

WHITE PAPER

Addressing Security Issues

The eCopy™ solution for document imaging

Contents

Product overview.....	1
User authentication.....	2
Document security	2
Activity logging	2
Device security	3
Personalization at the device	3
Handling complex environments	4
Summary.....	4

eCopy™ document imaging solutions integrate paper documents with your existing business applications — e-mail, fax, document management systems, and workflow management applications — and provide key features that make eCopy products the most secure document integration solutions available today.

eCopy solutions link office devices to mission-critical business applications. Whenever shared office scanners and copiers connect to your network, security is a prime concern. Additionally, since paper-based documents frequently contain information that is confidential or sensitive in nature, the privacy of scanned documents must be assured. At the same time, if organizations are to realize the huge cost savings that electronic document imaging makes possible, employees must readily adopt the technology-based process. It must be simple and easy to use—very easy to use. Our solutions work with standard digital copiers and office scanners, and provide a simple touch-screen interface that makes scanning as easy as copying.

eCopy has a proven track record spanning more than twelve years in electronic document imaging. eCopy has worked with numerous Fortune 500 companies, government agencies, and other organizations around the world to develop solutions that meet their most stringent security requirements.

Since every organization has a different set of security concerns, eCopy provides a flexible range of configuration options to suit your specific requirements.

eCopy solutions provide security in four key areas:

- User authentication
- Document security
- Activity logging
- Device security

Product overview

eCopy solutions use existing office devices to convert paper documents into digital files. eCopy ShareScan™ is software that is available for networked copiers in two forms.

eCopy ShareScan Embedded, the internal offering, runs inside copiers, enabling eCopy ShareScan to be accessed from the copier's touch screen.

eCopy ScanStation™, the external solution, attaches to the copier or scanner and includes an integrated, free-standing touch screen, keyboard, and PC.

Both solutions support color and black and white scanning. Destination options are shown as easy-to-read icons and may include Scan and Mail, Scan and Fax, Scan to Desktop, and Scan to Printer.

- **Scan and Mail** delivers scanned documents using your existing e-mail system. eCopy ShareScan includes complete native integration with Microsoft Exchange/Outlook or Lotus Notes, giving users access to existing server-based address lists and the ability to send documents from their personal mail account directly from the scanning device. ShareScan also supports SMTP mail servers, with LDAP address book integration available.
- **Scan and Fax** delivers documents by fax using your existing network fax application or print driver. eCopy ShareScan can work with any fax server that uses a Microsoft Exchange or Lotus Notes gateway, and offers native integration with Captaris RightFax. Internet fax services also are supported, so you can send and receive faxes by e-mail, without requiring any fax hardware.

- **Scan to Desktop** delivers scanned documents to your personal scan inbox. From there you can retrieve them using the eCopy Desktop™ client software, and manage, modify and share Adobe Portable Document Format (PDF) documents the same way you handle paper-based information.
- **Scan to Printer** sends scanned documents to a remote printer anywhere on your local or wide area network.

Bundled with the base product, eCopy Quick Connect™ can easily automate a single workflow by integrating scanned documents into existing business processes using versatile file naming, indexing, and custom “scan to” buttons, with no programming required. Additional Connectors provide integration capabilities that enable paper documents to be scanned and distributed to leading document management systems, including Microsoft SharePoint, and to e-mail, fax, cost recovery, and other business applications directly from the copier or scanner.

User authentication

A copier or scanner is typically a shared device in a public area. Authentication is essential to ensure that only authorized users can access your network, to verify the identity of the person sending the document, and to provide an audit trail of what was sent and by whom.

eCopy solutions use your existing network security infrastructure (Windows Active Directory, Novell NDS, Lotus Notes, etc.), and password-based authentication. Since security requirements vary from business to business, eCopy provides a range of authentication options, enabling you to implement a solution that suits your needs.

Authentication also provides productivity benefits, since Connectors can display dynamic content obtained from the target business application through impersonation based on the user’s logon credentials. For example, Connectors can limit the information displayed on a form according to the user’s profile, or present lists of user-specific options in ways that minimize typing. Since the data is generated programmatically at runtime, administrators do not need to maintain templates, update lists, or perform other routine maintenance, as is often required by other scanning products.

