iMail Best Practices Guide

for Configuring new TLS versions – ver. 1.1

The Crescent Office Park, 3 Eglin Road, Sunninghill, Johannesburg.

PO BOX 342, Strathavon, Sandton 2031 Tel +27112623632 Fax +27866378868 www.iMail.com

Best Practices Guideline for Migrations

Purpose

The purpose of this document is to detail the best practices and recommendations from iMail on how to set up the use of versions of TLS newer than 1.0 and 1.1 on versions of Windows, Mac and Outlook that do not support these by default.

Please take note the changes suggested in this document are recommendations and not guaranteed to resolve all issues for software that is no longer supported by the Vendor. We highly recommend these changes are made by an IT professional and that you are running fully supported software supplied by your vendor.

Supported OS Versions

Windows	
Version	*Status*
All versions earlier than Windows 7	Not supported
Windows 7/8: IE earlier than 8	Not supported
Windows 7/8: IE 8, 9, 10	Supported (but must be manually enabled)
Windows 7/8: IE 11	Supported
Windows 8.1 or 10	Supported

Apple Mac	
Version	*Status*
All MacOS versions earlier than 10.9	Not supported
MacOS version 10.9 and later: All versions earlier than Safari 7	Not supported
MacOS version 10.9 and later: Safari 7 and later	Supported

What you need to do to be setup correctly

Outlook 2010

If you are running Outlook 2010 you need to ensure that Outlook has at least SP2 installed otherwise Outlook 2010 will not be able to communicate on the higher TLS levels.

Windows 7

If you are running Windows 7 you need to ensure that Windows 7 has at least Service Pack 1 installed otherwise Windows 7 will not be able to communicate on the higher TLS levels.

The below registry patch needs to be downloaded and installed as well:

https://iMail.freshdesk.com/en/support/solutions/articles/12000085577-windows-7-tls-1-2-registry-fix

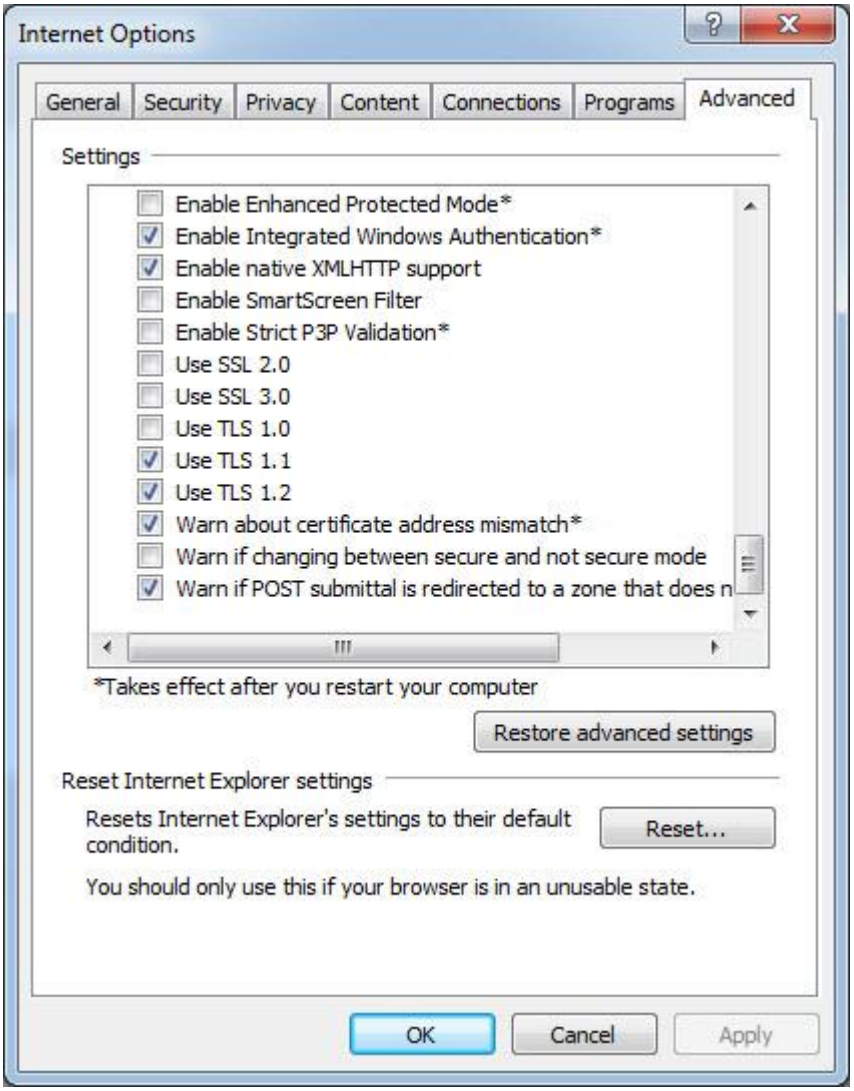
Please ensure that you backup your registry before running this patch so that you can revert if anything goes wrong.

