WorkCentre 4250/4260 Information Assurance Disclosure Paper V1.3

May 20, 2013

Revision History:
V1.1 (April 2010 – First Update)
V1.2 (March 2011 – Minor Updates)
V1.3 (May 2013 – Security updates for 4250)

Xerox Corporation
800 Phillips RoadWebster, NY 14580

Table of Contents:

Section 1. Introduction

The WorkCentre 4250/4260 is among the latest versions of Xerox copier and multifunction devices for the general office. From a security point of view this model provides similar capability to the monochrome WorkCentre 4150.

Important Note: This document applies to the post-launch release of the WorkCentre 4260 Device firmware internal name SMP1 for , which resolved some firmware issues.

1.1 Purpose

The purpose of this document is to disclose information for the WorkCentre 4250/4260 product with respect to device security. *Device Security,* for this paper, is defined as how image data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the WorkCentre products do not establish security for any network environment.

This document applies to the 'S', 'X' and 'XF' configurations of the product:

Model	4250-4260/S	4250-4260/X	4250-4260/XF
Standard functions	Copy, Network Print, Network Scan and E-mail	Copy, Network Print, Network Scan, E-mail and Fax	Copy, Network Print, Network Scan, Email, Fax, Extra paper Tray, High Cap Feeder
Optional functions	Network Accounting / Network Fax Server	Network Accounting / Network Fax Server	Network Accounting / Network Fax Server
Finisher	Optional	Optional	Standard
Hard Drive	Standard 80 or 160GB	Standard 80 or 160GB	Standard 80 or 160GB
Memory	256MB Standard / 256 Optional = 512MB	256MB Standard / 256 Optional = 512MB	256MB Standard / 256 Optional = 512MB

The purpose of this document is to inform Xerox customers of the design, functions, and features of the WorkCentre product relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or WorkCentre product features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics. However, a number of references are included in the Appendix.

1.2 Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

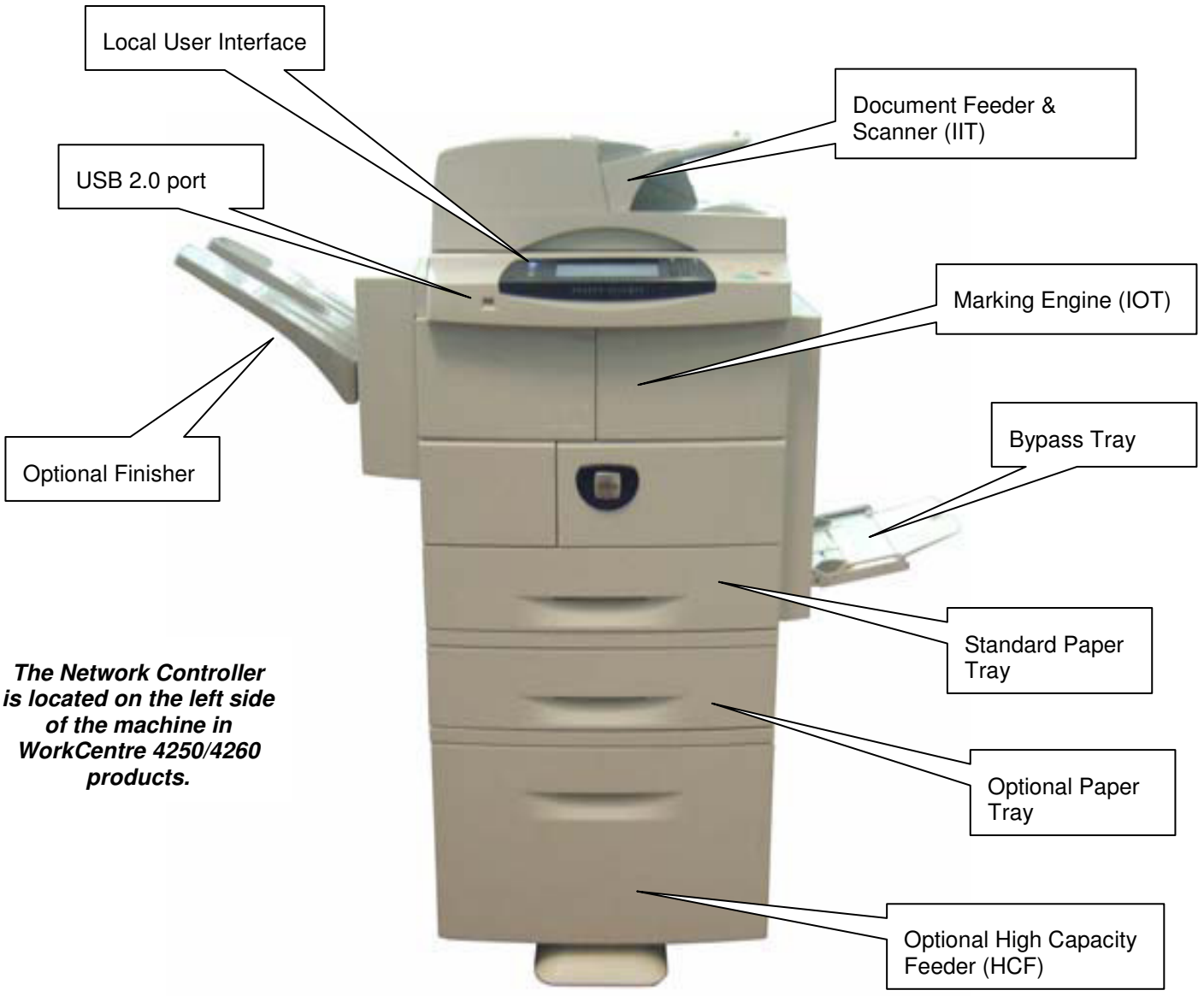
1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

Section 2. Device Description

WorkCentre 4250/4260 has two controllers: a Main Controller module that provides conventional Copy/FAX functions and features, and an embedded Network Controller module that provides the capability to connect the device to a LAN, enabling Network Print and Scan functionality.

Figure 1 WorkCentre 4250/4260 XF

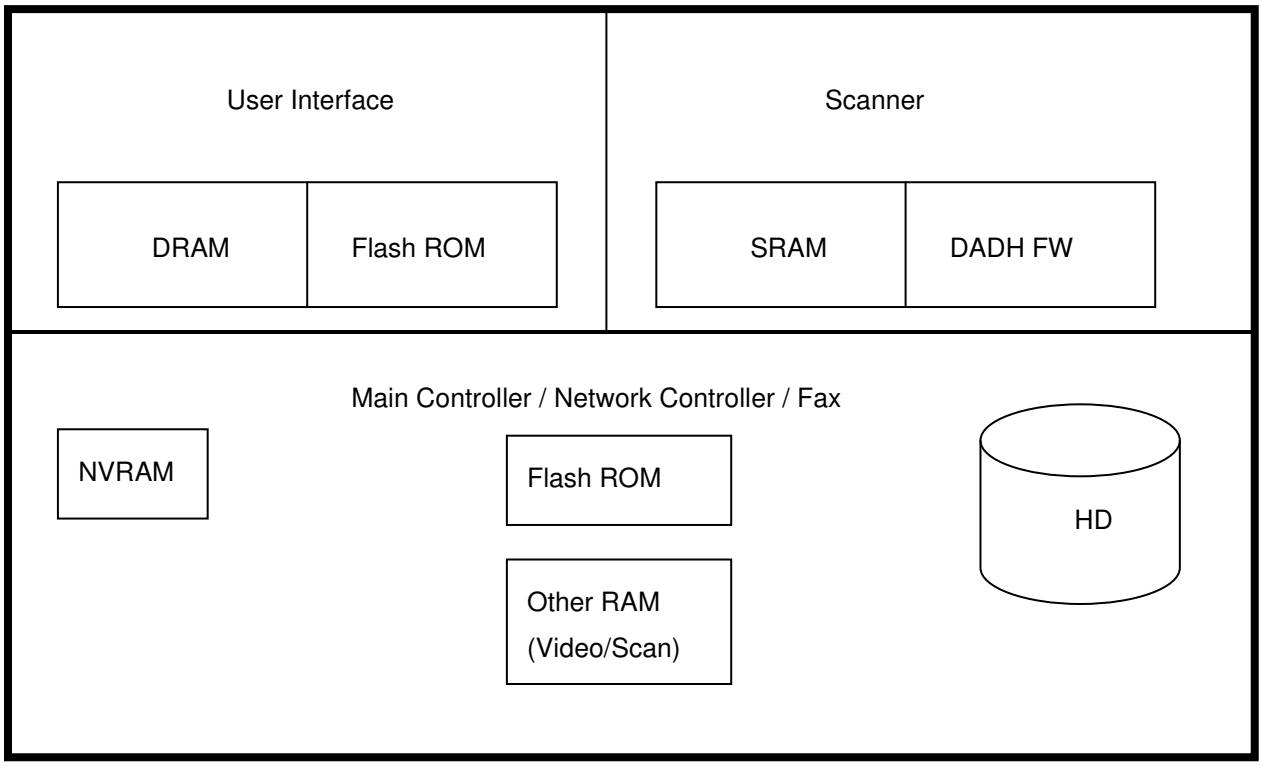


The Network Controller is located on the left side of the machine in WorkCentre 4250/4260 products.

2.1 Memory Devices

This section will detail the memory devices that are contained within the WorkCentre 4250/4260 product configurations. The system is partitioned as shown in Figure 2

Figure 2 System Partitioning



2.1.1 User Interface

No user image data is accessible at the user Interface, with the exception of the job queue, which displays the job name and its status. This is not image data. The displayed queue names are in different forms, depending on the job type:

Job Type	Displayed Job Name	Comment
Copy	Copy Job XXX	XXX is a sequential job number
Print	<Application><document name>	<Application> is sometimes shown (e.g. Microsoft Word), depending on the driver used. <document name> is the file name from the workstation.
Scan	Scan Job XXX	
Fax	Fax Job XXX	
Internal Reports	Report Job XXX	

The User Interface has 2 types of memory:

Name	Size –	Purpose / Explanation
Volatile DDRAM	128MB	User Interface: DDR SDRAM Used for display buffers of the user interface. No user image data is stored in this volatile memory. Specifically, cryptographic secrets are not entered via the GUI. This memory is initialized to a known state on every power up.
Non-volatile	32MB	User Interface: NOR Flash Contains the executable code, language dependent strings and icons that are displayed. Up to 20 languages are stored in flash memory.

