

OPTIS Connection Troubleshooting

Question: Why I am getting a “bad referrer” 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 Referrer” error occurs when this “connection” is lost.

Answer:

There are two general situations in which this can occur.

A. You are using the “Forward or Back” buttons  on your web browser instead of the OPTIS  **Back** button. Only system buttons shall be used to navigate around in OPTIS. 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. If this error occurs while you are opening a new window or trying to access attachments, your browser security setting or one (or more) popup blockers on your computer need to be modified by following these steps:

1. In Internet Explorer, select Tools > Internet Options > Security
2. Select “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
8. Click on “Settings” and type oregon.gov in the “Address of website to allow” field and click the “Add” button
9. Click “Close” and then click “OK”

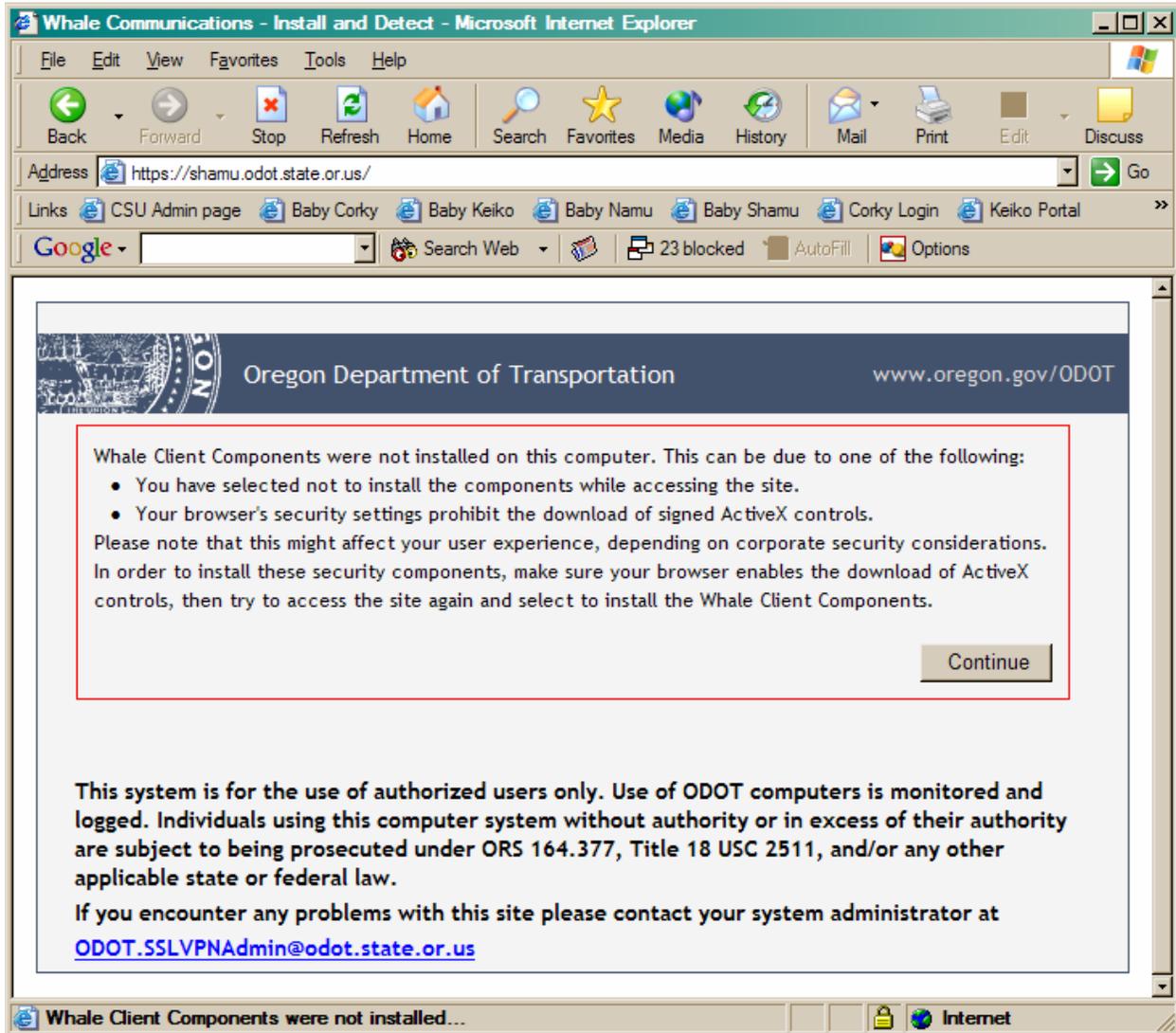
[Read more](#) “Disabling pop-up blocking” scenarios for browsers other than IE.

Question: Why are my pages are not displaying correctly?

Answer:

Internet Explorer 8 (IE8) is not fully compatible with many websites, including OPTIS. If you are a customer that has IE8 and are having a problem navigating OPTIS, we recommend that you turn on the “Compatibility View” feature by going to the Tools > Internet Options > Advanced > Browsing > check “Automatically recover from page layout errors with Compatibility View.” Once the compatibility option is turned on, the web pages should display appropriately.

