

# WorkCentre

## 7328/7335/7345



# Copyrights and Trademarks

Microsoft® is a registered trademark of Microsoft Corporation.

Windows NT®, Windows® 95, Windows® 98, Windows® Me, Windows® 2000, and Windows® XP are registered trademarks of Microsoft Corporation.

Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Active Directory® is a registered trademark of Microsoft Corporation.

Internet Explorer is a copyright protected program of Microsoft Corporation.

Novell® and NetWare® are registered trademarks of Novell, Inc.

Netscape® is a registered trademark of Netscape Communications Corporation.

Adobe® and PostScript® are registered trademarks of Adobe Systems Incorporated.

TIFF is a copyright of Adobe Systems Incorporated.

AppleTalk, LaserWriter, and Macintosh are trademarks of Apple Computer, Inc.

PCL® and HP-GL® are registered trademarks of Hewlett-Packard Corporation.

WinZip® is a registered trademark of Nico Mak Computing, Incorporated.

Digi is a trademark of Digi International.

ACITS LPR Printing for Windows 95 is a copyright of the University of Texas at Austin.

VTAM® is a registered trademark of IBM Corporation.

IPDS is a trademark of IBM Corporation.

Solaris and Java are trademarks of Sun® Microsystems.

Linux® is a registered trademark of Linus Torvalds.

Red Hat® is a registered trademark of Redhat, Inc.

Mandrake and Linux-Mandrake are trademarks of MandrakeSoft.

CUPS is a trademark of Easy Software Products.

VIPP® (Variable-data Intelligent PostScript Printware) is a registered trademark of Xerox Corporation.

XEROX®, CentreWare® and WorkCentre® are registered trademarks of Xerox Corporation.

FreeFlow™ and SMARTsend™ are trademarks of Xerox Corporation.

ScanSoft, PaperPort, ScanDirect, SET, FormTyper, DesktopDelivery, All-in-One Search, OmniPage and True Page are registered trademarks or trademarks of ScanSoft, Inc.

DocuWorks™ is a trademark of Fuji Xerox.

Equitrac® is a registered trademark of Equitrac Corporation.

Equitrac Office™ is a trademark of Equitrac Corporation.

Unicode™ is a trademark of the Unicode® Consortium.

# Table of Contents

<b>Network Connectivity</b>	<b>1</b>
<b>Installation Steps</b>	<b>1</b>
Xerox Unicode 3.0 for SAP Font Kit	2
<b>Configuration Report</b>	<b>3</b>
<b>Ethernet Speed Setting</b>	<b>4</b>
To Change the Network Speed	4
Go to your Device	4
<b>Enable Internet Services (HTTP)</b>	<b>5</b>
To access Internet Services Settings at the Device	5
Internet Services (HTTP) Enablement	6
Internet Services Port Number	6
Exiting the Internet Services Selection Menu	6
Exiting the Port Settings Menu and returning to the Device's Tools tab screen	6
<b>Proxy Server Settings</b>	<b>7</b>
<b>Parallel Port Configuration</b>	<b>8</b>
To access Parallel Port Settings at the Device	8
Port Status (Parallel Port Enablement)	9
Print Mode	9
PJL (Printer Job Language) Setting	10
Auto Eject time (Parallel Port Timeout)	10
Bi-Directional Communications	11
Input to Prime	11
Exiting the Parallel Port Selections Menu	12
Exiting the Port Settings Menu and returning to the Device's Tools tab screen	12
<b>USB Configuration</b>	<b>13</b>
<b>SNMP Configuration</b>	<b>14</b>
To access SNMP Settings at the Device	14
Port Status (SNMP Enablement)	15
Exiting the SNMP Selection Menu	15
Exiting the Port Settings Menu and returning to the Device's Tools tab screen	15
Configuring SNMP Community Names with Internet Services	16
<b>Changing the Administrator Password</b>	<b>17</b>
To Change the Numeric Password on the Device's Control Panel	17
To Change the Alphanumeric Password used by Internet Services	18
<b>Setting the Auto Clear Timer</b>	<b>19</b>
<b>Add or Remove All Services Screen Buttons</b>	<b>20</b>
Rearrange Icons	20
<b>Smart eSolutions (Meter Assistant and Supplies Assistant)</b>	<b>21</b>
<b>Machine Software Upgrades</b>	<b>23</b>
Prepare for the upgrade	23
At your workstation	23
<b>NOS Selection</b>	<b>24</b>
<b>TCP/IP Protocol Configuration</b>	<b>24</b>
To access the TCP/IP Protocol Settings at the Device	24
Ethernet Setting (Ethernet Rated Speed)	25
TCP/IP – IP Mode	25
IP Address Resolution	25
IPv4 IP Address	26
IPv4 Subnet Mask	26
IPv4 Gateway Address	26
IPv4 IP Filter (IP Address Restriction)	27
Exiting the Protocol Settings Menu and returning to the Device's Tools tab screen	28
<b>TCP/IP LPD Enablement</b>	<b>29</b>

To access LPD Settings at the Device .....	29
Port Status (LPD Enablement) .....	30
LPD Port Number .....	30
LPD Maximum Number of Sessions.....	30
Exiting the LPD Selections Menu .....	30
Exiting the Port Settings Menu and returning to the Device's Tools tab screen .....	30
<b>TCP/IP Dynamic Addressing .....</b>	<b>31</b>
TCP/IP Configuration Selection List .....	32
<b>IP Filtering (IP Address Restriction) .....</b>	<b>33</b>
<b>Configure Port 9100 (Raw Printing) .....</b>	<b>34</b>
<b>Microsoft (NetBIOS over IP) Networks .....</b>	<b>35</b>
Before You Start.....	35
Enabling the SMB Setting at the Device, if required.....	35
Viewing or Configuring the SMB Host Name or WINS Server with Internet Services .....	37
Note regarding DNS/WINS NetBIOS Name Resolution .....	38
To Set Up a Workstation to Print Directly to the Device .....	38
<b>IPP Configuration .....</b>	<b>39</b>
To access IPP Settings at the Device .....	39
Port Status (IPP Enablement) .....	40
IPP – Added Port Number.....	40
Exiting the IPP Selection Menu .....	40
Exiting the Port Settings Menu and returning to the Tools tab screen .....	41
Configuring IPP Settings with Internet Services.....	41
<b>EtherTalk (AppleTalk) Configuration .....</b>	<b>42</b>
To access EtherTalk Settings at the Device.....	42
Port Status (EtherTalk Enablement).....	43
Exiting the EtherTalk Selection Menu .....	43
Exiting the Port Settings Menu and returning to the Tools tab screen .....	43
Configuring EtherTalk Settings with Internet Services .....	44
AS400 Printing .....	45
AS400 Raw TCP/IP Printing to Port 9100 (CRTDEVPRT) .....	45
AS400 Printing using LPR (CRTOUTQ) .....	47
ONLY CHANGE THE PARAMETERS IN BOLD. ....	48
<b>Print Drivers .....</b>	<b>49</b>
<b>TCP/IP Peer to Peer (LPR or Standard TCP/IP)</b>	
<b>Printing .....</b>	<b>49</b>
Windows 2000 Server\Professional & XP Professional (& Vista) Print Driver Installation .....	49
Before you start .....	49
<b>NetBIOS over IP Peer to Peer Printing .....</b>	<b>51</b>
Before You Start .....	51
<b>An Alternate Procedure for Setting up NetBIOS over IP Peer to Peer Printing .....</b>	<b>52</b>
<b>NetBIOS over IP Client/Server Printing .....</b>	<b>53</b>
Before You Start .....	53
Windows 2000 & XP Professional Workstation Print Driver Installation.....	54
Verify that the Correct Protocols and Services are installed in the workstation.....	54
<b>Add the Printer to the Windows 2000 or Windows XP Desktop .....</b>	<b>55</b>
<b>Configure the Print Driver.....</b>	<b>55</b>
<b>IPP Printing (Windows 2000\XP\Vista) .....</b>	<b>56</b>
Before You Start .....	56
<b>Verify that TCP/IP is installed in the workstation .....</b>	<b>57</b>
<b>Add the Printer to the Windows 2000, Windows XP, or Vista Desktop .....</b>	<b>57</b>
<b>Configure the Print Driver .....</b>	<b>58</b>
<b>EtherTalk (AppleTalk) Peer to Peer Printing .....</b>	<b>59</b>
Before You Start.....	59
<b>Load the Print Driver into your Macintosh workstation.....</b>	<b>59</b>
Installation Instructions for 9.x.....	59

Installation Instructions for 10.x (OS X) .....	60
<b>Common UNIX Printing System (CUPS) .....</b>	<b>61</b>
Overview .....	61
Before You Start .....	61
Installing CUPS on the UNIX workstation .....	62
Installing the Xerox PPD on the workstation.....	62
Adding the Xerox printer .....	63
Printing with CUPS .....	63
<b>Options .....</b>	<b>64</b>
<b>Enabling Options with Software Keys .....</b>	<b>64</b>
<b>Hidden Features .....</b>	<b>65</b>
<b>Xerox Extensible Interface Program (XEIP) .....</b>	<b>66</b>
XEIP Setup.....	66
<b>Scan to Home .....</b>	<b>68</b>
To prepare for Scan to Home installation.....	68
Configure Scan to Home.....	69
<b>Scanning to the Device's Hard Drive (Mailboxes) .....</b>	<b>70</b>
Before You Start .....	70
Setting Up Mailboxes at the Device .....	71
Configuring Expiration Settings for Stored Documents .....	72
Setting Up Mailboxes with Internet Services.....	73
Scanning to Mailboxes .....	74
To scan to a Mailbox, perform these steps:.....	74
Retrieving Images from Mailboxes .....	75
<b>Installing and Using the Network Scanner Utility .....</b>	<b>76</b>
Before Installing the Network Scanner Utility .....	76
Installing the Network Scanner Utility.....	76
Uninstalling the Network Scanner Utility .....	76
Importing Scanned Data from the Mailbox to an Image-Editing Application .....	77
Importing Scanned Data from the Mailbox using Mailbox Viewer .....	78
Changing Network Utility or Mailbox Viewer Settings .....	78
<b>Scan to E-mail .....</b>	<b>79</b>
E-mail Overview .....	79
Preparations .....	80
Registering an E-mail account.....	81
Configuring E-mail Environment.....	81
Installation Procedure.....	82
Installation Overview.....	82
Enabling the E-mail Ports and Setting TCP/IP .....	83
Configuring the E-mail Environment.....	85
<b>Internet Fax (iFAX) .....</b>	<b>91</b>
iFAX Overview.....	91
Preparations .....	91
System Requirements for the Machine.....	91
Installation Procedure.....	92
Installation Overview.....	92
Enabling the E-mail Ports and Setting TCP/IP .....	93
Configuring the E-mail Environment.....	95
Testing iFAX.....	101
Send from the Device to another iFAX-capable Machine .....	101
<b>Server Fax .....</b>	<b>102</b>
Server Fax Overview.....	102
Installation Checklist.....	103
Configure a Fax Filing Location (Repository) .....	105
Configure a Fax Filing Repository using FTP .....	106
Installation Checklist.....	106

<b>Enter the Fax Repository Details via Internet Services .....</b>	<b>107</b>
<b>Configure General Settings .....</b>	<b>108</b>
Configure the Fax Server.....	108
<b>Test Faxing through the Server.....</b>	<b>108</b>
Configure a Fax Filing Repository using SMB .....	109
Installation Checklist.....	109
<b>Enter the Fax Repository Details via Internet Services .....</b>	<b>110</b>
<b>Configure General Settings .....</b>	<b>111</b>
Configure the Fax Server.....	111
<b>Test Faxing through the Server.....</b>	<b>111</b>
Configure a Fax Filing Repository using SMTP .....	112
Installation Checklist.....	112
<b>Enter the Fax Repository Details via Internet Services .....</b>	<b>113</b>
<b>Configure General Settings .....</b>	<b>114</b>
<b>Test Faxing through the Server.....</b>	<b>114</b>
Features that can be set in support of Server Fax .....	115
Address Book Setup .....	115
Group Send .....	115
Fax Mode Settings (Screen Defaults and Fax Defaults such as Delayed Start) .....	116
Color Mode, Resolution, File Format, and File Name.....	116
<b>Fax .....</b>	<b>117</b>
Fax Overview FP.....	117
Checking and Setting Critical Fax Parameters .....	117
Before You Start Fax .....	117
Before starting the setup:.....	117
Communications modes: .....	117
Connecting the phone line: .....	117
Local Terminal Information Settings .....	118
Address Book Setup .....	119
Group Send Setup .....	121
Comments .....	122
Create a Mailbox .....	123
File Destination / Output Destination .....	125
Fax Settings (including Fax Defaults and Fax Control) .....	126
Common Settings: Audio Tones and Reports. ....	126
Fax Mode Settings (including Fax Defaults and Fax Control) .....	128
To Configure Fax to Mailbox .....	131
LAN Fax (PCL Drivers) .....	132
Initial Setup.....	132
Adding a Recipient to a Fax Phonebook .....	132
Sending the Fax.....	132
LAN Fax (PostScript Drivers) .....	133
Initial Setup.....	133
Adding a Recipient to a Fax Phonebook .....	134
Sending the Fax .....	135
Stopping the Fax (when necessary) .....	135
<b>Scan to PC (FTP/SMB) .....</b>	<b>136</b>
Overview .....	136
Requirements for FTP .....	136
Requirements for SMB .....	136
Installation Procedure.....	137
Enabling Ports and Setting TCP/IP .....	138
Receiving Computer Configuration .....	141
Using with FTP .....	141
<b>Using with SMB.....</b>	<b>141</b>
Adding the Receiving Computer's Address to the Address Book .....	142

Using the Scan to PC (FTP/SMB) Feature.....	143
<b>Setup and Use of Job Flow Sheets with Mailboxes .....</b>	<b>144</b>
Overview .....	144
Features supported for Job Flow .....	144
Enabling Ports and Setting TCP/IP .....	145
Configuring the SNMP Port.....	147
Creating Job Flow Sheets .....	148
Creating a Mailbox and linking to a Job Flow Sheet (for automatic processing).....	149
Manually linking a Job Flow Sheet to documents in a Mailbox .....	151
Testing Job Flow Sheet operation (for automatic processing) .....	151
<b>Scan to PC Desktop .....</b>	<b>152</b>
Overview .....	152
Preparations .....	153
Software Installation Procedure .....	153
Configure Image Retriever 5.2 on Networked Workstations .....	153
Testing Scan to PC Operation.....	153
<b>Network Scanning (using templates) .....</b>	<b>154</b>
Overview .....	154
SMARTsend scanning services.....	154
Scan to PC Desktop .....	154
Additional Notes .....	155
Network Scanning User Authentication .....	155
Multifunction Device Authentication.....	155
Template Considerations when using SMARTsend .....	155
Use of a Validation Server .....	155
Installation Checklist.....	156
Configure a Scan Filing Location .....	157
Configure a Scan Filing Repository using FTP .....	158
Installation Checklist.....	158
Enter the Scan Repository Details via Internet Services .....	158
<b>Configure General Settings .....</b>	<b>159</b>
Configure a Scan Filing Repository using SMB .....	160
Installation Checklist.....	160
Enter the Scan Repository Details via Internet Services .....	160
<b>Configure General Settings .....</b>	<b>161</b>
Configure Scan to HTTP .....	162
To configure the Scan Repository Details using CentreWare Internet Services: .....	162
Setting up a Remote Template Pool Repository (optional) .....	163
Configuring the Default Template with Internet Services .....	164
Setting up a Remote Template Pool Repository (optional) .....	166
Testing Network Scanning (using templates).....	167
<b>Web Service (if available) .....</b>	<b>168</b>
Enable the WebDAV port (for name space management) .....	168
<b>Security – Authentication .....</b>	<b>169</b>
Overview .....	169
Users Controlled by Authentication .....	169
Authentication Configuration and related Types.....	169
Services Managed by User ID Authentication.....	170
When Local Machine Access is enabled .....	170
When Network Access is enabled .....	170
When Remote Access is enabled.....	170
Effects of Authentication on Job Flow Sheets and Mailboxes.....	171
Configuring Local machine authentication .....	171
Preparations: .....	171
<b>At Your Workstation:.....</b>	<b>171</b>
Configuring Remote Authentication.....	172

Preparations: .....	172
Configure Remote Authentication for Kerberos (Windows 2000) .....	173
At your Workstation: .....	173
Configure Remote Authentication for Kerberos (Solaris) .....	174
At Your Workstation:.....	174
Configure Remote Authentication for SMB .....	175
At Your Workstation:.....	175
Configure Remote Authentication for LDAP .....	176
LDAP User Mappings .....	177
LDAP Authentication.....	177
LDAP Group Access.....	177
Custom Filters.....	177
Configuring Network Authentication (by a Remote Accounting server) .....	178
Enable Network Authentication.....	178
Configure communications between the Accounting server and the device .....	179
Enable the Accounting option in workstation print drivers .....	180
Configuring Xerox Secure Access (Authentication) .....	181
Secure Access and Accounting .....	181
Information Checklist .....	181
Configuring Xerox Secure Access to work with Remote Authentication .....	182
Configure Remote Authentication for Kerberos (Windows 2000) .....	183
Configure Remote Authentication for Kerberos (Solaris) .....	184
Configure Remote Authentication for SMB .....	185
Configure Remote Authentication for LDAP .....	186
Enable Specific Xerox Secure Access Settings .....	188
Using Secure Access.....	189
Configure Color Copy Access for LDAP Group .....	190
LDAP Authentication .....	191
LDAP Group Access.....	191
802.1X Authentication .....	193
Information Checklist .....	193
Configure 802.1X with Internet Services .....	193
<b>Security – Encryption .....</b>	<b>194</b>
Encryption Service Overview .....	194
Types of Encryption Services Available.....	194
Configuration of HTTPS (SSL/TLS) Communication Encryption .....	196
Installation Overview.....	196
Configuring certificates with CentreWare Internet Services .....	197
Configuration on a Computer .....	198
Configuration of E-mail Encryption/Digital Signature .....	199
Installation Overview.....	199
Configuring S/MIME certificates with CentreWare Internet Services .....	200
Configuration on a Computer .....	203
Configuration of Scan File Signatures (PDF/XPS Documents).....	204
Installation Overview.....	204
Configuring Scan File certificates with CentreWare Internet Services .....	205
Configuration on a Computer .....	207
IP Sec.....	208
To enable IP Sec: .....	208
<b>Scheduled Image Overwrite .....</b>	<b>209</b>
<b>Security – Secure Watermark .....</b>	<b>210</b>
To configure Secure Watermark:.....	210
<b>Security – Secure Print .....</b>	<b>212</b>
<b>Xerox Standard Accounting .....</b>	<b>214</b>
Overview .....	214
Installation Checklist.....	214
Enable Xerox Standard Accounting (from Internet Services).....	215



Create a Group Account.....	216
Create a User Account and Set Usage Limits.....	217
Maximum Usage Limits and Resetting Individual Usage Limits.....	218
To Reset User Limits (if necessary).....	218
Using XSA at the machine .....	219
Resetting Usage Data .....	220
Print a Usage Report.....	221
Enable XSA in your Print Drivers .....	222
Backing Up XSA data and settings and Cloning to another device.....	223
Check that the device you want to clone settings to supports XSA.....	223
To clone a machine .....	223
To Restore Settings or Clone Settings to another Machine .....	224
<b>Audit Log .....</b>	<b>225</b>
Overview .....	225
Accessing the Audit Log feature.....	225
<b>Annotation (Bates Stamping) .....</b>	<b>226</b>
Overview .....	226
Configuring Bates Stamp Settings .....	226
Configuring a precise Bates Stamp location (if available).....	227
<b>Media Card Reader .....</b>	<b>228</b>
Overview .....	228
Media Card Reader Hardware .....	228
Supported Media and File Formats .....	228
Supported Media .....	228
Supported File Formats .....	228
Important Notes and Restrictions.....	229
Inserting and Ejecting Media.....	229
Selecting and Printing Text Files.....	229
Media Print Text Tab .....	230
Index Print.....	230
Advanced Settings.....	230
Selecting and Printing Photo Files .....	230
Media Print Photos Tab .....	230
Index Print .....	231
Advanced Settings.....	231
Problem Solving .....	231
<b>USB Printing .....</b>	<b>232</b>
Overview .....	232
USB Printing Hardware .....	232
Supported Media and File Formats .....	232
Supported File Formats .....	232
Important Notes and Restrictions.....	232
Selecting and Printing Text Files.....	234
To Select and Print Text Files:.....	234
Media Print Text Tab .....	234
Advanced Settings Tab.....	234
Selecting and Printing Photo Files .....	235
To Select and Print Photo Files: .....	235
Media Print Photos Tab .....	235
Advanced Settings Tab.....	235
<b>Thumbnail Preview .....</b>	<b>236</b>
To view a thumbnail preview and print a document.....	236
<b>Hard Disk Data Encryption .....</b>	<b>237</b>
Encryption Key For Confidential Data .....	237
<b>Internet Services.....</b>	<b>238</b>
<b>Enable Internet Services (HTTP) .....</b>	<b>238</b>

To access Internet Services Settings at the Device .....	238
Internet Services (HTTP) Enablement .....	239
Internet Services Port Number .....	239
Exiting the Internet Services Selection Menu .....	239
Exiting the Port Settings Menu and returning to the Tools tab screen.....	239
<b>Overview .....</b>	<b>240</b>
<b>Status Tab .....</b>	<b>241</b>
<b>Jobs Tab .....</b>	<b>242</b>
<b>Print Tab .....</b>	<b>243</b>
<b>Scan Tab .....</b>	<b>244</b>
<b>Properties Tab .....</b>	<b>245</b>
Descriptions of the folders and hot links in the Directory Tree .....	245
General Setup folder.....	245
Connectivity folder .....	246
Physical Connections subfolder .....	248
Services Folder .....	249
Accounting folder .....	250
Security folder .....	251
<b>Support Tab .....</b>	<b>252</b>
<b>Additional Details of some Properties Tab features .....</b>	<b>253</b>
Setting TIFF (and other PDL) Processing Properties .....	253
Setting PDL Emulations .....	254
Banner Sheet Printing .....	255
Set the Ethernet Speed .....	256
Configure TCP/IP Settings .....	257
TCP/IP Configuration Selection List .....	258
Configure LPD .....	259
Configure SNMP .....	260
SNMP Community Name properties that can be configured.....	260
Configuring SNMP Community Names with Internet Services.....	260
Configure Microsoft Networking (also known as SMB) .....	261
Configure IPP .....	262
Modify the HTTP (Internet Services) Settings .....	263
Configure WSD (Web Services on Devices) .....	264
Configure Port 9100 (Raw Printing) .....	265
IP Filtering (IP Address Restriction) .....	266
Configure EtherTalk (AppleTalk) .....	267
E-mail, SMTP, and POP3 Settings.....	268
Bonjour (if available for selection) .....	269
<b>Troubleshooting .....</b>	<b>270</b>
<b>General Troubleshooting Procedure .....</b>	<b>270</b>
<b>TCP/IP Troubleshooting .....</b>	<b>272</b>
Check Physical Media and Network Interface Cards .....	272
Print a Configuration Report at the Device and perform these tasks: .....	272
At the workstation, perform these tasks: .....	273
<b>NetBIOS over IP Troubleshooting .....</b>	<b>275</b>
Check Physical Media and Network Interface Cards .....	275
Print a Configuration Report at the Device and perform these tasks: .....	275
At the DNS or WINS Server .....	276
At the workstation, perform these tasks: .....	277
<b>IPP Troubleshooting .....</b>	<b>279</b>
Check Physical Media and Network Interface Cards .....	279
Print a Configuration Report at the Device and perform these tasks: .....	279
At the Windows 2000 workstation, perform these tasks:.....	280
<b>EtherTalk Troubleshooting .....</b>	<b>282</b>
Check Physical Media and Network Interface Cards .....	282

Print a Configuration Report at the Device and perform these tasks: .....	282
At the Macintosh workstation .....	283
<b>Scanning to Hard Drive Troubleshooting .....</b>	<b>284</b>
Before you start .....	284
Check Physical Media and Network Interface Cards .....	284
Print a Configuration Report at the Device and perform these tasks: .....	285
At the Device .....	285
At the Workstation .....	286



# Network Connectivity



## Installation Steps

**Step 1.** Connect one end of a Category 5 twisted pair cable to a live network drop. Connect the opposite end of the cable to the RJ-45 socket at the rear of the Device.