2.1.2 Scanner and Duplex Automatic Document Feeder (DADH)

The scanner is controlled from the Main processor board.

2.1.3 Main Controller

Among other common copier functions, the Main Controller enables electronic pre-collation, sometimes referred to as scan-once/print-many. When producing multiple copies of a document, the scanned image is processed and buffered in a proprietary format. The buffered bitmaps are then read from memory and sent to the Image Output Terminal (IOT) for marking on hardcopy output. For long documents, the production of hardcopy may begin before the entire original is scanned, achieving a level of concurrency between the scan and mark operations.

Name	Size –	Purpose / Explanation
Flash ROM	32MB	System Memory (for booting up): NOR Flash 32MB (2x16MB). All operating system and application executable control code resides here (e.g. boot loader, scanner, paper path, FAX, xerographic, finisher). No user image data is stored in this memory. Code can be upgraded by downloading a valid upgrade file through the Web UI or Type A USB 2.0 port. Ability to upgrade firmware can be controlled by the SA.
NVRAM	32KB + 1MB	Backup Memory: 32 KB EEPROM + NOR FLASH 1MB without battery back-up. This non-volatile memory has no image data stored in it. It contains: Device set points for xerographic image quality, paper path timing, and other process control.

Name	Size –	Purpose / Explanation
Hard disk	80 or 160GB (Total HDD Size separated into 4 partitions)	The HD is used to spool PDL jobs as well as Network Scan jobs prior to export and the only image data stored is the images for Sample, secure, delayed print. The HDD is also used to store intermediate files used by the PDL interpreters. Once the job is completed, the DRAM pointers are deleted. The image files are deleted when they are no longer needed, which is accomplished by removing the pointer from the File Allocation Table which is stored on the HDD. If Immediate Image Overwrite is enabled, the sectors containing job image data are overwritten using a 3-pass overwrite algorithm: PATTERN: the size of each pattern shall be one byte. The system shall support any characters from the ISO 8859 –1 (UTF-8) character set to be contained within a pattern. ALGORITHM: The algorithm for immediate image overwrite shall be as follows: The size of the pattern shall be one byte selected from the ISO 8859-1 character set. The patterns are written as follows: Step 1: The binary value of Pattern #1, shall be written to the disk area that is used for the job. Step 2: The complement of Pattern #1, shall be written to the disk area that is used for the job. Step 3: The binary value of Pattern #2, which shall be different from pattern #1, shall be written to the disk area that is used for the job. If On-Demand Image Overwrite is selected the device overwrites specific partitions of the HDD depending on the ODIO selected; Standard Overwrite or Full Overwrite. See Section 6 for specifics on which data is overwritten for Standard and Full Overwrite features. The overwrite process is as follows: The size of the pattern shall be one byte selected from the ISO 8859-1 character set. The patterns are written as follows: Step 1: The binary value of Pattern #1 shall be written to the entire area that is available for spooling and the CPSR feature. Step 2: The complement of Pattern #1 shall be calculated and written to the entire area that is available for spooling and the CPSR feature. Step 3: The binary value of Pattern #2, which shall be different from pattern #1, shall be written to the entire area that is available for spooling and the CPSR feature. Both IIO and ODIO are standard features on the WorkCentre 4250/4260. Spooled documents in PDL format from the network, as well as Network Scan jobs prior to export. All fax related items are stored on the HDD. All fax jobs are treated as if they were a spooled job, noted above. All resident fonts. (Please note that a Font Management Utility is available to permanently download fonts to the hard disk.) All scan to file templates that are locally stored are located on the HDD.

There are also a number of RAM buffers in the video path that are used for image manipulation (Reduce/Enlarge, etc.), and all have no data retention capability. When power is removed all data is lost. These buffers are typically built into the ASICs.

2.1.4 Fax Card

The analog FAX service uses the analog fax card to send and receive images over the telephone interface.

Name	Size –	Purpose / Explanation
HDD	Up to 160GB	Fax user document image data are stored in this non-volatile memory. Destination phone numbers are also stored here. Received fax jobs can be stored in user mailboxes. Fax send jobs may be held for delayed send.
MODEM #1	NA	Silicon Laboratories SI2435 Fax modem

The software that implements the FAX features is resident on the Main controller PWBA.

The FAX PWBA will only support data interchange to the device via FAX protocols. Any attempt to establish voice or data connections to the device is terminated.

2.1.5 Other RAM Devices

There are other memory devices in the machine, but these are used solely for low level I/O control. Some examples of this distributed control are:

- Video Memory
- Scan Memory

Name	Size –	Purpose / Explanation
Volatile DDRAM	32MB	Video Volatile Memory: SDRAM
	64MB	Scan Volatile Memory: SDRAM (2x 32MB)

2.1.6 Network Controller Memory

The Network Controller is equipped with ARM 926EJS microprocessor core. The Network Controller enables network connectivity supporting printing, network scanning, network fax, Web UI, and email services. Network fax is an optional feature.

The details of the memory devices in the Network Controller are:

Name	Size	Purpose / Explanation
Processor	NA	ARM 926EJS microprocessor core
DRAM	256MB	Network Controller: Not dedicated, uses common DIMM memory (DDR SDRAM 256MB) It is used for temporary storage of data files and images. This information is not backed up and is lost when the power is removed.

2.2 Operating Systems

The Main Controller contains a processor card with a proprietary (pSOS) real-time operating system. This controller does not have networking capability except via the Network Interface Controller (NIC).

The controller runs pSOS a Real Time Operating System. Unnecessary services such as rsh, telnet and finger are disabled in the OS. FTP is used in client-only mode by the optional Network Scanning feature for the filing of scanned images and the retrieval of Scan Templates (see section 5.3), however the NC does not contain an FTP server.

The IP networking layer uses packet-filtering technology to check incoming packets. Network and scan settings that include server IDs and passwords are secured with a System Administrator password. These features secure the image data on the device from improper retrieval through the LAN port.

Note that a user never accesses the pSOS operating system. All logons to WorkCentre 4250/4260 products are to application software, never to the OS. Hence the OS is inaccessible to the user.

Section 3. System Access

3.1 Physical Access

There are a variety of methods to physically access the system. To compromise the system, a person must be local to the device. Remote (logical) access is discussed in the next section. Please see Appendix D for pictures of the connectors.

This table is a summary of the methods of physically accessing the device:

Interface	Description / Usage
User Interface	Submit copy, fax & scan jobs; machine configuration; Job & Machine status
User Interface connection	Proprietary connection between the UI and Main Controller
10/100 MB Ethernet RJ-45 Network Connector (Network Controller)	Network Printing, Network scanning, Network fax, Web UI, and Email services.
USB 2.0 Target	Direct USB printing
SIM slot	Optional Accessory enablement
FAX line 1 RJ-11	Supports FAX Modem T.30 protocol only
Phone Line RJ-45	Supports Telephone extension
Foreign Device Interface	Allows connection of optional access control hardware
Scanner	Proprietary connection between the Scan Module and the Main Controller
USB 2.0 Host	Print, Scan, FW upgrade, Backup To / Restore From

3.1.1 User Interface

The User Interface is a touch screen mounted in the center of the device. Through the UI a user:

- obtains access to Copy, Scan, System, Network and Fax setups
- can control access rights to device setup (via Admin Login)
- can access job log-data (file name, time completed, etc.)

The User Interface does not allow access to images or access to the network.

The password to enter Tools is stored in the Main Controller NVM in packed BCD format.

The User Interface connects to the Main Controller via a USB interface using a proprietary protocol.

3.1.2 10/100 MB Ethernet RJ-45 Network Connector

This is the standard network connector, and allows access to the connectivity stacks and open ports described in the next section. This connector conforms to IEEE Ethernet 802.3 standards.

3.1.3 Main Controller USB Service Port

A type B USB connector exists on the left side of the WorkCentre 4250/4260. This USB port is designed for Direct-connect printing.

A type A USB connector exists on the front of the device to the left of the LUI. Two more type A USB connectors exist on the left side of the WorkCentre 4250/4260. These USB ports are designed for connecting external memory devices such as a flash thumb-drive. The USB ports allow for Firmware Upgrade, Backup To/From, printing and scanning.

3.1.4 SIM slot

The SIM slot is used to enable optional accessories such as Network Scanning. Follow the directions that come with the accessory kits to install these options.

3.1.5 Fax Lines

A one line fax kit is available. The fax connection supports the Fax Modem T.30 protocol only and will not accept data or voice communication attempts. An external (EXT) is available to connect an external in handset in this instance the FAX card acts as a pass through relay.

3.1.6 (Optional) Foreign Device Interface

This port is used to connect optional equipment to control access to the machine. A typical application is a coin-operated device where a user must deposit money to enable the machine to copy and/or print. Through the LUI the SA can restrict access to Scan and FAX transmission

The information available via the Foreign Device Interface is limited to optically-isolated pulses that can be used to count impressions marked on hardcopy sheets. This 15 pin D shell connector is on an optional board, and is only present if the Accessories PWBA is installed.

3.1.7 Scanner

This port is used to transmit image data between the scanner and Main Controller. The over-the-wire protocol is Xerox proprietary. This port cannot process any other protocol.

No user image data is stored on the scanner.

3.2 Logical Access

3.2.1 Network Protocols

The supported network protocols are listed in Appendix D and are implemented to industry standard specifications (i.e. they are compliant to the appropriate RFC) and are well-behaved protocols. There are no 'Xerox unique' additions to these protocols.

3.2.1.1 IPsec

The device supports IPSec tunnel mode. The print channel can be secured by establishing an IPSec association between a client and the device. A shared secret is used to encrypt the traffic flowing through this tunnel. SSL must be enabled in order to set up the shared secret.

When an IPSec tunnel is established between a client and the machine, the tunnel will also be active for administration with SNMPv2 tools (HP Open View, etc.), providing security for SNMP SETs and GETS with an otherwise insecure protocol. SNMP Traps may not be secure if either the client or the device has just been rebooted. IP Filtering can be useful to prevent SNMP calls from non-IPSec clients.

