

Xerox Product Implications When FTP Is Disabled

Purpose and Audience

This document is intended for use by Xerox customers, field support, and sales personnel. It describes some alternatives available for customers using Xerox products should they choose to disable the FTP (File Transfer Protocol) capability on their networks. Customers should check the appropriate vendor web site to assess the risk to other applications with respect to their work environment. If precautions are taken to secure networks and operating systems within a firewall, risk to operation of Xerox products may be minimal.

Overview

In response to U.S. legislation known as the Health Insurance Portability and Accountability Act (HIPAA), some customers are choosing to disable the FTP capability on their network because they believe that alternative means of transferring files on their networks are more secure than FTP.

It is important to note that **disabling FTP is *not* a HIPAA guideline**; rather, it is a response by individual customers to the HIPAA guidelines.

In addition to HIPAA, several other U.S. laws and regulations aim at increasing the privacy of an individual's information. Healthcare, Banking, Financial, and Educational industries have bills in various states of enforcement. Federal Government departments and agencies have also increased their requirements for security capabilities within products by specifying a common product evaluation/assurance policy called NIAP (National Information Assurance Partnership) Certification.

What is FTP?

FTP (File Transfer Protocol) is one of many transmission protocols used for sending files across the Internet. A protocol is "an agreed-upon format for transmitting data between two devices. A protocol determines the following:

- The type of error checking to be used
- The data compression method (if any)
- How the sending device will indicate that it has finished sending a message
- How the receiving device will indicate that it has received a message"¹

Your computer or device must support the right protocols if you want it to communicate with other computers or devices.

Xerox customers using networked Xerox printers and multifunction devices may be using FTP as the means for transferring files. If customers disable FTP on their network, users will be unable to perform certain tasks without the added configuration settings described in the table below.

This document applies only to Xerox customers who wish to disable FTP on their network.

Overview of U.S. Laws and Regulations

The following is a brief description of the U.S. laws that may have an impact on how companies are addressing network security and information privacy.

HIPAA is a U.S. Federal law targeted to create dramatic reform in the privacy of patient records in the U.S. healthcare system. It includes provisions geared towards Administrative Simplification, the protection of a patient's right to privacy, and the safeguarding of a patient's health information. The expected date for mandatory compliance with HIPAA is April 2003. See <http://www.healthcaresecurity.org/> for further information.

¹ Source: Webopedia

The Gramm-Leach-Bliley (GLB) Act, which was enacted in 1999 and has been in effect since July 2001, places requirements on financial institutions to protect the security and privacy of consumers' financial information. The law states that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. See <http://www.ftc.gov/privacy/glbact/glboutline.htm> for further information.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. It obligates educational institutions to protect the privacy of student records beyond what might be posted in a student directory. See <http://www.ed.gov/offices/Oll/fpco/ferpa/> for further information.

A U.S. government, cross-departmental purchasing policy exists for agencies and departments that deal with information of a national security interest. The policy (NSTISSP No. 11, dated January 2000) states that all IT (information technology) equipment placed in departments and agencies with national security concerns must be purchased from the Validated Products List. The basis for defining both the security capabilities and the evaluation process is the Common Criteria (CC), an international standard (ISO 15408) for information security. (See <http://csrc.nist.gov/cc/> for more information.) This policy requires that an independent, 3rd party laboratory must validate the security claims of an IT equipment product that provides or enables information assurance capabilities. Once certified (via NIAP certification), the product is placed on the approved vendors' list for purchasing by any of the 21 agencies and departments that fall under this policy.

Xerox Product Response

Most files available from the Xerox web site can be downloaded using HTTP (HyperText Transfer Protocol), so impact to Xerox customers should be minimal. Some downloadable files and utilities do currently rely on FTP; however, Xerox is working to further minimize the use of FTP on the web site.

The table below lists various Xerox products and their positions with respect to disabling FTP. Additional information will be added when it becomes available.