**Step 2.** Set the Device's power switch to ON and wait until the Main screen is displayed.

**Note: The actual screen displayed as the Main screen is selectable.** To determine the screen you would like displayed, press the Log In / Out button, enter the Administrator password (default of 11111), touch Enter, press the Machine Status button, and touch the Tools tab. Touch Common Service Settings, touch Screen/Button Settings, select Service Screen Default, touch Change Settings, make your selection and touch Save. Touch Close until the Tools tab is displayed. Wait for the Auto Clear service to log you out.

**Step 3.** Refer to the Configuration Report topic in this guide and print a Configuration Report using the instructions supplied.

**Step 4. Referring to the Configuration Report, determine if the appropriate ports and protocols are enabled for your Network environment.**

To support communicating with the Device's Internet Services, a series of internal Web Pages that enable remote configuration of operating settings, the TCP/IP protocol stack should be enabled. The Device should also have a valid IP Address, Subnet Mask, and Gateway displayed. If this is not the case, go to the **NOS Selection** section of this guide, locate the **TCP/IP Protocol Configuration** topic, and follow the instructions supplied.

Some Network Environment settings can only be configured through use of Internet Services. Also, **nearly all of the services, ports, and protocols that can be configured at the Device can be configured with Internet Services** running on a networked workstation. If Internet Services is shown as "disabled" on the Configuration Report, refer to the **Enable Internet Services (HTTP)** topic in this guide.

If you will be using SNMP Management software with this device, refer to the **SNMP Configuration** topic and follow the instructions supplied.

If you will be using the Parallel Port and wish to view or change its configuration, refer to the **Parallel Port Configuration** topic and follow the instructions supplied.

**Step 5.** Go to the NOS Selection section of this guide, then select your Network Operating System for Device installation instructions specific to your network environment. If you will be installing the Device in a Client/Server environment, make sure to have your Server's Operating System Manual available to refer to when required.

**Step 6.** Go to the **Print Drivers** section of this guide for the instructions required to set up individual desktop workstations to communicate with the Device.

**Step 7.** If you have purchased optional features for your Device, such as Scanning to the Device's Hard Drive, go to the **Options** section of this guide for configuration instructions.

*Note: For comprehensive information on the use of Internet Services as a browser-based, workstation tool for configuring your Device, go to the Internet Services section of this guide and click on relevant topics from the menu list.*

## Xerox Unicode 3.0 for SAP Font Kit

A Unicode font kit is available for this multifunction device. Installation of the Unicode fonts, per the kit's instructions, provides the required character sets to print documents in multiple languages, in an SAP printing environment. To order the kit, contact your Xerox representative.

# Configuration Report

To print a Configuration Report, with the Device switched **ON**, perform the following steps:

1. Press the **Machine Status button**.
2. Press the **Print Reports button**.
3. Press the **Copy Reports button**.
4. Press the **Configuration Report button**.
5. Press the large, green, **Start button**, located to the immediate right of the Control Panel's numeric keypad.
6. The printing process will be graphically displayed on the touch screen. Upon receipt of the Configuration Report, note that the multi-page print is formatted into two columns with horizontal ruled lines indicating four distinct data display areas on the print.
  - The first area displays System Settings.
  - The second area displays Copy Service Settings.
  - The third area displays Print Service Settings.
  - The fourth area displays Communication Settings.

# Ethernet Speed Setting

The Device's Ethernet Interface has speed settings of **Auto** (10 BASE-T/100 BASE-TX), **100 BASE-TX** (Half or Full Duplex), and **10 BASE-T** (Half or Full Duplex). By default the Ethernet Port Configuration will be set to **Auto**.

## To Change the Network Speed

### Go to your Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Protocol Settings**.
8. When the Protocol Settings menu displays, press the selection line labeled **Ethernet Rated Speed**.
9. Press the **Change Settings button**.
10. On the Ethernet Rated Speed screen note which one of the buttons is highlighted as the current setting for Ethernet speed. The available settings are Auto (10 BASE-T/100 BASE-TX), 100 BASE-TX (Half or Full Duplex), and 10 BASE-T (Half or Full Duplex). The default setting is Auto.
11. To change settings, press your setting of choice, then press the **Save** button.
12. To exit the Ethernet Setting screen, without making any changes, press the **Cancel** button.
13. To exit the Protocol Settings menu, returning to the Tools tab screen, press the rectangular **Close** button.
14. Wait several seconds and the Auto Clear service should log you out.

*Note that if you changed any settings in the Protocol Settings menu, the Device will automatically reboot to register and enable your new settings.*



# Enable Internet Services (HTTP)

Internet Services are a series of Web (HTML) Pages located within the Device enabling network communication settings to be conveniently configured from a web browser running on a remotely located workstation.

*Note: If Authentication is enabled, as stated in the **Security – Authentication** topic in the **Options** section of this guide, you will have to supply the Administrator User Name and Password when first accessing Internet Services, rather than supplying these credentials after configuring individual features with Internet Services.*

For further details on the many functions provided by the Internet Services Web Pages, refer to the **Internet Services** section of this guide.

## To access Internet Services Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. When the Port Settings menu displays, press the down arrow key to view additional selections.
9. Press the **Internet Services (HTTP)** selection line.
10. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
11. When the Internet Services (HTTP) menu displays, note that you have two settings available for selection. The Port Settings menu selections are **Port Status** and **Internet Services Port Number**. After pressing the selection line, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Internet Services (HTTP) Enablement

1. Press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the Port Status screen, note which of the two buttons is highlighted as the current setting for Internet Services Enablement. The available settings are Enabled or Disabled. In order to use Internet Services, this setting **MUST** be enabled.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### Internet Services Port Number

1. Press the selection line labeled **Internet Services Port Number**.
2. Press the **Change Settings** button.
3. On the Port Number screen, use the supplied keypad to enter the appropriate port number (default of 80).
4. To change settings, press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### Exiting the Internet Services Selection Menu

To exit the Internet Services Selection Menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

### Exiting the Port Settings Menu and returning to the Device's Tools tab screen

6. To exit the Port Settings menu, returning to the Device's Tools tab screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
7. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

# Proxy Server Settings

To use the Web Service button on the machine (if available), which enables the machine to access HTTP file servers on the Internet, you need to enter your Proxy Server information as described here.

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Select **Proxy Server Settings** in the list of hot links.
4. Place a checkmark in the **Use Proxy Server** checkbox.
5. From the **Proxy Setup** drop-down menu, select either Same Proxy for All Protocols, or Different Proxy for each Protocol, depending upon your Proxy Server setup.
6. In the **Addresses to Bypass Proxy Server** box, enter in up to 1024 characters of IP addresses, fully qualified host names, or wildcard host names (such as \*.eng), separated by semicolons. Functioning like the local address exception list in a typical web browser, these addresses will be permitted to bypass the Proxy Server.
7. For the **HTTP or HTTPS Server Names**, provide a name of up to 255 characters in length for one or both of these Proxy Servers. A fully qualified domain name or IP address can be used. **Note:** Make sure that DNS is enabled as stated in the TCP/IP Protocol Configuration topic in the NOS Selection section of this guide.
8. Leave the **Port Number** set to 8080 (the IANA recognized proxy port) unless you are using a different port number. If you are using a different port number, enter it in the available box.
9. Check the **Authentication** box if client authentication is required for the Proxy Server.
10. Enter the **Login Name** for access to the proxy server. Up to 32 characters can be entered.
11. Enter the **Password** for access to the proxy server. Up to 32 characters can be entered.
12. Click **Apply**.
13. Enter the System Administrator user ID and password when prompted and click **OK**.

# Parallel Port Configuration

To view or change the settings of the Device's parallel port, perform the following steps:

*Note: You must have purchased the Parallel (1284) Printing kit and installed the supplied hardware before you can configure this port.*

## To access Parallel Port Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. Press the line labeled **Parallel** on the Port Settings menu.
9. Press the **Change Settings button** in the lower right corner of the Port Settings menu screen.
10. When the Parallel Port selections menu displays, note that you have a choice of setting selections by numbered horizontal lines, with the current status of each setting shown. The up and down arrow keys provide access to additional selections and return you to the current selections display. The Close button in the upper right corner of the screen returns you to the Port Settings menu. After pressing a horizontal line selection, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Port Status (Parallel Port Enablement)

1. On the Parallel Port selections menu, press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the Parallel Port Status screen, note which of the two buttons is highlighted as the current setting for Parallel Port Enablement. The available settings are Enabled or Disabled.
4. To change settings, press your setting of choice, then click the **Save** button on the touch screen.
5. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

## Print Mode

1. On the Parallel Port selections menu, press the selection line labeled **Print Mode**.
2. Press the **Change Settings** button.
3. On the settings screen, note which one of the displayed buttons is highlighted as the current setting for Parallel Print Mode. This setting informs the Controller of the Page Description Language (PDL) being used by your print jobs. The available settings are Auto (default), PostScript, HP-GL/2, PCL, and TIFF. **Auto** enables the Controller to automatically detect and select the appropriate PDL.
4. To change settings, press your selection of choice, then click the **Save** button on the touch screen.
5. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

## PJL (Printer Job Language)Setting

1. On the Parallel Port selections menu, press the selection line labeled **PJL**.
2. Press the **Change Settings** button.
3. On the settings screen, note which of the two buttons is highlighted as the current setting for Job Control Language. This is the setting that enables the Controller's job processing parameters to be modified by HP PJL. The available settings are Enabled or Disabled.
4. To change settings, press your setting of choice, then click the **Save** button on the touch screen.
5. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

## Auto Eject time (Parallel Port Timeout)

1. On the Parallel Port selections menu, press the selection line labeled **Auto Eject Time**.
2. Press the **Change Settings** button.
3. On the settings screen, note the current display in seconds for the Parallel Port Timeout. This is the length of time that the Controller will wait for an end of job command before printing the current job. Up and down selection arrows are provided for modification of the timeout value in the increments shown.
4. To change settings, use the up or down selection arrow, then click the **Save** button on the touch screen.
5. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

## Bi-Directional Communications

1. Select the down arrow on the screen to see this setting.
2. On the Parallel Port selections menu, press the selection line labeled **Bi-directional communications**.
3. Press the **Change Settings** button.
4. On the settings screen, note which of the two buttons is highlighted as the current setting for Bi-Directional Communications. The available settings are Enabled or Disabled. To support high speed, bi-directional parallel communications, select the Enabled setting.
5. To change settings, press your setting of choice, then click the **Save** button on the touch screen.
6. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

## Input to Prime

1. Select the down arrow on the screen to see this selection.
2. On the Parallel Port selections menu, press the selection line labeled **Input Prime**.
3. On the settings screen, note which of the two buttons is highlighted as the current setting for Parallel Input to Prime. The available settings are Enabled or Disabled. In support of bi-directional communications, input to prime enables or disables the communication of a control signal over the parallel port (which is client (workstation) dependent). When in doubt, select the Enabled setting.
4. To change settings, press the setting of choice, then click the **Save** button on the touch screen.
5. To exit the screen, without making any changes, click the **Cancel** button on the touch screen.

### **Exiting the Parallel Port Selections Menu**

To exit the Parallel Port Selections Menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

### **Exiting the Port Settings Menu and returning to the Device's Tools tab screen**

1. To exit the Port Settings menu, returning to the Device's Tools tab screen, press the rectangular **Close** button in the upper right corner of the Ports Menu screen.
2. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*



# USB Configuration

The file folder on the Properties page of Internet Services (the device's internal web pages) contains a folder, labeled **Physical Connections**.

To access this folder, enter the IP address of the device in the Address line of your browser and press **Enter**. Click on the **Properties** tab, then click on the **Physical Connections** folder.

The Physical Connections folder contains Ethernet, Parallel Port (if available), and USB (if available) hot links. Note that the Parallel Port and USB hot links need an optional kit installed before they can be displayed.

Click on the **USB** hot link to view or change the **Auto Eject Time**, which is the length of time the Controller will wait for an end of job command before processing the job. Refer to the On-Line Help for assistance in configuring the Adobe Communication Protocol (if available).

# SNMP Configuration

SNMP (Simple Network Management Protocol) provides a method to remotely monitor and diagnose device performance on the network. Once SNMP has been enabled at the device, SNMP Management software, running on a host computer connected to the network, polls the device's agents for operating information and responds to traps from the device regarding specific events. Examples of such events might be notifications from the device that it is low on toner, or low on paper.

To view or change the Device's SNMP setting, perform the following steps:

## To access SNMP Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. When the Port Settings menu displays, press the **SNMP** selection line.
9. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
10. When the SNMP selection menu displays, note that you have only one selection available on a single, numbered horizontal line, with the current status of this setting shown. The Close button in the upper right corner of the screen returns you to the Port Settings menu. After pressing the selection, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Port Status (SNMP Enablement)

1. On the SNMP selection menu, press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the Port Status screen, note which of the two buttons is highlighted as the current setting for SNMP Enablement. The available settings are Enabled or Disabled. For SNMP to function, it must be set to Enabled.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### Exiting the SNMP Selection Menu

To exit the SNMP selection menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

### Exiting the Port Settings Menu and returning to the Device's Tools tab screen

6. To exit the Port Settings menu, returning to the Tools tab screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
7. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

## Configuring SNMP Community Names with Internet Services

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus symbol (+) to the left of the **Connectivity**, then the **Protocols** file folder.
4. Select **SNMP Configuration** in the directory tree, and check the **Enable** box for the version desired.
5. Click the **Edit Properties** button and supply the User Name (default of 11111) and Password (default of x-admin), if prompted.
6. Enter a name for the **Community Name (Read-Only)**. This is the password for SNMP GET requests from the SNMP Manager to the Agent in the Device.
7. Enter a name for the **Community Name (Read-Write)**. This is the password for SNMP SET requests from the SNMP Manager to the Agent in the Device.

**Caution:** *If you change the GET and/or SET Community Names, you must also change the names in all network applications that are communicating by SNMP with this Device.*

8. Enter a name for the **Community Name (Trap Notification)**. This is the default password for SNMP TRAPS sent from the device to the Manager by SNMP.
9. Optionally enter the System Administrator's name for packet identification purposes.
10. Select a trap and click **Edit** in the Trap Notification Settings section.
11. Select your transport method (IPX or UDP) and fill in the trap destination information for your selected method.
12. Select the event(s) that you wish to report on by checking the applicable box(es).
13. Click **Apply** to accept the changes, or **Undo** to return the settings to their previous values.

*Note: Changes to settings will not be applied until you restart the Device.*

# Changing the Administrator Password

There are two Administrator Passwords that control access to the Device's feature settings. One password is a numeric password (login ID) that controls access through the Device's Control Panel. The second password is an alphanumeric password (pass code) that controls access through the Device's Internet Services (embedded HTTP server application residing in the Device).

## To Change the Numeric Password on the Device's Control Panel

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. This is the factory default "password."
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press the **Authentication/Security Settings**.
7. Press **System Administrator Settings**.
8. Press **System Administrator Login ID**.
9. On the Login ID screen, select the **On** button.  
*Note: If you select the Off button, you cannot access the password setting or password changing functions.*
10. Press the keyboard button, and use the displayed keyboard to enter in a new numeric Login ID ranging from 1 to 32 characters in length.
11. Press the **Save** button.
12. Press **Next**, then press the keyboard button.
13. Use the displayed keyboard to enter in your new numeric Login ID a second time and press **Save** again.
14. Press **Save** on the Login ID screen to save the new Login ID.
15. If necessary, to exit the System Administrator Settings screen, press the rectangular **Close** button in the upper right corner of the screen.
16. Wait several seconds and the Auto Clear service should log you out.

## To Change the Alphanumeric Password used by Internet Services

*Note: If Authentication is enabled, as stated in the **Security – Authentication** topic in the **Options** section of this guide, you will have to supply the Administrator User Name and Password when first accessing Internet Services, rather than supplying these credentials after configuring individual features with Internet Services.*

1. Press the **Log In / Out button** on the Device's Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. This is the factory default "password."
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Authentication/Security Settings**.
7. Press **System Administrator Settings**.
8. Press **System Administrator Passcode**.
9. Press the keyboard button, and use the displayed keyboard to enter in a new alphanumeric password ranging from 4 to 12 characters in length.
10. Press the **Save** button.
11. Press the keyboard button, and use the displayed keyboard to enter in your new password a second time and press **Save** again.
12. Press **Save** on the Password screen to save the new password.
13. If necessary, to exit the System Administrator Settings screen, press the rectangular **Close** button in the upper right corner of the screen.
14. Wait several seconds and the Auto Clear service should log you out.

# Setting the Auto Clear Timer

For security purposes, the Auto Clear service will automatically log the System Administrator out of the machine's **Tools** tab, after a period of inactivity determined by the Auto Clear timer.

To set the Auto Clear Timer to a duration of up to 240 seconds, perform the following steps.

1. Press the **Log In / Out button** on the Device's Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times. This is the factory default "password."
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **System Settings** tab.
7. Press **Common Service Settings**.
8. Press **Machine Clock/Timers**.
9. Press **Auto Clear**, then **Change Settings**.
10. Use the displayed control to set the timer duration in a range of 30 to 240 seconds.
11. Press the **Save** button.
12. Press **Close** to return to the Tools tab screen.
13. Wait several seconds and the Auto Clear service should log you out.

# Add or Remove All Services Screen Buttons

## To Add or Remove All Services Screen Buttons:

1. Press the [Log In / Out] button to enter System Administration Mode.
2. Type the administrator password (11111 or current password).
3. Touch [Enter]
4. Press the [Machine Status] button on the Control Panel.
5. Touch the [Tools] tab.
6. Touch [System Settings].
7. In the Group column, touch [Common Service Settings].
8. Touch [Screen / Button Settings].
9. On the Screen / Button Settings screen, in the Items column, touch [All Services].
10. Touch [Change Settings].
11. To add a service screen button:
  - a. Touch a [Not Assigned] service button.
  - b. Touch the service to be added as a screen button.
  - c. Touch [Save].  
The screen refreshes and returns to the All Services screen.
  - d. Touch [Save] again.  
The screen refreshes and returns to the Screen / Button Settings screen.
12. To remove a service screen button:
  - a. Touch the service that you want to remove (for instance, Internet Fax).
  - b. Touch [Not Assigned].
  - c. Touch [Save].  
The screen refreshes and returns to the All Services screen.
  - d. Touch [Save] again.  
The screen refreshes and returns to the Screen / Button Settings screen.
13. Touch [Close].
14. Touch [Log In/Out] button.
15. Touch [Logout].

## Rearrange Icons

You can also use this feature to rearrange the icons. The service listed as #1 will be at the top left of the All Services screen, #2 will be to the right of it, and so on.



# Smart eSolutions (Meter Assistant and Supplies Assistant)

Select this feature in Internet Services to access and set up automatic billing meter reading and automatic machine supplies reporting. Note that this feature may currently be available only in the U.S.A.

## Information Checklist

Make sure that you have an account on Xerox.com. Add all devices in inventory that you wish to register for Automatic Meter Readings to your account. This is supported by Dallas eSupport 888-998-9922.

TCP/IP and HTTP protocols must be enabled on the device so that the device web browser can be accessed (for Device Direct registration, described in this procedure).

To use the optional Smart eSolutions Windows Client or CentreWare Web, you will need to enable SNMP as stated in this guide. For full information on these applications, visit [www.xerox.com/smarteresolutions](http://www.xerox.com/smarteresolutions).

## At Your Workstation

1. Open your Web Browser and enter the TCP/IP address of the machine in the Address or Location field and press **Enter**.
2. Click the **Properties** tab.
3. Click the symbol to the left of **General Setup**.
4. Click the symbol to the left of **Smart eSolutions**.
5. Click **Registration**.
6. Click **Enable Proxy Server**. **Note:** If your network does not require a Proxy Server, you can skip to step 13 below. You will, however, need to have DNS settings enabled (see TCP/IP Protocol Configuration in this guide).
7. Place a check mark in the **Use Proxy Server** box.
8. In the **Addresses to Bypass Proxy Server** box, enter in up to 1024 characters of IP addresses, fully qualified host names, or wildcard host names (such as \*.eng), separated by semicolons. Functioning like the local address exception list in a typical web browser, these addresses will be permitted to bypass the Proxy Server.
9. For the **HTTP or HTTPS Server Names**, provide a name of up to 255 characters in length for one or both of these Proxy Servers. A fully qualified domain name or IP address can be used. **Note:** Make sure that DNS is enabled as stated in the TCP/IP Protocol Configuration topic in the NOS Selection section of this guide.
10. Leave the Port Number set to 8080 (the IANA recognized proxy port) unless you are using a different port number.
11. Click **Apply** and supply the administrator User Name and Password, if prompted. The default is 11111 and x-admin.
12. If necessary to see the list of Registration hot links again, click your browser Back button.
13. Click **Register with Xerox Communication Server** to register this device with the Xerox Communication Server (Edge Host), which enables the automatic billing meter reading service. After registration, the device will poll the Edge Host routinely, and send meter readings only in response to requests from the Edge Host.

14. Place a check mark in the **Request Registration** box and **Server Communication** box. Note that you can now schedule Xerox Communication Server polling time. Make sure to check the server communication Enabled box.
15. Click **Apply** and supply the administrator User Name and Password, if prompted.
16. If necessary, use your browser Back button again, then click on **Setup E-mail Notification** to send billing meter (or supplies data) read notifications to the locally designated Administrator.
17. Enter the e-mail address of the designated Administrator in the box(es) supplied.
18. Place a check mark in the boxes associated with the type of notifications you wish to have e-mailed.
19. Click **Apply** and supply the administrator User Name and Password, if prompted. The default is 11111 and x-admin.
20. Click on the Meter Assistant or Supplies Assistant links at any time to see the status of your communications.

# Machine Software Upgrades

To upgrade, you must first obtain the upgrade software and then install it.

## Prepare for the upgrade

It is important to obtain the correct upgrade file for your machine. Determine the software version you are currently running, as follows:

1. Open your web browser and enter `http://` and the TCP/IP address of the machine in the Address or Location field, then press [Enter].
2. Click the [Properties] tab.
3. Click the [General Setup] folder.
4. Click [Configuration].
5. Scroll down to the Software section to see your System Software version. Write down the version number. Note whether the Controller ROM is listed as Controller ROM or Controller + PS ROM. This will determine which file to download from Xerox.com.
6. Download the software file:
  - a. Obtain the new software upgrade file (Controller ROM or Controller + PS ROM) for your machine from the [www.xerox.com](http://www.xerox.com) web site, or from your Xerox Customer Support Representative.
  - b. Download the upgrade file to a local or network drive.  
You will be able to delete the file after the upgrade procedure.
  - c. Extract the .bin file from the .zip archive.

