

Parasite Software Removal

Over the past several months of testing, we have determined that certain types of parasite software, also commonly known as Adware, Spyware, etc..., can severely affect the performance and stability of a UHS Finance PeopleSoft 8.4 Web Access sessions. We are recommending that all UHS Finance 8.4 users clean their desktop machines before accessing the UHS Finance 8.4 system.

Thousands of adware and spyware parasite software programs exist and many are promulgated by legitimate commercial sites. These software titles can infest your browser and desktop computer without your knowledge. You can find many discussions and documents on the Internet regarding this type of parasite software.

How to clean:

You may first try and review "Add / Remove Programs" from the control panel. Remove any software you know is a parasite (THIS CAN BE VERY DIFFICULT TO DETERMINE AND MAY REQUIRE SOME RESEARCH). If unsure don't remove it without consulting with your Information Technology Desktop Support personnel. Common parasite software titles are: Gator, Save.Now, Wild Tangent, HotBar, ClockSync, WeatherCast, etc... Many purport to be helper applications, but they may also collect and analyze your browsing habits and send information back to a host site for improved target marketing to you.

The best way to clean:

Use a legitimate spyware removal software program. Several exist, some are free and some are not. We have had success with the following products which are free and can be obtained from CNET's download.com: "SpyBot Search and Destroy 1.3" by PepiMK Software and "Ad-aware 6" by Lavasoft. If you are interested, go to www.download.com and search on "Spybot" or "Ad-aware" "in Windows".

You may need help installing, configuring, and running this software. Please consult with your IT desktop support personnel if you need help or are uncomfortable implementing a spyware / adware cleaner.

Spyware / Adware cleaners do not take the place of good anti-virus software. Always have good anti-virus software installed that is regularly updated with the latest virus definitions from the vendor or your campus site. You should scan your system for viruses at least once a week and always keep the background virus analyzer protection enabled. Consult with your IT desktop support personnel for more details.

Browser Settings

The recommended Internet Explorer browser settings listed below can improve the user's experience while navigating and working in the UHS Finance PeopleSoft 8.4 Web Access session.

It is also recommended that the user's desktop system have the most recent Microsoft Updates applied to their system and that they use the latest version of Internet Explorer 6.x.

They should also ensure that their system is free of viruses. Most user's are already using some type of anti-virus software, but do not schedule a regular full scan of their systems often enough. If they have not scanned their system for viruses in the last 7 days, they should do so now using the latest virus definition file from their anti-virus vendor. If needed, consult with Information Technology Desktop Support personnel on this subject.

If you are uncomfortable making these changes, consult with your Information Technology support personnel.

84 Desktop Tuning

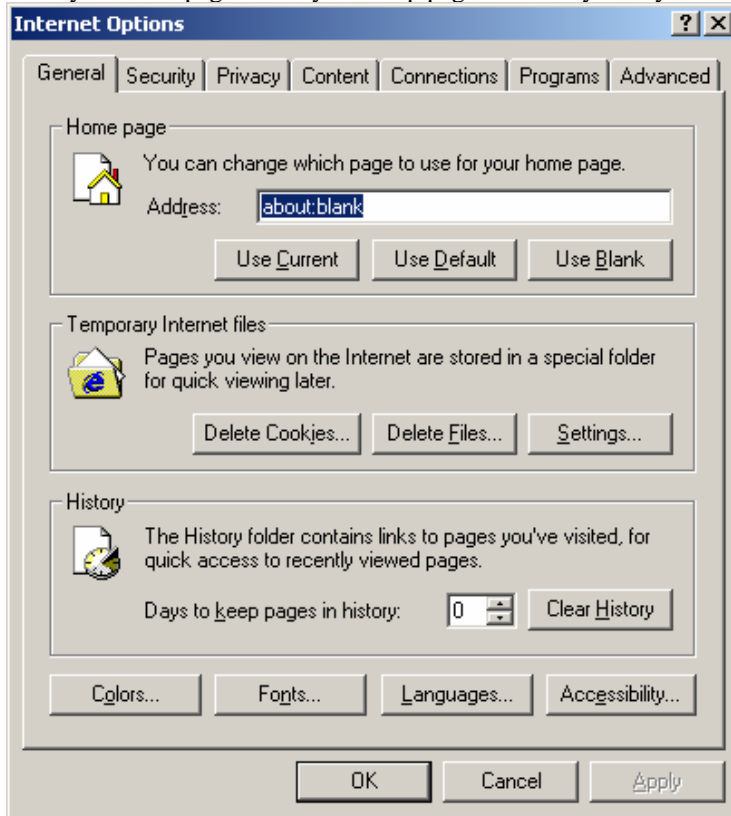
Internet Explorer 6.x Recommended Settings

