VA SOFTWARE SOURCEF RGE™	**SFEE 3.4 Authenticated PServer Frequently Asked Questions**

1. **Are there additional Authenticated PServer features available in SourceForge Enterprise Edition 3.4?**

   No. The SourceForge Authenticated PServer functionality is the same in SFEE 3.4 as in SFEE 3.3.

2. **What is Authenticated PServer?**

   Authenticated PServer is a protocol for communicating with CVS, instead of using SSH.

   Because the data transfer is unencrypted, there is a possible security risk using Authenticated Pserver. Therefore, it is recommended that clients use this protocol only for internal transfer of data.

3. **What are the benefits using the Authenticated PServer?**

   The benefits of using Authenticated PServer are:

   - It easy to set up

   - More UI/Web-based clients available compared to the one available for SSH in CVS (WinCVS)

4. **What should I do if my organization is not using PServer?**

   For security reasons, it is highly recommended that you disable the password-authenticating CVS server (pserver) if no projects will use it. The PServer is disabled by default on Solaris system. On Linux systems, modify the "disable" variable in the /sourceforge/etc/cvspserver configuration file as required. To disable it, assign the value "yes" to the "disable" variable in the configuration file.

   (See the SFEE 3.4 Installation and System Administration Guide for detailed instructions.)

5. **Is unauthenticated PServer supported?**

   No, unauthenticated PServer is not supported in SFEE 3.4.

6. Do I need to login to the server before accessing the CVS repository?

Yes, you need to login to the server to access the CVS repository. To login use the following command (If Authenticated Pserver is supported):

cvs -d:pserver:username@cvs.f00.com:/cvsroot/projectname login

7. Do I need to enter the password for every transaction?

No, you need not enter the password for every transaction. The password entered is recorded for later transaction.

8. By default, where are the passwords stored?

The passwords are stored in the file `$HOME/.cvspass'. They are encrypted and stored.

9. Why is the term "pserver" required in the CVS login command?

Without the term `:pserver:' in the login command the CVS will assume to use "rsh" to connect with the server.

10. Is the data transfer encrypted?

Unlike with SSH, the data transfer is not encrypted. This might pose a security threat. Therefore it is recommended that this protocol only be used within your organization or with trusted networks.

11. Will the session expire if I close the client window?

Yes, the session expires once the client window is closed.