## At your workstation

1. Verify that the machine is up and running, and is not in PowerSaver mode.
2. Open your web browser and enter the TCP/IP address of the machine in the Address or Location field, then press [Enter].
3. Click the [Properties] tab.
4. Click the [Services] folder.
5. Click the [Machine Software] folder.
6. In the [Machine Software] folder:
  - a. Click [Upgrades]. Click or verify the Enabled check box, then click [Apply].
  - b. Click [Manual Upgrade]. Click [Browse] and move through your file system to the new software. Click [Install Software] to install the software.

*Note: The Manual Upgrade link provides the ability to upgrade software manually, after enabling through the Upgrades link.*

# NOS Selection

## TCP/IP Protocol Configuration

To view or change the settings of the Device's TCP/IP Protocol Configuration, perform the following steps:

### To access the TCP/IP Protocol Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Protocol Settings**.
8. When the Protocol Settings menu displays, note that with the exception of selection one (Ethernet Rated Speed), the remaining selections are specific to TCP/IP address settings. Choose your setting of interest by pressing the numbered, horizontal selection line on the touch screen. Note that the current status of each setting is shown on the applicable line. After pressing a selection line, to access available settings press the **Change Settings** button in the lower right corner of the touch screen.

### **Ethernet Setting (Ethernet Rated Speed)**

9. On the Protocol Settings menu, press the selection line labeled **Ethernet Rated Speed**.
10. Press the **Change Settings** button.
11. On the settings screen, note which one of the buttons is highlighted as the current setting for Ethernet Speed. The available settings are **Auto** (10 / 100 Mbps), **100 Mbps** (Half or Full Duplex), and **10 Mbps** (Half or Full Duplex). By default the Ethernet Port Configuration will be set to **Auto**.
12. To change settings, press your setting of choice, then press the **Save** button.
13. To exit the screen, without making any changes, press the **Cancel** button.

### **TCP/IP – IP Mode**

14. Press the selection line labeled **TCP/IP – Mode**.
15. Press **Change Settings**.
16. Select the IP Mode best suited to your network environment. Note that your choices include IPv4 Mode, IPv6 Mode, and Dual Stack. The device supports IPv6 addressing with an automatically-built Link Local Address for broadcasting to routers that can supply the network layer configuration parameters.
17. For traditional networks (using an address space of xxx.xxx.xxx.xxx), select IPv4 and press **Save**.
18. Note that the machine may reboot.

### **IP Address Resolution**

19. On the Protocol Settings menu, press the selection line labeled IPv4 (or other mode) Address Resolution.
20. Press the **Change Settings** button.
21. On the settings screen, note which one of the buttons is highlighted as the current setting for the TCP/IP Addressing method. The available settings are DHCP, BOOTP, RARP, DHCP/Autonet, and STATIC. DHCP/Autonet is the factory default setting.
22. To change settings, press your selection of choice, then press the **Save** button.
23. To exit the screen, without making any changes, press the **Cancel** button.
24. Press **Close** and, if you made any changes, the system will reboot.

### IPv4 IP Address

1. Used for static IP Addressing (with "STATIC" selected as your addressing method), on the Protocol Settings menu, press the selection line labeled **IPv4 Address**. Note that the IP Address may be viewed, but not changed, with dynamic addressing enabled.
2. Press the **Change Settings** button.
3. On the settings screen, use the numeric keypad to enter in the appropriate IP Address.
4. To save settings, press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### IPv4 Subnet Mask

1. Used for static IP Addressing (with "STATIC" selected as your addressing method), on the Protocol Settings menu, press the selection line labeled **IPv4 Subnet Mask**. Note that the Subnet Mask may be viewed, but not changed, with dynamic addressing enabled.
2. Press the **Change Settings** button.
3. On the settings screen, use the numeric keypad to enter in the appropriate Subnet Mask.
4. To save settings, press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### IPv4 Gateway Address

1. Used for static IP Addressing (with "STATIC" selected as your addressing method), on the Protocol Settings menu, press the selection line labeled **IPv4 Gateway Address**. Note that the Gateway address may be viewed, but not changed, with dynamic addressing enabled.
2. Press the **Change Settings** button.
3. On the settings screen, use the numeric keypad to enter in the appropriate Gateway.
4. To save settings, press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### IPv4 IP Filter (IP Address Restriction)

1. Use your workstation's web browser to access the Internet Services (web pages) residing on the Device to set the IP Address or Addresses to use with this feature BEFORE enabling the feature, either here or with Internet Services. This will prevent unintentionally locking yourself out from communicating with the Device from your own IP address. For full instructions, refer to the **IP Filtering (IP Address Restriction)** topic in the **Internet Services** section of this guide.
2. In the Protocol Settings menu, press the selection line labeled **IPv4 IP Filter**.
3. Press the **Change Settings** button.
4. On the settings screen, note which of the two buttons is highlighted as the current setting for IP Address restriction. The available settings are **Enabled** or **Disabled**. **Disabled** is the factory default setting.
5. To change settings, press your setting of choice, then press the **Save** button.
6. To return to the Protocol Settings menu, without making changes, press the **Cancel** button.

### **Exiting the Protocol Settings Menu and returning to the Device's Tools tab screen**

1. To exit the Protocol Settings menu, returning to the Tools tab screen, press the rectangular **Close** button in the upper right corner of the Protocol Settings menu screen.
2. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Protocol Settings menu, the Device will automatically reboot to register and enable your new settings.*



# TCP/IP LPD Enablement

To support TCP/IP printing through the workstation's LPR port in the case of Windows XP, the LPD (Line Printer Daemon) MUST be enabled at the device.

To view or change the Device's LPD setting, perform the following steps:

## To access LPD Settings at the Device

1. Press the rectangular **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. When the Port Settings menu displays, press the selection line labeled **LPD**.
9. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
10. When the LPD selections menu displays, note that you have a choice of setting selections by numbered horizontal lines, with the current status of each setting shown. The Close button in the upper right corner of the screen returns you to the Port Settings menu. After pressing the selection, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Port Status (LPD Enablement)

1. On the LPD selections menu, press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the LPD Port Status screen, note which of the two buttons is highlighted as the current setting for LPD Enablement. The available settings are Enabled or Disabled. For the LPD to function, it must be set to Enabled.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### LPD Port Number

1. On the LPD selections menu, press the selection line labeled **LPD Port Number**.
2. Press the **Change Settings** button.
3. Note the setting of **Port 515**, which is the recommended, default value. To change the setting, use the keypad displayed on screen.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### LPD Maximum Number of Sessions

1. Select **LPD – Maximum Number of Sessions**.
2. Press **Change Settings**.
3. Select a number from 1 to 10.
4. To change settings, press **Save**.
5. To exit, without making changes, press **Cancel**.

### Exiting the LPD Selections Menu

To exit the LPD selections menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

### Exiting the Port Settings Menu and returning to the Device's Tools tab screen

1. To exit the Port Settings menu, returning to the Device's Tools tab screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
2. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

# TCP/IP Dynamic Addressing

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus symbol (+) to the left of the **Connectivity**, then the **Protocols** file folder.
4. Select **TCP/IP** in the directory tree
5. Review the available selections as displayed on your screen and explained in the **TCP/IP Configuration Selection List**, below.
6. Accept the default Host Name, or type in your own unique Host Name for this Device.
7. Select DHCP or BOOTP as your method for obtaining an IP Address.

**CAUTION:** Changing the IP address for the Device will affect LPR/LPD, FTP, SNMP, and Port 9100 printing. It will also interrupt the ability to communicate with the device using the Internet Services (series of web pages on the Device). When you change the Device's IP Address, make sure to print out a Configuration Report (as stated in this guide) so that you have a record of the TCP/IP addresses for use with workstations that need to communicate with the Device using TCP/IP.

*Note:* When using DHCP, set a reasonably long Lease Time for the IP Address so that the Device can be shut down and serviced, when required, without being continuously assigned a new IP Address.

*Note:* Upon rebooting, when the system comes up, if it can't locate a DHCP server on the network it will use whatever IP address it was previously configured with.

8. Determine the method to use to supply the DNS Server IP Addresses (to resolve Host Names with IP Addresses).
9. Determine whether or not Dynamic DNS should be enabled.
10. Click **Apply** when done.

## **TCP/IP Configuration Selection List**

As displayed on your screen, the following selections are available for TCP/IP Configuration.

### **IP Mode**

Select the IP Mode that applies to your network environment.

### **General**

Host Name. The default entry assures a name that is unique to this device on the network.

IP Address Resolution. Use this drop-down menu to select the method to use to assign IP Addresses. Select STATIC, DHCP, RARP, BOOTP, or DHCP/Autonet.

Note that with the Autonet option selected, if a Windows 2000 client can't contact the DHCP server, it will assign itself an IP address from the 169.254.0.0 class B address space. This is also known as zero configuration, or Bonjour, networking. Make sure to check the Enabled box for Self Assigned Address at the bottom of your screen.

IP Address entry box. To be filled in manually ONLY when Static addressing is selected.

Subnet Mask entry box. To be filled in manually ONLY when Static addressing is selected.

Gateway Address entry box. To be filled in manually ONLY when Static addressing is selected.

### **Domain Name**

Enter the fully qualified domain name here. For example: xerox.com.

### **DNS Configuration**

DHCP Address Resolution check box. If enabled with a check mark, the Device will contact the DHCP Server for the IP Addresses of up to three DNS Servers. If unchecked, this information must be entered manually.

Three DNS Address boxes are supplied for the manual entry of DNS Server addresses.

Dynamic DNS Update Box. If your DNS Server does not support dynamic IP address updates there is no need to enable this checkbox. Check the Overwrite box to enable DNS information overwriting.

Generate Domain Search List Automatically. A check box is provided for enabling automatic Domain searches.

Domain Names 1,2,3. Three text boxes are provided for the entry of Domains to search (for example, Xerox.com).

Connection Timeout. An entry box is provided for entering a Timeout for searches of Domains.

### **Zero Configuration Networking**

Used with DHCP/Autonet selected from the IP Address Resolution drop-down menu, when this box is checked the device will assign itself an IP address from the 169.254.0.0 class B address space.

*Note: Changes to TCP/IP settings will not be applied until you restart (reboot) the Device.*

# IP Filtering (IP Address Restriction)

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus symbol (+) to the left of the **Security** file folder.
4. Select **IP Filtering**.
5. In either the IPv4 area or the IPv6 area, complete the following steps.

*Note: IPv4 is the traditional (xxx.xxx.xxx.xxx) address space used with TCP/IP networks.*

  - a. To allow universal, unrestricted access to the device, clear the **Enabled** check box.
  - b. To restrict access to specific IP Addresses and Subnet Masks:
    - Click the **Enabled** check box.
    - Click **Add** or **Edit** to add or edit an IP address from which you intend to accept jobs. Click **Apply**.

*Note: IP filtering will not work until at least one IP address has been added. This prevents turning off ALL access to the device.*
    - Click **Delete** to delete an IP address. Click **Apply**.
6. Click **Apply** when done.
7. Send a test job.

# Configure Port 9100 (Raw Printing)

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
  2. Click the **Properties** tab.
  3. Click the plus (+) symbol to the left of the **Connectivity**, then the **Protocols** file folder.
  4. Select **Port 9100** in the directory tree. (1)
  5. The available selections include:
    - TCP Port Number, with a default value of 9100. This value typically does not need to be changed.
    - A TBCP Filter checkbox (displayed when PostScript is enabled). Click Help for an explanation of the use of this feature.
    - Connection Time-out Entry Box.
  6. Enter a **Time Out** value for jobs being sent to the Device through this Port. This is the length of time that the Controller will wait for an end of job command before printing the current job.
  7. Click the **Apply** button to accept changes, or the **Undo** button to return settings to their previous values. Note: Setting changes are not applied until you restart the Device.
- (1) Note: If Port 9100 is NOT displayed in the Properties Tab directory tree, click the **Port Status** hot link in the **Connectivity** folder in the tree. In the Port Status table, use your mouse to place a check mark in the checkbox on the Port 9100 line. Click the **Apply** button, then click the **Reboot** button (always available on the Status Tab) to remotely reboot the Device.

# Microsoft (NetBIOS over IP) Networks

## Before You Start

1. Print a **Configuration Report** as stated in the **Network Connectivity** section of this guide.
2. Referring to the report, **verify that SMB is enabled**. To enable SMB at the Device, if required, follow the procedure below.
3. Referring to the Configuration Report, **verify that DNS is enabled**. The use of Naming Servers is REQUIRED to resolve NetBIOS device names to IP addresses for packet routing over the TCP/IP network.
4. To enable the Device to communicate with the Naming Servers, refer to the instructions supplied in the topic "TCP/IP Dynamic Addressing", located in the **NOS Selection** section of this guide.
5. When using WINS or DNS, be sure to refer to your Server Operating System documentation for the appropriate procedure to use to enable NetBIOS name to IP address resolution on the Server.

## Enabling the SMB Setting at the Device, if required

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.

7. Press **Port Settings**.
8. When the Port Settings menu displays, press the **SMB** selection line.
9. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
10. When the SMB selection menu displays, note that you have only one setting available on a single, numbered horizontal line. Press this selection line.
11. Press the **Change Settings** button.
12. On the SMB Port Status screen, note which of the two buttons is highlighted as the current setting for SMB Enablement. The available settings are Enabled or Disabled. To enable SMB at the device, select the **Enabled** setting.
13. Press the **Save** button on the touch screen, which returns you to the SMB selection menu. (To exit the screen, without making changes, press the **Cancel** button.)
14. Exit the SMB selection menu and return to the Port Settings menu by pressing the rectangular **Close** button in the upper right corner of the touch screen.
15. Exit the Port Settings menu by pressing the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
16. To exit the Tools tab screen, wait several seconds for the Auto Clear service to log you out.



## Viewing or Configuring the SMB Host Name or WINS Server with Internet Services

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **Microsoft Networking** in the directory tree.
5. The available selections include:
  - A drop-down menu for Transport.
  - A text box indicating Workgroup name.
  - A text box indicating the SMB Host name.
  - An entry box for the maximum number of connections allowed, labeled Maximum Connections.
  - A TBCP Filter checkbox (displayed when PostScript is enabled). Click Help for an explanation of the use of this feature.
  - An enabling checkbox for supporting Unicode (supplying the Host name and Workgroup name in Unicode characters during SMB transmission).
  - An enabling checkbox for Auto Master Mode. When the master browser for the workgroup cannot be found, if this box is checked, this host will become the master browser.
  - An enabling checkbox for Password Encryption (during SMB transmission).
  - A WINS Server configuration section – for using a WINS Server to resolve NetBIOS names (SMB host names) to IP addresses.
6. Select TCP/IP from the Transport menu.
7. Accept the default value, or enter a value from 3 to 10, for maximum number of connections allowed in Maximum Connections.
8. Accept the Workgroup name shown, or enter in your own workgroup name.
9. Either accept the default **SMB Host Name**, which is automatically built by the Device to assure the name's uniqueness, or enter in your preferred name. Note that this will be the NetBIOS name that is resolved by the Naming Server (DNS or WINS) to an IP Address for the Device.
10. If using a WINS server, enable the WINS Server Address Resolution check box. When enabled, the Device will contact the DHCP Server for the IP Addresses of the Primary and Secondary WINS (Windows Internet Naming Service) Servers. Note that two IP Address lines, with entry boxes, are provided for manual entry (when DHCP is not selected).
11. To apply setting changes, click the **Apply** button, then click the **Reboot** button to reboot the device. To exit without making any changes, click the **Undo** button.

**Note regarding DNS/WINS NetBIOS Name Resolution**

To use the Device's NetBIOS name over the TCP/IP Network, the DNS and WINS Servers **MUST** be configured for NetBIOS name to IP address resolution. Also, make sure that the Device is informed of the addresses of the DNS/WINS Servers, using the instructions supplied in the TCP/IP Dynamic Addressing and Microsoft (NetBIOS over IP) Networks topics of this guide.

**To Set Up a Workstation to Print Directly to the Device**

Refer to the set up instructions supplied for **NetBIOS over IP Peer to Peer Printing** in the **Print Drivers** section of this guide.

# IPP Configuration

The Internet Printing Protocol provides a convenient way to print over the Internet or Intranet using the device's IP address. To support this type of printing, make sure that Port 9100 is enabled at the device as stated in the Note at the bottom of the **Configure Port 9100** procedure, in the **Internet Services** section of this guide. Specifically, click the Port Status link in the Connectivity folder on the Properties Tab of Internet Services and make sure that the check box on the Port 9100 line is checked. The Internet Printing Protocol must also be enabled at the device, and the Internet Print Service must be available and installed on the individual workstation's version of Windows. IPP support is already built into Windows 2000 and XP. For other desktop operating systems it is available as a download from Microsoft at [www.microsoft.com](http://www.microsoft.com). The final step is to install the IPP print driver, which is covered in the **Print Drivers** section of this guide.

## To access IPP Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. Press the **IPP** selection line on the Port Settings menu.
9. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
10. When the IPP selection menu displays, note that you have two selections available on numbered horizontal lines. The first selection is Port Status. The second is IPP – Added Port Number. The Close button in the upper right corner of the screen returns you to the Port Settings menu. After pressing the horizontal line selection, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Port Status (IPP Enablement)

1. On the IPP selection menu, press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the IPP Port Status screen, note which of the two buttons is highlighted as the current setting for IPP Enablement. The available settings are Enabled or Disabled. To print with IPP, this setting must be **Enabled**.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

## IPP – Added Port Number

*Note: If you just enabled the IPP port, the machine may have to reboot before you can view or change the Port Number.*

1. On the IPP Selection menu, press the selection line labeled **IPP – Added Port Number**.
2. Press the **Change Settings** button.
3. Use the displayed keypad to add a Port Number, such as 80 (the displayed default for HTTP).
4. To save the setting, press **Save**.
5. To exit the screen, without making any changes, press **Cancel**.

## Exiting the IPP Selection Menu

To exit the IPP selection menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

## Exiting the Port Settings Menu and returning to the Tools tab screen

1. To exit the Port Settings menu, returning to the Tools tab screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
2. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

## Configuring IPP Settings with Internet Services

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **IPP** in the directory tree.
5. The available selections include:
  - Port Number, with a default value of 631. This is the port number assigned by IANA (Internet Assigned Numbers Authority).
  - Additional Port Number Entry box.
  - A TBCP Filter checkbox (displayed when PostScript is enabled) Click Help for an explanation of the use of this feature..
  - Administrator Mode Checkbox. This is disabled by default. Consult the On-Line Help for use of this feature.
  - DNS Enablement Checkbox.
  - Connection Timeout Entry Box.
6. Verify that the **DNS** Enablement Checkbox is checked (enabled) by default. If enabled, the DNS Server will resolve Host Names to IP Addresses, in support of printing with IPP.
7. Enter a **Time Out** value for jobs being sent to the Device through this Port. This is the length of time that the Controller will wait for an end of job command before printing the current job.
8. Click the **Apply** button to accept changes, or the **Undo** button to return settings to their previous values. Note: Setting changes are not applied until you restart the Device.

# EtherTalk (AppleTalk) Configuration

The EtherTalk Protocol enables workstation to Device communications over the EtherTalk (AppleTalk) network.

## To access EtherTalk Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status button** on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. Press the **EtherTalk** selection line on the Port Settings menu.
9. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
10. When the EtherTalk selection menu displays, note that you have only one selection available on a single, numbered horizontal line, with the current status of this setting shown. The Close button in the upper right corner of the screen returns you to the Port Settings menu. After pressing the horizontal line selection, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Port Status (EtherTalk Enablement)

1. On the EtherTalk selection menu, press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the Port Status screen, note which of the two buttons is highlighted as the current setting for EtherTalk Enablement. The available settings are Enabled or Disabled. To print with EtherTalk, this setting must be **Enabled**.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

## Exiting the EtherTalk Selection Menu

To exit the EtherTalk selection menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

## Exiting the Port Settings Menu and returning to the Tools tab screen

1. To exit the Port Settings menu, returning to the Tools tab screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
2. Wait several seconds for the Auto Clear service to log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

## Configuring EtherTalk Settings with Internet Services

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** Tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **AppleTalk (EtherTalk)** in the directory tree.  
*Note: If this selection is unavailable, click on the Port Status hot link, check the EtherTalk box, then click Apply.*
5. The available selections include:  
Printer Name.  
Zone Name.
6. Enter the name that you wish to assign to this Printer. This is the name that will appear in the Chooser.
7. Either accept the default zone of \* which lets the closest router assign the Device to a zone, or assign the Device to a zone (with a 32 character naming limit).
8. Click the **Apply** button to accept changes, or the **Undo** button to return settings to their previous values. Note: Setting changes are not applied until you restart (reboot) the Device.



# AS400 Printing

## AS400 Raw TCP/IP Printing to Port 9100 (CRTDEVPRT)

### Purpose

This is the procedure to set up printing to a multifunction device from an AS/400 using the SNMP drivers.

### Assumptions

This procedure is intended for users familiar with the AS/400 system, especially those experienced with printing in an AS/400 environment.

The AS/400 must run V4R5 of OS/400 so that the SNMP drivers are present (or V4R3/V4R4 with the most current PTFs installed).

The multifunction device must have port 9100 enabled.

### Procedures

#### To enable port 9100

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press [Enter].
2. Click the [Properties] tab.
3. Click the symbol to the left of [Connectivity].
4. Click the symbol to the left of [Protocols].
5. Select [Raw TCP/IP Printing] in the directory tree.
6. Ensure the [Enabled] box is checked to enable Raw TCP/IP Printing.
7. Leave the [TCP Port Number] set to 9100 for Port 1.
8. Leave the [Bidirectional] and [Maximum Connections] settings at their default values.
9. Set the [End of Job Timeout] to the number of seconds to wait before processing a job without an End Of Job indicator.
10. Leave the [PDL Switching] Enabled box at its default value.
11. Click [Apply] to accept the changes, [Undo] to return the settings to their previous values, or [Default All] to enter printer defaults for all settings (recommended). NOTE: The settings are not applied until you restart the machine.
12. Click the [Status Tab] link.
13. Click the [Reboot Machine] button and click [OK] to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

#### To create an SNMP trap

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press [Enter].
2. Click the [Properties] tab.
3. Click the symbol to the left of [Connectivity].
4. Click the symbol to the left of [Protocols].
5. Select [SNMP] in the directory tree. You may be prompted for the current tools administrator user name and password. The default is [admin] and [1111]. Click [OK].
6. Check the [Enable] box to enable the protocol.
7. To edit SNMP properties click [Edit].

8. The default [TRAP Community Name] is SNMP\_trap, which you can use without changing. The Default TRAP community name is used to specify the default community name for all traps generated by this machine.
9. Click your browser Back button to return to the SNMP Configuration page, then click the [Advanced] button.
10. Click [Add IP Address] in the Trap Destination addresses box.
11. Enter the multifunction device's IP address and leave all other parameters at their default values.
12. Click [Apply] to accept the changes.
13. When finished, click [Apply] to accept the changes.

### **To identify the trap**

To identify the trap, create a device description from your terminal's command line.

1. Select the F-4 key to prompt the CRTDEVPRT command. Enter the following parameters:
  - Device Description: Xeroxprinter
  - Device Class: \*lan
  - Device Type: 3812
  - Device Model: 1

2. Press Enter to continue, and enter the following parameters:

- Lan Attachment: \*IP
- Port Number: 9100
- Online at IPL: \*yes
- Font Identifier: 11
- Form Feed \*autocut

*Note: For some versions of AS400, the default may match some of these parameters.*

3. Leave all other parameters at their defaults, press Enter, and enter the following parameters:

- Activation Timer: 170
- Inactivity Timer: \*sec15
- Host Print Transform: \*yes

4. Press [Enter] to continue, and enter the following parameter:

- Manufacturer Type and Model: \*hp5si

5. Leave the remaining parameters set to their default values and press Enter to continue. Enter the following parameters:

- Remote Location: Enter the IP address of the printer.
- User defined options: \*IBMSHRCNN
- System driver program: \*IBMSNMPDRV

6. Leave all other options set to the default values and press Enter. A message indicates that you created the device Xeroxprinter.

