

Disclaimer:

Every effort has been made to provide accurate information, however the content of this document is subject to change without notice.

HP 9100C Digital Sender

Index to Security:

PLEASE USE THE

SCROLL BARS

to move through the Document

OR

MOUSE CLICK

the shortcut links below:



[Data Security](#)

[Data Security in the HP 9100C
Digital Sender](#)

[Access Security](#)

[Protection from misuse](#)

[Controlling user access](#)

[How users gain access](#)

[Accounting with the
HP 9100C Digital Sender](#)

[‘User profiles’](#)

[HP Digital Sender Link](#)

[More about access security](#)

[Passwords](#)

[Password and network access to
the HP 9100C Digital Sender](#)

[Network File System \(NFS\) services](#)

[Summary](#)

[Back to
MAIN CONTENTS](#)

Security

Business Background White Paper: *Security Questions*

DATA/DOCUMENT SECURITY

High levels of security or confidentiality in data transmission are normally achieved using special algorithms to encrypt data before sending. The recipient of encrypted data - such as a confidential document - must then have the equipment containing the matching algorithms to 'decrypt' the document and return it to a readable format.

Note: ***The HP 9100C Digital Sender does NOT offer any kind of encryption currently.***

Data Security in HP 9100C Digital Sender

In the HP 9100C Digital Sender, documents are delivered in 'Clear' (unencrypted form) regardless of the distribution methods used, such as e-mail, fax, send to PC, etc. Using Clear data for sending avoids creating barriers between the sender and the receiver. Digitised documents sent by the Digital Sender, can be read and re-used easily.

However, data of a highly sensitive or confidential nature is not totally secure - especially when Internet e-mail is used for distribution. The e-mail attachments sent via the HP 9100C Digital Sender are no more and no less secure than any other e-mail messaging method using a common e-mail client such as MS Exchange, Lotus Notes cc:Mail or others. Most day-to-day business data sent via the Internet is reasonably secure, but material of a 'very highly sensitive nature' should not be sent over the Internet.

ACCESS SECURITY

Access Security relating to the HP Digital Sender, centres on how the administrator for the device can control access. The Digital Sender offers various access security switches which can be turned - ON or OFF - individually or in combination - by the administrator. This switchable 'access security' protection available

in the HP Digital Sender enables both, accurate accounting and administration and/or protection from misuse. The sections which follow, explain why and how.

Protection from misuse

The HP Digital Sender is a shared network device used for document distribution and will usually be installed in a common area along with other shared devices such as network printers, copiers and fax machines. By default, this kind of device has potential for misuse - in the same way as any shared fax machine. The Digital Sender sends directly to single or multiple e-mail destinations, printers, computers, and software applications. Anyone with access to the location of the Digital Sender can use its distribution capability to send material - particularly with e-mail - to any destination and in so doing, specify any sender name via 'From e-mail address'.

Controlling user access

The Digital Sender administrator can decide on the best configuration relating to 'access security' during setup, and decide whether the machine should be accessible to everyone or only to a limited set of users. The Security page of JetAdmin allows the Digital Sender administrator to activate or deactivate access security via 'GUEST' functionality. Leaving the 'GUEST' functionality enabled, may increase product versatility, but also leaves the Digital Sender liable to misuse. Disabling 'GUEST', means only known users (up to a maximum of 4096 users) can gain access to the HP 9100C Digital Sender.

How users gain access

With 'GUEST' disabled, users are only able to access the Digital Sender using their own special User Profile containing their name, email address, PC address and a password. When accessing the

CONTENTS

Security - INDEX

Security (continued)

HP 9100C Digital Sender, the User Profile is read by the device and validated against the entry prompted by the unit and keyed in by the user. If the name and password match the programmed criteria, then the Digital Sender provides full access to the user. Passwords protect each 'bona fide' user via a unique identity and also protect the contents of private address books, though currently there is no way to configure the system to force password usage. The use of Passwords is purely optional, but their use is a good idea and should be promoted by Digital Sender administrators.

Accounting with the HP 9100C Digital Sender

Accounting on a network means knowing exactly who is using the HP 9100C Digital Sender and this is only possible when 'GUEST' is disabled. The HP 9100C has an internal journal (log file) providing useful accounting information for the Digital Sender administrator. Using this system, all Digital Sender operations carried out by each user carry the user's 'signature' in the log. Operations are logged, together with the ID (identity) of each user, and information is grouped by user ID.

'User profiles'

The User Profiles are programmed via the HP Address Book Manager application either by the Digital Sender administrator or alternatively by each user who needs a User Profile. The Digital Sender administrator maintains control by configuring the system so that each 'user profile' generated by Digital Sender users must still be validated before it is usable in the HP 9100C's control panel. In addition, the administrator can also interrogate the Digital Sender via the Security Page of JetAdmin and request notification via e-mail when new profiles are created or existing profiles edited. The administrator can disable the user profile creation. All configurations are available from the Security page of JetAdmin.

'HP Digital Sender Link'

The Digital Sender can also be used to send documents directly to a PC on the network. This direct link can be enabled or disabled through the HP Digital Sender Link software installed on

the target personal computer. The PC owner controls the installation of the client Software (HP Digital Sender Link) which enables or disables the receiving of data via this Digital Sender feature.

MORE ABOUT ACCESS SECURITY

The following section provides more in-depth information regarding access security

Passwords

Passwords are secret and not displayed when users key them in at the HP 9100C Digital Sender control panel nor within the software which comes with the Digital Sender: HP JetAdmin and HP Address Book Manager. Each user password together with the other values contained in the user profile are stored in a database on the Digital Sender's internal disk.

The alphanumeric password can contain up to a maximum of 15 characters.

Password and network access to the HP 9100C Digital Sender

The password used by an approved user when identifying himself at the Digital Sender's control panel, is the same password used to connect the device with the HP Address Book Manager (ABM) application. When ABM is used, the password is sent through the network in 'Clear' to the connected HP 9100C Digital Sender unit.

Anyone using network monitors, (special software programs or physical devices which are used to capture everything that goes over the network cable), can detect the password used in the connection. This is the same 'security' level that other TCP-IP protocols such as FTP (File Transfer Protocol) offer. Using a password for the Digital Sender which is different from the rest of the network/working environment is the safest policy.

Network File System (NFS) services

A proprietary transfer protocol is used to move documents from the Digital Sender to the user's PC where 'Send to PC' is enabled and the HP Digital Sender Link application is installed. This protocol includes NFS (Network File System)

[CONTENTS](#)

[Security - INDEX](#)

Security (continued)

commands which might allow an external remote client to browse the disk of a computer which has HP Digital Sender Link installed. To combat this, NFS services are disabled by default and enabled only for the time they are needed. A special keyword stored in the Windows Registry controls NFS and is set to OFF when the HP Digital Sender Link program is installed.

SUMMARY

- In environments where accounting is required and access and usage control are key requirements, the best way to configure the HP 9100C Digital Sender is to disable 'GUEST' via JetAdmin. By doing this, the Digital Sender administrator has to rely on the information stored in the user profiles.
- For added access security, the administrator can disable the user profile creation or can set up the system so that each user profile must be validated before being used for the very first time. Validation must then be repeated if and when user profiles are edited at a later date.
- If usage restrictions are not needed in a shared usage environment, then enabling GUEST offers additional flexibility to potential users of the HP 9100C Digital Sender.