems do not recommend changing SMB or Op Locking settings unless you are experiencing file locking related issues within Opera. Pegasus currently recommend that SMB2 and Oplocks are both left on (the default)

Purpose of this document

This document is designed to supplement the standard Pegasus installation and pre-requisites documentation. It provides additional details on configuring a network for a Pegasus Opera II or Opera 3 system including anti-virus exclusions and system settings

Anti-Virus Exclusions

Pegasus Opera must be excluded from any on-demand scanning that takes place. This will involve adding a number of exclusions to the server and the client PC as detailed below, failing to do so can result in network related read/write and locking problems

Please note: you should also exclude the Opera locations from **Windows Defender scanning** if turned on**.**

Virus Scanning exclusions on workstations:

Exclusions should be applied to these folders and any subfolders contained within them

Server:

\Server VFP Static and Dynamic\ (or what ever Pegasus root folder has been named depending on site)

Locally on PC:

C:\Program Files\Pegasus or the equivalent C:\Program Files (x86)\Pegasus on 64 bit systems

C:\ProgramData\Pegasus\ for Vista/Windows 7 or C:\Documents and Settings\All Users\Application Data\Pegasus\ for XP

C:\Program Files\Common Files\Pegasus Shared

C:\Windows\System32\Spool (note the spool folder can be changed for each printer so if not default add any custom spool folders too)

If **XRL** installed the following also need excluding if the locations exist:

C:\Program Files (x86)\Common Files\Infor

C:\Program files (x86)\Common Files\Lasata Software

C:\Program Files (x86)\XRL or C:\Program Files (X86)\Infor

C:\Programdata\Infor Query & Analysis

C:\ProgramData\Lasata

Virus Scanning exclusions on server:

C:\Program Files\Pegasus or the equivalent C:\Program Files (x86)\Pegasus on 64 bit systems

C:\ProgramData\Pegasus\ or c:\ProgramData\Application Data\Pegasus or C:\Documents and Settings\All Users\Application Data\Pegasus\ depending on Windows version installed on server

C:\Program Files\Common Files\Pegasus Shared

If **XRL** installed the following also need excluding if the locations exist:

C:\Program Files (x86)\Common Files\Infor

C:\Program files (x86)\Common Files\Lasata Software

C:\Program Files (x86)\XRL or C:\Program Files (X86)\Infor

C:\Programdata\Infor Query & Analysis

C:\ProgramData\Lasata

Please note that the main Opera II folder should always be excluded from any scanning on the server if default locations are not used

Some Anti-Virus software versions (ie Kaspersky) also include an option to

Enable VBA Macros Monitoring. This is scanning the XRL add-in when loading and has been found to prevent the add-in loading automatically. **This should be un-checked if selected.** Please check if the AV version being used has a similar option.

User rights and permissions

User rights are a common source of problems with Opera. Whilst it may not be practice to give all users full admin rights they do at the least need full read/write/control rights over the Pegasus folders. In addition both the Opera Client and the CK Systems Bespoke Product Library need to be installed with full admin rights – failure to do so can result in a number of problems when running Opera. It is important to rectify any such user rights issues as they can have knock-on effects in other parts of the system and can sometimes slow general Opera system speed down

Symptoms

Permissions / user rights issue can manifest themselves in numerous ways including, but not limited to, the following:

1. A prompt to overwrite/create a new resource files when starting Opera.
2. User unable to create error logs in the event of a crash (Opera states it cannot write to file)
3. PDF printer driver related issues – printing to PDF freezes or printer not activated error message
4. An “error instantiating class” message upon logon or when backing up etc.

Solution

1. If they have CKS bespoke, uninstall the CKS Client Product Library
2. Uninstall the Opera Client
3. Locate the Client folders and delete. The usual locations are C:\Document and Settings\All Uses\Application Data\Pegasus for XP or C:\ProgramData\Pegasus for Windows Vista/7. Also, delete the client folder in C:\Program Files\Pegasus (or C:\Program Files (X86)\Pegasus).
4. Install the Opera Client by right clicking on the Setup.exe and choosing Run As… for Windows XP or Run as Administrator for Windows Vista / 7. If prompted for a username and password then enter the Administrator details if possible or if not available then enter the user details of a user that has FULL Administrator rights.
5. If they have CKS bespoke, Install the CKS Product Library Client by right clicking on the cksprods_client.exe file and choosing Run As… for Windows XP or Run as Administrator for Windows Vista / 7. If prompted for a username and password then enter the Administrator details if possible or if not available then enter the user details of a user that has FULL Administrator rights.
6. It is always good practice when installing/upgrading the main Opera Server install and the CKS Product Library main install to Run As Administrator

   If the above does not cure the problem then it may be necessary to relocate the foxuser.dbf resource file from the default location to a new path where the user does have full user rights

7. In the Opera client folder (usually c:\program files\pegasus\client vfp or similar) open the config.fpw file for editing in notepad
8. Look to see if there’s a line beginning RESOURCE= and if so change the path to one locally where the user has full admin rights – this could be an existing folder like c:\temp but usually directing it to the Opera temp folder will suffice, for example

   Before: RESOURCE=C:\programdata\Pegasus\Client VFP\foxuser.dbf

   After: RESOURCE=C:\programdata\Pegasus\Client VFP\temp\foxuser.dbf

If there is no RESOURCE= line present then add one in,
RESOURCE=c:\programdata\Client VFP\temp\foxuser.dbf

DEP Settings

For Operating Systems with DEP (Data Execution Protection), ie Windows Server, 2003, 2008, XP, Vista, Windows 7 with DEP turned on opera.exe needs to be added as an exception.