7. Set the device on and start a print writer. Then place a spool file in the appropriate queue to test the printer.

## AS400 Printing using LPR (CRTOUTQ)

### Creating a remote queue (LPR) on the AS400

At the command line, issue CRTOUTQ and press F4, then F9 for additional parameters. The setup is as follows:

Output queue: **queue name**

Library: **Library name**

Maximum spooled file size

Number of pages: \*NONE

Starting time: Time

Ending time: Time

Order of files on queue: \*FIFO

Remote system: \*INTNETADR

Remote printer queue: **virtual printer name\*\*** (queue for WorkCentre should be lp (lower case L and P))

Writers to autostart: 1

Queue for writer messages: QSYSOPR

Library: \*LIBL

Connection type: \*IP

Destination type: \*OTHER

Transform SCS to ASCII: \*YES

Manufacturer type and model: \*IBM42011 \*\*\*SEE NOTE BELOW\*\*\*

Workstation customizing object: xxxxxxxx (leave as default)

Library: xxxxxxxx (leave as default)

Internet address: xx.xxx.x.xx (IP address of printer)

VM/MVS class: \*SAME

Forms control Buffer: \*SAME

Destination options: **XAIX**

Text description:

Display any file: \*NO

Job separators: 0

Operator controlled: \*YES

Data Queue: \*NONE

Library:

Authority to check: \*DTAAUT

Press <enter> to create. Note that the Workstation Customizing Object is the file that was created in the previous step (step 2).

**ONLY CHANGE THE PARAMETERS IN BOLD.**

At this point, a spool file (document) should be able to be sent tot he WorkCentre.

*Note: If printing PCL, set this parameter to **HP5Si** (most of the HP drivers will work) and set Workstation customizing object as **\*none**.*

If printing ASCII, set this parameter to **\*IBM42011** (which is the default).

# Print Drivers

## TCP/IP Peer to Peer (LPR or Standard TCP/IP) Printing

### Windows 2000 Server\Professional & XP Professional (& Vista) Print Driver Installation

#### Before you start

Obtain the Print Driver for your workstation's operating system. Drivers are available on one of the CD-ROMs that came with your Device. They are also typically available for downloading in self-extracting Zip file format from the Internet at [www.xerox.com](http://www.xerox.com).

#### Verify that TCP/IP is installed in the workstation

On the Windows 2000 Desktop, right mouse click the **My Network Places** icon and select **Properties**. Right mouse click on the **Local Area Connection** icon and select **Properties**. On the Windows XP desktop, click **Start, Control Panel**, and double click **Network Connections**. Right mouse click on the **Local Area Connection** icon and select **Properties**. Verify that the **Internet Protocol (TCP/IP)** has been loaded. If it has, click on (highlight) this item with your mouse and click the **Properties** button to verify that this workstation is using either a dynamic or static method to obtain a valid TCP/IP address. If the TCP/IP protocol is NOT loaded, click the **Install...** button, then select **Protocol** as the type of network component that you wish to install. Click the **Add...** button and select **Internet Protocol (TCP/IP)**. With your Operating System Installer Disk readily available, click the **Have Disk...** button and follow any remaining instructions. Once the protocol has been installed, you can click on (highlight) the item with your mouse and click the **Properties** button to verify or set up the method being used for TCP/IP addressing.

#### Verify that Print Services for Unix is installed in the workstation (see Note below)

Note: You can skip this step and proceed directly to "Adding the Printer to the Desktop," if you prefer printing through the "Standard TCP/IP Port" (Port 9100), rather than through an LPR port.

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings, Control Panel**, then double-click **Add/Remove Programs**. On the Windows XP desktop, click **Start, Control Panel**, then double click **Add or Remove Programs**.
2. Select **Add/Remove Windows Components**. On Windows 2000 Professional you will need to be logged in with Administrator rights to perform this function.
3. Select **Other Network File and Print Services** and click **Details**.
4. Check the box to select **Print Services for Unix**. Click **OK** and **Next**. You will need to supply the Operating System Installer disk, when prompted. Close the Add/Remove Programs window.

### **Add the Printer to the Windows 2000 or Windows XP/Vista Desktop**

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**. The Vista path is Start\Control Panel\Printer(s).
2. On Windows 2000 or XP, double-click **Add Printer**.
3. When the "Add Printer Wizard" screen displays, click **Next**.
4. Select **Local Printer** and deselect "Automatically detect and install my Plug and Play printer." Click **Next**.
5. Select **Create a new port** and choose **LPR** from the **Type** drop-down menu. (LPR becomes available when Print Services for Unix is installed, as above). Note: If you prefer to print raw data to Port 9100 on the Printer, you can alternatively choose **Standard TCP/IP Port**. Click **Next**.
6. When prompted, enter the **IP address** of the printer.
7. Enter a name for the print queue (such as **raw**). If you selected the Standard TCP/IP port, you can accept the default name provided by Windows. Click **Next**.
8. You will be prompted for a print driver. Select **Have Disk** and browse to the location of your print driver.
9. Select the **.INF** file, then click **Open**.
10. When the "Install from Disk" screen displays, verify that the path and file name are correct and click **OK**.
11. Select the model that corresponds to your Printer and click **Next**.
12. Enter a name for your Printer and select either Yes or No for making this printer your default Windows printer. Select **Yes** if you will be printing primarily to this printer from your Windows applications. Click **Next**.
13. If the Printer Sharing Screen displays, select "Do not share this printer," unless the Printer is directly connected to your workstation and you wish to Share it with other network users. Click **Next**.
14. Select **Yes** to print a test page. Click **Next**.
15. Click **Finish**.

### **Configure the Print Driver**

16. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**. The Vista path is Start\Control Panel\Printer(s).
17. Right click on the Printer's icon and select **Properties**. Use the available Tabs to set the Printer's job processing defaults, including enabling Bi-Directional Communication. Additional settings may be accessed by clicking the **Printing Preferences** button on the General Tab.

# NetBIOS over IP Peer to Peer Printing

## Before You Start

1. Obtain the Print Driver for your workstation's operating system. Drivers are available on one of the CD-ROMs that came with your Device. They are also typically available for downloading in self-extracting Zip file format from the Internet at [www.xerox.com](http://www.xerox.com).
2. Print a **Configuration Report** as stated under the **Network Connectivity Tab** of this guide.
3. On the Configuration Report, **verify that "SMB" is enabled**. Also, **verify that TCP/IP is enabled** as one of the supported protocols. Verify that the **workgroup's default name is Workgroup**, or a valid, 15 character maximum, workgroup name. Also note the **Device's SMB Host Name** (which assures the uniqueness of the Device's name within the Workgroup). To enable "SMB," if required, follow the procedure stated under the Microsoft (NetBIOS over IP) item of the NOS Selection menu, accessed from the **Network Connectivity Tab** of this guide. To modify the name of the Workgroup, or Device's name (SMB Host name) within the workgroup, use your workstation's Web browser to access the Internet Services (Web Pages) residing in the Device, as described under the Configure SMB menu item, under the **Internet Services Tab** of this guide.
4. Make sure to configure the DNS/WINS Server(s) for NetBIOS name to IP address resolution. Then provide the Device with the addresses of the Servers as stated in the **Configure TCP/IP Settings** procedure of the Internet Services section of this guide.

## An Alternate Procedure for Setting up NetBIOS over IP Peer to Peer Printing

EXPERIENCED SYSTEMS ADMINISTRATORS can use the following procedure:

1. **On Windows 2000 and XP workstations**, from the "Properties selection" of the "Local Area Connection" icon, verify that the **Internet Protocol (TCP/IP)** is installed. Select the protocol and click **Properties**. Verify that TCP/IP is configured for use of the DNS Server. Click the **Advanced** button and select the **DNS** Tab. Verify that the checkbox labeled "Register this connection's addresses in DNS" is checked. Select the **WINS** Tab and verify that the NetBIOS setting is set to either "Use NetBIOS Setting from the DHCP Server," or that "NetBIOS is enabled over TCP/IP." Click Cancel twice and verify that the **Client for Microsoft Networks** is installed. Finally, with your Operating System Installer Disk readily available, through **Add/Remove Programs** and **Add/Remove Windows Components**, select Other Network File and Print Services. Click Details, check the box for **Print Services for Unix**, and click OK and Next.
2. When prompted for the "Name or address of server providing lpd" enter in the Device's **SMB Host Name** as seen on the Device's Configuration Report.
3. When prompted for a queue name, enter in your preference of an easily-identified name for this Printer.
4. Install the Print driver on your workstation and, when prompted to select a port to print through, select the LPR port that you just created.
5. Print a Test Print to verify successful communications with the printer.



# NetBIOS over IP Client/Server Printing

## Before You Start

1. Obtain the Print Driver for your workstation's operating system. Drivers are available on one of the CD-ROMs that came with your Device. They are also typically available for downloading in self-extracting Zip file format from the Internet at [www.xerox.com](http://www.xerox.com).
2. Print a **Configuration Report** as stated under the **Network Connectivity Tab** of this guide.
3. On the Configuration Report, **verify that "SMB" is enabled**. Also, **verify that TCP/IP is enabled** as one of the supported protocols. To enable "SMB," if required, follow the procedure stated under the Microsoft (NetBIOS over IP) item of the NOS Selection menu, accessed from the **Network Connectivity Tab** of this guide.
4. The Workstation Print Driver Installation Procedures below ASSUME that you have already Set Up a Server to Queue Jobs to the Printer. If you have NOT already set up a Server, for a quick-step set up procedure, refer to the instructions supplied under the selection "Microsoft (NetBIOS over IP)," located in the **NOS Selection** menu, under the **Network Connectivity Tab** of this guide.

# Windows 2000 & XP Professional Workstation Print Driver Installation

## Verify that the Correct Protocols and Services are installed in the workstation

1. Verify that the **Internet protocol (TCP/IP)** is installed in the Workstation. On the Windows 2000 Desktop, right mouse click the **My Network Places** icon and select **Properties**. Right mouse click on the **Local Area Connection** icon and select **Properties**. On the Windows XP desktop, click **Start**, **Control Panel**, and double click **Network Connections**. Right mouse click on the **Local Area Connection** icon and select **Properties**. Verify that the **Internet Protocol (TCP/IP)** has been loaded. If it has, click on (highlight) this item with your mouse and click the **Properties** button to verify that this workstation is using either a dynamic or static method to obtain a valid TCP/IP address. Also verify that this workstation is using a **DNS (or WINS) Server** for resolution of the NetBIOS Host name (typically the same name as the computer's Internet host name). If the TCP/IP protocol is NOT loaded, click the **Install...** button, then select **Protocol** as the type of network component that you wish to install. Click the **Add...** button and select **Internet Protocol (TCP/IP)**. With your Operating System Installer Disk readily available, click the **Have Disk...** button and follow any remaining instructions.
2. Verify that the **Client for Microsoft Networks** is installed in the Workstation. On the Windows 2000 Desktop, right mouse click the **My Network Places** icon and select **Properties**. Right mouse click on the **Local Area Connection** icon and select **Properties**. On the Windows XP desktop, click **Start**, **Control Panel**, and double click **Network Connections**. Right mouse click on the **Local Area Connection** icon and select **Properties**. If the Client for Microsoft Networks is NOT loaded, click the **Install...** button, then select **Client** as the type of network component that you wish to install. Click the **Add...** button and select **Client for Microsoft Networks**. With your Operating System Installer Disk readily available, click the **Have Disk...** button and follow any remaining instructions.

### Add the Printer to the Windows 2000 or Windows XP Desktop

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**.
2. On Windows 2000, double-click **Add Printer**. On Windows XP, from **Printer Tasks**, select **Add a printer**.
3. When the "Add Printer Wizard" displays, click **Next**.
4. Select Network Printer and click Next.
5. In Windows 2000, on the "Locate Your Printer" screen, select the radio button labeled "Type the printer name or click next to browse for a printer." Click **Next**.
6. In Windows XP, on the "Specify a Printer" screen, select the radio button labeled "Connect to this printer (or to browse for a printer, select this option and click Next)." As a shortcut, if you know the UNC (Universal Naming Convention) of the Device, enter it in the text box. Click **Next**.
7. When the "Browse for Printer" screen displays, wait for the screen to finish loading its list of **Shared Printers**. Note that the displayed format for many of these Shared Printers is the UNC of the Printer (for example, \\computer (i.e. Server) name\share (i.e. Printer) name).
8. On the "Browse for Printer" screen, either click on (select with your mouse) one of the displayed Servers or UNC's, or enter into the text box the UNC of your Server and its Shared printer, if you know it. Click **Next**.
9. When prompted for the driver files, select **Have Disk** and browse to the location of your print driver.
10. Select the **.INF** file then click **Open**.
11. When the "Install from Disk" screen displays, verify the path and file name are correct and click **OK**.
12. Select the model that corresponds to your Printer and click **Next**.
13. Enter a name for your Printer and select either Yes or No for making this printer your default Windows printer. Select **Yes** if you will be printing primarily to this printer from your Windows applications. Click **Next**.
14. Select **Yes** to print a test page. Click **Next**.
15. Click **Finish**.

### Configure the Print Driver

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**.
2. Right click on the Printer's icon and select **Properties**. Use the available Tabs to set the Printer's job processing defaults, including enabling Bi-Directional Communication. Additional settings may be accessed by clicking the **Printing Preferences** button on the General Tab.

# IPP Printing (Windows 2000\XP\Vista)

*Note: Supported by all Windows 2000, XP, and Vista workstations, IPP (the Internet Printing Protocol) enables the convenience of printing over the Internet or Intranet through the creation of an IPP network port. This printing "service" is available for other workstation operating systems through downloads from the Microsoft web site. Follow the instructions provided by Microsoft, or other trusted sources on the Internet, to install the IPP service on operating systems other than Windows 2000 and XP.*

## Before You Start

1. Obtain the Print Driver for your workstation's operating system. Drivers are available on one of the CD-ROMs that came with your Device. They are also typically available for downloading in self-extracting Zip file format from the Internet at [www.xerox.com](http://www.xerox.com).
2. Print a **Configuration Report** as stated under the **Network Connectivity Tab** of this guide.
3. On the Report, under the TCP/IP data label, verify that the Device has a **valid IP Address, Subnet Mask, and Gateway** displayed. If it does NOT, assign these addresses to the Device following the procedure stated under the **TCP/IP Protocol Configuration** item of the NOS Selection menu, accessed from the **Network Connectivity Tab** of this guide.
4. On the Report, verify that **Port 9100** is displayed with a Port Status of **Enabled**. If it is NOT, enable Port 9100 as stated in the Note at the bottom of the **Configure Port 9100** procedure, under the **Internet Services Tab** of this guide. Specifically, click the Port Status hot link in the Connectivity folder on the Properties Tab of Internet Services and make sure that the check box on the Port 9100 line is checked.
5. On the Report, **verify that IPP is enabled**. If it is NOT, enable the protocol following the procedure stated under the **IPP (Internet Printing Protocol)** item of the NOS Selection menu, accessed from the **Network Connectivity Tab** of this guide.
6. **Verify that IPP is using DNS** to resolve Host Names to IP Addresses in support of IPP printing. Using your workstation's Web browser, enter the TCP/IP Address of the Device in the Address or Location field and press **Enter**. Click the **Properties** button or Tab. Click the plus (+) symbol to the left of **Connectivity**, then on the **Protocols** file folder and **select IPP** in the directory tree. Verify that the DNS Enablement Checkbox is checked. If it is NOT checked, check it with your mouse and click **Apply**.

## Verify that TCP/IP is installed in the workstation

On the Windows 2000 Desktop, right mouse click the **My Network Places** icon and select **Properties**. Right mouse click on the **Local Area Connection** icon and select **Properties**. On the Windows XP desktop, click **Start, Control Panel**, and double click **Network Connections**. Right mouse click on the **Local Area Connection** icon and select **Properties**. Verify that the **Internet Protocol (TCP/IP)** has been loaded. If it has, click on (highlight) this item with your mouse and click the **Properties** button to verify that this workstation is using either a dynamic or static method to obtain a valid TCP/IP address. If the TCP/IP protocol is NOT loaded, click the **Install...** button, then select **Protocol** as the type of network component that you wish to install. Click the **Add...** button and select **Internet Protocol (TCP/IP)**. With your Operating System Installer Disk readily available, click the **Have Disk...** button and follow any remaining instructions. Once the protocol has been installed, you can click on (highlight) the item with your mouse and click the **Properties** button to verify or set up the method being used for TCP/IP addressing.

## Add the Printer to the Windows 2000, Windows XP, or Vista Desktop

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**. The Vista path is **Start\Control Panel\Printer(s)**.
2. On Windows 2000, double-click **Add Printer**. On Windows XP, from **Printer Tasks**, select **Add a printer**.
3. When the "Add Printer Wizard" displays, click **Next**.
4. Select **Network Printer** and click **Next**.
5. To create an IPP printer select **Connect to a printer on the Internet.....**
6. Type **http://** followed by the printer's fully qualified Domain name or IP address in the URL field. Note that you may have to type **/ipp** after the Printer's name or IP address. The Printer's Name can be either the Internet Host Name or the SMB Host Name as shown on the Device's Configuration Report, depending on the name resolution used by your network (DNS or WINS).
7. Click **Next**.
8. When prompted for the driver files, select **Have Disk** and browse to the location of your print driver.
9. Select the **.INF** file then click **Open**.
10. When the "Install from Disk" screen displays, verify the path and file name are correct and click **OK**.
11. Select the model that corresponds to your Printer and click **Next**.
12. Enter a name for your Printer and select either Yes or No for making this printer your default Windows printer. Select **Yes** if you will be printing primarily to this printer from your Windows applications. Click **Next**.
13. Select **Yes** to print a test page. Click **Next**.
14. Click **Finish**.

### **Configure the Print Driver**

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**. The Vista path is Start\Control Panel\Printer(s).
2. Right click on the Printer's icon and select **Properties**. Use the available Tabs to set the Printer's job processing defaults, including enabling Bi-Directional Communication. Additional settings may be accessed by clicking the **Printing Preferences** button on the General Tab.

# EtherTalk (AppleTalk) Peer to Peer Printing

## Before You Start

1. Obtain the Adobe PostScript Print Driver for your Macintosh (OS 9.x) workstation. Drivers are available on one of the CD-ROMs that came with your Device. They are also typically available for downloading in self-extracting file format from the Internet at [www.xerox.com](http://www.xerox.com).
2. Print a **Configuration Report** as stated in the **Network Connectivity** section of this guide.
3. On the Report, under the **EtherTalk** data label, verify that the EtherTalk port is enabled, and that the Device has been assigned an EtherTalk (Printer) Name and an EtherTalk zone. If one or more of these parameters needs to be configured, follow the instructions supplied in the **EtherTalk (AppleTalk) Configuration** topic of the NOS Selection section of this guide.

## Load the Print Driver into your Macintosh workstation

1. Load the Drivers CD-ROM into your CD drive.
2. Open the CD and locate the Drivers folder.
3. Locate and open the Mac folder.

## Installation Instructions for 9.x

1. Double-click the installer file to install the printer driver on your Macintosh.
2. Click **Continue**.
3. Click **Agree** or **Accept** to accept the License Agreement.
4. Click **Install**.
5. Your Mac may need to be restarted. Click **Yes** to continue.
6. The driver will install. Select **Restart**.
7. Once the Mac has restarted, select **Apple**, then **Chooser**.
8. Select the printer icon, then select the Printer Name which corresponds to the name given to the device under the EtherTalk data label on your Configuration Report.
9. Select **Create**.
10. Select the PostScript Printer Description (PPD) that matches your machine model.
11. Click **Select**.
12. Click **Setup**.
13. Click **Configure**.
14. Select the installed options which correspond to your machine configuration.
15. Click **OK**.
16. Click **OK** and close the Chooser.
17. Print a document from an application to verify that the printer is installed correctly.

## Installation Instructions for 10.x (OS X)

1. Double click to open the folder containing the drivers for version 10.x.
2. Double click to open the [machine model.dmg].
3. Double click to open the [machine model.pkg] file.
4. When the Welcome screen displays, click **Continue**.
5. Click **Continue**, then **Agree** or **Accept** to accept the License Agreement.
6. Select the required disk (if necessary) where you want to install the printer. Click **Continue**.
7. Click **Install**.
8. Click **Close**, and restart the workstation.
9. When the workstation has restarted, double click the hard drive icon.
10. Double click the Applications icon.
11. Double click the Utilities folder.
12. Double click Print Center icon.
13. Double click **Add** to add a new printer.
14. Select AppleTalk as your network protocol.
15. Select the required AppleTalk zone.
16. Select the printer that you wish to set up.
17. Select the Printer Model (that is, choose the PPD for your printer).
18. Click **Add**.
19. Print a document from an application to verify that the printer is installed correctly.



# Common UNIX Printing System (CUPS)

## Overview

The Common Unix Printing System (CUPS) was created by Easy Software Products in 1998 as a modern replacement for the Berkeley Line Printer Daemon (LPD) and AT&T Line Printer (LP) system designed in the 1970's for printing text to line printers.

Currently available for downloading from a number of sources on the Internet, such as [www.cups.org](http://www.cups.org), CUPS is offered in both source code and binary distributions.

## Before You Start

Verify that IPP and Port 9100 are enabled at your device.

For instructions, refer to the **IPP Configuration** and **Configure Port 9100** topics in the **NOS Selection** section of this guide.

## Installing CUPS on the UNIX workstation

The instructions for installing and building CUPS are contained in the CUPS Software Administrators Manual, written and copyrighted by Easy Software Products and available for downloading at [www.cups.org/documentation.php](http://www.cups.org/documentation.php). An Overview of the Common UNIX Printing System, Version 1.1 by Easy Software is also available at this site.

A case history of the building and installation of CUPS source code on a FreeBSD 4.2 machine, is described in the article entitled Using CUPS--the Common UNIX Printing System, by Ralph Krause, available at [www.cups.org](http://www.cups.org), through the links/documentation/tutorials/BSD Today - Using CUPS selections. Directory locations for the CUPS files, as described in this article, are the following:

Programs were copied to /usr/local/bin and usr/local/sbin.

Documentation was copied to /usr/local/share/docs/cups.

A directory called /usr/local/share/cups was created for various CUPS data files.

The configuration files were copied to /usr/local/etc/cups.

The binary distribution of CUPS is available in tar format with installation and removal scripts, as well as in rpm and dpkg formats for RedHat and Debian versions of Linux. After logging into the workstation as root (su) and downloading the appropriate files to the root directory, the CUPS installation process begins as follows:

Tar format:

After untarring the files, run the installation script with `./cups.install` (and press Enter).

RPM format:

`rpm -e lpr`

`rpm -i cups-1.1-linux-M.m.n-intel.rpm` (and press Enter).

Debian format:

`dpkg -i cups-1.1-linux-M.m.n-intel.deb` (and press Enter).

Note: RedHat Linux, versions 7.3 and newer, include CUPS support, so software downloading is unnecessary. Also, CUPS is the default printing system used by Mandrake Linux.

## Installing the Xerox PPD on the workstation

The Xerox PPD for CUPS should be available on one of the CD-ROMs that came with your device and available for downloading from the Internet at [www.xerox.com](http://www.xerox.com).

From the CD-ROM or from the downloaded Internet file, with root privileges copy the PPD into your cups ppd folder on your workstation. If you are unsure of the folder's location, use the Find command to locate the ppd's. An example of the location of the ppd.gz files in RedHat 8.1 is /usr/share/cups/model.

