

Oracle Hospitality Install Document

OPERA OXI Interface Configuration to use protocol TLS 1.2

LAST UPDATED ON | 13 JUNE 2018



Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Version Control

Version	Date	Author	Description
0.5	June 1, 2018	James York	Original documentation creation
1.0	June 5, 2018	Diane L. Pol	Formatting and edit



Table of Contents

Disclaimer	i
Version Control	ii
Intended Audience	1
About this Document	1
Advisories and Considerations	1
Minimum Opera Version	1
Document History Information	1
Implementing the Changes	2

Intended Audience

Hotel IT Personal in-charge of maintaining the OPERA OXI Server. This solution is intended for OPERA OXI Servers connecting to external system hosted outside of Hotel network / cloud hosted that requires secure protocol TLS 1.2 for communication. It is only supported for Windows 7 and Windows 2008 R2. In Windows 8 and above, TLS 1.1 and TLS 1.2 are enabled by default.

About this Document

As of 30 June, SSL and early TLS support will be discontinued and implementing a more secure encryption protocols (TLS 1.2 is strongly encouraged) in order to meet PCI Compliance requirement. OXI Vendors will stop the service thru these protocols and force hotel to cut over to TLS 1.2, otherwise the communication will be affected.

This document provides the detail step to configure the OXI server to use protocol TLS 1.2.

Advisories and Considerations

- » The steps described in this document requires to change Windows registry settings. We recommend that IT personnel create a windows restore point or create a backup of the existing registry settings prior to making the changes.
- » Windows updates need to be applied to the latest available.
- » This document is only for OXI installed on Windows 7 and 2008 R2. If the hotel is using earlier version of Windows, please contact [Oracle Sales team](#) in the region to engage the consulting team for the OXI migration to new machine with newer version of Windows and apply the required changes as described in this document.

Minimum Opera Version

TLS 1.2 Support for OXI: OPERA 5.4.0.x and higher.

Document History Information

Revision	1.0
Original Document Author	James York; Putu Gs
Changes	June 2018: Document created.

Implementing the Changes

1. Adding WinHTTP Support for TLS 1.2 to Windows Registry

WinHTTP is a Microsoft HTTP posting function used by OXI program to generate the requests to vendors. The OS must support TLS 1.2 for successful communication.

Microsoft released an update to add support for DefaultSecureProtocols registry entry that allows the system administrator to specify which SSL protocols should be used when the WINHTTP_OPTION_SECURE_PROTOCOLS flag is used.

See this MS Article for a detailed explanation on the WinHTTP sub-keys: <https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in>

Download the Easy Fix from the Microsoft article above, and run the executable to add the registry keys for the WinHTTP. This is the recommended approach.

Easy fix

To add the DefaultSecureProtocols registry subkey automatically, click the **Download** button. In the **File Download** dialog box, click **Run** or **Open**, and then follow the steps in the easy fix wizard.

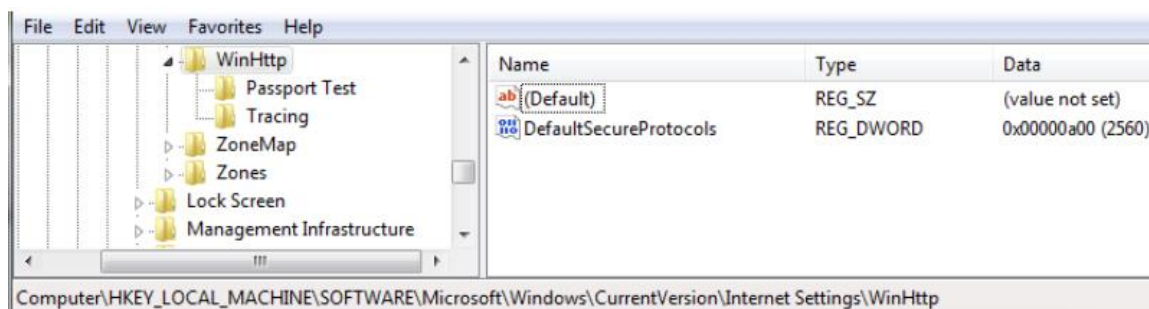
Notes

- This wizard may be in English only. However, the automatic fix also works for other language versions of Windows.
- If you are not on the computer that has the problem, save the easy fix solution to a flash drive or a CD and then run it on the computer that has the problem.