These recommendations may improve performance and stability when using the UH Finance PeopleSoft 8.4 Web Interface. They are not required, but recommended.

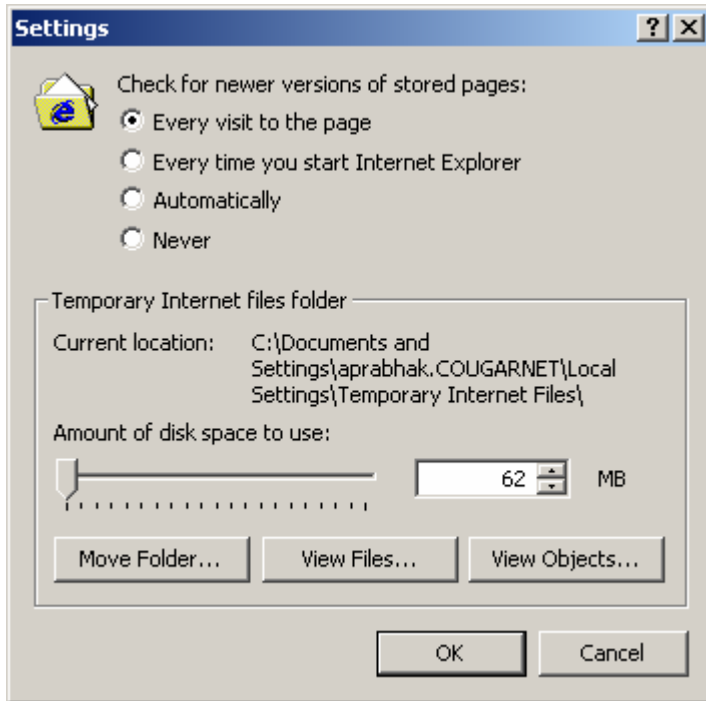
These settings are for Internet Explorer (IE) 6.x, but may also work with IE 5.5.

It is highly recommended that you upgrade to the latest version of IE 6.x. (See your desktop support person or visit the Microsoft Windows Update Site)

Open your IE browser. At the top, choose “Tools”, “Internet Options” to get to the window shown below. (You can leave your homepage and days to keep pages in history how you have them set)