Session Logon

Session Logon provides a single sign-on interface that is shared by all eCopy Connectors. Anyone wishing to scan must first log on using their Windows or Novell logon credentials. Once authenticated, the eCopy software maintains a security token that remains valid for the duration of the session, and the person can use any Connector that supports Session Logon without having to log on again. A timeout period ensures that a user who fails to log off does not remain logged on.

You can implement security at the Connector level. For example, you might decide that authentication is required for “scan and mail” but not for “scan to desktop.” In this case, the logon screen is presented after selecting “scan and mail,” and the logon remains in effect only while using that Connector.

Authentication for Scan and Mail

eCopy’s e-mail solutions provide the same safeguards and audit trail you get when sending documents from your desktop. They also ensure that no anonymous or untraceable e-mail can be sent from the copier or scanner

When using Microsoft Exchange/Outlook or Lotus Notes, users select their name from the global address list and enter their password. The eCopy software authenticates the user and embeds the sender’s name and

e-mail address in the “From” field. A copy of the message is stored in the user’s Sent Items folder (Exchange) or delivered to the user’s inbox (Notes).

You can also send mail through any SMTP mail server. ShareScan validates the sender’s identity against a Windows, Novell, or LDAP server using standard password authentication. It then locks the authenticated user’s return e-mail address in the “From” field, preventing anonymous or fraudulent e-mails. Occasionally this is not possible (for example, if the user’s login name and e-mail name don’t match), in which case the user’s name is embedded in the message body, ensuring that all mail can be traced back to the sender.

Authentication for Scan and Fax

eCopy supports many different “scan and fax” implementations. Basic implementations provide functionality similar to that of a standalone fax machine (i.e., local address book support, but no sender authentication). More advanced implementations using Microsoft Exchange, Lotus Notes, or Captaris RightFax offer sender authentication and a “copy to sender” option for audit trails (ShareScan also supports sender authentication with SMTP fax gateways).

Authentication for Scan to Desktop

Scan to Desktop allows for easy delivery of scanned documents to the user’s personal scan inbox. Authentication using existing network passwords is available to prevent users from delivering scanned documents to another user’s inbox.

Authentication for eCopy Quick Connect

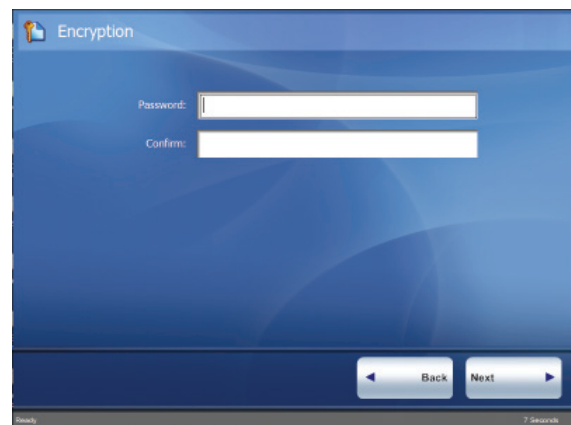
Since eCopy Quick Connect enables fast, one-touch scanning, password authentication is not typically used. However, if you want to restrict access to certain destinations, you can secure those folders and enable authentication.

Document security

eCopy products are in use at government agencies, banks, hospitals, military sites, and other locations where maintaining the security of confidential documents is critical. eCopy solutions include document encryption, secure deletion of temporary files, and scan inbox security to ensure your scanned documents are only visible to those with proper authorization.

Document encryption

To ensure the confidentiality of scanned pages, ShareScan provides optional 128-bit document encryption to provide security when sending documents over a public network. When enabled, the user is prompted to enter a password that is used to create the encryption key.