[Download](#)

The Easy Fix will add the required *DefaultSecureProtocols* registry editor entry for enabling TLS 1.1 and 1.2 in the following paths:

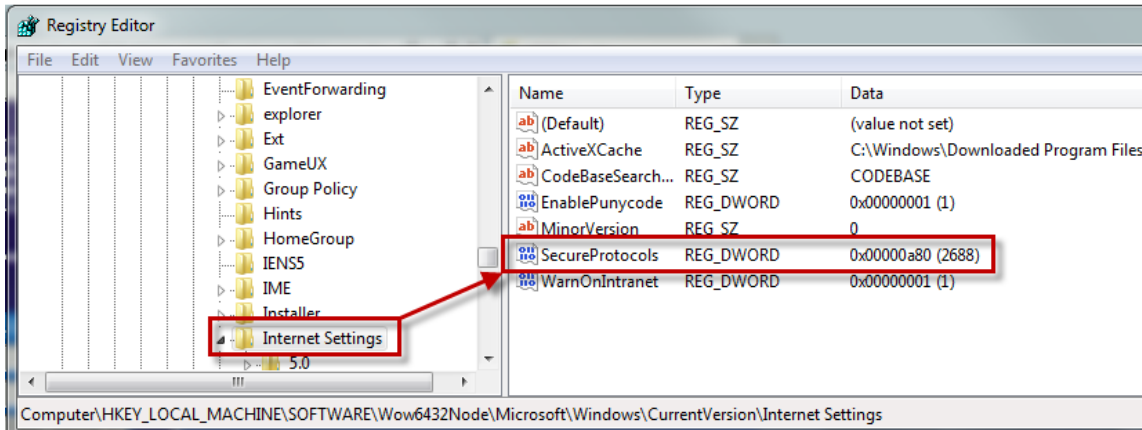
- » HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Setting\WinHttp
- » HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp



2. Adding Internet Setting Support for TLS 1.2 to Windows Registry

This is a very important setting for OXI Interface program to use TLS 1.2 protocol when connecting to external systems.

- » RegEdit Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- » RegEdit Path:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings



To enable the TLS 1.2 protocol, create a *SecureProtocols* entry in the appropriate *Internet Settings* sub-key. This entry does not exist in the registry by default. After you have created the entry, change the DWORD value to *a80* to Enable TLS 1.2 support.

3. Adding SCHANNEL for TLS 1.2 to Windows Registry

The Microsoft Secure Channel or SCHANNEL is an encryption security package that allows users to select which protocols (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2) they want to enable or disable.

SCHANNEL is used by OXI to negotiate secure connectivity with External Systems.

As previously discussed above the protocol used is mandated by the vendor and if the client also supports the protocol then that is what is used for the connection. This means that multiple protocols can be enabled without fear of OXI using the wrong one.

By default SSL 3.0 and TLS 1.0 are enabled, but for TLS 1.1 and TLS 1.2 you need to manually add sub-keys for the following location on Windows 7 and Windows Server 2008 R2 platforms:

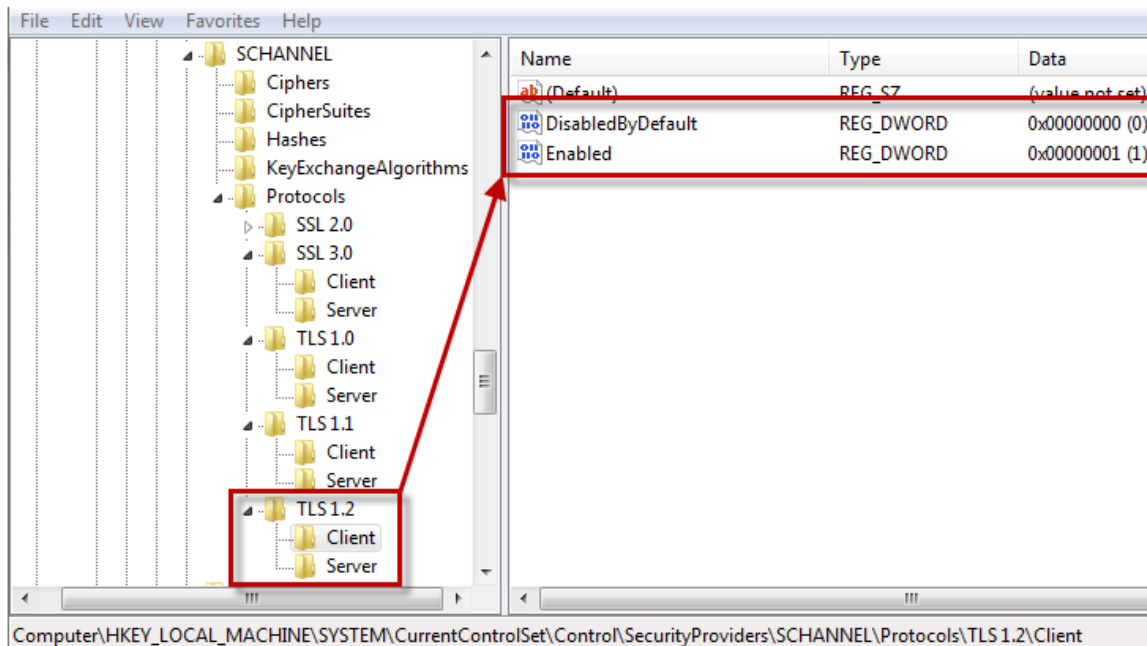
» Regedit path: HKLM SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