The method for changing DEP varies from OS to OS – in Windows Help search for Data Execution Protection then Add the opera.exe file as an exception

Windows Firewall Settings

If Windows Firewall is in use on the server and/or workstations then Opera can be a program allowed through the firewall.

The settings to allow this are found in Control Panel\Windows Firewall – allow a program or feature through windows firewall.

Network Adaptor Settings

We recommend that you disable the “Allow the computer to turn off this device to save power” setting on the network card as this can cause Opera to run slowly.

You can use Device Manager to change the power management settings for a network adapter. To disable this setting in Device Manager, expand Network Adapters, right-click the adapter, click Properties, click the Power Management tab, and then clear the Allow the computer to turn off this device to save power check box.

Changing SMB settings on Vista/Windows 7/Server 2008

Pegasus recommend SMB2 is ENABLED as long as the hotfix or Service Pack 1 for 2008 or later is installed. It will be enabled by default and these instructions should only be used if you are specifically advised to disable it for any reason

SMB 2.0 was introduced in Windows Vista and Windows Server 2008. SMB 2.0 is designed for the needs of the next generation of file servers. Windows Server 2008 and Windows Vista support both SMB 1.0 and SMB 2.0 in order to preserve backward compatibility. However in an environment that has mixed operating systems including older XP PC's that will use SMB 1.0, you might sometimes want to consider disabling SMB 2.0. You need to do on both the "client" and the "server" operating systems.

To disable SMB 2.0 for Windows Vista (and now Windows 7) or Windows Server 2008 systems that are the "client" systems, run the following commands:

```
sc config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc config mrxsmb20 start= disabled
```

Note there's an extra " " (space) after the "=" sign.

To enable back SMB 2.0 for Windows Vista or Windows Server 2008 systems that are the "client" systems run the following commands:

```
sc config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi
sc config mrxsmb20 start= auto
```

Again, note there's an extra " " (space) after the "=" sign.

To disable SMB 2.0 on the server-side computer, follow these steps:

Warning!
If you make any error while editing the registry, you can potentially cause Windows to fail or be unable to boot, requiring you to reinstall Windows. Edit the registry at your own risk. Always back up the registry before making any changes.

1. Run "regedit" on Windows Server 2008 based computer.
2. Expand and locate the sub tree as follows.

   HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

3. Add a new REG_DWORD key with the name of "Smb2" (without quotation mark)

   Value name: Smb2
   Value type: REG_DWORD
   0 = disabled
   1 = enabled

4. Set the value to 0 to disable SMB 2.0, or set it to 1 to re-enable SMB 2.0.
5. Reboot the server.

Opportunistic Locking Configuration

Please note Opportunistic Locking will be enabled by default and it is not advisable to turn them off unless specifically advised to – please do not disable unless CK Systems have advised otherwise

Disabling Oplocks on Windows Client PCs

To disable oplocks on a Windows client PC change or add (dword) the following Registry values:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters **OplocksDisabled = 1**

Disabling Oplocks on SMB1 Windows Servers

To disable oplocks on a SMB1 Windows server change or add (dword) the following Registry values:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters **EnableOplocks = 0**

Disabling Oplocks on SMB2

Oplocks **cannot** be turned off for SMB2 - you can only disable SMB2 itself (see above)

Settings to help with Speed Related Issues

One setting that can help with Opera speed, and in particular the time taken in loading forms, is disabling “Interrupt Moderation” which is held under the network adapter section. It’s present on major brands of network cards (Intel, Broadcom, Realtek etc.).

Before the following is undertaken ensure the PC is not running any network programs.

In Windows open up Control Panel, Network and Sharing Centre, click on Change Adapter Settings, open Properties on your Local Area Connection (sometimes #2, #3, or something if you have more network cards), click on the Configure button, then the Advanced tab, select Interrupt Moderation, change the value to Disabled, while there look for any settings with the word Offload and enable them all, and then click the OK button to make the changes. This will restart your network card driver and make the settings effective.

Most network cards from popular manufacturers such as Intel, Broadcom, Realtek, etc. hold network packets in a buffer until enough time goes by before raising a hardware interrupt and telling the processor, operating system, and network driver that there are packets waiting to be serviced. By disabling Interrupt Moderation you instruct the network driver and card to raise the interrupt every single time a packet comes in, thus making your processor service the network card much faster thus decreasing latency on the packets held in the buffer and also increasing bandwidth by allowing more packets to flow through faster. This increases your processor utilization by a significant amount 10-30% but if you have a recent dual, quad, hex, octo-core processor and recent network drivers that are multi-threaded with multi-core support and have Receive Side Scaling support then the increased processor utilization is negligible to your computer and if you are running a network server then network performance should be a priority anyway.

No other network driver setting had as much performance impact as Interrupt Moderation.