## Adding the Xerox printer

1. Use the PS command to make sure that the CUPS daemon is running. The daemon can be restarted from Linux using the init.d script that was created when the CUPS RPM was installed. The command is `> /etc/init.d/cups restart`. A similar script or directory entry should have been created in System V and BSD. For the example of CUPS built and installed on a FreeBSD 4.2 machine from the source code, run `cupsd` from `/usr/local/sbin`. (`cd /usr/local/sbin` `cupsd` `press Enter`).
2. Type <http://localhost:631/admin> into the address (URL) box of your web browser and press Enter.
3. For User ID, type root. For the requested password, type the root password.
4. Click Add Printer and follow the on screen prompts to add the printer to the CUPS printer list.

## Printing with CUPS

CUPS supports the use of both the System V (`lp`) and Berkeley (`lpr`) printing commands.

Use the `-d` option with the `lp` command to print to a specific printer.

```
lp -dprinter filename (Enter)
```

Use the `-P` option with the `lpr` command to print to a specific printer.

```
lpr -Pprinter filename (Enter)
```

For complete information on CUPS printing capabilities, see the CUPS Software Users Manual available from [www.cups.org/documentation.php](http://www.cups.org/documentation.php).

# Options

## Enabling Options with Software Keys

Options such as **Scanning** (E-Mail, Mailbox, Network, Twain), **Security** (Disk Overwrite, Secure Watermark), **Internet Fax** (iFAX), **Server Fax**, and **Job Based Accounting**, require purchase and subsequent enabling with a supplied 12 character key before they will work. Software keys are usually included with the kit documentation as a sticker on the manual, or they may be already installed on the device as per the purchase agreement.

Upon receipt of the software key, use the following procedure to enable the associated Option.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Press the **Machine Status** button on the Control Panel.
4. Touch the **Tools** tab.
5. Touch **Common Service Settings**.
6. Touch **Maintenance**. Note that you may have to use the scrolling arrow to see this selection.
7. Touch **Software Options** and enter the key, using the on-screen keyboard, in the box provided.
8. Touch **Save**, then touch **Reboot**.



# Hidden Features

Specialized features are enabled by typing special codes at the device. These are not major options like scanning or faxing. They are minor changes, such as changing the durations of built-in timers, that allow users to customize the device to their own needs.

Contact your Xerox representative for further information about hidden features.

## **To enable a hidden feature:**

1. Press the **Log In / Out button** on the Control Panel.
2. On the keypad enter the code for the hidden feature. The code may be as many as 10 digits long. Touch **Enter** when finished.
3. Reboot the device.  
When the device reboots, the software will be activated.

# Xerox Extensible Interface Program (XEIP)

Xerox Extensible Interface Platform enables independent software vendors and partners to develop customized programs to access directly from the Xerox device. Users can enter their authentication login at the device and access a set of features and options designed specifically for their business needs.

For example, a hospital could customize the device to help better manage patient forms. By touching an icon on the display, a healthcare worker could access the hospital's Web-based document management system and browse a list of patient forms.

Users can quickly scan and capture paper documents, preview thumbnails, and add them to frequently used document storage locations. For example:

- A tutor can scan notes directly to a specific course repository for students to access
- A student can scan assessment papers to their course folder for their tutor to mark.

Xerox Extensible Interface Platform utilizes web-based Xerox Partner solutions including Omtool™, Equitrac™ and FreeFlow™ SMARTsend™ to enable users to access document repositories at the device display screen.

Additional resources may be required on the device depending on the solution.

For further information, contact your Xerox Sales Representative.

## XEIP Setup

1. At your workstation:
  - a. Open your Web browser.
  - b. Enter the IP address of the machine in the Address or Location field.
  - c. Press [Enter].
2. To enable the machine for EIP applications:
  - a. Click the [Properties] tab.
  - b. Click the [Services] folder, the [Custom Services] folder, then the [Custom Services] link.
  - c. In the Custom Services area, in the Enabled box, click [Enabled].
  - d. Click [Apply].
3. To enable a digital certificate (if needed):
  - a. Click the [Properties] tab.
  - b. Click the [Security] folder, then the [Machine Digital Certificate Management] link.
  - c. Click the [Create New Self Signed Certificate] button.  
The Machine Digital Certificate Management page refreshes and displays the Self -Signed Certificate area.
  - d. In the the Self -Signed Certificate area, click [Apply].
4. To enable SSL:
  - a. Click the [Properties] tab.
  - b. Click the [Security] folder, then the [SSL/TLS Settings] link.
  - c. If prompted, type or enter your System Administrator user name and password.
    - user name (default): 11111
    - password ( default): x-admin
  - d. In the SSL/TLS Settings area, on the HTTP - SSL / TLS Communication line, click [Enabled].

- e. Click [Apply].
  - f. If changes were made to the SSL settings you may need to:
    - Reboot the system.
    - Close and reopen the client browser.
5. To enable the ports:
- a. Click the [Properties] tab.
  - b. Click the [Connectivity] folder, then Port Settings.
  - c. On the SNMP line, click [Enabled].
  - d. On the SMB line, click [Enabled].
  - e. On the FTP Client line, click [Enabled].
  - f. On the SOAP line, click [Enabled].
  - g. Click [Apply].  
If changes were made to the SSL settings you may need to reboot the system.
6. To ensure that IPv4 is enabled by default:
- a. Click the [Properties] tab.
  - b. Click the [Connectivity] folder, then the [Protocols] folder.
  - c. In the [Protocols] folder, click [TCP/IP].
  - d. In the IP Mode area, on the IP Mode line, click or verify IPv4.
  - e. If you clicked IPv4, click [Apply].  
EIP applications can now register to the device.
  - f. You may need to map buttons to Custom Services at the Local User Interface in order to see the new applications.

# Scan to Home

The Scan to Home option is supported through the Network Scanning service. Essentially, it is a template file (.xst) stored locally on the device, but in a different directory than the network scanning templates or mailbox folders.

Users access the Scan to Home template by pressing the [Network Scanning] button on the Services screen of the User Interface. The device queries LDAP to acquire the authenticated user's home directory, or appends the authenticated user's login name to a predefined network home path.

Ensure that the following items are available and that the preliminary procedures have been performed.

## To prepare for Scan to Home installation

1. Ensure the machine is fully functioning on the network prior to installation.
2. Enable the Scan to Home option. For instructions, refer to the Enabling Options with Software Keys topic, in the Options section of this guide. Contact your Xerox Sales Representative if you have not purchased the Scan to Home option.
3. Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional. This is required to access CentreWare Internet Services to configure Network Scanning. The Internet Services function is accessed through the embedded HTTP server on the machine and allows System Administrators to configure scan settings by using an Internet browser.
4. Enable LDAP authentication on the device as explained in the Authentication section of this guide. LDAP is enabled through Internet Services (the embedded HTTP server on the machine) using the following path: open your web browser, enter the IP address of the device, select Properties, select Security, select Authentication Configuration, and finally, select Remotely on the Network for User Credential validation.
5. Configure the LDAP protocol for the System (or an Authenticated User) to log in to the LDAP server. LDAP is configured through Internet Services (the embedded HTTP server on the machine) using the following path: open your web browser, enter the IP address of the device, select Properties, select Connectivity, select Protocols, and finally, select LDAP. For more information, see Addressing – Internal Address Book (LDAP) in the E-mail section of this guide.



## Configure Scan to Home

*Note: Scan to Home does not work without Remote Account mode.*

1. At the device, press the [Log In / Out] button to enter System Administration Mode.
  2. On the keypad enter [11111] or the current password. Touch [Enter] when finished.
  3. Press the [Machine Status] button on the Control Panel.
  4. Touch the [Tools] tab.
  5. Touch [Authentication / Security Settings], then [Authentication], then [Login Type]. Select [Login to Remote Accounts].
- 
1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press [Enter].
  2. Click the [Properties] tab.
  3. Select [Security].
  4. Select [Remote Authentication Servers].
  5. Select [Authentication System], select LDAP, then click Apply. The device will reboot.
- 
1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press [Enter].
  2. Click the [Properties] tab.
  3. Select [Security].
  4. Select [Authentication Configuration].
  5. In the Login Type box, select [Login to Remote Accounts], then click Apply. The device will reboot.
- 
1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press [Enter].
  2. Click the [Properties] tab.
  3. Select [Services].
  4. Select [Scan to Home].
  5. Select [General].
  6. On the Scan to Home page, in the Status area:
    - a. On the Status line, click the enabled box.
    - b. In the Friendly Name box, type in a user-recognizable name of up to 127 characters for the template that will appear in Template Details on the machine's User Interface.
    - c. On the Determine Home Directory line, ensure that the radio button next to LDAP Query is selected.  
The device will query the LDAP server with the user's authenticated login name and retrieve the user's home directory to set up the template scanning path to that directory.
  7. In the LDAP Mapping for Home Directory area:
    - a. To define the LDAP home directory to a name other than homeDirectory, click the [LDAP Mapping for Home Directory] link.
    - b. To create a scanning subdirectory within the user's home directory, select [Automatically Create Subdirectory] and specify a general name.

# Scanning to the Device's Hard Drive (Mailboxes)

## Before You Start

**It is assumed that you purchased the Scanning option** to enable Scanning to the Hard Drive with your Device. If you did not, contact your Xerox Representative to purchase this option.

Refer to the Enabling Options with Software Keys in this section to enable your purchased option on the machine with the supplied 12 character key.

*Note: Jobs stored in a mailbox cannot be forwarded or re-routed*

## Setting Up Mailboxes at the Device

*Note: Scanning to the Device's hard drive requires the set up of individual Mailboxes to receive scanned files. Up to 200 Mailboxes can be set up to support this type of scanning. To set up Mailboxes, perform the following steps:*

1. Press the **Log In / Out button** on the Control Panel.  
**Note:** If you log in as Administrator (11111), all mailboxes are created with the owner as System Administrator. However, you do NOT have to login as the Administrator to create a mailbox.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Press the **Tools tab**.
5. Press **Setup & Calibration**.
6. Press the **Create Mailbox** button.
7. When the numbered list of Mailboxes is shown on screen, use the supplied arrow keys to scroll through the list to locate an unassigned Mailbox number.
8. Select an unassigned Mailbox number from the displayed list.
9. Press the rectangular **Create & Delete** button in the lower right corner of the Mailbox selection screen.
10. When the **New Mailbox - Password** screen displays, use the **On** and **Off** buttons on the left-hand side of the screen to determine whether or not a password will be required to access the Mailbox. If **On** is selected, use the Device's numeric keypad to enter in a numbered password.
11. Press the **Save** button to save your settings. (To exit the screen, without saving settings, press the Cancel button.)
12. When the Mailbox settings screen displays (after assigning a password), note that you have five setting selections displayed on five numbered horizontal lines. The available selections include: Mailbox Name, Check Password, Delete Documents After Retrieval, Delete Documents with Expire Date, and Link Job Flow Sheet to Mailbox.
13. To assign a name to the Mailbox, press the **Mailbox Name** selection line.

14. Press the rectangular **Change Settings** button.
15. Use the touch screen keyboard to enter in a name for your Mailbox.
16. When finished entering in a name, press the **Save** button in the upper right corner of the screen. (To exit the screen, without saving changes, press the Cancel button.)
17. On the Mailbox settings screen, press any other selection lines of interest and use the **Change Settings** button, as previously described, to access and make setting changes. Use the **Save** button to save your changes.
18. To exit the Mailbox settings screen, press the rectangular **Close** button in the upper right corner of the screen.
19. To exit the screen that lists all assigned and unassigned Mailboxes, press the rectangular **Close** button in the upper right corner of the screen.

### **Configuring Expiration Settings for Stored Documents**

This setting allows the System Administrator to set a document expiration timer to delete documents stored in, but not retrieved from, mailboxes.

1. Press the **Log In / Out button** on the Control Panel.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. From the **Tools tab screen**, use the arrow control in the **Group** menu to scroll to **Stored Document Settings**.
4. Select **Mailbox Document Expiration Date** and touch **Change Settings**.
5. Select **On**, set the timer controls, and touch **Save**.
6. Make any other selections desired, press **Change Settings**, then press **Save**.
7. Press **Close** to return to the Tools tab screen.
8. To exit the Tools tab screen, wait several seconds for the Auto Clear service to log you out.

## Setting Up Mailboxes with Internet Services

*Note: Scanning to the Device's hard drive requires the set up of individual Mailboxes to receive scanned files. Up to 200 Mailboxes can be set up to support this type of scanning. To set up Mailboxes, perform the following steps:*

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Scan** tab.
3. Select **Mailbox** in the directory tree.
4. When the numbered list of Mailboxes is shown, locate an unassigned Mailbox number from the displayed list and click the **Create** button for that Mailbox.
5. Type in a name for this Mailbox in the **Mailbox Name** entry box.
6. Type in a pass code in the **Passcode** entry box.
7. Confirm the pass code by retyping it in the **Re-enter Passcode** box.
8. Use the drop-down arrow to set **Check Passcode** to **Always** (recommended) to secure your mailbox.
9. Place a checkmark in the **Delete Documents after Print or Retrieve** box if you wish to delete documents from your mailbox after retrieving same.
10. Place a checkmark in the **Delete Documents with Expiration Date** box to use this feature in place of, or as an augmentation to, Auto Delete.
11. Click **Apply** when done.

## Scanning to Mailboxes

*Note: Scanning to the Device's hard drive requires the set up of individual Mailboxes to receive scanned files. Up to 200 Mailboxes can be set up to support this type of scanning. To learn how to set up an individual Mailbox, refer to the Setting Up Mailboxes topics in the Scanning to the Device's Hard Drive (Mailboxes) section of this guide, and follow the instructions supplied.*

*Note: Jobs stored in a mailbox cannot be forwarded or re-routed*

### To scan to a Mailbox, perform these steps:

1. From the Device's Main screen, press the **Scan to Mailbox button**.
2. When the **Scan to Mailbox** screen displays, a list of Mailboxes will be shown. Use the supplied arrow to scroll through the icons to locate your Mailbox.
3. Select your Mailbox by pressing its selection line on the touch screen.
4. When the **Password** screen displays, enter your password (series of numbers) using the Control Panel's numeric keypad.
5. Press the **Confirm** button on the touch screen.
6. Use the displayed controls to set up scanning parameters, then place your document in the document handler, and press the Control Panel's large, green **Start button**.
7. Press the **All Services button** to return to the Device's Main screen.

## Retrieving Images from Mailboxes

1. Images are retrieved from Mailboxes using Internet Services. To access Internet Services from your workstation, with your Internet Browser program running, enter the Device's IP Address (as seen on the Configuration Report) into the Address or Location field of the browser. Press the **Enter** key on your keyboard.
2. Click the **Scan** Tab.
3. In the Directory Tree, on the left side of the screen, click the **Mailbox** hot link.
4. Locate your Mailbox, then click the rectangular, **Document List** button.
5. Enter your Passcode when prompted and click **Apply**.
6. Use your mouse to place a check mark in the box in front of the file that you wish to retrieve.
7. After selecting individual retrieval options, click the **Retrieve** button. Note that you can also specify printing options and print the document by clicking the Print Document button.
8. Click the **Save this Link** hot link provided on the next screen displayed to begin the image downloading process.
9. Note that after downloading a document, you can delete that document from your Mailbox by rechecking the box in front of the file just downloaded and clicking the **Delete** button.

# Installing and Using the Network Scanner Utility

To retrieve scanned documents directly from the Device's mailbox(es) into an image-editing application such as Adobe® Photoshop®, you need to install the Network Scanner Utility (scan driver) on your workstation.

You can additionally install and use an application known as Mailbox Viewer to view and import scanned files, without using a client-side image-editing program. For Mailbox Viewer installation instructions, refer to instructions contained on the Driver/Network Utility CD ROM that came with the Device.

## Before Installing the Network Scanner Utility

Before installing the Network Scanner Utility, make sure that your workstation meets the following requirements:

- You must be running Windows 2000 or XP. Windows 2000 Server/Advanced Server Terminal Service is NOT compatible with this feature.
- Your workstation must be operating with a i486DX4/100 MHz processor or faster, have 32 MB RAM or greater, and have 40 MB or more of free hard drive space (not including space for storing scanned data).
- Your workstation must be connected to a network using the TCP/IP protocol.
- Your image-editing application must be compatible with the TWAIN interface to import scanned data.

## Installing the Network Scanner Utility

1. Insert the Driver/Network Utility (Windows) CD ROM into your workstation's ROM drive.
2. Open Windows Explorer (NOT Internet Explorer), click the drive letter for your CD ROM drive, and open **Drivers\Scan\Disk1**.
3. Double click **Setup.exe** and follow the instructions displayed on screen.

## Uninstalling the Network Scanner Utility

1. From the Windows 2000 desktop, from the Start menu, select Settings, Control Panel, then double click **Add/Remove programs**. On the Windows XP desktop, click Start, Control Panel, then double click **Add or Remove Programs**.
2. Select Fuji Xerox Network Scanner Utility, then click **Add Remove**.
3. Click **Yes**.



## Importing Scanned Data from the Mailbox to an Image-Editing Application

1. Start a TWAIN-compatible application program, such as Photoshop.
2. From the **File** menu, select the command for selecting the scan source (Import/Twain Source, in Photoshop).
3. Select **FX Network Scan** from the displayed list and click **Select**.
4. From the **File** menu, select the command to import the image from the scanner. In Photoshop, for example, this would be Import/Twain.
5. If the scanner doesn't automatically display on screen allowing its selection with the **Select Scanner** button, perform the next six steps. Otherwise go to step 12 below.
6. Click Refresh.
7. Click Options.
8. Click Change Display in the scanner selection box.
9. To display scanners on other sub-networks, register them under Scanner Registration.
10. To learn about other fields in the displayed dialog box, click on Help.
11. Click **OK**.
12. Select the scanner for connection from the displayed list, then click **Select Scanner**. Note that you could also just double click the displayed scanner's name.
13. Enter the mailbox number and password when prompted.
14. Click **Open Mailbox**.
15. From the displayed document list, select the document you wish to import and click **Import**.

## Importing Scanned Data from the Mailbox using Mailbox Viewer

1. On your Windows desktop, select Start\Programs\FujiXerox\Network Scanner Utility\Mailbox Viewer.
2. Select the scanner for connection from the displayed list, then click **Select Scanner**.
3. If no items are shown in the list, click Refresh, then Options, then Change Display and register the scanner's IP address and name. Click OK when done.
4. Enter the mailbox number and password when prompted.
5. Click **Open Mailbox**.
6. From the displayed document list, select the document you wish to import and click **Import**.

## Changing Network Utility or Mailbox Viewer Settings

Consult the on-line Help for help in changing any of the settings.

# Scan to E-mail

## E-mail Overview

**It is assumed that you purchased the Scanning option** to enable Scanning to the E-mail with your Device. If you did not, contact your Xerox Representative to purchase this option.

The machine is capable of exchanging E-mails.

The following features are available by exchanging E-mails.

- E-mail
- iFAX
- E-mail Printing
- Mail Notice
- Job Completion Notice

### E-mail

Scanned documents can be converted into an electronic format and transmitted via E-mail.

### iFAX

Unlike conventional fax machines which utilize public phone lines, the machine can transmit or receive scanned data as e-mail attachments using either corporate networks or the Internet.

Contents of E-mail are processed according to the settings of [Print iFax Headers and Contents] in CentreWare Internet Services.

### E-mail Printing

E-mail with attachments in either TIFF or PDF format can be sent to the machine from computers. Received E-mail will automatically be printed.

Contents of E-mail are processed according to the settings of [Print Mail Headers and Contents] in CentreWare Internet Services.

### Consumables Status Notice

E-mail containing contents (status of consumables, paper, and replaceable parts, etc.) set in [Mail Notice Settings] of CentreWare Internet Services is sent to a specified recipient. You can properly determine when to replace toner and drum cartridges by receiving their status periodically.

It is recommended that you register the address of a network administrator or a shared address.

### Job Completion Notice

When a computer has submitted a job to the machine, a notification of the job's completion can be sent by E-mail.

Register the address of a network administrator or a shared address as necessary.

## Preparations

The following items are required in order to use the E-mail feature.

Item	Description	E-mail via SMTP	E-mail via POP3	iFAX via SMTP	iFAX via POP 3	iFAX Direct (1) via SMTP	E-mail Printing	Mail Notice	Job Completion
TCP/IP address	The TCP/IP address for the machine. TCP/IP is used for e-mail.	O	O	O	O	O	O	O	O
Subnet mask	Required when the network is divided into subnets.	s	s	s	s	s	s	s	s
Gateway address	Required when multiple networks are connected by gateways.	s	s	s	s	s	s	s	s
Administrator E-mail address	Set the E-mail address for the machine administrator.	O	O	O	O	O	O	O	O
Machine E- mail address	Used as a sender address when the machine sends E-mail.	O	O	O	O	O	O	O	O
DNS server address	Required when the addresses for a POP3 server and a SMTP server are set with a domain name format instead of their IP addresses.	s	s	s	s	s	s	s	s
SMTP server address	The machine uses a SMTP server to send E-mail. The SMTP server can also be used for receiving E- mail.	O	O	O	O	—	O	O	O

Item	Description	E-mail via SMTP	E-mail via POP3	iFAX via SMTP	IFAX via POP 3	IFAX Direct (1) via SMTP	E-mail Printing	Mail Notice	Job Completion
SMTP authentication user name and password	If an SMTP server requires authentication, specify the authentication user name. Also specify a password as required.	s	s	s	s	—	s	s	s
POP3 server	If a POP3 server is used to receive E-mails, register the machine's E-mail address and a user to the POP3 server. Also, it is necessary to set the POP3 server address on the machine.	—	○	—	○	—	s	s	s
POP user name and password	Set the POP receiving user address. Also specify a password as required.	—	○	—	○	—	s	s	s
S/MIME settings	Set the S/MIME information.	s	s	s	s	s	s	X	X

○ Required setting. s Optional setting. — Not required to set. x Not supported.

(1) When you use iFAX Direct, select System Settings, Fax Settings, iFAX Operation Control, and then select Direct (P2P) under IFAX Communication Pathway.

### Registering an E-mail account

A mail account for the machine needs to be registered to a mail server.

*Note: For information on mail account registration, refer to your mail server documentation.*

### Configuring E-mail Environment

Enable the E-mail ports and configure the machine E-mail address, TCP/IP environment, and E-mail server from the machine.

*Note: The configuration can also be performed using CentreWare Internet Services. For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.*

# Installation Procedure

## Installation Overview

This section describes the configuration procedure to use the E-mail feature on the machine.

The following two steps are necessary to use the E-mail feature.

- Enabling the E-mail ports and setting TCP/IP  
Set the machine to be able to use TCP/IP.
- Configuring the E-mail Environment  
Set the items for E-mail on the machine.

## Enabling the E-mail Ports and Setting TCP/IP

First enable the E-mail ports, then set the IP address.

*Note: The configuration can also be performed using CentreWare Internet Services.*

*Note: For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.*

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad or the keyboard displayed on screen, and select **Enter**.

*Note: The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".*
  - c. Select the **Machine Status** button on the Control Panel.
2. Enable the ports used for E-mail.
  - a. Select the **Tools** tab.
  - b. Select **Connectivity & Network Setup**.
  - c. Select **Port Settings**.
  - d. On the Port Settings screen, select **Send E-mail** and then select **Change Settings**.
  - e. On the Send E-mail screen, select **Port Status** and select **Change Settings**.
  - f. On the Send E-mail Port Status screen, select **Enabled** then select **Save**.
  - g. Select **Close**.
  - h. On the Port Settings screen, select **Receive E-mail**, then select **Change Settings**.
  - i. On the Receive E-mail screen, select **Port Status**, then **Change Settings**.
  - j. On the Receive E-mail Port Status screen, select **Enabled**, then select **Save** and **Close**.
  - k. On the Port Settings screen, select **Mail Notice Service**, then select **Change Settings**.
  - l. On the Mail Notice Service screen, select **Port Status**, then **Change Settings**.
  - m. On the Mail Notice Service – Port Status screen, select **Enabled**, then **Save**.
  - n. Select **Close** until the Tools tab screen is displayed.