To Enable or Disable the TLS 1.2 protocol, create *Enabled* & *DisabledByDefault* entries in the appropriate *Client* sub-key. This entry does not exist in the registry by default. After you have created the entry, change the DWORD value to 0 to disable the sub-key or 1 to enable the sub-key.

You will need to create the *TLS 1.2* → *Client* Path in Regedit and then add *Enabled* & *DisabledByDefault* in the *Client* sub-key.

Set DisabledByDefault to 0

Set Enabled to 1

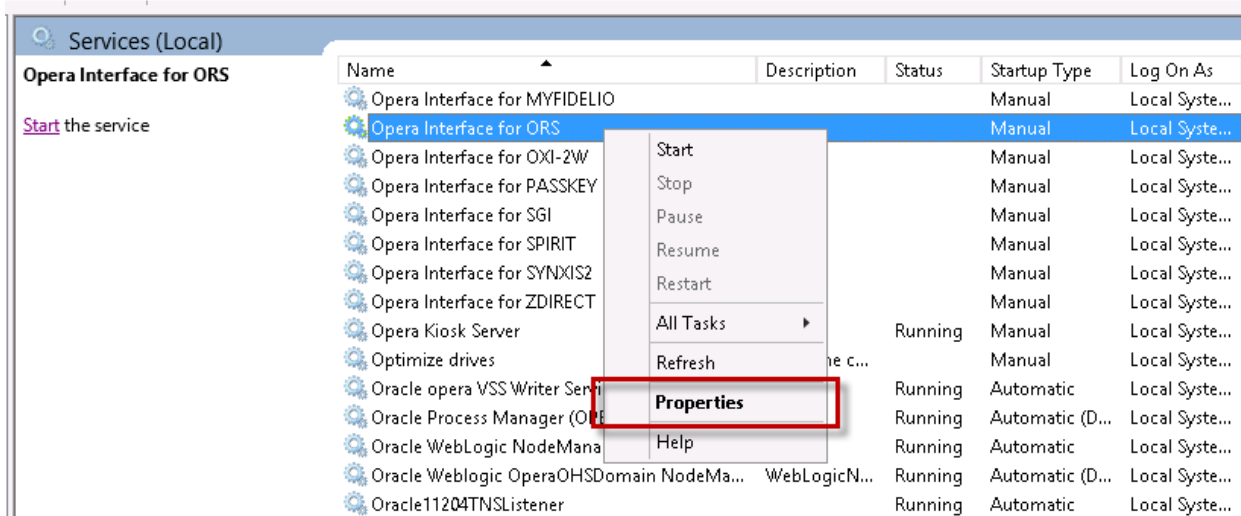


4. Enable TLS 1.2 for Windows Service

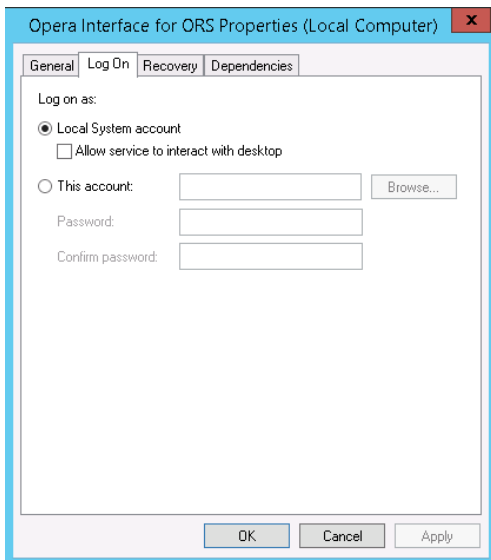
Interfaces such as OXI are run as an MS account called Local System Account, this user is unique from OS level users in that it picks up different registry editor keys when determining which protocol to use.