Once an IPSec channel is established between two points, it stays open until one end reboots or goes into power saver. Only network clients and servers will have the ability to establish an IPSec tunnel with the machine. Thus device-initiated operations (like scanning) cannot assume the existence of the tunnel unless a print job (or other client initiated action) has been previously run since the last boot at either end of the connection.

3.2.2 Ports

The following table summarizes all potential open ports and subsequent sections discuss each port in more detail.

Default Port #	Type	Service name
25	TCP	SMTP
53	UDP	DNS
68	UDP	BOOTP/DHCP
80	TCP	HTTP
88	UDP/TCP	Kerberos
137	UDP	NETBIOS- Name Service
138	UDP	NETBIOS-Datagram Service; SMB filing and Scan template retrieval
139	TCP	NETBIOS; SMB filing and Scan template retrieval
161	UDP	SNMP
162	UDP	SNMP trap
389	UDP	LDAP
396	TCP	Netware
427	UDP	SLP
443	TCP	SSL
515	TCP	LPR
631	TCP	IPP
636	TCP	sLDAP
1900	UDP	SSDP
3003	TCP	http/SNMP reply
9100	TCP	raw IP

Please note that there is no ftp port in this list. ftp is only used to export scanned images and to retrieve Scan Job Templates, and will open port 21 on the remote device. An ftp port is never open on the Network Controller itself.

3.2.2.1 Port 25, SMTP

This unidirectional port is open only when Scan to E-mail or is exporting images to an SMTP server. SMTP messages & images are transmitted to the SMTP server from the device.

3.2.2.2 Port 53, DNS

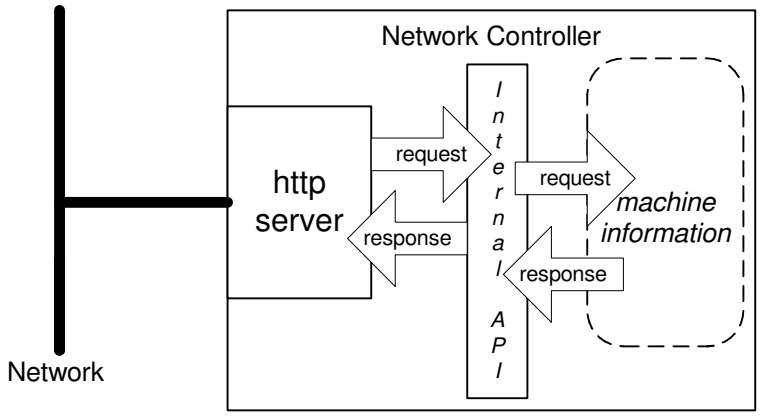
Designating a DNS server will allow the device to resolve domain names. This can be configured via the Web UI.

3.2.2.3 Port 68, DHCP

This port is used only when performing DHCP, and is not open all of the time. To permanently close this port, DHCP must be explicitly disabled. This is done in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the Web UI.

3.2.2.4 Port 80, HTTP

The embedded web pages communicate to the machine through a set of unique APIs and do not have direct access to machine information:



The HTTP port can only access the HTTP server residing in the Network Controller. The embedded HTTP server is proprietary. The purpose of the HTTP server is to:

- Give users information of the status of the device;
- View the job queue within the device and delete jobs;
- Allow users to download print ready files as well as PDF & TIFF files for direct printing. Scan to File Job Templates can also be programmed….
- Allow remote administration of the device. Many settings that are on the Local UI are replicated in the device's web pages. Users may view the properties of the device but not change them without logging into the machine with administrator privileges.

The HTTP server can only host the web pages resident on the hard disk of the device. It does not and cannot act as a proxy server to get outside of the network the device resides on. Hence the server cannot access any networks (or web servers) outside of the customer firewall.

When the device is configured with an IP address, it is as secure as any device inside the firewall. The web pages are accessible only to authorized users of the network inside the firewall.

This service (and port) may be disabled in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the Web UI. Please note that when this is disabled, IPP Port 631 is also disabled.

HTTP may be secured by enabling Secure Sockets Layer (see Sec. 0.0.0.3.2.2.12).

3.2.2.5 Proxy Server

The device can be configured to communicate through a proxy server. Features that can make use of a proxy server include the Automatic Meter Read feature, scanning to a remote repository, or retrieving scan templates from a remote template pool.

3.2.2.6 *Port 88, Kerberos*

This port is only open when the device is communicating with the Kerberos server to authenticate a user, and is only used only to authenticate users in conjunction with the E-mail or Network Scanning feature. To disable this port, authentication must be disabled, and this is accomplished via the Local User Interface.

This version of software has Kerberos 5.1.3.5 – with DES (Data Encryption Standard) and 64-bit encryption. The Kerberos code is limited to user authentication, and is used to authenticate a user with a given Kerberos server as a valid user on the network. Please note that the Kerberos server (a 3rd party device) needs to be set up for each user. Once the user is authenticated, the Kerberos software has completed its task. This code will not and cannot be used to encrypt or decrypt documents or other information.

This feature is based on the Kerberos program from the Massachusetts Institute of Technology (MIT). The Kerberos network authentication protocol is publicly available on the Internet as freeware at http://web.mit.edu/kerberos/www/. Xerox has determined that there are no export restrictions on this version of the software. However, there are a few deviations our version of Kerberos takes from the standard Kerberos implementation from MIT. These deviations are:

1) The device does not keep a user's initial authentication and key after the user has been authenticated. In a standard Kerberos implementation, once a user is authenticated, the device holds onto the authentication for a programmed timeout (the usual default is 12 hours) or until the user removes it (prior to the timeout period). In the Xerox implementation, all traces of authentication of the user are removed once they have been authenticated to the device. The user can send any number of jobs until the user logs off the system, either manually or through system timeout.
2) The device ignores clock skew errors. In a standard implementation of Kerberos, authentication tests will fail if a device clock is 5 minutes (or more) different from the Kerberos server. The reason for this is that given enough time, someone could reverse engineer the authentication and gain access to the network. With the 5-minute timeout, the person has just 5 minutes to reverse engineer the authentication and the key before it becomes invalid. It was determined during the implementation of Kerberos for our device that it would be too difficult for the user/SA to keep the device clock in sync with the Kerberos server, so the Xerox instantiation of Kerberos has the clock skew check removed. The disadvantage is that this gives malicious users unlimited time to reverse engineer the user's key. However, since this key is only valid to access the Network Scanning features on a device, possession of this key is of little use for nefarious purposes.
3) The device ignores much of the information provided by Kerberos for authenticating. For the most part, the device only pays attention to information that indicates whether authentication has passed. Other information that the server may return (e.g. what services the user is authenticated for) is ignored or disabled in the Xerox implementation. This is not an issue since the only service a user is being authenticated for is access to an e-mail directory. No other network services are accessible from the Local UI.

Xerox has received an opinion from its legal counsel that the device software, including the implementation of a Kerberos encryption protocol in its network authentication feature, is not subject to encryption restrictions based on Export Administration Regulations of the United States Bureau of Export Administration (BXA). This means that it can be exported from the United States to most destinations and purchasers without the need for previous approval from or notification to BXA. At the time of the opinion, restricted destinations and entities included terrorist-supporting states (Cuba, Iran, Libya, North Korea, Sudan and Syria), their nationals, and other sanctioned entities such as persons listed on the Denied Parties List. Xerox provides this information for the convenience of its customers and not as legal advice. Customers are encouraged to consult with legal counsel to assure their own compliance with applicable export laws.

3.2.2.7 *Ports 137, 138, 139, NETBIOS*

These ports support the submission of scan files as well as support Network Authentication through SMB. Port 137 is the standard NetBIOS Name Service port, which is used primarily for WINS. Port 138 supports the CIFS browsing protocol. Port 139 is the standard NetBIOS Session port. Ports 138 and 139 may be configured in either (1) User Tools via the Local User Interface, or (2) in the Properties tab of the device's web pages, but Port 137 can only be configured via the web.

For Network Scanning features, ports 138 and 139 are used for both outbound (i.e. exporting scanned images and associated data) and inbound functionality (i.e. retrieving Scan Templates). In both instances, these ports are only open when the files are being stored to the server or templates are being retrieved from the Template Pool. For these features, SMB protocol is used.

3.2.2.8 *Ports 161, 162, SNMP*

These ports support the SNMPv1, SNMPv2c, and SNMPv3 protocols. Please note that SNMP v1 does not have any password or community string control. SNMPv2 relies on a community string to keep unwanted people from changing

values or browsing parts of the MIB. This community string is transmitted on the network in clear text so anyone sniffing the network can see the password.

NOTE: Xerox strongly recommends that the customer change the community string upon product installation.

SNMP is configurable, and may be explicitly enabled or disabled in the Properties tab of the device's web pages.

The device supports SNMPv3, which is an encrypted version of the SNMP protocol that uses a shared secret. Secure Sockets Layer must be enabled before configuring the shared secret needed for SNMPv3.

3.2.2.9 Port 389, LDAP

This is the standard LDAP port used for address book queries in the Scan to Email feature.

3.2.2.10 Port 396, Netware

This configurable port is used when Novell Netware is enabled to run over IP.

3.2.2.11 Port 427, SLP

When activated, this port is used for service discovery and advertisement. The device will advertise itself as a printer and also listen for SLP queries using this port. It is not configurable. This port is explicitly enabled / disabled in the Properties tab of the device's web pages.

3.2.2.12 Port 443, SSL

This is the default port for Secure Sockets Layer communication. This port can be configured via the device's web pages. SSL must be enabled before setting up SNMPv3, sLDAP, or before retrieving the audit log (see Sec. Section 4). SSL must also be enabled in order to use any of the Web Services (Scan Template Management, Automatic Meter Reads, or Network Scanning Validation Service).

SSL should be enabled so that the device can be securely administered from the web UI. If the optional scanning feature has been purchased, SSL can be used to secure the filing channel to a remote repository.

SSL uses X.509 certificates to establish trust between two ends of a communication channel. When storing scanned images to a remote repository using an https: connection, the device must verify the certificate provided by the remote repository. A Trusted Certificate Authority certificate should be uploaded to the device in this case.