Password authentication security summary

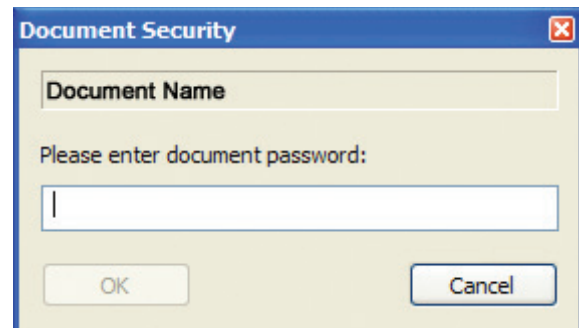
Security feature	Major benefits	IT impact	End-user impact
Session Logon	Eliminates the need to log on multiple times if sending documents using various Connectors	None	User logs on once and can then access all Connectors that support Session Logon
Send from personal Exchange/Outlook mail account	All email can be traced back to an individual Users receive a copy in Sent Items folder Non-delivery receipt is sent to the user if an e-mail address cannot be found	None	User selects name from Exchange global address list and enters network password
Send from personal Notes mail account	All e-mail can be traced back to an individual User receives a copy in Notes inbox	Requires configuration of a pass-through database on a Domino HTTP server	User selects name from Notes global address list and enters Notes password
Mail via SMTP	All email can be traced back to an individual Sender receives a copy	None if SMTP and LDAP servers are already configured	User selects name from LDAP address list and enters network password
Scan to Desktop authentication	Prevents the ability to save to a disk that cannot be traced back to an individual	None	User must enter network password
eCopy Quick Connect authentication	Prevents unauthorized users from scanning to eCopy Quick Connect destinations	None	When enabled, user must enter password to access the destination

The sender must communicate the password to the recipient over a secure channel. The recipient then enters a password to open the file.

Note: Encryption is only as strong as the password used to create the encryption key. eCopy recommends using passwords of sufficient length that meet standard secure password guidelines.

Secure deletion of temporary files

ShareScan includes an option to securely remove temporary files at the end of each scanning operation. When enabled, files are purged by overwriting the disk locations multiple times with random characters.



Inbox security

Scan to Desktop delivers scanned documents to the user’s personal scan inbox. The user retrieves the file using eCopy Desktop or any application that can read files of the selected storage type. NTFS or Novell permissions are applied automatically to prevent users from accessing other user’s documents. The inboxes can be folders created specifically for temporary storage of scanned documents, or subdirectories of existing Windows or Novell home directories.

Note: Inbox security is not available in workgroup implementations.

Using eCopy inboxes

eCopy inboxes are created through a short sign-up process that each user completes at the scanning device. The inboxes can be located on the ShareScan Services Manager’s hard drive or on a network server. When the inbox folder is created, the eCopy software assigns the following permissions.

Group	Permission
Administrators	Full control
ShareScanAdmin	Full control
<owner>	Read/delete

The ShareScanAdmin group enables the eCopy software to write scanned image files to user inboxes. You must create this group on the domain or NDS server. In the eCopy administration console, you specify an account in this group for use when storing scanned documents.

Using Windows or Novell home directories

You can configure the eCopy software to use network home directories for temporary storage of scanned documents. Each user completes a short sign-up process at the scanning device, which registers the user’s name and creates the scan inbox subdirectory. During the scanning process, the user is prompted to log on to the network. This enables ShareScan to connect to the selected scan inbox as that user and save the scanned document.

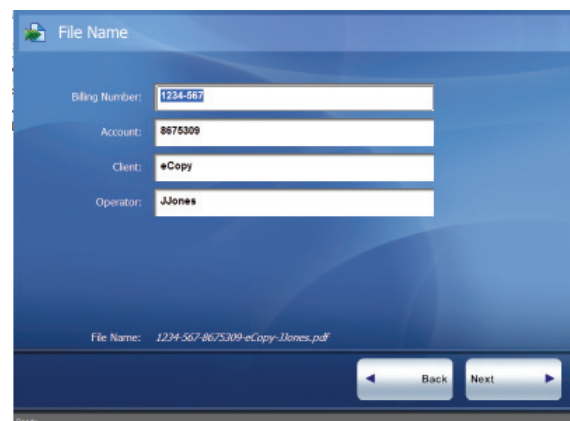
Activity logging

Activity logging enables you to monitor usage of the scanning device and capture tracking information about each scanned document. When tracking is enabled, the user is prompted to enter one or more customizable fields, like account number, department, or patient ID, before the file is sent. Additionally, eCopy solutions support optional integration with cost recovery systems, including those from industry leaders Equitrac, Copitrak, Sepialine, nQueue, and Billback Systems.