In some cases it has been observed that the Local System Account used by OXI is unable to pick up the TLS 1.2 protocol sub-keys and may default back to TLS 1.0.

If applying the *three changes* above still does not allow OXI to use TLS 1.2, then you can work around the use of the Local System Account and set the OXI Windows Service to Log On as an OS Admin User (after the WINHTTP, Internet Settings and SCHANNEL keys have been added to support TLS 1.2).



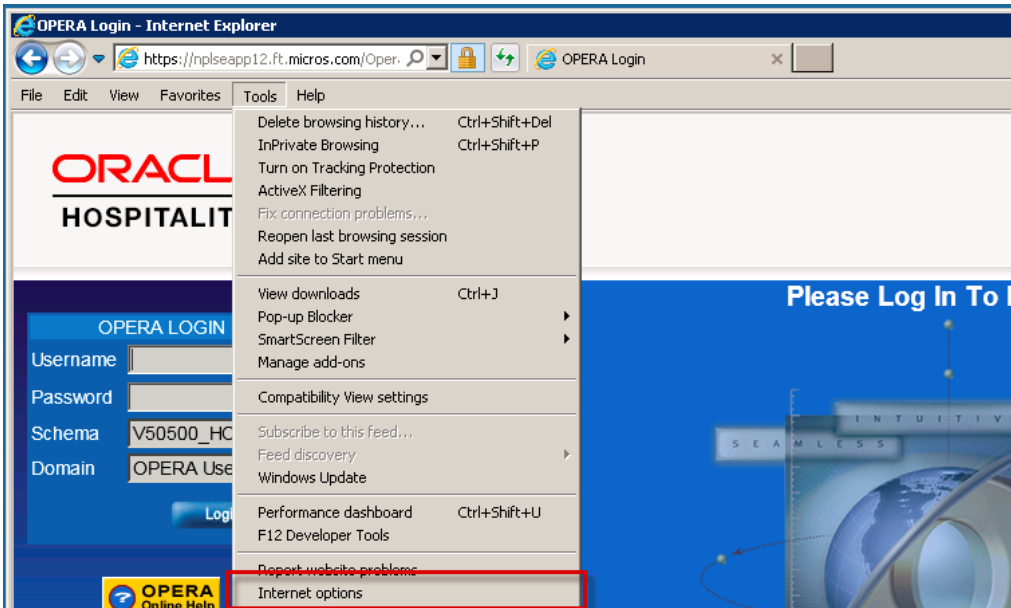
By Default OXI uses Local System Account but if you need to change it to an Admin OS user that can use the WINHTTP and SCHANNEL sub-keys you can use the Log On Tab in Services for the OXI Interface and add the user.



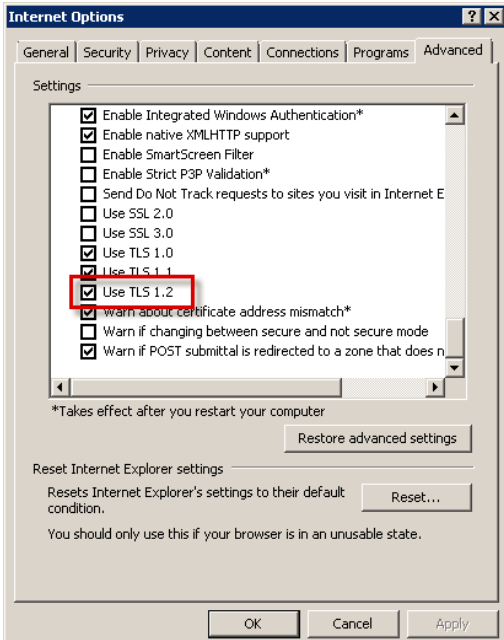
5. Enable TLS 1.2 for Internet Explorer and Java JRE

There are several OPERA components that check the IE and Java Settings to see if TLS 1.2 is enabled such as the OXI Processor Windows Services (Uses IE Settings) and GetID operations from OPERA UI (uses Java Settings) for Merchant Link.