Xerox Solutions and Software Products	
CentreWare Web, CentreWare Web Asset Manager	CentreWare Web and CentreWare Web Asset Manager do <i>not</i> use FTP.
EMS Solutions (IBM Tivoli NetView, HP Openview NNM, CA Unicenter)	EMS Solutions (IBM Tivoli NetView, HP OpenView NNM, and CA Unicenter) do <i>not</i> use FTP.
DigiPath	DigiPath 2.1 and 3.0 use FTP to transmit job data from DigiPath to DocuSP-based production printers for job submission. DigiPath also uses FTP to retrieve data from DocuSP through Network Agent. A valid login name and password are required prior to any transmission. All transmissions are specific to a unique printer IP address. DigiPath provides an optional installable software package called WFTPD Pro that provides an FTP server for other Xerox printer/scan products to submit jobs to DigiPath in a more secure environment. More specifically, this offers interoperability with the Document Centre products. See also the DocuSP-based products response.
DocuShare	DocuShare 2.x does <i>not</i> use FTP.
Flowport	Flowport uses FTP to accept jobs from Document Centre products and then route those files to a designated repository or user's workstation. If FTP is disabled, two optional transfer protocols are available: Internet Fax and SMB Filing. SMB Filing is available only with the Document Centre 5xx series products. See the Document Centre response for further details.
DPSEver for AIX, DPSEver for NT	DPSEver for AIX does <i>not</i> use FTP. DPSEver for NT does <i>not</i> use FTP.

<p>CentreWare Internet Services for Document Centre products</p>	<p>Most CentreWare Internet Services functionality does <i>not</i> use FTP, with the following exceptions:</p> <ul style="list-style-type: none"> • File Destination via FTP • Fax Destinations via FTP • Template Pool Destinations via FTP <ul style="list-style-type: none"> The user can still use all three of these functions, but via NCP over Novell Netware IPX networks or via SMB Filing rather than FTP. • Machine software auto upgrade <ul style="list-style-type: none"> A service representative must do the upgrade on each machine.
<p>CentreWare Scan Services WIA driver with Windows XP</p>	<p>CentreWare Scan Services uses FTP on the Scan Server Repository to accept jobs from Document Centre products. NCP over Novell Netware IPX is an available alternative for filing. See the Document Centre response for further details.</p> <p>The WIA driver for Xerox Document Centre devices included with Windows XP uses FTP on the client workstation to receive documents from the Document Centre.</p>

Xerox Printers and Multifunction Devices

<p>Document Centre products</p>	<p>Document Centre products do not use FTP for printing, copying, or system management functions. For these capabilities, disabling FTP will have no adverse effect on using the Document Centre products.</p> <p>When using scanning capabilities (a user purchasable option), the customer has various mechanisms for scan image delivery:</p> <ul style="list-style-type: none"> • Document Centre 4xx series: <ul style="list-style-type: none"> ○ Scanned images can be exported through either E-Mail (SMTP) or FTP. If the customer chooses to disable FTP, then they can use E-Mail (SMTP) for delivering scanned images. The customer should be aware that using E-Mail allows for authentication of the sender, but that it does not encrypt the data. ○ For customers with a Novell Netware environment, NCP over Novell Netware IPX is an available alternative for filing. ○ A 3rd party firewall appliance that can be used with Document Centre products to provide an SSL (Secure Socket Layer) connection. • Document Centre 5xx series: <ul style="list-style-type: none"> ○ In addition to E-Mail, NCP over Novell Netware IPX, and FTP, the 5xx series provides filing capability via SMB protocol.
<p>DocuSP-based products</p>	<p>DocuSP products do <i>not</i> require FTP in order to operate. DocuSP products never originate an FTP connection.</p> <p>DocuSP products may be configured during installation (or afterwards) to provide FTP access to DigiPath, legacy command line clients, and 3rd party applications requiring FTP; however, if this functionality is not required, FTP should be disabled.</p> <p>If DigiPath is not being used and security is enabled, security scripts that come with DocuSP 3.1 and 3.6 disable FTP, in addition to making other changes to the Solaris Operating Environment to make it more secure.</p> <p>DocuSP products are configured to provide read-only anonymous FTP access; however, if this functionality is not required, it should be disabled.</p> <p>Also see the DigiPath product response.</p>
<p>DocuPrint NPS/IPS series</p>	<p>DocuPrint NPS/IPS products do <i>not</i> require FTP in order to operate. DocuPrint NPS/IPS products never originate an FTP connection.</p> <p>DocuPrint NPS/IPS products may be configured during installation (or afterwards) to provide read-only anonymous FTP access to printer PPD files and to a copy of the Xerox "print" client program; however, if this functionality is not required, it should be (and is by default) disabled.</p> <p>DocuPrint NPS/IPS products may also be configured during installation (or afterwards) to provide read-write FTP access with a "well known" username for legacy XDOD clients to submit documents for printing; however, if older XDOD clients are not in use, FTP should be (and is by default) disabled.</p>
<p>DocuColor EX2000 family (X12/XP12/EX12/EX2000/EX2000v/EX2000d)</p>	<p>DocuColor EX2000 products do <i>not</i> use FTP.</p>

