

# Document Security

Information is your company's greatest asset. Xerox can help you keep it safe.



**Document security means peace of mind.** One of the hallmarks of the Xerox multifunction product line is a commitment to information security. Our systems, software and services comprehend and conform to recognized industry standards and the latest governmental security regulations.

## Certified secure

Common Criteria Certification provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality, and availability for systems and data, accountability at the individual level, and assurance that all goals are met.

## Common Criteria certified devices

- ColorQube® 9201/9202/9203\*
- ColorQube 9301/9302/9303\*
- WorkCentre® 4250/4260
- WorkCentre 5135/5150
- WorkCentre 5225/5230
- WorkCentre 5325/5330/5335\*
- WorkCentre 5735/5745/5755
- WorkCentre 5765/5775/5790
- WorkCentre 7120/7125\*
- WorkCentre 7525/7530/7535/7545/7556\*
- WorkCentre 7775\*
- Xerox 4112/4127 Copier/Printer
- Xerox Color 550/560 Printer
- Xerox Color 700

\* Certification pending

## Key Security Goals

### Confidentiality

No unauthorized disclosure of data during processing, transmission, or storage.

### Integrity

No unauthorized alteration of data.

### Availability

No denial of service for authorized users.

### Accountability

Actions of an entity can be traced directly to that entity.

### Non-Repudiation

An entity cannot deny having sent or received a message.

# Xerox Multifunction Printers Security

## Protect your business-critical information

### Security features available on Xerox devices

#### Network Authentication with per-user authorization for individual services.

Customized access to individual services such as Scan to Email can be set up to require user authentication at the device. Authentication can require a device-based password or be seamlessly integrated into an IT environment via MS Active Directory.

**Xerox Extensible Interface®.** Interfaces with the authentication features of EIP solutions to ensure access security.

**Xerox Standard Accounting.** Manages access to and utilization of copy/print/fax/scan by user or group.

**Systems Administrator Authentication with Device Access Password Protection.** Ensures administrative set-up screens and remote network settings cannot be viewed or altered without a user name and password.

**Audit Log.** Captures job activity and enables this activity to be exported via a log through HTTPS.

**Certificate-based security using HTTPS (SSL).** Provides a secure link to the Web User Interface (CentreWare® Internet Services).

**SNMP V3.** Provides encrypted network management communications with the device. Supported by CentreWare Web and other popular management tools.

**802.1X.** Ensures devices connected to the network are properly authenticated.

**Image Overwrite.** Performs a three-pass overlay of a predefined pattern of 1s and 0s which overwrites images on the hard disk. This overwrite can be performed after every job, on demand or scheduled for a specific time.

**IP Filter.** Allows a system administrator to restrict access by IP address or a range of IP addresses.

**IPv6.** Devices include built-in support for networks utilizing the IPv6 standard.

**IPsec.** IPv6 support includes full enablement of the new IPsec standard, one of the strongest and most versatile security standards in existence today.

**Secure Watermark.** The Secure Watermark feature places a predefined watermark on copy and print jobs, preventing unauthorized duplication of sensitive documents.

**Password Protected PDF.** When creating a PDF from a scanned document, a user can create a unique password that will be required to open the file.

**Encrypted PDF.** PDFs are encrypted using 128-bit AES or RC4 encryption standards.

**Encrypted Email.** Email sent from the WorkCentre® device to the mail server is encrypted using digital keys and S/MIME.

**Encrypted Printing.** Print jobs are sent using Secure Socket Layer (SSL) or TLS communication.

**Encrypted Hard Disk.** Data stored on the hard disk carries 128-bit encryption.

**Secure Print.** Allows a print job with a unique PIN to be sent to the WorkCentre device, where the job prints once the user enters the PIN at the device's front panel interface.

**Fax and Network Isolation.** Separating the fax board from the network controller eliminates the security risk of hacking into an office network via the fax line.

**Smart Card technology.** Some devices support the Smart Card technology used by the U.S. Department of Defense for its Common Access Card (CAC)\* system, which protects against unauthorized access. Users can be authenticated using a two-factor identification system — including both card-based identification and a personal identification number entered at the device user interface — to gain access to the walkup features at the device and the network.

### Secure Access

Xerox Secure Access integrates with a customer's existing employee/student ID badge solution. A flexible and convenient authentication system, Secure Access enables users to log into a WorkCentre device with a swipe of their magnetic or proximity ID card. This gives users quick, easy and secure access to device functions that need to be tracked for accounting or regulatory requirements.

#### Gain flexibility with Follow-You Print™.

With Secure Access in place, users can securely release print jobs at any device in their printer environment by swiping their ID card. Users have the option of submitting print jobs to a secure print queue, then printing them at their device of choice. This system minimizes document output costs and hard-copy waste, since users print only what they want and collect everything they print.

**Save user time.** Secure Access saves steps by giving the multifunction system the ability to pre-populate certain data fields, based on the user's credentials presented at sign-in. For example, the device will auto-fill the "to" and "from" fields when using Scan to Email.

**Save IT time.** Secure Access is easily administered using a task-based management console and seamlessly integrates with the customer's existing network card-identification infrastructure.

Call today. For more information, call 1-800-ASK-XEROX or visit us at [www.xerox.com/office](http://www.xerox.com/office)