To enable TLS 1.2 for Internet Explorer open the **IE Browser** and go to **Tools → Internet Options**

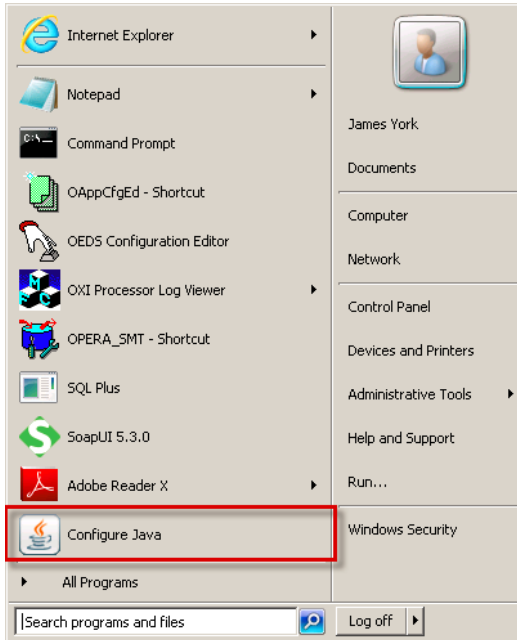


Go to **Advanced** and scroll down to the bottom, there you will find the **Use TLS 1.2 checkbox**, this needs to be ticked. Click OK when finished.

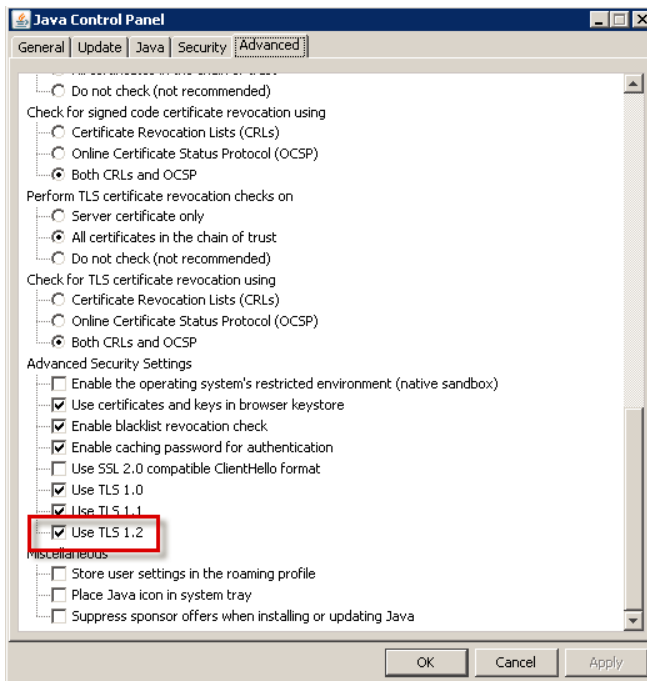


Java JRE Setting is only for **OPERA 5.5.0 and above**.

Open the Configure Java App



Go to **Advanced** and scroll down to the bottom, there you will find the **Use TLS 1.2 checkbox**, this needs to be ticked. Click OK when finished.



Once all changes are in place, you should see TLSv1.2 being used in your network monitoring tools when communicating with OXI Vendors.





Time	Source	Destination	Protocol	Length	Info
474037	11641.305312	92.168.1.204	TLSv1.2	679	Application Data
474038	11641.305314	92.168.1.204	TLSv1.2	455	Application Data
474059	11641.344529	92.168.1.204	TLSv1.2	375	Application Data
474084	11641.888052	92.168.1.204	TLSv1.2	344	Client Hello
474085	11641.888450	92.168.1.204	TLSv1.2	259	Server Hello, Change Cipher Spec, Encrypted Handshake Message
474088	11642.136043	92.168.1.204	TLSv1.2	72	Change Cipher Spec
474089	11642.136044	92.168.1.204	TLSv1.2	167	Encrypted Handshake Message
474091	11642.139508	92.168.1.204	TLSv1.2	679	Application Data
474092	11642.139510	92.168.1.204	TLSv1.2	455	Application Data
474187	11642.185704	92.168.1.204	TLSv1.2	375	Application Data
474459	11646.591957	92.168.1.204	TLSv1.2	151	Encrypted Alert
474540	11649.979729	92.168.1.204	TLSv1.2	151	Encrypted Alert
474564	11650.601801	92.168.1.204	TLSv1.2	151	Encrypted Alert
474612	11652.443452	92.168.1.204	TLSv1.2	151	Encrypted Alert



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0618



Oracle is committed to developing practices and products that help protect the environment