Question: I received the following ActiveX error, what do I do?



Answer:

The Whale SSL VPN uses ActiveX controls and in order to get full functionality, you must enable Download of signed Active X controls in Internet Explorer as follows:

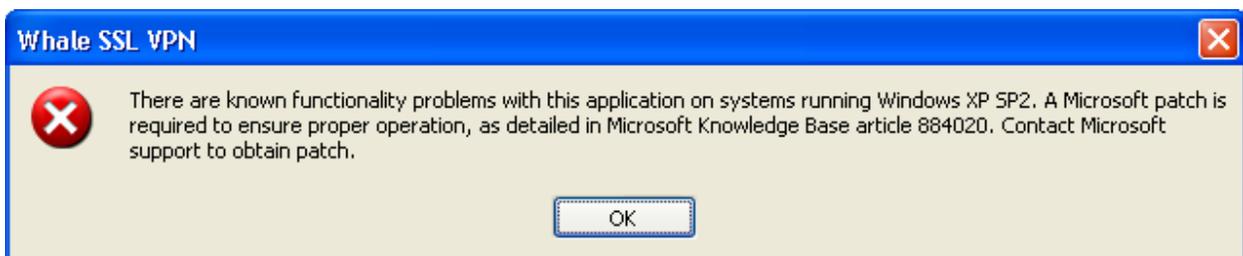
1. Start Internet Explorer
2. On the Tools menu, click Internet Options
3. Click the Security tab
4. Click Internet, and then click Custom Level
5. In the ActiveX controls and plug-ins section, under Download signed ActiveX controls, click either "Enable" or "Prompt" according to your preference. Selecting "Prompt" will cause you to be prompted whether to enable or disable each script that is loaded from a Web page.
6. Click OK
7. Click OK

Question: Do I have to allow pop-ups for the SSL VPN?

Answer:

Yes, pop-ups must be enabled for this site so that the SSL VPN will function correctly. There are many third-party programs that are designed to prevent pop-up and pop-under windows from being opened. These programs may cause side effects, such as preventing a Web site from opening a new window or other script-related problems. ODOT does not support the installation, functionality, or use of any such third-party programs.

Question: I am using a computer running Windows XP with Service Pack 2 and I got the following message from the Whale, what do I do?



Answer:

Click OK, then go to the Microsoft website to download and install the appropriate Microsoft patch. The URL is <http://support.microsoft.com/default.aspx?kbid=884020>. This patch corrects the way the XP with Service Pack 2 handles the loopback address used by the SSL VPN.

Question: My Personal Firewall keeps saying that some applications named Whl### are trying to get to the internet. Is that okay?

Answer:

Yes, those applications are the Whale Components and require access to the internet to provide full functionality of the SSL VPN. If you would like the messages to stop, you can choose to tell your personal firewall to always allow access for those applications.

Question: I am running a Personal Firewall that is compatible with the SSL VPN but the Detect results still show that the only Firewall running on my system is the XP SP2 Firewall and I am denied access. How do I resolve that?

Answer:

The Detect functionality of the Remote Access portal can have trouble recognizing an additional software firewall product if the XP SP2 firewall was enabled on the computer prior to the software firewall installation. The following steps may fix the problem by having the software firewall recognized as the primary firewall on the system:

1. Turn off the XPSP2 firewall - see: <http://support.microsoft.com/default.aspx?scid=kb;en-us;283673>

2. Reboot the system
3. Verify that the software firewall is running and that it is detected by the SSL VPN by checking the system information in the System Test portal, <http://systest.odot.state.or.us>.

If the firewall is displayed correctly in the system information, the software firewall you are using is now being detected correctly and you will have full function of the remote access portal. If you choose to do so, you can re-enable the XP SP2 firewall at this time and it shouldn't cause further conflicts in most cases. If the problem does re-occur, you may have to repeat the steps outlined above.

Question: I am running a Personal Firewall and/or an Antivirus that came with my computer. It was pre-installed and when I check, it says it is the same version as a current supported version on the ODOT supported clients list. Why won't it work?

Answer:

Firewalls and Antivirus products are supplied with many new computers. Many of these are called OEM or Trial versions. Frequently these are not full versions of the product or created unique for the new computer vendor and will not be supported by the SSL VPN. You will need to purchase a full licensed version of these products to be recognized as a valid firewall or antivirus.

Internal Users Only

Question: When trying to connect remotely while using an ODOT laptop, I get a message stating “Computer does not meet the Security Requirements.”

Answer:

If you are using an ODOT laptop and have not been connected to the domain in the last week, you will need to update your Office Scan antivirus.

1. In the lower right hand corner of your desktop on your toolbar you'll see a blue octagonal shape (similar to a blue stop sign). This is the icon for Office Scan.
2. Right click on the icon
3. Select “Update Now!”
4. An “Update Now Settings” dialog box will open
5. Click the Update Now button

The system will begin updating the Office Scan components. The System will advise when the update is complete.