To securely administer the device, the user's browser must be able to verify the certificate supplied by the device. A certificate signed by a well-known Certificate Authority (CA) can be downloaded to the device, or the device can generate a self-signed certificate. In the first instance, the device creates a Certificate Signing Request (CSR) that can be downloaded and forwarded to the well-known CA for signing. The signed device certificate is then uploaded to the device. Alternatively, the device will generate a self-signed certificate. In this case, the generic Xerox root CA certificate must be downloaded from the device and installed in the certificate store of the user's browser.

The device supports only server authentication.

3.2.2.13 Port 500 ISAKMP

This port is used for IKE in order to establish an IPsec SA (Security Association), and is open all of the time for IKE communication. When the product communicates to an external device as a client, the port number of the product and that of the external device are both 500. A key operator can disable IPsec via local UI or from CentreWare Internet Services.

3.2.2.14 Port 515, LPR

This is the standard LPR printing port, which only supports IP printing. It is a configurable port, and may be explicitly enabled or disabled in User Tools via the Local User Interface or in the Properties tab of the device's web pages.

3.2.2.15 Port 631, IPP

This port supports the Internet Printing Protocol. It is not configurable. This is disabled when the http server is disabled (see 3.2.2.4).

3.2.2.16 Port 636, sLDAP

This is the LDAP port for secure LDAP. All traffic on this port will be encrypted using secure SSL.

3.2.2.17 Port 1900, SSDP

This port behaves similarly to the SLP port. When activated, this port is used for service discovery and advertisement. The device will advertise itself as a printer and also listen for SSDP queries using this port. It is not configurable. This port is explicitly enabled / disabled in the Properties tab of the device's web pages.

3.2.2.18 Port 3003, http/SNMP reply

This port is used when the http server requests device information. The user displays the Web User Interface (Web UI) and goes to a page where the http server must query the device for settings (e.g. Novell network settings). The http server queries the machine via an internal SNMP request (hence this port can only open when the http server is active). The machine replies back to the http server via this port. It sends the reply to the loopback address (127.0.0.0), which is internally routed to the http server. This reply is never transmitted on the network. Only SNMP replies are accepted by this port, and this port is active when the http server is active (i.e. if the http server is disabled, this port will be closed). If someone attempted to send an SNMP reply to this port via the network, the reply would have to contain the correct sequence number, which is highly unlikely, since the sequence numbers are internal to the machine.

3.2.2.19 Port 9100, raw IP

This allows downloading a PDL file directly to the interpreter. This port has limited bi-directionality (via PJL back channel) and allows printing only. This is a configurable port, and may be disabled in either (1) User Tools via the Local User Interface, or (2) in the Properties tab of the device's web pages.

3.2.3 IP Filtering

The device contains a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address.

3.3 Login and Authentication Methods

There are a number of methods for different types of users to be authenticated. In addition, the connected versions of the product also log into remote servers. A description of these behaviors follows.

3.3.1 User Tools [All product configurations]

Users must authenticate themselves to the device. To access the User Tools via the Local UI, a numerical password is required. The customer can set the password to anywhere from 4 to 12 digits in length. This password is stored in the Main Controller NVM and is inaccessible to the user. Xerox strongly recommends that this password be changed from its default value immediately upon product installation. The same password is used to access the Administration screens in the Web UI.

3.3.2 Service [All product configurations]

Xerox Service Technicians also require authentication via a unique 4-digit password. This PIN is the same for all product configurations and cannot be changed. Please see Sec. 3.4 for details.

3.3.3 Printing

The device may be set up to connect to a print queue maintained on a remote print server. The login name and password are sent to the print server in clear text.

Network Scanning:

Network Scanning may require the device to log into a server. The instances where the device logs into a server are detailed in the following table. Users may also need to authenticate for scanning. This authentication is detailed in subsequent sections.

3.3.3.1 Device log on

Scanning feature	Device behavior
Scan to File, Public Template	The device logs in to the scan repository as set up by the SA in User Tools.
Scan to E-mail	The device logs into an LDAP Server as set up by the SA in User Tools. It will only log into the Server when a user attempts to use the scan-to-email feature. At the time the LDAP server must be accessed, the device will log into the LDAP server. The device can use simple authentication or a secure connection using SSL (where all credentials are encrypted) on the LDAP server. A network username and password must be assigned to the device. The device logs in as a normal user, with read only privileges. User credentials are not used for this authentication step, and are never transmitted over the network.
Scan to Fax Server	The device logs in to the Fax Server as set up by the SA in User Tools on the Local UI or from the Properties tab on the Web UI.

Please note that in all cases when the device logs into any server the device username and password are sent over the network in clear text.

3.3.3.2 Scan Template Management

This is a web service that allows the SA to manage templates stored in a remote template pool. The connection to the remote pool can be secured with SSL (see Sec. 0.0.0.3.2.2.12).

3.3.3.3 Off-box validation

This is a web service that can be used to allow the WorkCentre 4250/4260 to communicate with a remote server/service to validate information that a user has input through the Control Panel. Two optional system features may be configured to use this web service.

1. The Network Scanning feature may use this capability to validate data that has been entered by a user into a Job Template Document Management Field. This would typically be configured as part of a scanning workflow.

2. The Network Accounting feature may use this capability to validate user account data. This communication would take place with an Accounting service on the network.

In both cases, this capability is disabled by default.

3.3.3.4 User authentication

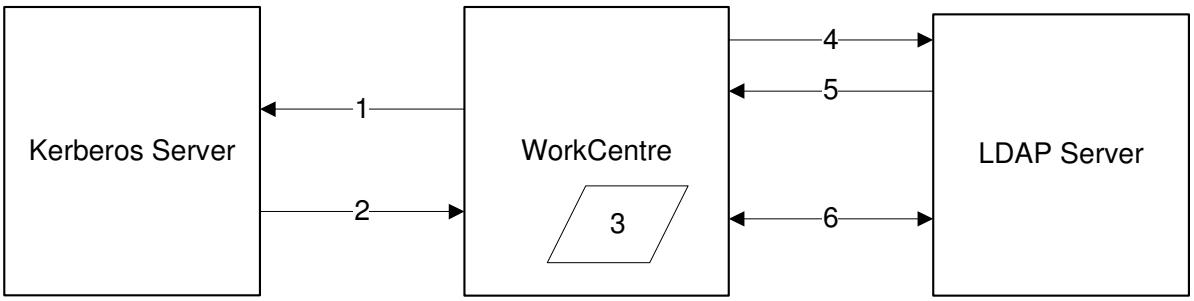
Users may authenticate to the device using Kerberos, SMB Domain, or LDAP authentication protocols. Once the user is authenticated to the device, the user may proceed to use the Network Scanning features listed above.

The Web UI allows an SA to set up a default authentication domain a back-up authentication domain and as many as 6 additional alternate authentication domains. The device will attempt to authenticate the user at each domain server in turn until authentication is successful, or the list is exhausted.

Kerberos Authentication (Unix/Linux or Windows 2000/Windows 2003)

This is an option that must be enabled on the device, and is used in conjunction with all Network Scanning features (Scan to File, Scan to E-mail and Scan to Fax Server). The authentication steps are:

1) A User enters a user name and password at the device in the Local UI. The device sends an authentication request to the Kerberos Server.
2) The Kerberos Server responds with the encrypted credentials of the user attempting to sign on.
3) The device attempts to decrypt the credentials using the entered password. The user is authenticated if the credentials can be decrypted.
4) The device then logs onto and queries the LDAP server trying to match an email address against the user's Login Name, it is recommended that the channel be secured with sLDAP.
5) If the LDAP Query is successful, the user's email address is placed in the From: field. Otherwise, the default From: is used.
6) The user may then add recipient addresses by accessing the Address Book on the LDAP server. Please see the User Manual for details. Each addition is a separate session to the LDAP server.



SMB Authentication (Windows NT 4 or Windows 2000/Windows 2003)

This is also an option that may be enabled on the device, and is used in conjunction with all Network Scanning features (Scan to File, Scan to E-mail and Scan to Fax Server). The authentication steps vary somewhat, depending on the network configuration. Listed below are 3 network configurations and the authentication steps.

Basic Network Configuration: Device and Domain Controller are on the same Subnet

Authentication Steps:

1) The device broadcasts an authentication request that is answered by the Domain Controller.
2) The Domain Controller responds back to the device whether or not the user was successfully authenticated.

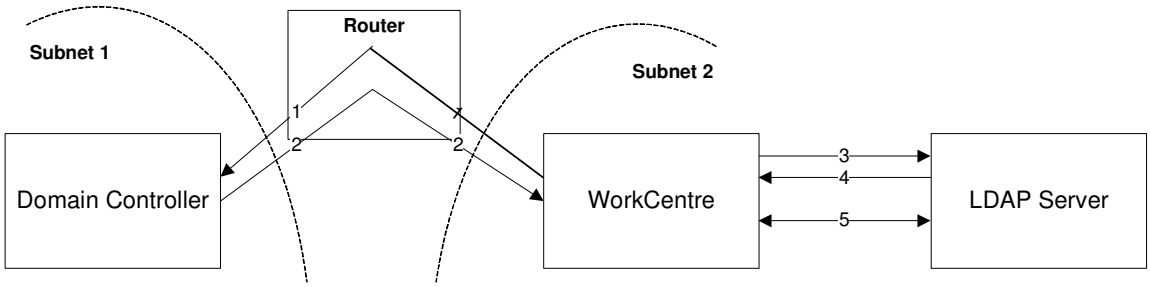
If (2) is successful, steps 3 – 5 proceed as described in steps 4 – 6 of the Kerberos section.

Device and Domain Controller are on different Subnets, SA defines IP Address of Domain Controller

Authentication Steps:

1) The device sends an authentication request directly to the Domain Controller through the router using the IP address of the Domain Controller.
2) The Domain Controller responds back to the device through the router whether or not the user was successfully authenticated.

If (2) is successful, steps 3 – 5 proceed as described in 4 - 6 of Kerberos section.