3. Set an IP address.

**If an IP address is already set, this step is not necessary.** Also, in an environment with DHCP or BOOTP, configure the way to obtain an IP address. If the address cannot be obtained automatically or static configuration is preferred, configure an IP address, a subnet mask, and a gateway address as stated below.

- a. Select **Protocols**.
- b. Select **IPv4 (or other mode) Address Resolution** and then select **Change Settings**.
- c. Select one from [DHCP], [BOOTP], [RARP], [DHCP/Autonet] or [Static] and then select **Save**. If you select anything other than [Static], proceed to Step 4.

*Note: When using a DHCP server, also configure the DNS, or WINS (Windows Internet Name Service) server (WINS for SMB support). To set a DHCP server, use CentreWare Internet Services. For details, refer to the Internet Services section of this guide.*

- d. On the Protocols screen, select **TCP/IP - IP Address** and select **Change Settings**.
- e. Enter the IP address using the numeric keypad.

*Notes:*

*Enter address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*When you make an entry mistake, press the <C> (Clear) button and enter again.*

*When moving to the next value without entering all 3 digits, select [Next].*

- f. Select **Save**.
- g. Configure **TCP/IP - Subnet Mask** and **TCP/IP - Gateway Address** using the same process as stated above.

*Notes:*

*Enter the Gateway address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*Specify the subnet mask by a combination of the numbers 0, 128, 192, 224, 240, 248, 252, 254, and 255. However, you cannot use 0 between non-zero values.*

*If you do not set the gateway address, enter "0.0.0.0".*

4. Select **Close** until the Tools tab screen is displayed.
5. Wait several seconds for the Auto Clear service to log you out.
6. If you changed any settings, the Device will automatically reboot to register and enable your new settings. After the machine is restarted, print out a Configuration Report to confirm that the ports are enabled and TCP/IP is correctly configured.

For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.



## Configuring the E-mail Environment

**Note:** This configuration can also be performed using CentreWare Internet Services.

For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad or the keyboard displayed on screen, and select **Enter**.

**Note:** The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".

- c. Press the **Machine Status** button on the Control Panel.
2. Set the E-mail address, host name, and domain name.
  - a. Select the **Tools** tab.
  - b. Select **Connectivity & Network Setup**.
  - c. Select **Machine E-mail Address/Host Name**.
  - d. Select **E-mail Address** and then select **Change Settings**.
  - e. Enter an E-mail address using the displayed keyboard.
  - f. Select **Save**.
  - g. Set a host name and a domain name.
  - h. Select **Close**.

### **If [SMTP] has been selected for the [Mail Receiving Protocol]**

Aliases cannot be configured. A user can decide an account name (the left side of the @ mark). An address (the right side of the @ mark) is a combination of a host name and a domain name.

Example: mymail@myhost.example.com

- Account name : mymail
- Host name : myhost
- Domain name : example.com

**If [POP3] has been selected for the [Mail Receiving Protocol]**

Specify a POP user name to an account name (the left side of the @ mark), and a POP3 receiving mail server to an address (the right side of the @ mark). A user can decide an alias such as mymail@example.com.

Example: mymail@mb1.abc.example.com

Account name : mymail

3. Set the protocol for receiving E-mail.
  - a. From the Connectivity & Network Setup list, select **Other Settings**.
  - b. Select **E-mail Receive Protocol** and then select **Change Settings**.
  - c. Select either **SMTP** or **POP3** as appropriate for your environment.
  - d. Select **Save** and then press **Close**.

**If [SMTP] has been selected for the [Mail Receiving Protocol]**

- a. From the Connectivity & Network Setup list, select **Outgoing/Incoming** (i.e. E-mail Send/Receive Settings).
- b. Select **SMTP Server Settings** and then set the following items for the SMTP server.

**[SMTP Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 25.

**If [POP3] has been selected for the [Mail Receiving Protocol]**

- a. From the Connectivity & Network Setup list, select **Outgoing/Incoming** (i.e. E-mail Send/Receive Settings).
- b. Select **POP3 Server Settings** and then set the following items for the POP3 server.

**[POP3 Server Name/Address]**

Enter the POP3 Server Name/IP Address and press **Save**.

*Note:*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

**[POP3 Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 110.

**Note:** Do not use the numbers of any other ports.

**[POP3 Server Check Interval]**

Set the interval for checking the e-mail on the POP3 server.

**[POP3 Server Login Name]**

Enter the name to log in to the POP3 server and press **Save**.

**[POP3 Server Password]**

Enter the same password twice in the [New Password] and [Re-enter Password]. If you do not set the password, leave it blank and select **Save**.

**[POP3 Password Encryption]**

Select **On (APOP)** to encrypt the password, if desired.

- c. Select **Save** and then press **Close**.
4. Set the protocol for sending E-mail.
  - a. From the Connectivity & Network Setup list, select **Outgoing/Incoming**, then select **SMTP Server Settings**, and set the following items for the SMTP server.

**[SMTP Server Name/Address]**

Enter the SMTP Server Name/IP Address and press **Save**.

*Note:*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

**[SMTP Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 25.

**Note:** This configuration is not necessary if [SMTP] has been selected for the [Mail Receiving Protocol] and has already been configured.

**[E-mail Send Authentication]**

Select one from [Off], [POP before SMTP], or [SMTP AUTH]. **Tip:** If you are having trouble sending E-mail, to see if Authentication is the problem, set this item to **Off** and set the SMTP Server IP Address (above) to a server that does not require authentication.

**Note:** If [POP before SMTP] is selected, the POP3 settings must be set.

**[SMTP AUTH Login Name]**

Set this item if [SMTP AUTH] is selected for [E-mail Send Authentication].

**[SMTP AUTH Password]**

Set this item if [SMTP AUTH] is selected for [E-mail Send Authentication]. Enter the same password twice in the [New Password] and [Re-enter Password]. If you do not set the password, leave it blank and select [Save].

- b. Select **Close** until the Connectivity & Network Setup list is again displayed.

5. Setting S/MIME (Security), if desired.
  - a. From the Connectivity & Network Setup list, select **Security Settings**. If the selection is not visible, use the scrolling arrow to display it.
  - b. Select **S/MIME Settings** and set the following items.

#### **Device Certificate - S/MIME**

Link a certificate to the machine. You **MUST** have an S/MIME certificate on the machine to perform encryption. For information on S/MIME certificates, refer to the Configuration of E-mail Encryption/Digital Signature topic in the Security section in this guide.

#### **S/MIME Communication**

Set whether to enable or disable S/MIME Communication when a certificate ID is set.

#### **Receive Untrusted E-mail**

Set whether to receive untrusted E-mail or not.

**Receive Untrusted iFAX** - if available on screen.

Set whether to receive untrusted iFAX or not.

#### **Message Digest Algorithm**

Select a message digest algorithm from [SHA1] or [MD5].

#### **Message Encryption Method**

Select a contents encryption method from [3DES], [RC2-40], [RC2-64], or [RC2-128].

#### **Digital Signature - Outgoing E-mail**

Set whether to always attach a digital signature to E-mail or to select a digital signature when sending E-mail.

**Digital Signature - Outgoing iFAX** - if available on screen.

Set whether to always attach a digital signature to iFAX or to select a digital signature when sending iFAX.

#### **Certificate Auto Store**

Select whether or not to automatically store a S/MIME certificate attached with the E-mail when receiving E-mail sent from an address registered in the address book.

6. Select **Close** repeatedly until the Tools tab screen is displayed.
7. Wait several seconds for the Auto Clear service to log you out.
8. After the machine is restarted, print a Configuration Report to confirm that each item is configured.  
For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.
9. Test the E-mail transmission from the machine by pressing the **All Services button**, then touching the on-screen **E-mail** button, then the **New Recipient** button. Type in your E-mail address, then press **Close**. Place a document in the document handler and press the large, green, **Start button**, located to the immediate right of the Control Panel's numeric keypad.

*Note: To set up the address book for use with **LDAP** (network search), refer to the Configure Authentication for **LDAP topic** in the Security section of this guide.*

# Internet Fax (iFAX)

## iFAX Overview

When the iFAX feature is enabled, the machine can transmit scanned data as an e-mail attachment using either corporate networks or the Internet, unlike conventional fax machines which utilize public phone lines. Also, the machine can receive e-mails transmitted from other machines which support the iFax service. When the machine receives e-mail from an iFAX-compatible machine, the received document is printed automatically.

*Note: It is assumed that you purchased the Internet Fax option to enable iFAX with your Device. If you did not, contact your Xerox Representative to purchase this option.*

## Preparations

The following describes the necessary conditions to use iFAX on the machine.

### System Requirements for the Machine

- Internet Fax kit
- The machine is connected to the network and communication through TCP/IP is available.
- The environment is prepared for e-mail exchange.

# Installation Procedure

## Installation Overview

The configuration procedure to use the iFAX feature on the machine is comprised of the following steps.

1. Enable the ports which are used for the iFAX feature, and set an IP address of the machine.
2. Configure the items for the iFAX feature on the machine.

*Note: Configuration can also be performed using CentreWare Internet Services.*



## Enabling the E-mail Ports and Setting TCP/IP

First enable the ports for the e-mail feature, then set the IP address. The procedure for setting the machine is as follows.

First enable the E-mail port, then set the IP address.

*Note: The configuration can also be performed using CentreWare Internet Services.*

*For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.*

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad or the keyboard displayed on screen, and select **Enter**.

*Note: The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".*
  - c. Select the **Machine Status** button on the Control Panel.
2. Enable the ports which are used for E-mail.
  - a. Select the **Tools** tab.
  - a. Select **System Settings**.
  - b. Select **Connectivity & Network Setup**.
  - c. Select **Port Settings**.
  - d. On the Port Settings screen, select **Receive E-mail** and then select **Change Settings**.
  - e. On the Receive E-Mail screen, select **Port Status** and select **Change Settings**.
  - f. On the Receive E-Mail Port Status screen, select **Enabled**, then select **Save**.
  - g. Select **Close** until the Port Settings screen is displayed.
  - h. On the Port Settings screen, select **Send E-Mail**, and then select **Change Settings**.
  - i. On the Send E-Mail screen, select **Port Status** and select **Change Settings**.
  - j. On the Send E-Mail Port Status screen, select **Enabled** then select **Save**.
  - k. Select **Close** until the Tools tab screen is displayed.

3. Set the IP address.

**If an IP address is already set, this step is not necessary.** Also, in an environment with DHCP or BOOTP, configure the way to obtain an IP address. If the address cannot be obtained automatically or static configuration is preferred, configure an IP address, a subnet mask, and a gateway address as stated below.

- a. Select **Protocol Settings**.
- b. Select **IPv4 (or other mode) Address Resolution** and then select **Change Settings**.
- c. Select one from [DHCP], [BOOTP], [RARP], [DHCP/Autonet] or [Static] and then select [Save]. If you select anything other than [Static], proceed to Step 4.

*Note: When using a DHCP server, also configure the DNS, or WINS (Windows Internet Name Service) server (WINS for SMB support). To set a DHCP server, use CentreWare Internet Services. For details, refer to the Internet Services section of this guide.*

- d. On the Protocol Settings screen, select **TCP/IP - IP Address** and select **Change Settings**.
- e. Enter the IP address using the numeric keypad.

*Notes:*

*Enter address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*When you make an entry mistake, press the <C> (Clear) button and enter again.*

*When moving to the next value without entering all 3 digits, select [Next].*

- f. Select **Save**.
- g. Configure **TCP/IP - Subnet Mask** and **TCP/IP - Gateway Address**.

*Notes:*

*Enter the Gateway address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*Specify the subnet mask by a combination of the numbers 0, 128, 192, 224, 240, 248, 252, 254, and 255. However, you cannot use 0 between non-zero values.*

*If you do not set the gateway address, enter "0.0.0.0".*

4. Select **Close** until the Tools tab screen is displayed.
5. Wait several seconds for the Auto Clear service to log you out.
6. If you changed any settings, the Device will automatically reboot to register and enable your new settings. After the machine is restarted, print out a Configuration Report to confirm that the ports are enabled and TCP/IP is correctly configured.

For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.

## Configuring the E-mail Environment

**Note:** This configuration can also be performed using CentreWare Internet Services.

For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad or the keyboard displayed on screen, and select **Enter**.

**Note:** The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".

- c. Press the **Machine Status button** on the Control Panel.
2. Set the E-mail address, host name, and domain name.
  - a. Select the **Tools tab**.
  - b. Select **Connectivity & Network Setup**.
  - c. Select **Machine E-mail Address/Host Name**.
  - d. Select **E-mail Address** and then select **Change Settings**.
  - e. Enter an E-mail address using the displayed keyboard.
  - f. Select **Save**.
  - g. Set a host name and a domain name as above.
  - h. Select **Close**.

### **If [SMTP] has been selected for the [Mail Receiving Protocol]**

Aliases cannot be configured. A user can decide an account name (the left side of the @ mark). An address (the right side of the @ mark) is a combination of a host name and a domain name.

Example: mymail@myhost.example.com

- Account name : mymail
- Host name : myhost
- Domain name : example.com

**If [POP3] has been selected for the [Mail Receiving Protocol]**

Specify a POP user name to an account name (the left side of the @ mark), and a POP3 receiving mail server to an address (the right side of the @ mark). A user can decide an alias such as mymail@example.com.

Example: mymail@mb1.abc.example.com

Account name : mymail

3. Set the protocol for receiving E-mail.
  - a. From the Connectivity & Network Setup list, select **Other Settings**.
  - b. Select **E-mail Receive Protocol** and then select **Change Settings**.
  - c. Select either **SMTP** or **POP3** as appropriate for your environment.
  - d. Select **Save**.
  - e. Select Close.

**If [SMTP] has been selected for the [Mail Receiving Protocol]**

- a. From the Connectivity & Network Setup list, select **Outgoing/Incoming** (i.e. E-mail Send/Receive Settings).
- b. Select **SMTP Server Settings** and then set the following items for the SMTP server.

**[SMTP Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 25.

**If [POP3] has been selected for the [Mail Receiving Protocol]**

- a. From the Connectivity & Network Setup list, select **Outgoing/Incoming** (i.e. E-mail Send/Receive Settings).
- b. Select **POP3 Server Settings** and then set the following items for the POP3 server.

**[POP3 Server Name/Address]**

Enter the POP3 Server Name/IP Address and press **Save**.

*Note:*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 – 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

**[POP3 Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 110.

**Note:** Do not use the numbers of any other ports.

**[Polling Interval]**

Set the interval for checking the e-mail on the POP3 server.

**[Login Name]**

Enter the name to log in to the POP3 server and press **Save**.

**[Password]**

Enter the same password twice in the [New Password] and [Re-enter Password]. If you do not set the password, leave it blank and select **Save**.

**[POP3 Password Encryption]**

Select **On (APOP)** to encrypt the password, if desired.

- c. Select **Save**.
- d. Select **Close**.

4. Set the protocol for sending E-mail.
  - a. From the Connectivity & Network Setup list, select **Outgoing/Incoming**, then select **SMTP Server Settings**, and then set the following items for the SMTP server.

**[SMTP Server Name/Address]**

Enter the SMTP Server Name/IP Address and press **Save**.

*Note:*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

**[SMTP Server Port Number]**

Enter a value in the range from 1 to 65535. The default is 25.

**Note:** This configuration is not necessary if [SMTP] has been selected for the [Mail Receiving Protocol] and has already been configured.

**[E-mail Send Authentication]**

Select one from [Off], [POP before SMTP], or [SMTP AUTH]. **Tip:** If you are having trouble sending E-mail, to see if Authentication is the problem, set this item to **Off** and set the SMTP Server IP Address (above) to a server that does not require authentication.

**Note:** If [POP before SMTP] is selected, the POP3 settings must be set.

**[SMTP AUTH Login Name]**

Set this item if [SMTP AUTH] is selected for [E-mail Send Authentication].

**[SMTP AUTH Password]**

Set this item if [SMTP AUTH] is selected for [E-mail Send Authentication]. Enter the same password twice in the [New Password] and [Re-enter Password]. If you do not set the password, leave it blank and select [Save].

- b. Select **Close** until the Connectivity & Network Setup list is again displayed.

5. Setting S/MIME (Security), if desired.

- a. From the Connectivity & Network Setup list, select **Security Settings**. If the selection is not visible, use the scrolling arrow to display it.
- b. Select **S/MIME Settings** and set the following items:

**Device Certificate - S/MIME**

Link a certificate to the machine. You **MUST** have an S/MIME certificate on the machine to perform encryption. For information on S/MIME certificates, refer to the Configuration of E-mail Encryption/Digital Signature topic in the Security section in this guide.

**S/MIME Communication**

Set whether to enable or disable S/MIME Communication when a certificate ID is set.

**Receive Untrusted E-mail**

Set whether to receive untrusted E-mail or not.

**Receive Untrusted iFAX**

Set whether to receive untrusted iFAX or not.

**Message Digest Algorithm**

Select a message digest algorithm from [SHA1] or [MD5].

**Message Encryption Method**

Select a contents encryption method from [3DES], [RC2-40], [RC2-64], or [RC2-128].

**Digital Signature - Outgoing E-mail**

Set whether to always attach a digital signature to E-mail or to select a digital signature when sending E-mail.

**Digital Signature - Outgoing iFAX**

Set whether to always attach a digital signature to iFAX or to select a digital signature when sending iFAX.

**Certificate Auto Store**

Select whether or not to automatically store a S/MIME certificate attached with the E-mail when receiving E-mail sent from an address registered in the address book.

6. Select **Close** repeatedly until the Tools tab screen is displayed.
  7. Wait several seconds for the Auto Clear service to log you out.
  8. After the machine is restarted, print a Configuration Report to confirm that each item is configured.
- For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.



## Testing iFAX

### Send from the Device to another iFAX-capable Machine

Test the iFAX transmission from the machine.

1. Press the **All Services button**, then touch the **Internet Fax** button to display the Internet Fax screen.
2. Select New Recipient, then the To button, in the Recipient's drop-down list.
3. Enter the destination address, using the displayed keyboard.
4. Touch the Add button, then touch Close.
5. Place your document in the document handler and press the Start button located to the immediate right of the Control Panel's numeric keypad.
6. Check to see if the other machine printed the incoming iFAX.

*Note: To set up the address book for use with **LDAP** (network search), refer to the Configure Authentication for **LDAP topic** in the Security section of this guide.*

# Server Fax

## Server Fax Overview

The Server Fax feature enables you to fax documents without having a telephone line directly connected to your multifunction device. This is achieved by sending the documents to a separate, networked fax server with its own links to the telephone system.

It is assumed that you already purchased and enabled the Scanning option. If you did not, contact your Xerox Representative to purchase same. A hard disk and network card are required device hardware. Their presence can be confirmed by printing a Configuration Report, as stated in the Configuration Report topic in the Network Connectivity section of this guide.

The Server Fax option also needs to be purchased from your Xerox Representative, then enabled on the multifunction device using a software key (see Enabling Options with Software Keys in this guide).

As stated in this section, you will be setting up a network connection to a Xerox-certified, third party fax server (server running fax management software) which will receive, store, and redirect incoming documents to the server's fax boards, or other destinations determined by fax server software setup.

*Note: The FAX or Internet Fax (iFAX) features and the Server Fax feature are mutually exclusive. If Server Fax is enabled, even if the machine is equipped with an internal fax board, scanning to the internal FAX will be disabled. While the Server Fax feature is enabled, the iFAX service will also be disabled. Also note that Mailbox to FAX (a Job Flow Sheet destination) and Direct Fax (LAN Fax) are not supported when Server Fax is enabled. You can use Internet Services, however, to select which Fax Service to enable, as described in this section.*

## Installation Checklist

Please ensure that the following items are available or have been performed.

1. Ensure the machine is fully functioning on the network prior to installation.
2. Enable the purchased Scanning option. For instructions, refer to the Enabling Options with Software Keys topic, in the Options section of this guide. Contact your Xerox Sales Representative if you have not purchased the Scanning option.
3. Enable the purchased Server Fax option. For instructions, refer to the Enabling Options with Software Keys topic, in the Options section of this guide. Contact your Xerox Sales Representative if you have not purchased the Server Fax option.
4. Verify that Scan to Fax Server is now the currently enabled Fax Service, as follows:
  - a. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
  - b. Click the **Properties** tab.
  - c. Click on the **Services** folder.
  - d. Click on the **Fax** folder.
  - e. Click the **Fax Repository Setup** link and verify that Scan to Fax Server is displayed in the selection box.
  - f. If Scan to Fax is displayed instead, use the selection arrow to select Scan to Fax Server and click **Apply**.
  - g. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

5. Ensure that the TCP/IP and HTTP protocols are configured on the device and are fully functional. This is required to access the multifunction device's CentreWare Internet Services web pages, which can be used to configure Server Fax settings from a network-connected workstation.

To verify that the TCP/IP and HTTP protocols are correctly configured, print a Configuration Report as stated in the Configuration Report topic in the Network Connectivity section of this guide.

To configure TCP/IP, refer to the TCP/IP Configuration topic in the NOS Selection section of this guide.

6. To enable HTTP, refer to the Enable Internet Services (HTTP) topic in the Network Connectivity section of this guide.
7. Ensure that the FTP Client and SMB port are enabled on the device. To verify this, print a Configuration Report as stated in the Configuration Report topic in the Network Connectivity section of this guide.

To enable SMB, refer to Enabling the SMB Setting at the Device in the Microsoft (NetBIOS over IP) Networks topic of this guide. To enable FTP, use the same SMB enabling procedure, and simply choose FTP as the port to enable.

8. Install and configure the Xerox-certified, third party fax server per the fax management software manufacturer's instructions.

*Note: If the fax server will be using TCP/IP to communicate, it is recommended that the server be assigned a static IP address.*

## Configure a Fax Filing Location (Repository)

Faxing from the multifunction device to a fax server is very similar to the other methods of faxing available to users on the multifunction device. The user simply selects the Fax button from the All Services screen, enters a Recipient phone number when prompted, places a document in the document handler, and presses Start.

The scanned document is converted into a TIFF file, and a job log is sent along with the image data to the fax server.

The transferred image resides in a directory on the fax server (commonly known as the fax repository). The server monitors the repository for documents to be faxed, and faxes any documents it finds per the routing instructions contained in the job log. The System Administrator uses a web browser on any networked workstation to access the Internet Services web pages, residing on the device, to configure communications with the fax server, and designate the location of the repository on the server.

Protocols available for use in communicating with the fax server include:

**FTP (File Transfer Protocol):** Requires an FTP service running on the fax server.

**SMB (Server Message Block):** Available for filing to an environment that supports the SMB protocol.

**SMTP:** Follow the basic instructions for enabling the E-mail ports in the Scan to E-mail section of this guide. You will need to know the fully qualified domain name of the fax server on your network (e.g. SMTP.yournet.net). Also, follow the fax server software manufacturer's instructions to establish fax server to email server communications in your network environment.