DocuColor 2045/2060(xx) with CSX2000	DocuColor 2045/2060(xx) with CSX2000 products do <i>not</i> use FTP.						
Phaser products	<p>Phaser products support a very limited subset of FTP but do not require it for normal printing functions. Xerox customers using Phaser color printers are largely unaffected by disabling FTP within a network. Standard printer drivers for Phaser products use AppSocket (Port 9100), LPR, USB, IPP, EtherTalk, Novell NetWare, or parallel connection for printing from all operating systems (e.g., Microsoft Windows, Sun UNIX, Apple Macintosh). While printing via FTP is supported, it is not the normal method.</p> <p>The following table lists FTP features supported by Phaser products and the primary protocols for accomplishing the same tasks. FTP is never the primary method of accessing these features; so disabling FTP leaves the primary access methods intact.</p> <table border="1" data-bbox="462 531 1458 732"> <thead> <tr> <th>Feature</th> <th>Feature available through:</th> </tr> </thead> <tbody> <tr> <td>Printing</td> <td>Port 9100, LPR, Parallel connection - One of these is set up during normal printer installation.</td> </tr> <tr> <td>Retrieve Job Accounting Information</td> <td>HTTP – Embedded web server provides access to job accounting information. Automatically enabled during any network installation.</td> </tr> </tbody> </table> <p>If FTP is enabled, the following options are available:</p> <ul style="list-style-type: none"> • Disable FTP. • Set FTP password. • Set access control list. FTP will only respond to user-specified individual IP addresses or address ranges. • Set print job language (PostScript, PCL). • Set print job filtering (change interpretation of special characters). • Set print job pipelining (FTP can accept a new job as soon as the PDL interpreter is done, or not until entire job is printed). 	Feature	Feature available through:	Printing	Port 9100, LPR, Parallel connection - One of these is set up during normal printer installation.	Retrieve Job Accounting Information	HTTP – Embedded web server provides access to job accounting information. Automatically enabled during any network installation.
Feature	Feature available through:						
Printing	Port 9100, LPR, Parallel connection - One of these is set up during normal printer installation.						
Retrieve Job Accounting Information	HTTP – Embedded web server provides access to job accounting information. Automatically enabled during any network installation.						
DocuPrint N series products	DocuPrint N Series products do <i>not</i> use FTP.						
WorkCentre Pro 685/785	FTP is used to upgrade the firmware of the device. The Network Control Centre also uses it when configuring and managing the device. Both of these features would not work if FTP were disabled. All other features would be unaffected.						
WorkCentre Pro 416 & 421	FTP is used to upgrade the firmware of the device only. This feature would not work if FTP were disabled. All other features would be unaffected.						
WorkCentre Pro 423 & 428	FTP is used to upgrade the firmware of the device as well as for Scan to Server. Both of these features would not work if FTP were disabled. All other features would be unaffected.						

Contact

For additional information or clarification on any of the product information given here, contact Xerox support.

Disclaimer

The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. 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 Xerox Product Response 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. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. XEROX cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service marks. All product names are trademarks of their respective companies.