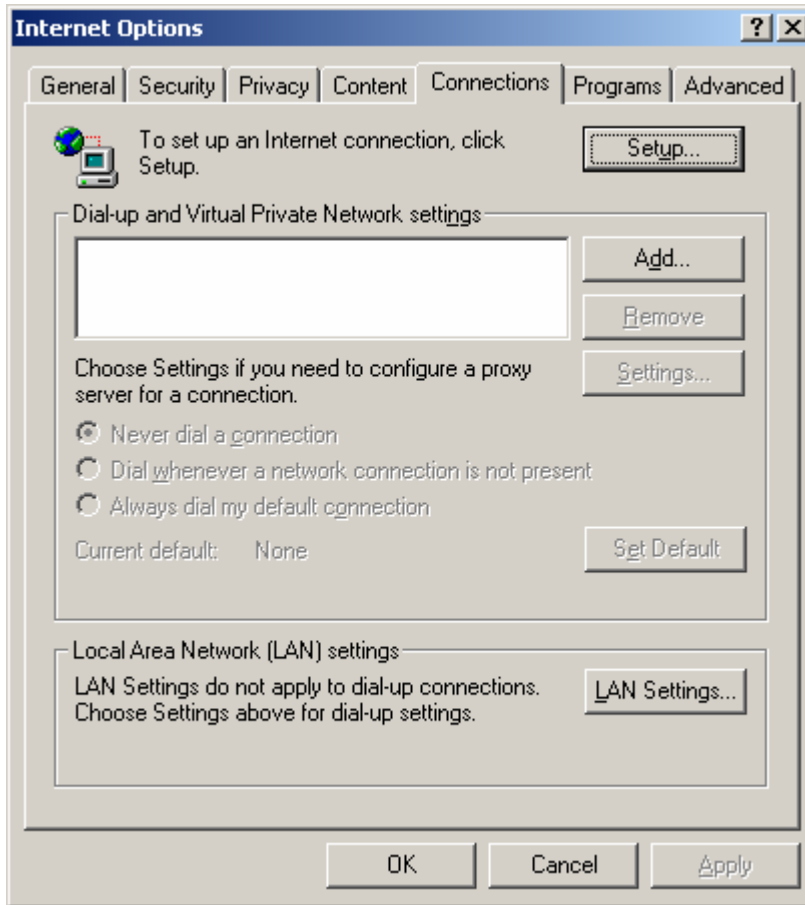
1. Delete Cookies and Delete Files (check Delete All Offline Content when deleting files).
2. Click on “Settings”.



3. Choose every visit to the page.

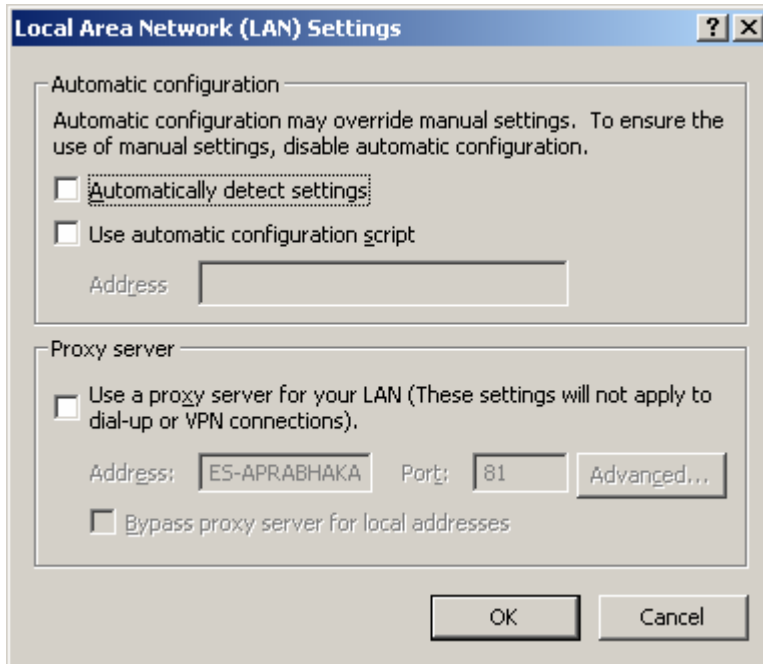
4. Set Amount of disk space to use to anywhere from 5 to 65 MB (this is just a recommendation, you can choose more if you prefer).

