# The eCopy™ Solution

*Product Brief: Addressing Security Issues*

eCopy™

# Contents

# Introduction

eCopy document distribution solutions integrate paper documents with your existing business applications (e-mail, fax, document management systems, workflow management applications, etc.).

Our solutions work with standard digital copiers and office scanners, and provide a simple touch screen interface that makes scanning as easy as copying. This paper outlines the key features that make eCopy products the most secure document integration solutions available today.

eCopy solutions link office devices to mission-critical business applications. Since they use shared office scanners and copiers that 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 distribution makes possible, the scanning process must be simple. eCopy has a proven track record in the electronic document distribution business, spanning more than

twelve years. 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.

eCopy solutions provide security in four key areas:
- Authentication
- Document security
- Activity tracking
- Device security

Since every organization has a different set of security concerns, eCopy provides a flexible range of configuration options to suit your specific requirements. This product brief presents an overview of the product functionality and addresses each of these key areas in turn.

# Product Overview

eCopy solutions use existing office devices to convert paper documents into digital files. eCopy ShareScan is available as both a product that will run inside your copier, eCopy embedded, or as an external piece of hardware that attaches to your copier, the eCopy ScanStation.

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

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

Both solutions support both color and black & white scanning, destination options are shown as easy-to-read icons and may include: Scan and Mail, Scan and Fax, Scan to Desktop, Scan to Printer, and Scan to document management system or enterprise application.

- 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, so users giving 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 are also 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 here you can retrieve them using the eCopy Desktop™ client software, which provides an intuitive, user-friendly interface that enables users to manage, modify and share Adobe Portable Document Format (PDF) documents the same way they handle paper-based information at their desktops.

- eCopy Quick Connect sends scanned documents to a network folder or FTP site, where they can be retrieved by applications using a release script or other automated file acquisition method. eCopy Quick Connect offers configurable file naming, file batching, indexing, and custom "scan to" buttons on the eCopy touch screen, with no programming required.
- Scan to Printer sends scanned documents to a remote printer anywhere on your local or wide area network.
- Scan to SharePoint sends documents to your Microsoft SharePoint Portal Server using configurable workflows and lets you specify column information (metadata).

Numerous additional "Connector" products are available from eCopy and third parties to support integration with various document management systems and other backend applications. For more information, visit the eCopy Web site (www.ecopy. com).

3

# Authentication

A copier or scanner is typically a shared device in a public area, so
authentication is essential for the following reasons:

- To ensure that only authorized users can access your network
- To verify the identity of the person sending the document
- To provide an audit trail of what was sent and by whom

eCopy solutions use password based authentication using your existing network security infrastructure (Windows, Active Directory, Novell NDS, Lotus Notes, etc.), thus eliminating the need for additional passwords. Since security requirements vary from site to site, 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 the user does not remain logged on after walking away without logging off.

Alternatively, 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[1], users select their name from the global address book 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.

## Password Authentication Security Summary

| Security feature | Major benefit | 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 e-mail can be traced back to an individual <br> • User receives a copy in Sent Items folder <br> • Non-delivery receipt is sent to the user if an e-mail address cannot be found | None | User selects name from the Exchange global address book and enters network password |
| Send from personal Notes mail account | • All e-mail can be traced back to an individual <br> • User receives a copy in Notes inbox | Requires configuration of a pass-through database on a Domino HTTP server | User selects name from the Notes global address book and enters Notes password |
| Mail via SMTP | • All e-mail can be traced back to an individual <br> • 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 |

1 When sending mail from a personal account using Lotus Notes, you must configure a pass-through database on a Domino HTTP server.

Login credentials are sent to the Domino server via an HTTP or secure HTTPS/SSL connection.

# 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.



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.

