HP 9250C Digital Sender – Security & Authentication

How do I	Steps to perform
1 Use network authentication	The digital sender's most basic security feature is its ability to require a network login before a user can use the digital sending functions. This prevents unauthorized users from walking up to the device and sending documents. Additionally, the digital sender supports several authentication methods that offer a high level of encryption and security.
2 Secure e-mail	A number of third-party software vendors offer services for secure e-mail delivery. The Secondary email feature is designed to work with one of these third-party software programs for users that require an extra measure of data security.
3 Restrict software access	By default, the digital-sending configuration options in the embedded Web server (EWS) are disabled when the digital sender begins using the HP DSS service. The digital sender can then only be configured by using the HP MFP DSS Configuration Utility. This centralizes configuration tasks and helps control security. You should make sure that the HP DSS is installed on a secure server and that the HP MFP DSS Configuration Utility cannot be used by unauthorized users. In addition, you can also set a password in EWS to prevent access to the device-settings tabs. After the password has been set, users can only see the EWS **Information** tab. The final software program that can be used to control the digital sender is the HP Web Jetadmin program. This program can also be configured to require a password before any changes can be made. It should also be installed on a secure server and should be protected from unauthorized use.
4 Use the security lock	The security lock is a mechanical lock that prevents the removal of internal device components. The lock used is a third-party computer lock such as the ones that are used to secure laptop computers. Purchase the lock separately, and then install it on the device in the location shown.