|  |  |  |
| --- | --- | --- |
| **Key Software Components** | | **NOTES** |
| **Web Hosting Process:** | sftpplus-service-shawl.exe |  |
| **Web Hosting Process Child:** | sftpplus-worker.exe |  |
| **Web Hosting Process Parent:** | services.exe |  |
| **Web Hosting Process Grandparent:** | winnit.exe |  |
| **Web Hosting Process Working Directory:** | C:\Program Files\SFTPPlus\lib\Scripts\sftpplus-service-shawl.exe |  |
| **Web Hosting Process Command Line:** | C:\Program Files\SFTPPlus\lib\Scripts\sftpplus-service-shawl.exe run --name sftpplus --stop-timeout 30000 --no-restart --cwd "\\?\C:\Program Files\SFTPPlus" -- "C:\Program Files\SFTPPlus\lib\sftpplus-worker.exe" -m chevah.server.\_\_init\_\_ start-in-foreground --config configuration\server.ini |  |
| **Admin Portal:** | <https://127.0.0.1:10020/> | https://127.0.0.1:10020/manager#!/status when authenticated |
|  |  |  |
| **Log Sources for Common Attacker Actions** | | **NOTES** |
| **New User Creation:** | Found in admin log in portal |  |
| **User Authentication Event to Admin Console:** | C:\Program Files\SFTPPlus\log |  |
| **Configuration File Location** | configuration/server.ini | [https://www.sftpplus.com/documentation/sftpplus/latest/configuration/configuration-file.html  Testing environment keeps logs for 30 days at log/server-testing.log Production environment keeps logs for 120 dats storing them at logs/server-production.log](https://www.sftpplus.com/documentation/sftpplus/latest/configuration/configuration-file.html) |
| **SqLite Database Location** | C:\Program Files\SFTPPlus\configuration |  |
| **Default Logs** | windows - C:\Program Files\SFTPPlus\log linux - /opt/sftpplus/log/server.log | <https://www.sftpplus.com/documentation/sftpplus/latest/configuration/introduction.html> |
| **SSH Key Locations** | windows - C:\Program Files\SFTPPlus\.ssh\authorized\_keys linux - /opt/sftpplus/.ssh/authorized\_keys |  |
| **Admin Console Access Logs:** | C:\Program Files\SFTPPlus\log |  |
| **File Activity Events:** | C:\Program Files\SFTPPlus\log |  |
|  |  |  |
| **Command Execution via MFT Automation:** | |  |
| **Command Execution via MFT Automation Activity within MFT Datastore:** |  |  |
| **Command Execution via MFT Auomation Activity within Logs:** |  |  |
|  |  |  |
| **ADDITIONAL DATA** | | **NOTES** |
| **Version** |  |  |
| **Web Admin Console Default Credentials** | username: admin / pw: pass | <https://www.sftpplus.com/documentation/sftpplus/latest/configuration/local-manager.html> |
| **Test Account Default Credentials** | username: "test\_user" / pw: test\_password | account is disabled by default |
| **Default Install Dir** | C:\Program Files\SFTPPlus |  |
| **Default Linux Install Dir** | /opt/sftpplus |  |
| **Default Ports** | Web-based manager console - 10020 ftp and explicit FTPS - 10021 HTTPS - 10443 SSH (SFTP/SCP) - 10022 Only OS root account is allowed to bind ports below 1014 (LINUX) Proxy port connection to remote server - 1080 connect to server - 21, 443, 445, 990 non-TLS connections - 5672 TLS connections - 5671 LDAP Server - 389 | proxy port - https://www.sftpplus.com/documentation/sftpplus/latest/configuration-client/sftp.html connect to server - https://www.sftpplus.com/documentation/sftpplus/latest/configuration-client/sftp.html TLS/Non-TLS Connections - https://www.sftpplus.com/documentation/sftpplus/latest/configuration-events/rabbitmq.html LDAP - https://www.sftpplus.com/documentation/sftpplus/latest/configuration-auth/ldap.html |
| **Windows Event Logs** | Events sent to Application category using Informational level | <https://www.sftpplus.com/documentation/sftpplus/latest/configuration-events/windows-eventlog.html> |
| **Documentation Page** |  | <https://www.sftpplus.com/documentation/sftpplus/latest/index.html> |
| **Important Page for IR** |  | <https://www.sftpplus.com/documentation/sftpplus/latest/guides/event-handlers.html> |





