

XEROX®

Technology | Document Management | Consulting Services

security features



Document Security

Xerox WorkCentre®

5632/5638/5645/5655/5665/5675/5687*

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 system line is a commitment to information security. Our systems, software and services comprehend and conform to recognised industry standards and the latest governmental security regulations.

Certified secure

The WorkCentre 5632/5638/5645/5655/5665/5675/5687 products have been submitted for Common Criteria Certification. Common Criteria Certification sets specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level and validation that all goals are met. Certification includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to evaluate products against functional security requirements based on predefined Evaluations Assurance Levels (EALs).

Xerox has established a strong track record of certification. Information concerning the certification of the WorkCentre 5600 series will be available soon.



Key Security Goals



Confidentiality

No unauthorised disclosure of data during processing, transmission or storage



Integrity

No unauthorised alteration of data



Availability

No denial of service for authorised 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

Security Features

- **Network Authentication with per-user authorisation for individual services.** Customised 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 utilisation 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)** 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** Image Overwrite function 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** IP filter technology allows a system administrator to restrict access by IP address or a range of IP addresses.
- **IPv6** Devices include built-in support for networks utilising the IPv6 standard.
- **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.

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. Secure Access will also pre-populate certain fields such as the "From" field in Scan to Email. Also Secure Print jobs can be retrieved at any Secure Access-enabled device on the network.

Added Benefits

- **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 minimises 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.