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.
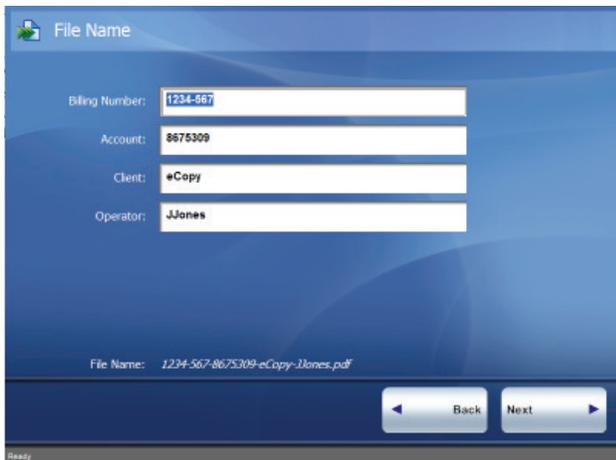




Since the log is in a standard comma delimited format, you can import the file into a spreadsheet or report generator for billing or security tracking purposes.
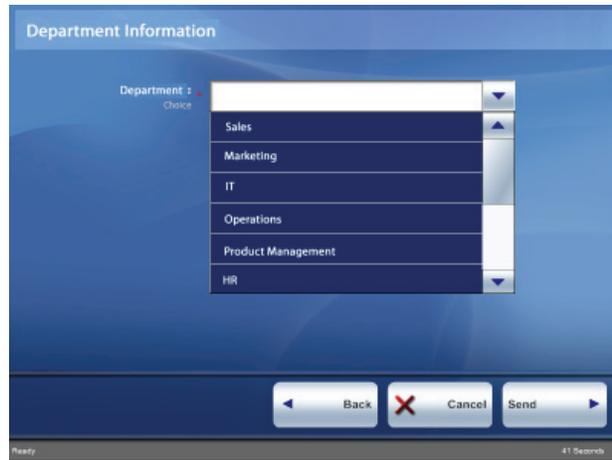
Tracking of this kind, when used in conjunction with the appropriate administrative procedures, is important in any environment where sensitive information is stored in paper form and its distribution must be monitored.

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

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

These ensure that it cannot be used for unauthorized purposes or for activities that cannot be traced back to an individual user.

### Restricted Network Access

The PC is logged on to your network using a dedicated login account during normal operation. This account requires only limited access to the network, restricting the ability of anyone gaining access to the device to browse 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:

| 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 |

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

Note: The eCopy ShareScan embedded solution does not require a dedicated PC at each copier, so the security features listed in this section do not apply.

**Application lock-down**

eCopy ShareScan 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.
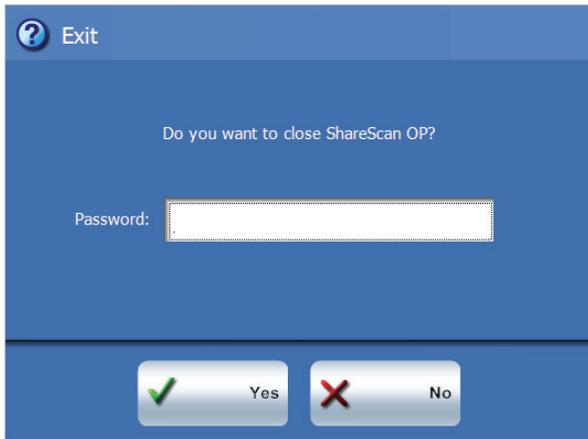


**Automatic logon and application startup**

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.

**Physical security**

The eCopy ScanStation includes a lockable cover for the PC that prevents anyone from physically accessing the device.

**No removable drives**

eCopy ScanStations have no floppy drive. Additionally, you can disable the PC's USB ports to prevent unauthorized use of USB devices. This limits the possibility of someone introducing unauthorized software or viruses onto your network via this device. The eCopy ScanStation ships with the required operating system software, application software, device drivers, and administration tools. You can perform user administration and software updates remotely over the network.

### Device Security Summary (eCopy ScanStations only)

| Security feature | Major benefit | 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 lock-down | 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 |

# Summary

## eCopy provides a comprehensive range of security-related options enabling companies to maintain their security standards.

eCopy software provides security in the following four areas:

• Authentication
• Document security
• Activity tracking
• Device security

By selectively implementing the security features you need, you can configure your eCopy ShareScan software for easy walk-up access, while adhering to the security requirements of your environment.

For more information on document distribution and integration, please contact sales@ecopy.com, or visit the eCopy Web site at www.ecopy.com.

eCopy™