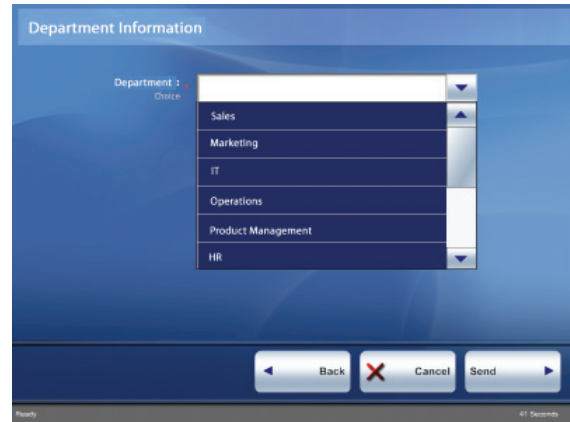
The eCopy administrator can define tracking fields that are included with each entry in the eCopy activity log file. Users are prompted to enter this information each time they select a scanning function.

Since the log is in a standard comma-delimited format, you can import the file into a spreadsheet or report generator for billing or security tracking purposes.

Fields can be defined as “required” or “optional.” In addition, the administrator can determine whether previously-keyed values are available for selection from a dropdown list to speed up data entry.



Tracking of this kind, when used in conjunction with the appropriate administrative procedures, is important in any environment where sensitive information is stored in paper form and its distribution must be monitored.



Device security

The eCopy ScanStation includes a customized PC running Microsoft Windows XP or Windows 2000. This makes it easy to configure and administer using the Windows-based administration program and the tools you already use for device configuration, software updates, and network management. Since the ScanStation is a public device, it includes various security features to prevent unauthorized use.

The following eCopy ScanStation features limit the activities that can be performed at the copier or scanner:

- Restricted network access
- Application lockdown
- Automatic logon and application startup
- Physical security
- No removable drives

These features prevent its use for unauthorized purposes or for activities that cannot be traced back to an individual user.

Restricted network access

The ScanStation PC is logged on to your network during normal operation using a dedicated login account. This account requires only limited access to the network, restricting the ability of anyone gaining access to the device to browse the network resources or perform activities that cannot be traced back to an individual user. The access rights required depend on the scanning functions you choose to implement.

You can selectively disable individual scanning functions. When you disable a function, its button is removed from the eCopy interface and it cannot be used.

eCopy supports the security features of the Windows and Novell network operating systems. This means that the ScanStation PC provides the same level of network security as any desktop system on your network:

- Password authentication can be required for access to any network resources
- Passwords are encrypted before transmission over the network and whenever stored
- Authentication is done by the domain controller or Novell Directory Services

Scanning function	Network access requirements
Scan and Mail	An account on the mail server (used to access the global address list)
Scan to Desktop	None
Scan and Fax	An account on the network fax server or mail server (for "Fax via Mail")
Scan to Printer	Access to the designated printer
eCopy Quick Connect	May require write access to Quick Connect destinations, depending on configuration
Scan to SharePoint	None

Application lockdown

eCopy ShareScan software runs full-screen, blocking access to the taskbar, start menu, and desktop icons. The application includes a password lock that prevents unauthorized users from exiting eCopy ShareScan and using other applications.

Automatic logon and application startup

You can configure the eCopy PC to log on to the network automatically using the restricted eCopy login account. This limits the possibility of someone gaining unauthorized access to the PC following a reboot. The PC is configured to launch the eCopy software automatically at startup.

eCopy’s comprehensive range of security features provides the flexibility that companies need to prevent unauthorized document access, restrict and limit access to certain functions, and track activity by user and document. In addition, stringent document and device security standards enable companies to extend their electronic security protection to paper documents.

eCopy ScanStation security summary

Security feature	Major benefits	IT impact	End-user impact
Restricted network access	Prevents anonymous access to network resources	Requires a dedicated eCopy ShareScan login account per site	None
Auto-logon and application startup	Prevents unauthorized use of the device for other purposes	Requires installation and configuration of an auto-login utility like Microsoft Tweak UI	No user intervention required following a reboot
Application lockdown	Prevents unauthorized use of the device for other purposes	Password required to exit eCopy ShareScan	None
Physical security	Prevents tampering with the device	Physical lock required	None
No removable drives	Prevents introduction of unauthorized software or viruses	Additional software must be installed over the network	None
Secure deletion of temporary files	Securely purges all temporary files created during the scanning process	None (simple configuration option in eCopy ShareScan administration console)	None

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.

ONE WAYSIDE ROAD
BURLINGTON, MA 01803

781 565 5000
NUANCE.COM