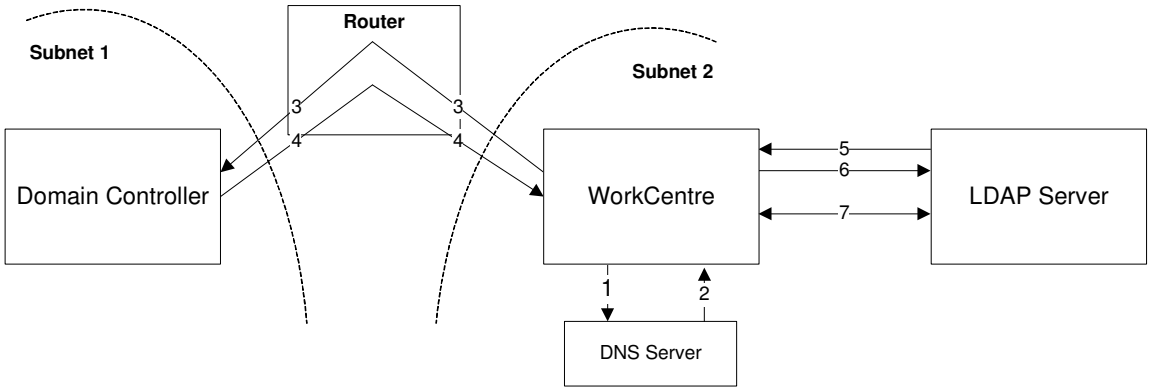


Device and Domain Controller are on different Subnets, SA defines Hostname of Domain Controller

Authentication Steps:

1) The device sends the Domain Controller hostname to the DNS Server.
2) The DNS Server returns the IP Address of the Domain Controller
3) The device sends an authentication request directly to the Domain Controller through the router using the IP address of the Domain Controller.
4) The Domain Controller responds back to the device through the router whether or not the user was successfully authenticated.

If (4) is successful, steps 5 – 7 proceed as described in steps 4 - 6 of the Kerberos section.



3.3.3.4.1DDNS

The implementation in the device does not support any security extensions.

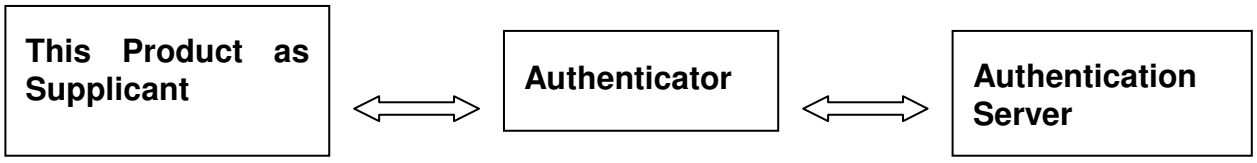
3.3.4 802.1x

The following device authentication method is provided.

Device Authentication Mode	Operation
802.1x	Wired 802.1X authentication is supported. When the product is activated using the User ID and password set for the product, authentication to the switch device starts in order to connect to the LAN port.

3.3.4.1 802.1x Authentication

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch 24 as shown below, the Authentication server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result. The product starts authentication processing at startup when the startup settings for 802.1X authentication is enabled.



Of the authentication methods in 802.1X Authentication, the product supports the following:

802.1X Authentication Method	Operation
MD5	Performs authentication using the ID information in plain text and MD5 hashed password.
MS-CHAPv2	Performs authentication using the ID information in plain text and MD5 hashed password that is encrypted using a key generated from random numbers.
PEAP/MS-CHAPv2	Performs authentication in the SSL-encrypted channel established between the product and the Authentication server using the following information: - ID information in plain text. - Password encrypted in MN-CHAPv2 method.

3.4 Diagnostics

3.4.1 Accessible Data

The only files that are accessible are FAX phonebook entries, no image data is available. The CSE is expected to seek permission from the customer before beginning service on the device.

3.4.2 Summary

In the extremely unlikely event that someone did spoof the Xerox proprietary protocols, only diagnostic activities can be executed.

Section 4. Security Aspects of Selected Features

4.1 Audit Log

The device maintains a security audit log. Recording of security audit log data can be enabled or disabled by the SA. The audit log is implemented as a circular log containing a maximum of 15000 event entries, meaning that once the maximum number of entries is reached, the log will begin overwriting the earliest entry. Only an SA will be authorized to download the log from the device. The log may only be exported over an https: connection, so SSL must be set up before retrieving the log (see Sec. 0.0.0.3.2.2.12). The log is exported in MS-Excel comma-separated file format. The log does not clear when it is disabled, and will persist through power cycles.

The following table lists the events that are recorded in the log:

Event ID	Event description	Entry Data
1	System startup	Device name Device serial number
2	System shutdown	Device name Device serial number
3	ODIO Standard started	Device name Device serial number
4	ODIO Standard complete	Device name Device serial number Overwrite Status
5	Print job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID
6	Network scan job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-net-destination net-destination.
7	Server fax job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers net-destination.
8	IFAX (Not a supported feature on the WC4260)	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-of-smtp-recipients smtp-recipients
9	Email job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-of-smtp-recipients smtp-recipients

10	Audit Log Disabled	Device name Device serial number
11	Audit Log Enabled	Device name Device serial number
12	Copy	Job Name User Name Completion Status Accounting User ID Accounting Account ID
13	Embedded fax	Job Name User Name Completion Status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
14	Lan Fax Job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
15	Data Encryption	Device name Device Serial number
16	Scheduled ODIO Standard started	Device name Device serial number
17	Scheduled ODIO Standard complete	Device name Device serial number
18	Scheduled ODIO Full started	Device name Device serial number
19	Scheduled ODIO Full complete	Device name Device serial number
20	Scan to Mailbox job	Job name or Dir name User Name Completion Status IIO status
21	Delete File/Dir (CPSR)	Job name or Dir name User Name Completion Status IIO status
22	USB	Job name or Dir name User Name Completion Status : completed - normal or completed – error IIO status ‘not-supported’
23	Scan to Home	Job name or Dir name User Name Completion Status IIO status
24	System Configuration Data Changes	Device name Device serial number

4.2 Xerox Standard Accounting

Xerox Standard Accounting (XSA), intended primarily for use as an accounting service, can be used as an internal authorization service. XSA tracks copy, scan (including filing and email), print and fax usage by individual user. The system administrator can enable/disable the feature via the LUI or Web UI, add or delete users, and set usage limits by service for each user. If XSA is enabled, a walk-up user must enter a valid XSA ID before being allowed access to the device. The device will confirm that the entered XSA ID matches an authorized user, and that the usage limits for the selected service have not been exceeded. In this sense, XSA acts as an authorization service. The system administrator can limit access to device services by setting the usage limits on specific services to zero for users that should not have rights to use the feature. After each page or image is completed, the user's balance is updated by the number of impressions or scans performed. Services become unavailable to the user when the usage limits are exceeded.

When XSA is enabled in the print driver or on the Web UI, before a print job is submitted, an XSA ID must also be entered. The ID is sent to the Network controller for validation. If the submitted ID is valid, the job will print, and the user's balance will be updated by the number of impressions performed. If the submitted ID is invalid, the job is deleted and an error sheet is printed in its place.

On demand, the SA will be able to download a report that shows activity for all of the users. The SA can add, modify or remove users and their allocations at any point.

An end user will be able to review their balances by entering a User ID at the LUI or web UI.

4.3 Automatic Meter Reads

Automatic Meter Reads (AMR) is a service that allows devices to electronically report meter readings back to Xerox.

The device can be set to communicate via a proxy server on the customer's network. The proxy server address is set up via SNMP.

The Xerox AMR server will check whether it is time in the monthly billing cycle to update the meter readings. If so, the server will request reads from the device, and the device will then respond by sending the meter reads back to the server via the proxy server.

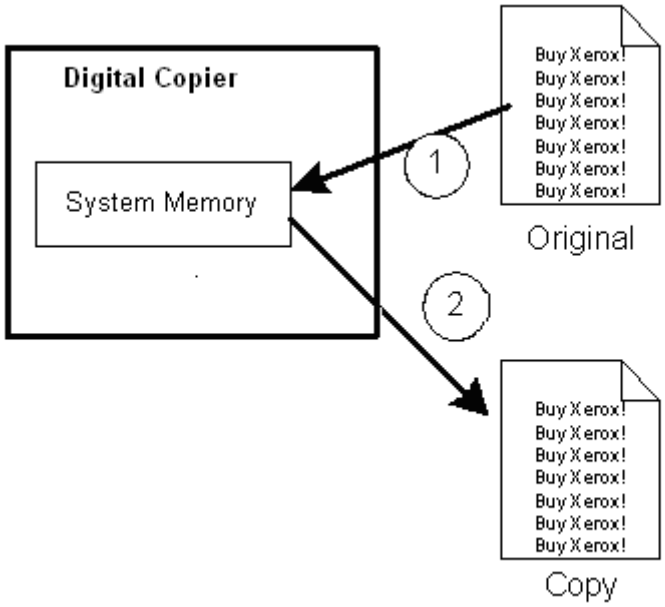
4.4 File Encryption

Any file created as a result of a device action and that uses the hard drive as a temporary storage location is encrypted using the AES algorithm with a 256-bit key. The key is generated dynamically on each boot, and is kept only in volatile memory.
This feature is automatically enabled and cannot be disabled by the SA.
*For the 4250 only – FIPS 140-2 certified, RSO-BSAFE, Cert ID# 1836:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Section 5. Document Flows

The following sections diagram the image flow through the system. Only the memory devices that store image data are shown.

5.1 Copy



Copy jobs are processed exclusively by the Main Controller module.