5. Click on OK.

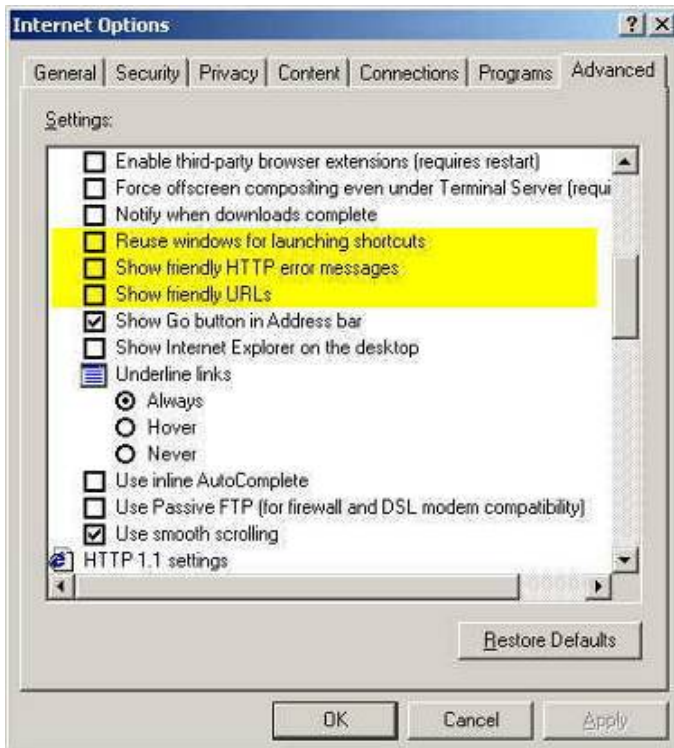
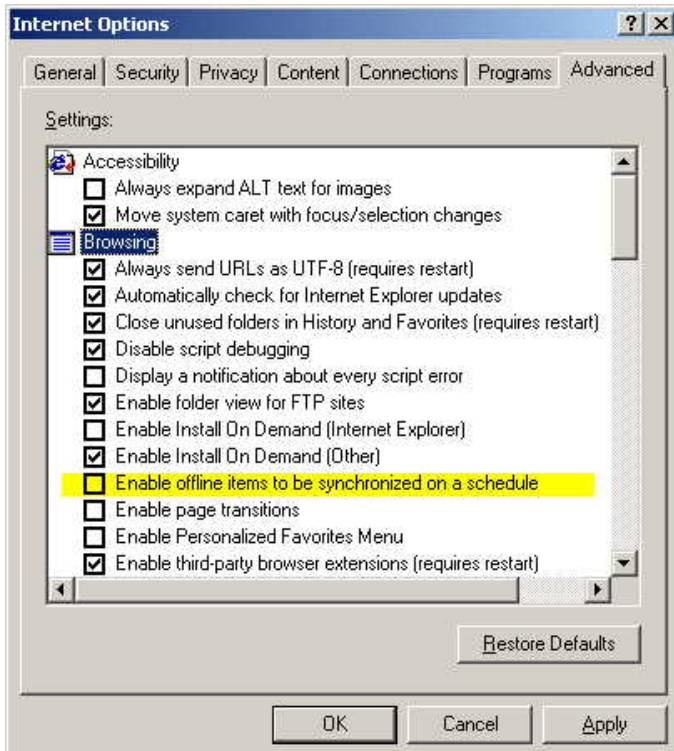