Browser changes

This is for browsers running on Windows 8 or earlier that are not the latest Browser version.

Microsoft Internet Explorer

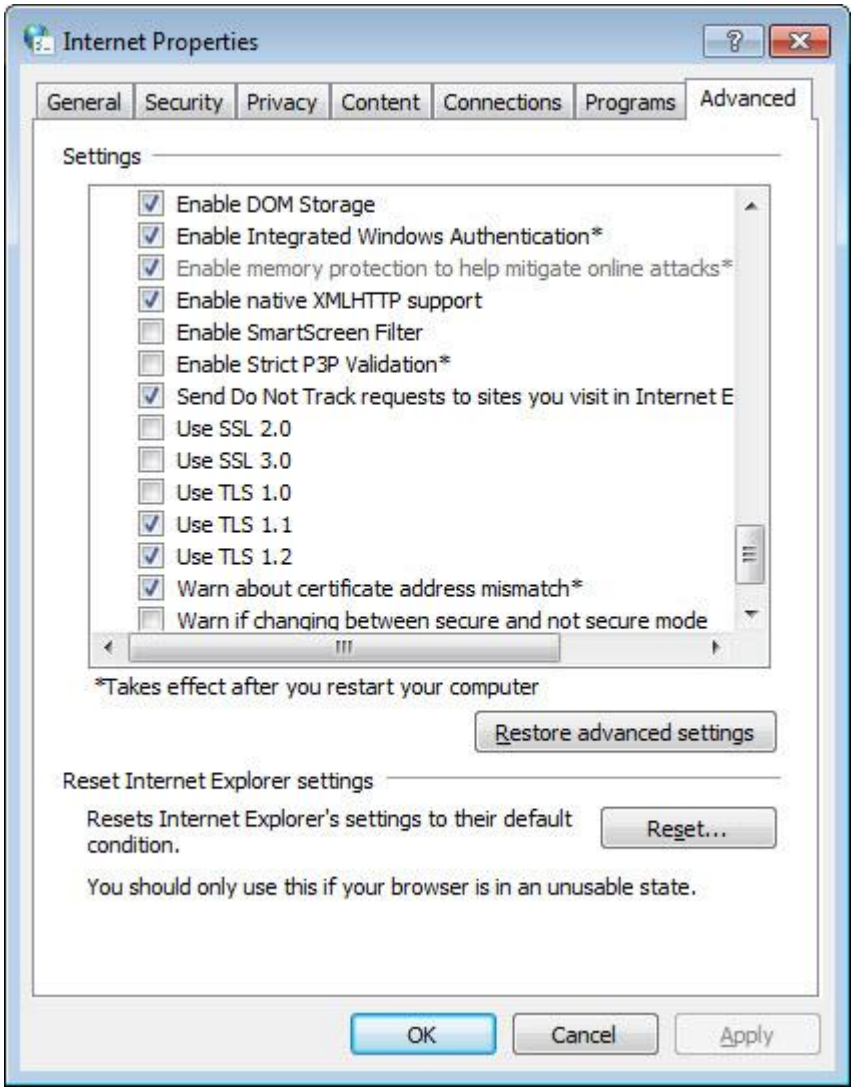
1. Open Internet Explorer
2. From the menu bar, click Tools > Internet Options > Advanced tab
3. Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2