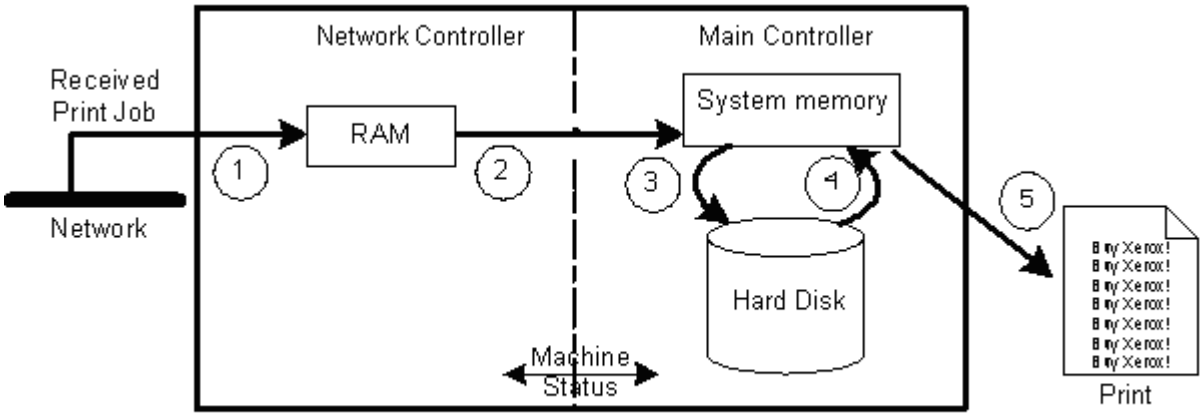
1) The scanner scans the documents and stores them as compressed bitmaps in proprietary format into the system memory.
2) The images are transferred to the video print path to print a hard copy. The video print path does any required image manipulation (n-up, booklet, etc), using system memory as buffer space.
3) Even if enabled, Immediate Image Overwrite does not take place for any copy jobs including all reports.

The Network Controller is informed of the marking engine status as states (e.g. cycling up, scanner idle, paper tray empty, etc.). The Main Controller is informed of the Network Controller status as required (on line, off line, etc.). The Network Controller does not and cannot have any copy image data transferred to it, nor can it access copy image data.

In addition, subsequent jobs will overwrite the current document so there is no long term retention of image data in the system memory. Also, system memory is volatile, and as such, loses all image data on power down.

5.2 Print

Five (5) types of print jobs are supported – Normal, Secure, Delay, Sample Set and Saved. A Normal Print job will be illustrated first and then the differences with Secure, Delay, Sample Set and then Saved will be discussed.



Normal Print

1) The Network Interface Card (NIC) receives a print job from the Network
2) The NIC buffer stores the PDL onto memory and then transfers the data to the Main Controller
3) If the system is processing jobs, the PDL is stored onto the Hard disk. If there are no jobs currently being processed, the Main Controller then decomposes the print job into a bitmap and parses out the job parameters. The bitmap and job parameters are transferred as they are created, and are stored into the system memory.
4) The bitmap image(s) is/are compressed (via the same hardware as in copy) and stored in the system memory, as are the job parameters.
5) The images are transferred to the video print path to print a hard copy. The video print path does any required image manipulation (n-up, etc), using system memory as buffer space.
6) If Immediate Image Overwrite has been enabled, all temporary files associated with the print job that were created on the Hard disk will be overwritten prior to the job being marked as complete.

The Network Controller is informed of machine status as states in the marking engine change.

The client is informed of Job Status as their job progresses through the system.

Secure Print:
Prior to step 1, above, the user must designate the job as a Secure Print Job and enter a 4-10 digit PIN in the print driver. The PIN is encrypted with a 32-80 bit (4-10 character) key, and is added to the header of the PDL.

In step 2, the PIN is extracted from the PDL with the other job parameters.

The job is stored on the hard drive (after Step 2 above), it is held until the user selects the job and enters the PIN at the Local UI, at which point, processing proceeds to Step 3.

Note that the pdl is not encrypted for a Secure Print. 'Secure' applies to the addition of a PIN.

The device can be set to make the process of releasing a sequence of jobs easier. If enabled by the SA, the device will release all jobs sent by a user, assuming the same PIN was used for each job. This eliminates the need to release each job in a sequence individually.

If a user has forgotten to release their Secure Print jobs, a logged-in SA will have the ability to delete Secure Print jobs.

Sample Print
Prior to step 1, above, the user must designate the job as a Sample Set Print Job.

The first set of the job is printed (just like a Normal Print Job) and the job is stored on the hard drive, but the job is placed in a held state in the Controller. The remaining sets are printed when they are explicitly released by the user at the Local UI.

In this case the job state will not be ready for completion processing until the remaining sets are printed. At this point Immediate Image Overwrite will execute as above if it has been enabled.

Delay Print

Prior to step 1, above, the user must designate the time (within the next 24 hours) for the job to print. The pdl file is spooled on the hard disk and held until this time is reached, at which time the print process proceeds according to Steps 4-6 above.

Please note that a Secure or Sample Print will expire and be automatically deleted after a programmable time-out (default is 72 hours, programmable from 1 to 120 hours) if the user has not released them by this time. If Immediate Image Overwrite has been enabled, it will execute at this point.

Saved (Save and Print)

Prior to Step 1 above, the user must designate the job as a Saved (Save and Print) job. A Job Name and Folder must also be inputted. The user also has the option of printing and saving the job to the hard drive or to save it to the hard drive only with no print output.

The job is printed (just like a Normal Print Job) and the job is stored on the hard drive using the file and folder name inputted by the user. The job that is stored on the hard drive can then be accessed at any time by a user and reprinted at will from the device's LUI.

Files and folders created in this manner can be deleted at the LUI by the user or by the SA performing a Full ODIO. Details about ODIO can be found in Section 6.

5.3 Analog Fax (also known as Embedded Fax)

The fax card connects directly to the Copy Controller processor card. It is physically separated from the Network Controller. The fax card does not have its own processor and local memory but uses the Main processor and reserved memory on the HDD. The card contains a fax-only modem that supports the T.30 protocol. If anything other than the T.30 protocol is detected, the modem will disconnect.

5.3.1 Walk-up Fax Send

1) The scanner scans the documents and stores image data in the HDD.
2) The image(s) are transferred from the HDD to the fax card, where they are stored in compressed format.
3) In default mode the fax card will not initiate the call until the entire image has been transferred from system memory. When this is complete, the fax card will place the call and conduct the fax transmission. In manual dial mode the fax card will place the call and start the fax transmission as soon as the first page is scanned. If Immediate Image Overwrite has been enabled, it will execute once the entire fax image has been transmitted.

5.3.2 Walk-up Fax Receive

1) The fax card answers a call and receives the fax. The fax card will receive the entire job into the HDD, storing the data in compressed format.
2) Marking proceeds identically to a copy job. If Immediate Image Overwrite has been enabled, it will execute once the fax has printed out.

5.3.3 Internal Fax Server

The WorkCentre 4250/4260 device does not implement an Internal Fax Server, i.e. fax jobs cannot be sent from the network out through the fax line, or conversely, received faxes cannot be sent out over the network. The Network Fax does not utilize the functions of the fax card.

5.4 Network Scanning

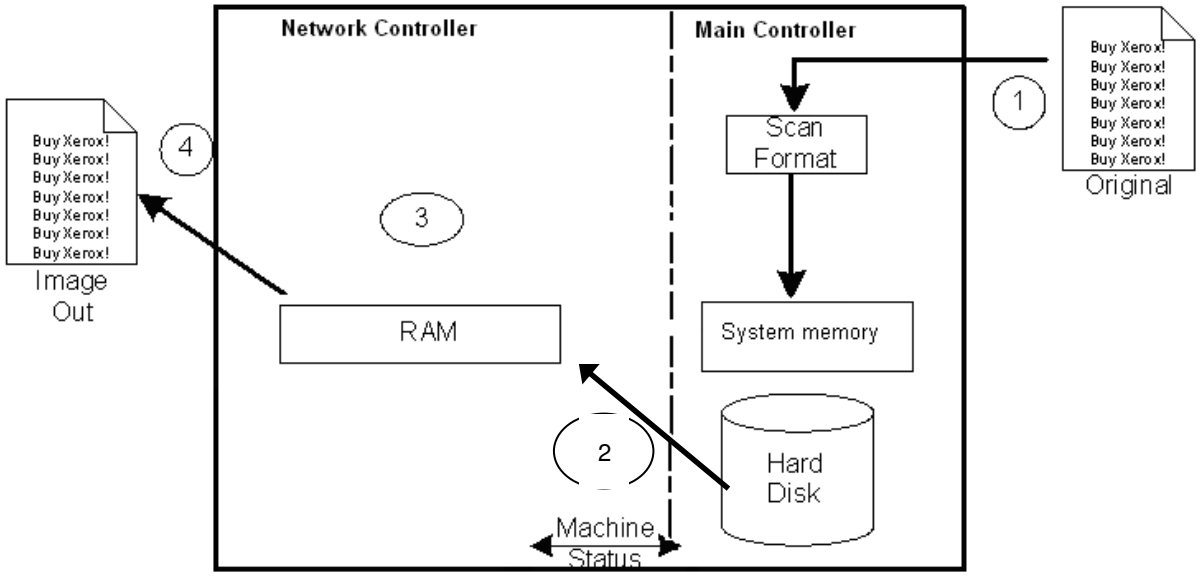
There are three (3) types of Network Scanning:

1. Scan to File – the Scan Job (images and associated data) is stored on a file server.
2. Network Faxing – the Scan Job is sent to a Network Fax Server that faxes the document via telephone lines.

3. Scan to E-Mail – the Scan Job is sent to an SMTP server to be e-mailed to the recipient.

5.4.1 Scan to File

The user selects a Scan template, places the document in the DADH or on the platen and then presses Start.



1) The scanner scans the documents and the images are compressed (via hardware) in a G4 format for black and white scanning and JPEG for color scanning.
2) The images are converted into a JPEG, TIFF or PDF file
3) Scanned images are sent to the Network Controller from system memory.
4) The converted files are then stored to the Network Repository specified by the Scan Template.
5) If Immediate Image Overwrite has been enabled, it will execute when the file has been transferred.

A confirmation sheet is printed (if requested by the user) (not shown).

5.4.1.1 Scan Templates

Scan Templates are created and are used by the device to program the scan job. They contain the scanning parameters (resolution, image type, etc.) and destination parameters (where to export the scanned images). Templates are accessed via 2 methods: remote retrieve or local storage.

5.4.1.2 Remote Retrieve

Templates are created and stored in a central repository (the 'Template Pool') on a file server as simple ASCII files. The SA configures the device to access this Template Pool, and all templates are retrieved as needed (via ftp, HTTP, HTTPS or SMB) for local use. The Template Pool is queried for the list of templates that is displayed on the Local UI. This method allows many devices to share a common set of Scan Templates. Retrieved templates are stored on the hard disk drive.