## **Configure a Fax Filing Repository using FTP**

### **Installation Checklist**

1. Ensure that a File Transfer Protocol (FTP) service is running on the fax server where images scanned by the machine will be stored. Write down the IP address or Host Name.
2. Create a user account (login name) and password for the machine on the server. When a document is scanned, the machine logs in using the account, transfers the file to the server, and logs out. Write down the user account (login name) and password.
3. Following the fax server software manufacturer's instructions, create a directory (repository) on the server (likely within the FTP root) to be used as a scan filing location. Write down the directory name and path to same.
4. If allowed by the fax server software manufacturer, test the FTP connection by logging into the scan directory from a remote PC using the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function, check the user account access rights and FTP service setup. Note that you can also simply wait until you have finished setting up device to server communications, as stated in this section, then send a fax to the server to test the communications setup.

## Enter the Fax Repository Details via Internet Services

5. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
6. Click the **Properties** tab.
7. Click the **Services** folder.
8. Click on the **Fax** folder.
9. Click the **Fax Repository Setup** link.
10. Select **FTP** for Protocol.
11. Enter either an IP Address or Host Name for the fax server in the box or boxes provided.
12. Enter 21 for Port Number (for FTP).
13. For Document Path, type in the name of the folder on the server that has been set up to receive device scans. Do not use forward slashes.
14. Supply the **Login Name** and **Password** for the machine to log into the fax server.
15. Re-enter the password in the Retype Password box.
16. Click **Apply**.
17. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

The screenshot shows a web browser window with a dark blue header. Below the header are three tabs: 'Print / Scan', 'Properties', and 'Support'. The 'Properties' tab is selected. The main content area is titled 'Fax Repository Setup'. Below this title is a section labeled 'Fax Destination'. Inside this section, there are several input fields: 'Protocol' with a dropdown menu showing '\*FTP', 'IP Address / Host Name and Port' with a text box and a port number box, 'Document Path' with a text box, 'Login Name' with a text box, 'Password' with a masked text box, and 'Retype password' with a masked text box. At the bottom of the form are two buttons: 'Apply' and 'Undo'.

## Configure General Settings

18. Click the **Defaults** link.
19. To print a Scan File Transfer Report, select Auto Print On, Auto Print Off, or Print when delivery fails, from the drop-down menu. Note that the Transfer Report only shows whether data was sent to the fax server. It does not show whether the fax was successfully sent by the fax server.
20. Check the User Name and Domain Name (Realm) boxes if you want these items to appear on the Job Log. The Job Log is filed with the scan job.
21. Click **Apply**.
22. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

## Configure the Fax Server

23. Configure the fax server so that it is able to monitor the fax repository for incoming documents. Refer to the fax management software manufacturer's documentation to complete this task.

## Test Faxing through the Server

24. Go to the machine and press the **All Services** button.
25. Press the **Fax** button.
26. Enter a valid fax number.
27. Place a document in the document handler and press the **Start** button located to the immediate right of the Control Panel's numeric keypad.
28. Verify that the fax was received by the specified fax machine.



## **Configure a Fax Filing Repository using SMB**

### **Installation Checklist**

1. Following the fax server software manufacturer's instructions, create a shared folder on the fax server to be used as a scan filing location (repository) for scanned documents. Write down the Share Name of the folder and the Computer Name or Server Name.
2. Create a user account (login name) and password for the machine on the server. Make sure that the machine has full access rights to the scan directory. Write down the user account (login name) and password.
3. If allowed by the fax server software manufacturer, test the settings by attempting to connect to the shared folder from another PC by logging in with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights and Share setup. Note that you can also simply wait until you have finished setting up device to server communications, as stated in this section, then send a fax to the server to test the communications setup.

## Enter the Fax Repository Details via Internet Services

4. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
5. Click the **Properties** tab.
6. Click the **Services** folder.
7. Click on the **Fax** folder.
8. Click on **Fax Repository Setup** and select **SMB** for Protocol.
9. Enter an IP Address or Host (NetBIOS) Name.
10. Enter 139 for Port Number.
11. Enter the Share name.
12. For Document Path, type in the name of the folder on the server that has been set up to receive device scans. Do not use back slashes.
13. Supply the **Login Name** and **Password** for the machine to log into the fax server.
14. Re-enter the password in the Retype Password box.
15. Click **Apply**.
16. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

The screenshot shows a web browser window with a dark blue header. Below the header are three tabs: "Print/Scan", "Properties", and "Support". The "Properties" tab is selected. The main content area is titled "Fax Repository Setup". Below this title is a section labeled "Fax Destination". Inside this section, there are several fields and a dropdown menu:

- Protocol**: A dropdown menu showing "\*SMB".
- IP Address / Host Name (NetBIOS) and Port**: A text input field followed by a colon and a port number input field.
- Share**: A text input field.
- Document Path**: A text input field.
- Login Name**: A text input field.
- Password**: A text input field with masked characters (dots).
- Retype password**: A text input field with masked characters (dots).

At the bottom of the form, there are two buttons: "Apply" and "Undo".

## Configure General Settings

17. Click the **Defaults** link.
18. To print a Scan File Transfer Report, select Auto Print On, Auto Print Off, or Print when delivery fails, from the drop-down menu. Note that the Transfer Report only shows whether data was sent to the fax server. It does not show whether the fax was successfully sent by the fax server.
19. Check the User Name and Domain Name (Realm) boxes if you want these items to appear on the Job Log. The Job Log is filed with the scan job.
20. Click **Apply**.
21. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

## Configure the Fax Server

22. Configure the fax server so that it is able to monitor the fax repository for documents. Refer to the fax management software manufacturer's documentation to complete this task.

## Test Faxing through the Server

1. Go to the machine and press the **All Services** button.
2. Press the **Fax** button.
3. Enter a valid fax number.
4. Place a document in the document handler and press the **Start** button located to the immediate right of the Control Panel's numeric keypad.
5. Verify that the fax is received by the specified fax machine.

## **Configure a Fax Filing Repository using SMTP**

### **Installation Checklist**

1. Ensure that the TCP/IP protocol is configured on the device and is fully functional. To configure TCP/IP, refer to the TCP/IP Configuration topic in the NOS Selection section of this guide.
2. Follow the basic instructions for enabling the E-mail ports in the Scan to E-mail section of this guide.
3. Also, in the Scan to E-mail section, follow the instructions for Configuring E-mail Environment to set the Machine E-mail Address. This address will then be displayed in the From field of the Fax.
4. You will need to know the fully qualified domain name of the fax server on your network (e.g. SMTP.yournet.net).
5. Follow the fax server software manufacturer's instructions to create a directory (repository) on the server to be used as a scan filing location.
6. Follow the fax server software manufacturer's instructions to determine what, if any, additional protocols or ports need to be enabled at the multifunction device to support SMTP (email) filing with the server.
7. Follow the fax server software manufacturer's instructions to establish fax server to email server communications in your network environment.

## Enter the Fax Repository Details via Internet Services

1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Services** folder.
4. Click on the **Fax** folder.
5. Click on **Fax Repository Setup** and select **SMTP** for Protocol.
6. In the Domain Name box, enter the fully qualified domain name of the fax server on your network (e.g. SMTP.yournet.net).
7. For E-mail Address Display Format, choose whether to add "FAX=" in front of E-mail addressing. If in doubt, select Do not add "FAX=".
8. Click **Apply**.
9. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

The screenshot shows a web browser window with a dark blue header. Below the header are three tabs: "Print / Scan", "Properties", and "Support". The "Properties" tab is selected. The main content area is titled "Fax Repository Setup". Below this title is a section labeled "Fax Destination". Inside this section, there are three rows of configuration options:

- Protocol:** A dropdown menu with "SMTP" selected.
- Domain Name:** A text input field. Below it, a small example text reads "Example: hostname.xerox.com".
- E-mail Address Display Format:** A dropdown menu with "Do not add 'FAX='" selected.

At the bottom of the configuration section, there are two buttons: "Apply" and "Undo".

## Configure General Settings

10. Click the **Defaults** link.
11. To print a Scan File Transfer Report, select Auto Print On, Auto Print Off, or Print when delivery fails, from the drop-down menu. Note that the Transfer Report only shows whether data was sent to the fax server. It does not show whether the fax was successfully sent by the fax server.
12. Check the User Name and Domain Name (Realm) boxes if you want these items to appear on the Job Log. The Job Log is filed with the scan job.
13. Click **Apply**.
14. Enter the administrator User Name and Password and click OK. The default is 11111 and x-admin.

### Configure the Fax Server

15. Configure the fax server so that it is able to monitor the fax repository for documents. Refer to the fax management software manufacturer's documentation to complete this task.

## Test Faxing through the Server

1. Go to the machine and press the **All Services** button.
2. Press the **Fax** button.
3. Enter a valid email address.
4. Place a document in the document handler and press the **Start** button located to the immediate right of the Control Panel's numeric keypad.
5. Verify that the email was received by the specified recipient.

## Features that can be set in support of Server Fax

### Address Book Setup

Use of this feature enables Fax users to select recipients by 3 digit numbers. Note that a maximum of 50 characters can be designated for each destination and that only fax destinations can be used. Also note that all Address Book information other than Fax Number, Destination Name, and Index Character will be ignored. For example, the Extension/Outside line attribute of address book will be ignored.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**.
6. Touch **Address Book**.
7. Select an available Address Number.
8. Touch **Create/Delete**.
9. Touch **Address Type**, then touch **Change Settings**.
10. Touch **Fax**, then touch **Save**.

### Group Send

This setting supports Group Send (broadcast) Fax transmissions to up to 20 address numbers in a pre-designated group.

*Note: When Group Send is designated with Server Fax, the group number retained by the server is used instead of the group number retained by the device. You will have to know what group the three digit number represents at the server, before selecting its use at the device's control panel.*

## **Fax Mode Settings (Screen Defaults and Fax Defaults such as Delayed Start)**

These settings include Screen Defaults and Fax Defaults.

**Screen Defaults** sets the screen displayed at the device's Control Panel when the Fax button is pressed.

**Fax defaults** lets you set the parameters for **Delayed Start** communications. This can be a useful feature for saving time-based phone charges. Note that the fax will be immediately sent from the device to the fax server repository, however the server will send the fax at the time designated by this feature.

1. If necessary, press the **Log In / Out** button and enter [11111] or the current password. Touch **Enter**, then press the **Machine Status button** on the Control Panel..
2. Touch the **Tools tab**, then touch **Fax Mode Settings**.
3. Touch **Screen Defaults**.
4. Select a Line to enter or change, then touch **Change Settings**. Touch **Save** to save any new settings.
  - Fax Screen Default. Select General Settings or Address Book. This will be the Fax service screen that users see when they touch the Fax button.
  - Address Book Default. Leave this setting at the default of 1, or enter an address book (Fax mailbox) number to display when the Address Book button is touched by users of the Fax service screen. Note that the Fax mailbox needs to be created in advance of this setting.
5. Touch **Close** until the Fax Mode Settings selections are again displayed.
6. Touch **Fax Defaults**.
7. Select **Delayed Start – Start Time**.
8. Touch **Change Settings**, make the desired changes, then touch **Save**.
9. Touch **Close** until the Tools tab screen is displayed.
10. Wait several seconds for the Auto Clear service to log you out.

## **Color Mode, Resolution, File Format, and File Name**

Note that when using Server Fax, these features are set to fixed values which cannot be changed. The setting for Color Mode is Monochrome. The setting for Resolution is Fine, and the setting for File Format is TIFF. In addition, the Server Fax feature also automatically assigns file names.



# Fax

## Fax Overview FP

The optional Fax feature works much the same as a standard facsimile machine. **Extra features**, covered in this section, **such as the Address Book, Group Dial, Comments, and the use of Mailboxes, are meant to provide additional capabilities** in support of the Fax feature.

*Note: It is assumed that you purchased the appropriate 1 or 3 line Fax hardware kit for use with your Device. If you did not, contact your Xerox Representative to purchase this option.*

### Checking and Setting Critical Fax Parameters

**Refer to the Fax Settings Topic** (including Fax Defaults and Fax Control) in this section **to determine if Fax Defaults and Fax Control parameters are correctly set for your environment.**

## Before You Start Fax

### Before starting the setup:

- You cannot use this machine with a call waiting service.
- A facsimile located close to a main unit of a cordless phone can cause distorted images or interrupted transmission. This machine should be installed at least five meters away from the main unit of the cordless phone.
- If the digital line leased for your company network is multiplexed, facsimile communication may be restricted as follows:

The features using our unique transmission method, such as Recipient Print Sets, Relay Broadcast and Remote Mailbox, are not available.

The transmission speed is limited.

Super G3 cannot be used.

### Communications modes:

- G3 (Auto) - Normal Fax communications. The machine automatically switches modes in the following order of priority: Unique SG3 - Unique ECM - Unique G3 - ITU-T SG3 - ITU-T ECM - ITU-TG3 depending on the capabilities of the remote terminal.
- F4800 - Select this mode when transmitting over noisy or bad telephone lines, as can be the case with overseas calls.

### Connecting the phone line:

LINE 1 Connect the fax to a public switched telephone network (PSTN). An external telephone cannot be connected.

TEL An external telephone is connected here.

LINE 2 (Line 2) Connect to a public line.

LINE 4 (Line 4) Connect to a public line.

## Local Terminal Information Settings

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Touch **Fax Mode Settings**.
6. Touch **Local Terminal Information**.
7. Select the items to enter information and touch **Change Settings**.
  - a. Enter in a Local Name, up to 20 characters, then touch **Save**.
  - b. Enter a Company Logo, up to 30 characters, then touch **Save**.
  - c. Enter a Machine Password, up to 20 digits, then touch **Save**. Note: The password prevents your machine from receiving faxes, or being polled by other machines that are not F-Code compatible.
  - d. Enter G3 Fax ID, up to 20 digits, then touch **Save**.
  - e. Enter G3 Dial Type, Tone, 10pps, or 20pps, then touch **Save**.
  - f. Enter G3 Line Type, PSTN or PBX, then touch **Save**.
8. When complete, touch **Close** repeatedly until the Tools tab screen is displayed.
9. Wait several seconds for the Auto Clear service to log you out.

## Address Book Setup

Use of this feature enables Fax users to select recipients by 3 digit numbers, which can be used to support speed dialing.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Touch the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**.
6. Touch **Address Book**.
7. Select an available Address Number.
8. Touch **Create/Delete**.
9. Touch **Address Type**, then touch **Change Settings**.
10. Touch **Fax**, then touch **Save**.

11. Select the items you would like to enter information for and touch **Change Settings**.
  - a. Fax Number, up to 128 characters, then touch **Save**.
  - b. Name, up to 18 characters, then touch **Save**.
  - c. Index, only 1 digit (used for a quick find), then touch **Save**.
  - d. Relay Station setup, On or Off, then touch **Save**.
  - e. Starting Rate, G3 Auto or Forced4800bps, then touch **Save**.
  - f. Resolution, choose one, then touch **Save**.
  - g. Cover Note, On or Off, then touch **Save**.
    - If On, select Comment (Recipient Comment) then touch **Save**.
  - h. Maximum Image Size, choose one then touch **Save**.
  - i. Delayed Start, On or Off, then touch **Save**.
    - If On, choose Start Time, then touch **Save**.
  - j. Remote Mailbox, On or Off, then touch **Save**.
    - If On, enter Mailbox number, then touch Next, and password if required.
  - k. F Code, On or Off, then touch **Save**.
    - If On, enter F Code and password, then touch Next. **Note:** F Code is the transmission procedure set by the Communications and Information Network Association of Japan. DTMF Method: G3 Fax machines that support Manual Send can also make Relay Broadcasts for the machine. Refer to the Fax section of the Device's User Guide for full information.
  - l. Relay Broadcast, On or Off (This feature supports transmitting documents through a Relay Station. Refer to the Fax section of the Device's User Guide for full information.)
    - If On, enter 2 digit Relay Station ID, touch Enter/Change Recipients.
    - Enter Address Number or the Group Number and touch Add.
    - Print at Relay Station, On or Off, then Touch Save.
12. When complete, touch **Save** to exit the settings screen.
13. Touch **Close** to exit the Address Book screen, returning to the Tools tab screen.
14. To exit the Tools tab screen, if desired, wait several seconds for the Auto Clear service to log you out.

## Group Send Setup

This setting supports Group Send (broadcast) Fax transmissions to up to 20 address numbers in a pre-designated group. Refer to the Group Send topic in the Device's User Guide for full information. To set up a Group, perform the following steps.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Touch the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**.
6. Touch **Group Send**.
7. Select a Group number.
8. Touch **Create/Delete**.
9. Use the numeric keypad to enter the three-digit Address Numbers of recipients contained in the machine's Address Book.

*Note: Refer to the Address Book Setup topic in this section to learn how to set up address numbers so that they are available for selection here.*

10. Touch **Add to this Group** to add recipients, one number at a time, to the group.
11. When complete, touch **Save**.
12. Touch **Close** to return to the Tools tab screen.
13. To exit the Tools tab screen, if desired, wait several seconds for the Auto Clear service to log you out.

## Comments

This feature can be used to add comments to a Cover Note (Cover Page).

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Touch the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**.
6. Touch **Comments**.
7. Select a Comment number.
8. Touch **Create/Delete**.
9. Enter a Comment, up to 18 characters, then touch **Save**.
10. When complete, touch **Close** until the Tools tab screen is displayed.
11. To exit the Tools tab screen, if desired, wait several seconds for the Auto Clear service to log you out.

## Create a Mailbox

The machine has 200 mailboxes available.

A mailbox must be created before you can use Remote Mailbox or route received documents into mailboxes (using the File Destination / Output Destination settings). Mailbox Fax Receive or Private Polling documents are stored in the Mailbox. This is also convenient for differentiating between received documents and documents to be transmitted (such as by Private Polling).

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**.
6. Touch **Mailbox**.
7. Select an unassigned Mailbox number from the displayed list.

8. Touch **Create/Delete**.
  - a. Check Passcode – Select On or Off, then touch **Save**. Note that it is recommended that you select On, then provide a password, to secure access to your Mailbox.
  - b. Mailbox Name – Enter a name, then touch **Save**.
  - c. Check Passcode – the selections below are viewable when On is selected.
    - Save (Write) - A password is required in selecting a mailbox.
    - Print/Delete (Read) - A password is required to print and delete mailbox documents.
    - Always (All Operations) - A password is required for both operations described above.
  - d. Delete Documents After Retrieval:
    - No - Saves documents in Mailbox.
    - Yes - Deletes documents from Mailbox.
  - e. Delete Documents with Expiration Date:
    - No – Continues to save documents in Mailbox.
    - Yes – Documents will be deleted from Mailbox after expiration date.
  - f. Link Job Flow Sheet to Mailbox: Select this option, then touch Change Settings to link a Job Flow Sheet to this Mailbox. The Job Flow Sheet routes incoming jobs to other destinations specified on the Job Flow Sheet. To create a new Job Flow Sheet, to link to an existing Mailbox, touch **Create/Change Link**. **Note:** For full information on the use of Job Flow Sheets, refer to **Setup and Use of Job Flow Sheets with Mailboxes** in the Options section of this guide.
9. When complete, touch **Close** until the Tools tab screen is displayed.
10. To exit the Tools tab screen, wait several seconds for the Auto Clear service to log you out.



## File Destination / Output Destination

Received Fax documents will be routed to the output tray or Mailbox specified by these settings.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Touch **Fax Mode Settings**.
6. Select **File Destination/Output Destination**.
7. Select the **Box Selector – Line Setup** button.
8. Touch **Change Settings**.
9. Make the appropriate selections and touch **Save** when done.

*Note: If Box Selector is selected as an Output Destination, when On is selected, you will have to enter a mailbox number, then touch Save.*

10. When complete, touch **Close** until the Tools tab screen is displayed.
11. Wait several seconds for the Auto Clear service to log you out.

## Fax Settings (including Fax Defaults and Fax Control)

### Common Settings: Audio Tones and Reports.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Touch **Common Service Settings**.
6. Touch **Audio Tones**.
  - Select an item to change (Tone, Volume, etc...), touch **Change Settings**, set the item, and touch **Save**.
7. Touch **Close** to return to Common Service Settings selections.

8. Touch **Reports**.

Select each item of interest, then touch **Change Settings** to modify the desired setting. Touch **Save** to save any new settings.

- a. Job History Report - Automatically print every 50 print operations. Default is 0=Off.
- b. Activity Report - Automatically print every 100 transactions. Select either On or Off.
- c. Transmission Report-Undelivered - Automatically print. Select either On or Off.
- d. Transmission Report-Job Deleted - Automatically print. Select either On or Off.
- e. Mailbox Report - Automatically print. Select either On or Off.
- f. Broadcast/Multi-poll Report - Automatically print. Select either On or Off.
- g. Relay Broadcast Report - Automatically print. Select from the choices below:

Off

Send to Relay Station

Print at Local Station

Send to Relay, Print at Local

**Note:** A Relay Station is another Fax-capable machine to which faxes can be sent. Use of the second machine can help to cut down on broadcast Fax phone charges, such as those associated with long distance calls.

- h. Scan File Transfer Report
- i. 2 Sided Report - Default is 1 Sided.
- j. Recipient on Activity Report - How many characters from other party is printed on Activity Report. Select from the choices below:
  - First 40 characters.
  - Last 40 characters.
- k. Job Flow Error Report – Automatically print. Select either On or Off.

9. Touch **Close** to return to the Tools tab screen.

## Fax Mode Settings (including Fax Defaults and Fax Control)

These settings include: Screen Defaults, Fax Defaults, Fax Control, File Destination / Output Destination, Reduce/Enlarge Presets, Original Size Defaults, and Local Terminal Information.

For information on **File Destination / Output Destination settings** and **Local Terminal Information settings** refer to the separate topics, with those names, in this Fax section of this guide.

*Note: Information on Fax Defaults and Fax Control is critical to the operation of the Fax feature and should be carefully evaluated to assure that settings are correct for the current working environment.*

1. If necessary, press the **Log In / Out** button and enter [11111] or the current password. Touch **Enter**, then press the **Machine Status button** on the Control Panel.
2. Touch the **Tools tab**, then touch **Fax Mode Settings**.
3. Touch **Screen Defaults**.
4. Select a Line to enter or change, then touch **Change Settings**. Touch **Save** to save any new settings.
  - Fax Screen Default. Select General Settings or Address Book. This will be the Fax service screen that users see when they touch the Fax button.
  - Address Book Default. Leave this setting at the default of 1, or enter an address book (Fax mailbox) number to display when the Address Book button is touched by users of the Fax service screen. Note that the Fax mailbox needs to be created in advance of this setting.
  - Transmission Screen. Select either On or Off.
5. Touch **Close** until the Fax Mode Settings selections are again displayed.
6. Touch **Fax Defaults**.
7. Select a Line to enter or change, then touch **Change Settings**. Touch **Save** to save any new settings.
  - Resolution.
  - Original Type.
  - Lighten/Darken.
  - Mixed Size Originals.
  - Starting Rate – Select G3 Auto or Forced4800bps.
  - Delayed Start – Start Time. This can be a useful feature for saving time-based phone charges.
  - Transmission Header Text. Select On or Off. This adds the sender name and phone number to faxes.
  - Confirmation Options. Select On or Off. If set to On a report will print when transmission completes successfully.
  - Delivery Receipts/Read Receipts.
  - IFax Profile.
  - Ifax Subject.

8. Touch **Close** until the Fax Mode Settings selections are again displayed.
9. Touch **Fax Control**.
10. Select the Line to enter or change, then touch **Change Settings**. Touch **Save** to save any new settings.
  - Re-enter Recipients
  - Re-enter Broadcast Recipients
  - Re-enter Speed Dial Recipients
  - Transmission Header Text – Polling. You can leave this setting at its default value.
  - Documents for Polling – Auto Delete. Set as desired to delete documents from Mailboxes after polling same.
  - Rotate 90 degrees.
  - Sender ID.
  - Save Undelivered Faxes.
  - Save Deleted Faxes.
  - Saved Faxes – Auto Delete.
  - Transmission Interval.
  - Batch Send.
  - Manual Send/Receive Default. Select the default setting for manual Fax operations.

