

ODOT UAG Tips/Troubleshooting Guide

These helpful tips are provided by ODOT Computer Support to help those using a non-ODOT PC and running into issues with connecting the UAG/VPN. This is a best-effort guide - we hope this will be helpful if you are experiencing issues connecting.

UAG = Unified Access Gateway

VPN = Virtual Private Networking

Things to try:

1. Verify Antivirus software is installed and update if necessary
 - a. [Click here to jump to the "Supported Anti-Virus Products" section](#) (or scroll down in this document.)
 - b. This is also true for internal ODOT users on ODOT laptops – look in the taskbar (lower right of desktop) for the blue OfficeScan icon:



Right click that icon, select Update Now, and in the dialog box that opens, click the Update Now button. You will be advised when the update is complete.

2. Verify Personal Firewall is installed
3. If using Internet Explorer 10 or 11, regardless of the version of Windows, you must use "Compatibility View" (this could also be useful in some earlier versions of IE, such as IE8.)
 - a. [Click here to jump to the "Browser Information" section](#) below (or scroll down in this document) for more information.
 - b. If using Windows 8.1, this link will show you how to allow Internet Explorer 11 to work as 10 with the UAG software:
<http://blogs.msdn.com/b/testingspot/archive/2013/09/09/fix-for-microsoft-uag-connection-errors-when-using-internet-explorer-11-with-windows-8-1.aspx>
4. If using Firefox, try using Internet Explorer if you have that option.
5. Ensure pop-up blockers are all turned off for the zigzag site (**including** those provided with Yahoo, Google, and Bing **toolbars**.) –address for the zigzag site: <https://zigzag.odot.state.or.us>
6. Clear Browser Cache
7. Reset Browser to default settings
8. Uninstall and reinstall the UAG Components (if installed)
 - a. Note: After clicking the  link on the PTD website, you may see to a blue box that offers options to install UAG or "Continue" (or "Continue with LIMITED functionality".)

Many users successfully use OPTIS when they select "Continue" (or "Continue with LIMITED functionality") rather than installing UAG.

- b. For issues with ActiveX installation in Internet Explorer, [click here to jump to the "Installation Issues" section](#) (or scroll down in this document.)
9. For OPTIS-specific errors (encountered while logged in to OPTIS), [click here to jump to the "OPTIS Connection Troubleshooting" section](#) (or scroll down in this document.)

Browser Information

For best compatibility, use one of the following:

- Internet Explorer Versions 8, 9 & 10 (32 Bit version only) Windows 7
 - Windows XP support ends on April 8th, 2014 and will not be supported in UAG after that time.
 - In Version 10, 64 Bit, is supported (Windows 8)
- FireFox Version 10 thru current Windows 7 & 8
 - FireFox may not display some UAG components correctly, but you may use it. If you have difficulty, contact us for assistance at OPTIS@odot.state.or.us or 503-986-3300.

Supported Anti-Virus Products

- AVG AntiVirus
- CA eTrust Anti-Virus
- CA eTrust ITM Anti-Virus
- CA Secure Content Manager
- Command Authentium Antivirus
- Cox Authentium Antivirus
- F-Prot Anti-Virus
- F-Secure Anti-Virus
- H+B EDV AntiVir
- Kaspersky Anti-Virus
- McAfee Anti-Virus
- McAfee Total Protection
- McAfee VirusScan ASAP
- Microsoft Forefront Anti-Virus
- Microsoft OneCare Anti-Virus
- NOD32 AntiVirus
- Panda ClientShield AntiVirus
- SoftWin BitDefender Anti-Virus
- Sophos Anti-Virus
- Symantec/Norton Anti-Virus
- Symantec Norton 360 Anti-Virus (and Anti Spyware)
- Symantec Endpoint Protection (and Anti Spyware)
- Trend Micro Internet Security (and Anti Spyware)
- Trend Micro OfficeScan Anti-Virus
- Trend Micro PC-Cillin Anti Virus
- Trend Micro ServerProtect Anti-Virus
- V-Com SystemSuite Anti-Virus
- ZoneAlarm Anti-Virus

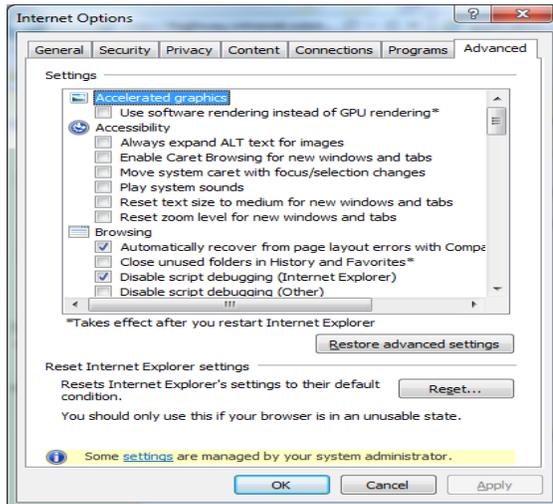
UAG also supports WMI based detection via the Windows Security Center (a.k.a Action Center), which extends support to virtually any modern security product that has been designed to integrate with the Security/Action center mechanism.

Installation Issues – Active X

Reset Internet Explorer to Default Settings

Note: You may want to backup IE favorites before proceeding

1. Go to Tools | Internet Options and click on the Advanced Tab



2. Check "Delete Personal Settings" and Click on Reset



3. Close and Reopen Internet Explorer
4. Go back to the OPTIS link, and you should be prompted to run the necessary components

You can also do the following:

1. In Internet Options, click on the Security tab
2. Click Internet, and then click Custom Level
3. In the ActiveX controls and plug-ins section, under Download signed ActiveX controls, click
4. either "Enable" or "Prompt" according to your preference. Selecting "Prompt" allows you to enable/disable each script that is loaded from a Web page.
5. Click OK twice, Close and Reopen Internet Explorer, then go back to the OPTIS link.

OPTIS Connection Troubleshooting

Question: Why I am getting a “bad referer” message?

Note: This error is related to system “cookies”. In a secure system, “cookies” are what keeps the application in communication with the secure server. The “bad referer” error occurs when this “connection” is lost.

Answer: There are two general situations in which this can occur:

- a. When you use the Forward/Back buttons in your web browser instead of the OPTIS buttons – use only OPTIS system buttons to navigate in OPTIS. If you close and reopen your web browser and log back in to OPTIS, you should be able to continue the task you were working on when you encountered the original problem.
- b. When you open a new window or try to access attachments – if your browser security setting blocks popups, you must modify your settings. If you use Internet Explorer, follow these steps:
 1. In Internet Explorer, select Tools > Internet Options > Security.
 2. Select the “Trusted sites” icon and click on the “Sites” button.
 3. In the next screen, type <https://oregon.gov>. Click the “add” button. Then click “Close” at the bottom of the box.
 4. Select the “Privacy” tab.
 5. Select “Sites”.
 6. Type oregon.gov in the “Address of website” field and click “Allow”. Then click “OK” at the bottom of the box.
 7. In the “Pop-up Blocker” section of the “Privacy” area, the block pop-up box should be selected. Click on “Settings” and type oregon.gov in the “Address of website to allow” field and click the “Add” button.
 8. Click “Close” and then click “OK”.
 9. Close and reopen Internet Explorer.