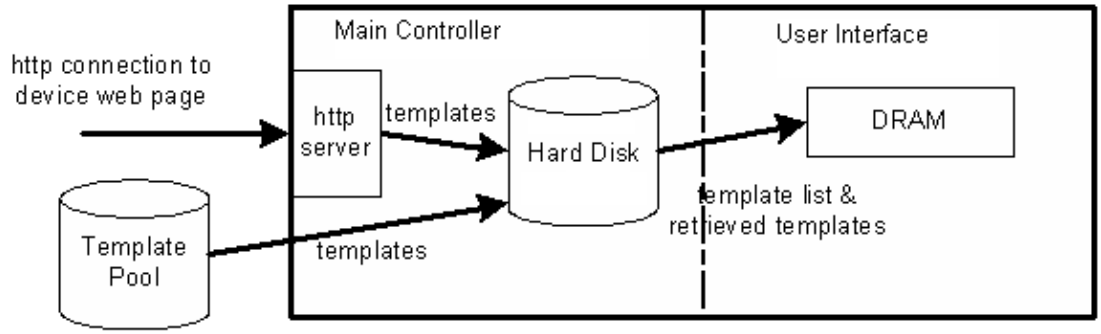
5.4.1.3 Local Storage

Templates may be created directly on a specific device via the resident http server. The local Template Pool is unique to each device. The templates are accessible only via the http server and the local UI for that device. The templates are stored on the hard disk drive.

Although the template currently selected on the Local UI may be edited to change certain parameters, edited templates cannot be exported from the device to the Template Pool.

There is no method of locking a local (i.e. Web UI created) template. Once a local template is on the device, anyone may modify it. Users who have access to the file system would have the same access to the template files.

Local scan templates can also be accessed by utilizing scan template API's. This allows access of the local scan templates without using CWIS.



For more details on template creation and use, see the customer documentation.

5.4.2 Network Faxing

Although the user model for Network Faxing is nearly identical to any other fax machine, the actual fax transmission is accomplished by a third-party server-based fax solution available on the LAN.

The differences to Network Scanning are that only TIFF files will be exported; pdf and jpeg are not supported and a Fax Server must be the destination.

After the Fax Server has completed the fax job, a confirmation sheet is submitted as a print job from the fax server (if requested by the user).

If Immediate Image Overwrite has been enabled, all temporary files associated with the network fax job that were created on the Hard disk will be overwritten prior to the job being marked as complete.

5.4.3 Scan to E-Mail

The difference to Network scanning is that an SMTP Server must be the destination.

As with all other scanning features, if Immediate Image Overwrite has been enabled, all temporary files associated with the scan to e-mail job that were created on the Hard disk will be overwritten prior to the job being marked as complete.

5.4.4 Summary of Network Scanning differences

The table below summarizes the differences of the Network Scanning job types. Copy is also included since it can also be thought of as a 'scan' job.

Job Type	Format stored into HDD	Formats exported by the Network Controller	Exported to this type of server
Copy	compressed bitmaps	n/a	n/a
Network Scan	G3/G4 compressed bitmaps	TIFF, pdf (non-searchable), JPEG	Any file server
Walk Up (Network) Fax (receive only)	G3/G4 compressed bitmaps	TIFF	Fax Server
Scan to E-Mail	G3/G4 compressed bitmaps	TIFF, pdf (non-searchable), JPEG	SMTP server

5.5 Network Fax Receive

Fax Receive, from the device point of view, is identical to a submitted print job.

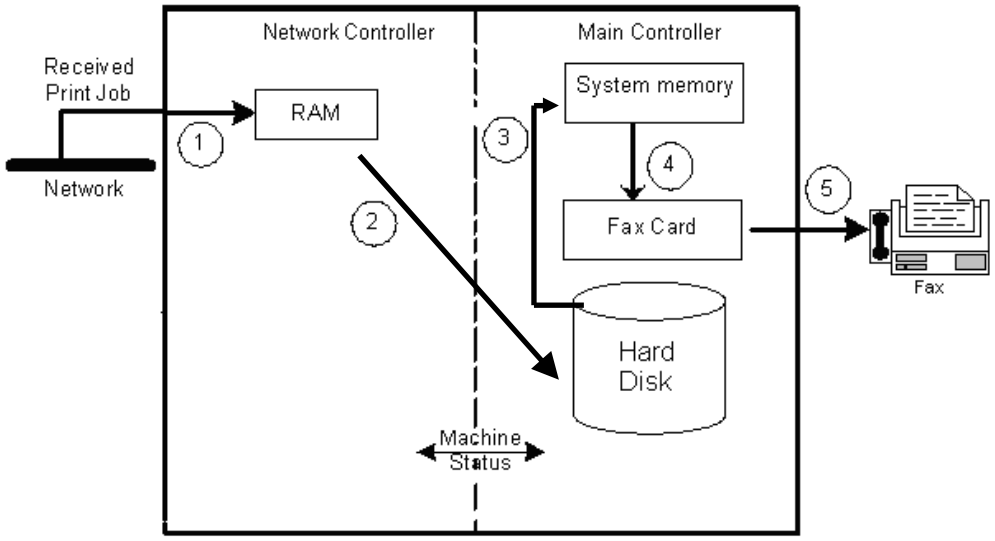
1) The Network Fax Server receives a fax over the telephone line.

2) The Fax Server submits the fax job as a print job to the device.

3-7) The job progresses just like a print job (see steps 2-5 in the print flow diagram). If Immediate Image Overwrite has been enabled, it will execute when the fax has printed completely.

5.6 LanFax

LanFax jobs are similar to print jobs. A user selects LanFax in the driver and enters the destination phone number. The job is sent to the device, where it is processed and then routed to the analog fax card. From there the job is sent as a regular fax over the telephone network.



---

1) The Network Controller receives a print job from the Network and stores the PDL onto its hard disk.
2) If there are no jobs currently being processed, the Network Controller then decomposes the print job into a bitmap and parses out the job parameters. The bitmap and job parameters are transferred as they are created, and are stored into the Network Controller DRAM.
3) The bitmap image(s) is/are compressed (via the same hardware as in copy) and stored in the copier system memory, as are the job parameters.
4) The images are transferred to the NVRAM resident on the analog fax card
5) The analog fax card connects to the destination and sends the fax.

Section 6. Image Overwrite

The Security Image Overwrite provides both Immediate Image Overwrite (IIO) and On-Demand Image Overwrite (ODIO) functions. When IIO is enabled, immediately before a job is considered complete, IIO will overwrite any temporary files associated with print, network scan, embedded fax, network fax, or e-mail jobs that had been created on the Hard disk. The ODIO feature can be executed at any time by the SA. The SA will have the option of performing either a standard ODIO or a Full ODIO at either the LUI or WebUI. Scheduling of a Standard or Full ODIO can be done at the WebUI as well.

Standard ODIO will overwrite all jobs stored in image data as well as fax card image data. Standard ODIO will not overwrite fax mailbox, Poll store (mailbox 0) and dial directory information, or folders created with the Save Job for Reprint feature, if these features are installed on the machine.

Full ODIO will overwrite and delete all fax image data, including mailboxes, Poll store and dial directories on the fax card. Full ODIO will also overwrite any images that have been stored in folders created with the Save Job for Reprint feature.

6.1 Algorithm

The overwrite mechanism for both IIO and ODIO conforms to the U.S. Department of Defense Directive 5200.28-M (Section 7, Part 2, paragraph 7-202, and is common to all WorkCentre and Phaser devices that utilize this feature. The algorithm for the Image Overwrite feature is:

Step 1: Pattern #1 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x35 (ASCII "5")).

Step 2: Pattern #2 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0xCA (ASCII compliment of 5)).

Step 3: Pattern #3 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x97 (ASCII "ú")).

Step 4: 10 % of the overwritten area is sampled to ensure Pattern #3 was properly written. The 10 % sampling is accomplished by sampling a random 10 % of the overwritten area.

6.2 User Behavior

Once enabled, IIO is invoked automatically immediately prior to the completion of a print, network scan, embedded fax, network fax, or e-mail job. If IIO completes successfully, the status is displayed in the Completed Job Queue. However, if IIO fails, a LUI string message will appear on the Local UI indicating the IIO failed and recommends that the user run a Full ODIO. The SR3 message will remain until the Full ODIO is performed. The device can be used normally, however no IIO will take place until the Full ODIO is performed.

ODIO may be invoked from the Local UI in Tools Pathway or by using CWIS. Network functions will be delayed until the overwrite is completed. Copying and all other Local UI functions are unavailable while the overwrite itself is underway.

Once a Standard or Full ODIO has begun, it cannot be cancelled by the SA at anytime either at the LUI or via CWIS.

Upon completion and verification of the ODIO process, a confirmation sheet is printed which indicates the status of the overwrite. The completion status can be successful or failed.

Note that all jobs in the queue are deleted prior to invocation of ODIO.

Scheduled ODIO:

The device also supports automatic invocation of Standard and Full ODIO. Scheduling a Standard or Full ODIO can only be performed via CWIS by the authorized SA. The SA can determine the frequency as well:

Daily: SA selects the hour, minutes and AM/PM variable of that given day.

Weekly: SA selects day of the week, hour, minutes and AM/PM variable.

Monthly: SA selects day of the month, hour, minutes and AM/PM variable.

6.3 Overwrite Timing

Standard ODIO and Full ODIO take approximately 9 and 45 minutes respectively, but longer times are possible depending on the amount of data that must be overwritten.

IIO is performed as a background operation, with no user-perceivable reduction in copy, print or scan performance.

Section 7. Responses to Known Vulnerabilities

7.1 Security @ Xerox (www.xerox.com/security)

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see www.xerox.com/security.

