

# Secure file transfer

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-12/msg00021.html>

---

- *From:* [evans@xxxxxxxxxxxxxxxxxxxxxx](mailto:evans@xxxxxxxxxxxxxxxxxxxxxx)
  - *Date:* Sun, 16 Dec 2007 12:34:06 -0800 (PST)
- 

What I am trying to do is to protect my password and file contents in the best way when I connect to my hosted domain, and hopefully in a way that does not require a tremendous amount of work or advanced knowledge.

I have two programs: Core FTP Lite, and Winscp, both the latest versions.

## Part I – Core FTP

In Core FTP, is it better to use AUTH SSL or SSH/SFTP?

This may (or not) have a bearing on it. When I connected using AUTH SSL, the connection script said:

```
....  
AUTH SSL  
500 This security scheme is not implemented  
....
```

It then went on with the connection. I contacted the people who are hosting my account and the first guy said that :

"That error message is misleading, it means that the ssl cannot be authenticated but it will still use the encryption layer."

When I wrote back re-quoting the above script and asking them to confirm what they had said, the second guy did not comment one way or the other but said that I should be using SSH. Core FTP has that option. My question is, which should I be using?

## Part II – Winscp

In Winscp, which only uses SSH (and I have that enabled in my account), One of the fields in the login screen is "Private Key File". Core FTP did not have such a field. In any case, what happens if I leave that field blank? (I would not even know what to create or how.) Is my password and data going out unencrypted if I have not set up a private key?

Thank you.