1. Click OK
2. Close your browser and restart Internet Explorer

Google Chrome

1. Open Google Chrome
2. Click Alt F and select Settings
3. Scroll down and select Show advanced settings...
4. Scroll down to the Network section and click on Change proxy settings...
5. Select the Advanced tab
6. Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2

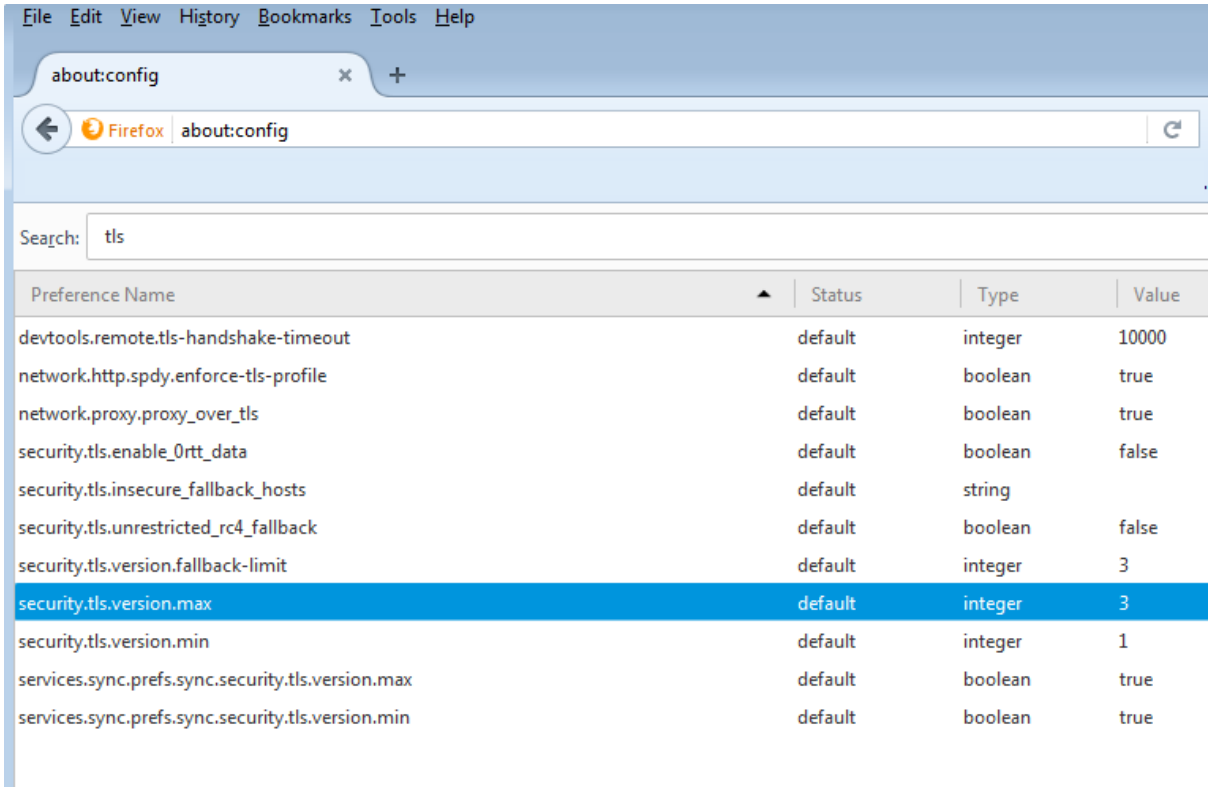


1. Click OK
2. Close your browser and restart Google Chrome

Mozilla Firefox

1. Open Firefox
2. In the address bar, type about:config and press Enter
3. In the Search field, enter tls. Find and double-click the entry for security.tls.version.max