Section 8. APPENDICES

8.1 Appendix A – Abbreviations

ADF	Automatic Document Feeder
API	Application Programming Interface
AMR	Automatic Meter Reads
ASIC	Application-Specific Integrated Circuit. This is a custom integrated circuit that is unique to a specific product.
CCITT	Comite Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consultative Committee) [now ITU-T]
CSE	Customer Service Engineer
CWIS	**CentreWare Internet Services**
DADF/DADH	Duplex Automatic Document Feeder/Handler
DC	Digital Copier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server. A centralized database that maps host names to static IP addresses.
DDNS	Dynamic Domain Name Server. Maps host names to dynamic IP addresses.
DRAM	Dynamic Random Access Memory
EGP	Exterior Gateway Protocol
FIPS	**Federal Information Processing Standard**
GB	Gigabyte
HDD	Hard Disk Drive
HP	Hewlett-Packard
HTTP	Hypertext transfer protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IIO	Immediate Image Overwrite
IIT	Image Input Terminal (the scanner)
IT	Information Technology
IOT	Image Output Terminal (the marking engine)
IP	Internet Protocol
IPX	Internet Protocol Exchange
ITU	International Telecommunications Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP Server	Lightweight Directory Access Protocol Server. Typically the same server that is used for email. It contains information about users such as name, phone number, and email address. It can also include a user's login alias.
LED	Light Emitting Diode
LPR	Line Printer Request
LZ	Lempel Ziv (a type of compression)
MAC	Media Access Control
MIB	Management Information Base
n/a	not applicable
NC	Network Controller
NDPS	Novell Distributed Print Services
NETBEUI	NETBIOS Extended User Interface
NETBIOS	Network Basic Input/Output System
NOS	Network Operating System

NVRAM	Non-Volatile Random Access Memory
NVM	Non-Volatile Memory
ODIO	On-Demand Image Overwrite
PCL	Printer Control Language
PDL	Page Description Language
PIN	Personal Identification Number
PROM	Programmable Read-Only Memory
PWBA	Printed Wire Board Assembly
PSW	Portable Service Workstation
PWS	alternative acronym for Portable Service Workstation
RFC	Required Functional Capability
ROM	Read Only Memory
ROS	Raster Output Scanner
SA	System Administrator
SIMM	Single In-line Memory Module
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
UI	User Interface
URL	Uniform Resource Locator
UDP	User Datagram Protocol
Web UI	Web User Interface – the web pages resident in the WorkCentre. These are accessible through any browser using the machine's IP address as the URL.
XCMI	Xerox Common Management Interface
XSA	Xerox Standard Accounting

8.2 Appendix B – Supported MIB Objects

NOTES :

(1) The number of objects shown per MIB group represents the number of objects defined by the IETF standard for that MIB group. It does not represent the instantiation of the MIB group which may contain many more objects.

(2) Some MIB objects defined within Input and Output groups of the Printer MIB (*RFC 1759*) have a MAX-ACCESS of RW. However, the Printer MIBv2 defines a MIB-ACCESS of RO for these MIB objects within the Input and Output groups and all machines assessed support RO access. Therefore, RO access to these MIB objects is considered IETF compliant.

(3) It is assumed that mandatory IETF string-related MIB objects shall contain meaningful data; not blank strings

(4) The "**(C)**" notation indicates that the previously stated item is a true caveat condition. The "**(I)**" notation indicates that the previous stated item should be regarded as information only.

(5) MIB objects that CANNOT be populated with meaningful data (e.g. a machine may not have paper level sensors, hence, can only support "0" or "-3 for more than 1 sheet" for prtInputCurrentLevel) will be considered a caveat, denoted as "(C)".

(6) The Printer MIB requires a few groups from RFC 1213 and RFC 1514 to be supported. Therefore, this assessment will indicate that these groups are "supported" as long as the basic MIB structures have been implemented.

SNMP version / Network Transport support	WorkCentre
SNMPv1 (RFC 1157)	supported
SNMPv2P (RFCs 140x)	supported
SNMPv2C (RFCs 190x)	supported
SNMPv3 (RFCs 1902, 2572, 2574)	supported
SNMP over UDP (IP)	supported
SNMP over IPX (Netware)	not supported
SNMP over NETBEUI (Microsoft Networking)	not supported

RFC 1759 - Printer MIB Group	WorkCentre
RFC 1213 - System group	supported
RFC 1213 - Interface group	supported
RFC 1514 - Storage group	supported
RFC 1514 - Device group	supported
General group [*7 objects*]	supported
Covers group [*3 objects*]	supported
Localization group [*4 objects*]	supported (only US English language supported)
Responsible Party group [*2 objects*] – **OPTIONAL**	Not supported
System Resources group [*4 objects*]	supported
Input group [*12 objects*]	supported
Extended Input group [*7 objects*] **- OPTIONAL**	supported
Input Media group [*4 objects*] - **OPTIONAL**	supported
Output group [*6 objects*]	supported
Extended Output group [*7 objects*] - **OPTIONAL**	supported
Output Dimensions group [*5 objects*] **OPTIONAL**	supported
Output Features group [*6 objects*] - **OPTIONAL**	supported
Marker group [*15 objects*]	supported
Marker Supplies group [*9 objects*] - **OPTIONAL**	supported
Marker Colorant group [*5 objects*] - **OPTIONAL**	supported
Media Path group [*11 objects*]	supported
Channels group [*8 objects*]	supported
Interpreter group [*12 objects*]	supported
Console group [*4 objects*]	supported
Console Display Buffer group [*2 objects*]	supported
Console Display Light group [*5 objects*]	Not supported
Alert Table group [8 *objects*]	supported
Alert Time group [*1 object*] - **OPTIONAL**	supported

RFC 1514 – Host Resources MIB group	WorkCentre
System group [*7 objects*]	supported
Storage group [*8 objects*]	supported
Devices group [*6 objects*]	supported
Processor Table [*2 objects*]	supported
Network Interface Table [*1 object*]	supported
Printer Table [*2 objects*]	supported
Disk Storage Table [*4 objects*]	supported
Partition Table [*5 objects*]	supported
File System Table [*9 objects*]	supported
Software Running group [*7 objects*] – **OPTIONAL**	Not supported
Software Running Performance group [*2 objects*] – **OPTIONAL**	Not supported

RFC 1514 – Host Resources MIB group	WorkCentre
Software Installed group [*7 objects*] – **OPTIONAL**	Not supported

RFC 1213 - MIB-II for TCP/IP group	WorkCentre
System group [*7 objects*]	supported
Interfaces group [*23 objects*]	supported
Address Translation group [*3 objects*]	supported, but this group has been DEPRECATED by the IETF
IP group [*42 objects*]	supported
ICMP group [*26 objects*]	supported
TCP group [*19 objects*]	supported
UDP group [*6 objects*]	supported
EGP group [*20 objects*]	not applicable because Exterior Gateway Protocol not supported by machine
Transmission group [*0 objects*]	not applicable because the group has not yet been defined by the IETF
SNMP group [*28 objects*]	supported
System Object Resources Table/objects per RFC 1907 [*8 objects*]	supported

Additional Capabilities / Application Support	WorkCentre
ability to change GET, SET, TRAP PDU community names	supported
Printer MIB traps	supported = printerV1Alert, printerV2Alert
SNMP Generic Traps	supported = coldStart, warmStart, authenticationFailure
Vendor-specific Traps	supported = xcmJobV1AlertNew, xcmJobV2AlertNew for job monitoring alerts
set trap destination address(es) for any 3rd party Net Mgmt apps.	supported via Web UI
polling for IETF status objects using any 3rd party Net Mgmt apps.	supported
walking IETF MIB tree structure using any 3rd party Net Mgmt app. (e.g. HP OpenView, etc.) / shareware program	supported
New type 2 enumerations from next generation Host Resources MIB supported	optional, not supported because Host Resources MIBv2 has NOT entered the standards track
New type 2 enumerations from next generation Printer MIB supported	supported
New Printer MIBv2 objects implemented	optional, not support because Printer MIBv2 has NOT entered the standards track
IETF AppleTalk MIB (RFC 1243) implemented	not supported
Job monitoring via MIBs	supported via Xerox MIBs
Vendor-specific client application(s) provided	CentreWare Services
required Windows2000 MIB objects supported	supported
Embedded Web Server support	supported
Xerox PrinterMap application support	supported
Xerox PrintXchange support	supported
Novell Distributed Print Services support	supported = w/ Xerox NDPS Gateway solution w/ improved device status
Dazel Output Management Environment	supported
HP OpenView snap-in module	supported
CA Unicenter snap-in module	supported
IBM/Tivoli NetView snap-in module	supported

8.3 Appendix C –Standards

Network Controller Hardware

PCI Specification (PCI Local Bus Specification Revision 2.1)

100 Megabit Ethernet (IEEE 802.3)

Universal Serial Bus 1.1

Network Controller Software

Function	RFC/Standard
Internet Protocol	950
Internet standard subnetting procedure	919
Broadcasting internet datagrams	922
Transmission Control Protocol (TCP)	793
User Datagram Protocol	768
Standard for the transmission of IP datagrams over Ethernet networks	894
Standard for the transmission of IP datagrams over IEEE802 networks	1042
ICMP – ICMP Echo, ICMP Time, ICMP Echo Reply, and ICMP Destination Unreachable message.	792
Reverse Address Resolution Protocol (RARP)	903
Bootstrap Protocol (BOOTP)	951
Clarifications and Extensions for the Bootstrap Protocol (BOOTP)	1542
X.500 Distinguished Name RFC references	1779, 2253, 2297, 2293
SLP	2608
Dynamic Host Configuration Protocol (DHCP)	2131
DHCP Options and BOOTP Vendor Extensions	2132
X.509 Certificate RFC references	2247, 2293, 2459, 2510, 2511, 3280
Hyper Text Transfer Protocol version 1.1 (HTTP)	2616
Line Printer Daemon (LPR/LPD)	1179
File Transfer Protocol (FTP)	959
SNMPv1	1157
SNMPv2	1901, 1905, 1906, 1908, 1909
Structure of Management Information (SMI) for SNMPv1	1155, 1212
Structure of Management Information (SMI) for SNMPv2	1902, 1903, 1904
IETF MIBs: MIB II Host Resources RFC 1759 (Printer), Printer MIB V2	 1213 1514 1759
SNMP Traps	1215
Document Printing Application (DPA)	10175
AppleTalk	Inside AppleTalk, Second Edition

Printing Description Languages

Postscript Language Reference, Third Edition

PCL6 (PCL5E 5SI emulation)

PCL6 (PCLXL 5M emulation)

TIFF 6.0

JPEG

Portable Document Format Reference Manual Version 1.3

8.4 Appendix D – Connector Layouts

'S', 'X' and 'XF' Configuration

8.5 Appendix E – References

Kerberos FAQ	http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html
IP port numbers	http://www.iana.org/assignments/port-numbers