6. Click on Connections Tab.

7. Click on LAN Settings button.

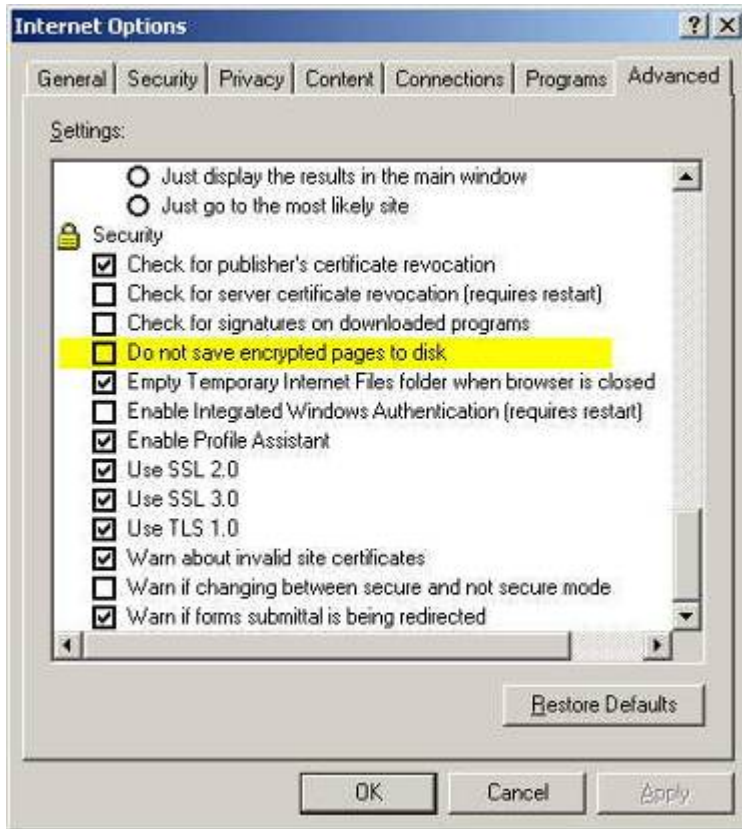


8. Turn off (uncheck) Automatically Detect Settings.
9. Click OK.
10. Click on Advanced Tab and scroll down to the Browsing Section.

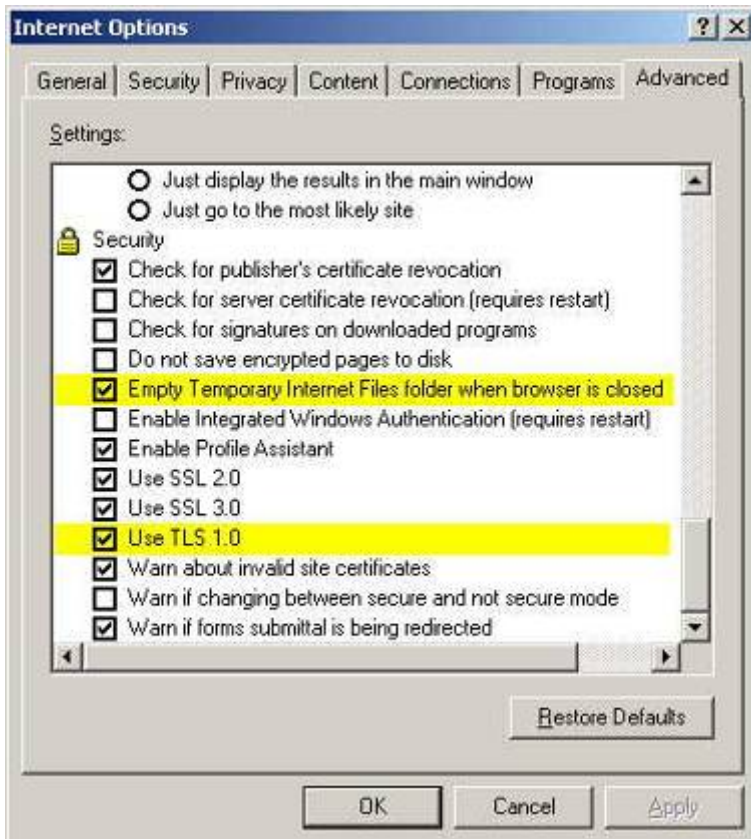


11. Make sure the highlighted items are NOT checked.

12. Scroll down to the Security section.



13. Again make sure the highlighted item is NOT checked.



14. In the same security section, make sure the highlighted items ARE checked.
15. Click Apply.
16. Click OK.
17. Close your IE browser and any other IE browser window that you have open.
18. You are done.