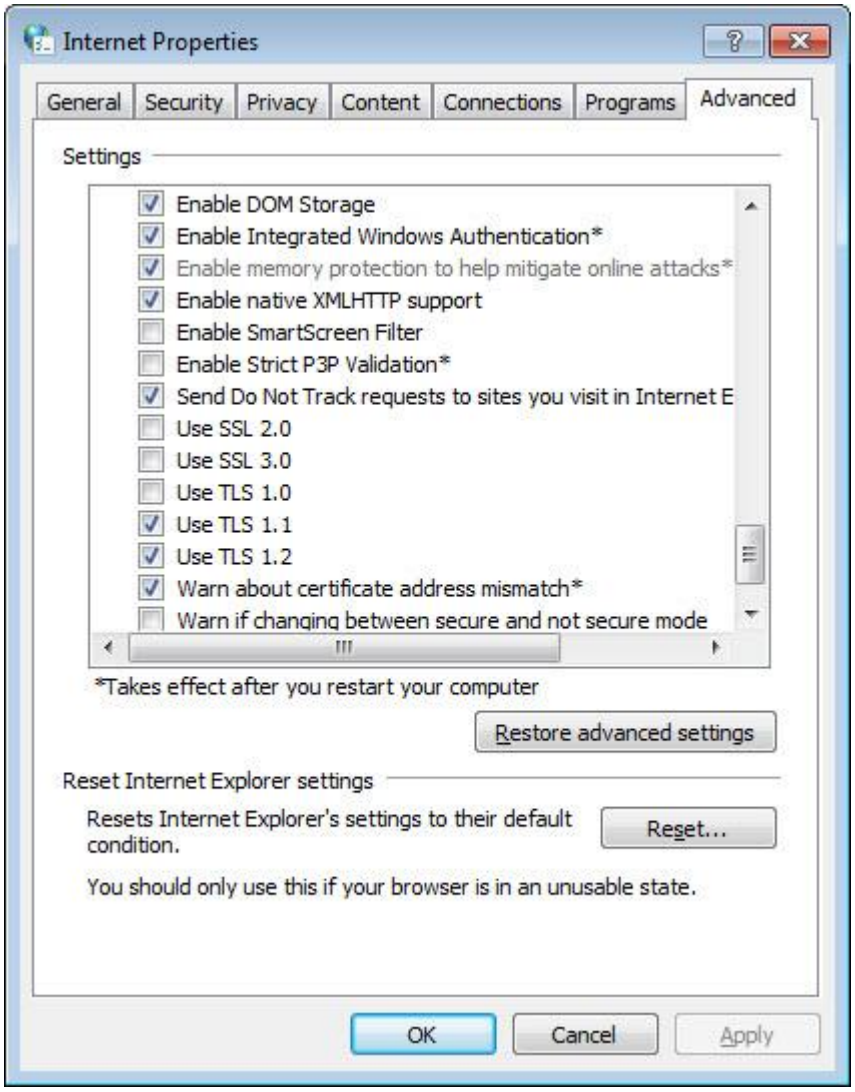
4. Set the integer value to 3 to force protocol of TLS 1.2



1. Click OK
2. Close your browser and restart Mozilla Firefox

Opera

1. Open Opera
2. Click Ctrl plus F12
3. Scroll down to the Network section and click on Change proxy settings...
4. Select the Advanced tab
5. Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2



1. Click OK
2. Close your browser and restart Opera

Apple Safari

There are no options for enabling SSL protocols. If you are using Safari version 7 or greater, TLS 1.1 and TLS 1.2 are automatically enabled.