- Fax Receiving Mode. Leave this setting at Auto Receive for unattended operation.
- Border Limit.
- Auto Reduce on Receipt.
- Tray for Printing Incoming Faxes.
- 2 Pages up on Receipt.
- 2 Sided Print.
- Edge Erase – Top & Bottom Edges.
- Edge Erase – Left & Right Edges.
- Reduce 8.5x11 Original to A4.
- Pseudo-Photo Gradation Mode
- Box Selector - Line Setup. Enable this setting to enable Fax Mailboxes to receive incoming faxes.
- Memory Full Procedure.
- Maximum Stored Pages.
- Mixed Sized Originals Scanning Mode.
- Mailbox Receive Display (Priorities 1 through 3).
- Direct Fax – To use Direct Fax from the PCL or PostScript driver, make sure this setting is Enabled.

11. When complete, touch **Close** until the Tools tab screen is displayed.

12. Wait several seconds for the Auto Clear service to log you out.

## **To Configure Fax to Mailbox**

1. Log in at the device.
2. On the Tools tab, touch System Settings.
3. In the Group column, touch Fax Service Settings.
4. Touch System Settings. Under Group, select Fax Service Settings.
  - a. Under Features, touch Fax Control.
    - Touch Mailbox Selector Setup.
    - Touch Change Settings.
    - Touch Enable.
    - Touch Save.
    - Touch Close.
  - b. Under Features, select Fax Received Options.
    - Touch Mailbox Selector Setup.
    - Touch the line you wish to configure.
    - Touch Change Settings.
    - Touch On.
    - Enter the mailbox number (use leading zeros).
    - Touch Save.
    - Touch Close.
    - Touch Close.
5. Log out.

## LAN Fax (PCL Drivers)

You can facsimile documents directly from your PC in the same way you would print a document. This is known as the LAN Fax.

### Initial Setup

Refer to the TCP/IP Peer to Peer (LPR or Standard TCP/IP) Printing topic, in the Print Drivers section, and add the printer to the Windows 2000 or Windows XP desktop using a Standard TCP/IP Port. After the driver has been installed, perform the following steps:

1. Right mouse click on the Printer's icon and select **Properties**.
2. Click the **Options** tab, then click the **Get Information from Printer** button.
3. The **Network Address** box should now be displaying the printer's IP address and a checkmark should appear in the **Enable Bi-Directional Communication** checkbox. Also, the Fax Module listing in the **Items** box should now be displayed as Available.

### Adding a Recipient to a Fax Phonebook

1. From the File menu of your program, select **Print** to display the Print dialog.
2. Check that the correct (PCL) printer is selected, and then click **Properties** to display the Properties dialog.
3. On the **Paper/Output** tab, select **Fax** from the **Job Type** drop-down menu. The options on the Fax tab will now be available for your selection.
4. Select the necessary settings on the Fax tab.
5. Click the **Fax Phonebook** button to select your fax recipient or to enter a new recipient.
6. If your recipient is not selectable from an existing Phonebook, select **New...**, select **Individual**, click **OK**, enter the recipient's Name and Fax number, and click **OK**.
7. Click the **Help** button for any additional help you might need.
8. Click **Close** to close the Fax Phonebook dialog, then click **OK**.

### Sending the Fax

1. When the Print dialog is displayed, click **OK**.
2. On the Fax Recipient dialog, to send to the previously-entered, new recipient, click **Look Up Phonebook**.
3. Double click the name of the new individual previously entered (in step 6 above) and click **OK**.  
*Note: Alternatively, you can manually enter in a Name (of up to 30 characters) and a Fax Number.*
4. Click **OK**, then **OK** again to send your Fax.



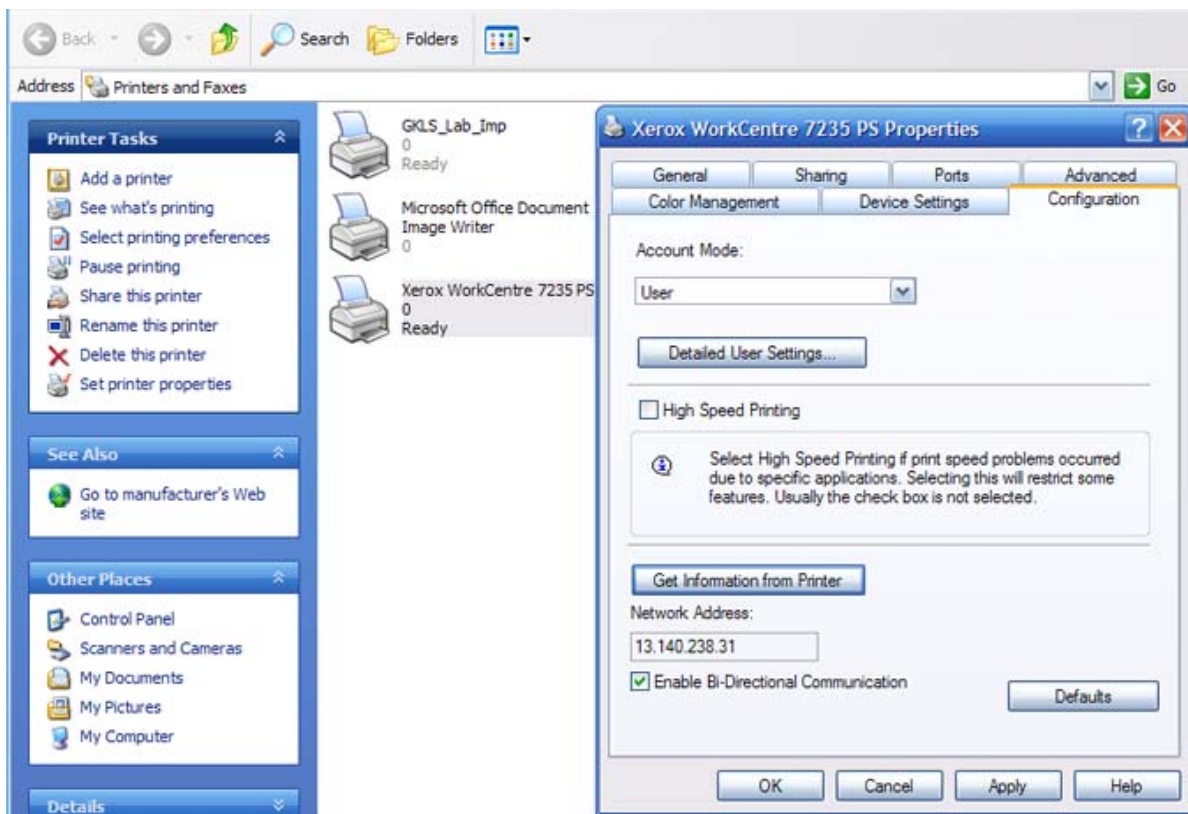
## LAN Fax (PostScript Drivers)

You can facsimile documents directly from your PC in the same way you would print a document. This is known as the LAN Fax.

### Initial Setup

Refer to the TCP/IP Peer to Peer (LPR or Standard TCP/IP) Printing topic, in the Print Drivers section, and add the printer to the Windows 2000 or Windows XP desktop using a Standard TCP/IP Port. After the driver has been installed, perform the following steps:

1. Right mouse click on the Printer's icon and select **Properties**.
2. Click the **Configuration** tab, then click the **Get Information from Printer** button.
3. The **Network Address** box should now be displaying the printer's IP address and a checkmark should appear in the **Enable Bi-Directional Communication** checkbox. Also the Fax Module listing, in the Installable Options folder on the Device Settings tab, should now be displayed as Available. If it is shown as Not Available, click on the selection and set the Fax Module listing to Available.



### Adding a Recipient to a Fax Phonebook

1. From the File menu of your program, select **Print** to display the Print dialog.
2. Check that the correct (PS) printer is selected, and then click **Properties** to display the Properties dialog.
3. On the **Paper/Output** tab, select **Fax** from the **Job Type** drop-down menu. The options on the Fax tab will now be available for your selection.
4. Select the necessary settings on the Fax tab.
5. Click the **Fax Phonebook button** to select your fax recipient or to enter a new recipient.
6. If your recipient is not selectable from an existing Phonebook, select **New...**, select **Individual**, click **OK**, enter the recipient's Name and Fax number, and click **OK**.
7. Click the **Help** button for any additional help you might need.
8. Click **Close** to close the Fax Phonebook dialog, then click **OK**.

### **Sending the Fax**

1. When the Print dialog is displayed, click **OK**.
2. On the Fax Recipient dialog, to send to the previously-entered, new recipient, click **Look Up Phonebook**.
3. Double click the name of the new individual previously entered (in step 6 above) and click **OK**.  
*Note: Alternatively, you can manually enter in a Name (of up to 30 characters) and a Fax Number.*
4. Click **OK**, then **OK** again to send your Fax.

### **Stopping the Fax (when necessary)**

1. Go to the multifunction device and press the **Job Status** button.
2. Select the fax job you wish to cancel, in the **Current and Pending Jobs** list.
3. Press **Cancel** to cancel the job.

# Scan to PC (FTP/SMB)

## Overview

This feature is designed to convert scanned data to TIFF, JPEG, or PDF format, and then use the FTP or SMB protocol to send the data to a computer (server or workstation) on the network.

### *Notes:*

*It is assumed that you purchased the Scanning option to enable Scanning to FTP/SMB with your Device. If you did not, contact your Xerox Representative to purchase this option.*

*For scanning to SMB, make sure that a shared folder is created for saving scanned data on the network.*

*For scanning to FTP, make sure that the server is running the FTP service and that you have created a directory within the FTP root to be used as a scan filing location.*

## Requirements for FTP

When using FTP transmission, one of the following FTP servers, with an account on that server (login name and password), is required.

- Microsoft Windows Server 2003  
FTP service of Microsoft Internet Information Server 6.0
- Microsoft Windows 2000 Server, Microsoft Windows 2000 Professional, or Microsoft Windows XP  
FTP service of Microsoft Internet Information Server 3.0 or later
- Mac OS X  
FTP service of Mac OS X 10.1.5/10.2.x/10.3.8/10.3.9/10.4.2  
Refer to the manual provided with the software for how to configure the FTP service.

## Requirements for SMB

When using SMB transmission, a computer running one of the following Operating Systems, which includes a shared folder, is required.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows XP

## Installation Procedure

This section describes the configuration procedure to use the Scan to PC (FTP/SMB) feature on the machine.

The following two steps are necessary to use the Scan to PC (FTP/SMB) feature.

- Enabling the required ports and Setting TCP/IP

Enable the FTP port and SMB port on the Device, and then set the machine's IP address. If you will be using SMB on a Microsoft Network, make sure to enable either DNS or WINS as part of the TCP/IP configuration. For FTP, make sure that DNS is enabled.

- Preparing an FTP directory or SMB shared folder on the receiving computer (server or workstation).

Create an FTP directory or SMB shared folder to receive scanned documents over the network.

## Enabling Ports and Setting TCP/IP

To use Scan to PC (FTP/SMB) you need to enable the applicable Ports (SMB or FTP client) on the Device, and make sure that an IP address has been set on the machine.

*Note: The configuration can also be performed using CentreWare Internet Services.*

*For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.*

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad or the keyboard displayed on screen, and select **Enter**.

*Note: The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".*
  - c. Press the **Machine Status button** on the Control Panel.
  - d. Touch the **Tools tab**.
2. When using the SMB protocol, enable the SMB port.
  - a. Select **Connectivity & Network Setup**.
  - b. Select **Port Settings**.
  - c. Select **SMB** and then select **Change Settings**.
  - d. Select **Port Status** and then select **Change Settings**.
  - e. Select **Enabled** then select **Save**.
  - f. Select **Close** until the Port Settings screen is displayed.

3. When using the FTP protocol, enable the FTP client port.
  - a. From the Tools tab screen, select **Connectivity & Network Setup**, then **Port Settings**.
  - b. From the Port Settings screen, select **FTP Client** and then select **Change Settings**.
  - c. Select **Port Status** and then select **Change Settings**.
  - d. Select **Enabled** then select **Save**.
  - e. Select **Close** repeatedly until the **Tools tab** screen is displayed.

4. Set an IP address.

**If an IP address is already set, this step is not necessary.** Also, in an environment with DHCP or BOOTP, configure the way to obtain an IP address. If the address cannot be obtained automatically, or static configuration is preferred, configure an IP address, a subnet mask, and a gateway address as follows.

- a. Select **Protocol Settings**.
- b. Select **IPv4 (or other mode) Address Resolution**, then select **Change Settings**.
- c. Select one from [DHCP], [BOOTP], [RARP], [DHCP/Autonet] or [Static], and then select **Save**. If you select anything other than [Static], proceed to Step 5.

*Note: When communicating by TCP/IP make sure to enable the use of a DNS (or WINS for SMB) server. This is done using the machine's Internet Services web pages, displayed by typing the machine's IP address into your web browser (as stated in the TCP/IP Dynamic Addressing Topic of this guide).*

- d. On the Protocol Settings screen, select **TCP/IP – IP Address** and then **Change Settings**.
- e. Enter the IP address using the numeric keypad.

*Note*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

- f. Select **Save**.
- g. Configure **TCP/IP – Subnet Mask** and **TCP/IP – Gateway Address** using the same process as stated above.

*Notes*

*Enter the Gateway address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*Specify the subnet mask by a combination of the numbers 0, 128, 192, 224, 240, 248, 252, 254, and 255. However, you cannot use 0 between non-zero values.*

*If you do not set the gateway address, enter "0.0.0.0".*

5. Select **Close** until the Tools tab screen is displayed.
6. Wait several seconds for the Auto Clear service to log you out.
7. If you changed any settings, the Device will automatically reboot to register and enable your new settings. After the machine is restarted, print out a Configuration Report to confirm that the ports are enabled and TCP/IP is correctly configured.

For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.



# Receiving Computer Configuration

The following describes the configuration procedure for the receiving computer (server or workstation).

## Using with FTP

1. Ensure that File Transfer Protocol (FTP) services is running on the server or workstation where images scanned by the machine will be stored. Note down the IP address or host name.
2. Create a user account and password for the machine. When a document is scanned, the machine logs in using the account, transfers the file to the server or workstation and logs out. Note down the user account and password details.
3. Create a directory within the FTP root to be used as a scan filing location (repository). Note down the directory path.
4. Test the FTP connection by logging in to the scan directory from a PC with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights and the FTP service setup.

## Using with SMB

1. Create a shared folder to be used as a scan filing location (repository) for scanned documents. Note the Share Name of the folder and the Computer Name or Server Name.
2. Create a user account and password for the machine with full access rights to the scan directory. Note down the user account and password.
3. Test the settings by attempting to connect to the shared folder from another PC by logging in with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights.

## Adding the Receiving Computer's Address to the Address Book

To direct your scanned documents to the appropriate receiving computer (server or workstation) you will need to add the Receiving Computer's Address to the machine's Address Book as follows.

1. Press the **Log In / Out button** on the Device's Control Panel.
2. On the keypad enter {11111} or current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel.
4. Touch the **Tools tab**.
5. Select **Setup & Calibration**, then touch **Address Book**.
6. Select an available Address Number.
7. Touch **Create/Delete**.
8. Touch **Address Type**, then touch **Change Settings**.
9. Select **Server** as the address type, and select **Save**.
10. Select each item to be set, and select **Change Settings**. When each setting is complete, select **Save**.
11. Select **Transfer Protocol** from the Configuration Report and select **FTP** or **SMB** or **SMB (UNC format)**.
12. When FTP or SMB is selected, touch **Server Name/IP Address** on the Configuration Report and enter the Host name or IP Address of the computer (server or workstation) designated to receive scanned files. When entering a Host name, use the fully qualified domain name. For example: myhost.example.com. Do NOT use forward or backward slashes.
13. Select **Shared Name (SMB Only)** to enter in the name of the shared folder on the receiving computer. Enter in the name only, without any backward slashes.
14. Select **Save In** to enter the directory for storing documents. When FTP or SMB is selected, supply the name of the directory (without any forward or backward slashes). When SMB (UNC format) is selected, if available, use the Universal Naming Convention format such as \\host name\\shared name\\directory name.
15. Select **User Name** and provide the User account name assigned to the directory on the receiving computer.
16. Select **Password** and provide the password to access the User account on the receiving computer.
17. Select **Port Number** to set the communications port number. A sensible selection is **Standard Port**.
18. When done changing and saving settings, touch **Close** (repeatedly, if necessary) to exit to the Tools tab screen.
19. Wait several seconds for the Auto Clear service to log you out.

## Using the Scan to PC (FTP/SMB) Feature

After the appropriate Ports have been enabled, TCP/IP has been configured, and the receiving computers address added to the Address Book, the Scan to PC (FTP/SMB) feature can be used as follows.

1. Select **Scan to PC** from the All Services screen.
2. Touch **Transfer Protocol**, select a protocol, and touch **Save**.
3. Note that you can touch the blank lines on the screen and manually enter Server settings, or touch **Address Book**. For SMB you can also browse the Microsoft Network.
4. Select the Receiving Computer (workstation or server) in the list contained in the Address Book and touch **Save**.
5. Place your document in the document handler and press the Control Panel's large, green **Start button**. Progress of the data transfer will be displayed on screen.

# Setup and Use of Job Flow Sheets with Mailboxes

## Overview

Job flow is a feature for executing a series of registered actions.

The target of a job flow is documents stored in a Mailbox.

Two methods are available: 1) automatically start a job flow when a document is stored in a Mailbox, or 2) select a job flow to manually act on documents stored in a Mailbox.

To start a job flow, you must **link** the job flow sheet to a Mailbox, or to documents within a Mailbox. Documents are then processed as specified on the job flow sheet.

To automatically link document processing in a Mailbox with a job flow sheet, see **Creating a Mailbox and linking to a Job Flow Sheet (for automatic processing)** in this section of this guide.

To manually link document processing in a Mailbox with a job flow sheet, see **Manually linking a Job Flow Sheet to documents in a Mailbox** in this section of this guide.

### Features supported for Job Flow

Incoming Mailbox Documents	Available Outgoing processing
Faxes for private polling	Printing, Fax forwarding (up to 100 recipients), iFAX transmission (up to 100 recipients)
Scanned documents	Printing, Fax forwarding (up to 100 recipients), iFAX transmission (up to 100 recipients)
Fax to Mailbox	Printing, Fax forwarding (up to 100 recipients), iFAX transmission (up to 100 recipients)
iFAX received	Printing, Fax forwarding (up to 100 recipients), iFAX transmission depending on System Administration mode settings

## Enabling Ports and Setting TCP/IP

In order to use the job flow service, you must enable the SOAP port, the SNMP port, the Internet Service (HTTP) port, and set IP addresses. The procedure for setting the machine is as follows.

*Note: The configuration can also be performed using CentreWare Internet Services.*

*For information on how to use CentreWare Internet Services, refer to the Internet Services section of this guide.*

1. Display the System Administrator Menu screen.
  - a. Press the **Log In/Out** button.
  - b. Enter the user ID with the numeric keypad, or the keyboard displayed on screen, and select **Enter**.

*Note: The default user ID is "11111". When using the Authentication feature, a password is required. The default password is "x-admin".*
  - c. Press the **Machine Status** button on the Control Panel, then touch the **Tools** tab.
2. Enable the SOAP port.
  - a. Select **Connectivity & Network Setup**.
  - b. Select **Port Settings**.
  - c. Select **SOAP** and then select **Change Settings**.
  - d. Select **Port Status** and then select **Change Settings**.
  - e. Select **Enabled** then select **Save**.
  - f. Select **Close** until the Port Settings screen is displayed.

3. Enable the SNMP port.
  - a. Select **SNMP** and then select **Change Settings**.
  - b. Select **Port Status** and then select **Change Settings**.
  - c. Select **Enabled** then select **Save**.
  - d. Select **Close** until the **Port Settings** screen is displayed.
  - e. Enable the **Internet Service (HTTP) port** using the same process as stated above.
  - f. Select **Close** repeatedly until the **Tools tab** screen is displayed.
4. Set an IP address.

**If an IP address is already set, this step is not necessary.** Also, in an environment with DHCP or BOOTP, configure the way to obtain an IP address. If the address cannot be obtained automatically, or static configuration is preferred, configure an IP address, a subnet mask, and a gateway address as follows.

- a. Select **Protocol Settings**.
- b. Select **IPv4 (or other mode) Address Resolution** and then select **Change Settings**.
- c. Select one from [DHCP], [BOOTP], [RARP], [DHCP/Autonet] or [Static], and then select **Save**. If you select anything other than [Manual], proceed to Step 5.

*Note: When communicating by TCP/IP make sure to enable the use of a DNS (or WINS for SMB) server. This is done using the machine's Internet Services web pages, displayed by typing the machine's IP address into your web browser (as stated in the TCP/IP Dynamic Addressing Topic of this guide).*

- d. On the Protocol Settings screen, select **TCP/IP – IP Address** and then **Change Settings**.
- e. Enter the IP address using the numeric keypad.

*Note:*

*Enter the address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

- f. Select **Save**.
- g. Configure **TCP/IP – Subnet Mask** and **TCP/IP – Gateway Address** using the same process as stated above.

*Notes:*

*Enter the Gateway address in the format "xxx.xxx.xxx.xxx". The "xxx" should be a numeric value in the range from 0 to 255. However, 224 - 255.xxx.xxx.xxx and 127.xxx.xxx.xxx cannot be used.*

*Specify the subnet mask by a combination of the numbers 0, 128, 192, 224, 240, 248, 252, 254, and 255. However, you cannot use 0 between non-zero values.*

*If you do not set the gateway address, enter "0.0.0.0".*

5. Select **Close** until the Tools tab screen is displayed.
6. Wait several seconds for the Auto Clear service to log you out.
7. If you changed any settings, the Device will automatically reboot to register and enable your new settings. After the machine is restarted, print out a Configuration Report to confirm that the ports are enabled and TCP/IP is correctly configured.

For information on how to print a Configuration Report, refer to the Configuration Report topic in the Network Connectivity section of this guide.

## Configuring the SNMP Port

Configure the transport protocol for the SNMP port using CentreWare Internet Services.

1. Start a web browser on a network connected workstation.
2. Enter the machine's IP address in the address box of the browser and press **Enter**.
3. Click the **Properties** tab.
4. Click **Port Status**.
5. Select (place a checkmark in) the UDP check box next to SNMP.
6. Click **Apply**.
7. Enter the System Administrator user ID and password when prompted and click **OK**.
8. Click the **Reboot button** when it displays. If a Reboot button fails to display, click the Status tab and click Reboot Machine from that screen.

## Creating Job Flow Sheets

Before you can link a job flow sheet to a mailbox, you need to create at least one job flow sheet. To create a job flow sheet, perform the following steps.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel, then touch the **Tools tab**.
4. Select **Setup & Calibration**.
5. Touch **Create Job Flow Sheets**. Note: If this selection is unavailable, follow the instructions in the next topic, **Creating a Mailbox and Linking to a Job Flow Sheet**, to create your flow sheet.
6. Touch **Create**.
7. Select items to be set from the displayed item list, then touch **Change Settings**. When done, touch **Save**.
8. **Name** – Set the name, up to 128 characters in length, for the job flow sheet.
9. **Description** – Set the description, up to 256 characters in length, for the job flow sheet.
10. **Keyword** – Enter a keyword, up to 12 characters in length, for job flow search.
11. **Send as Fax** – Specify the fax transmission address. You can specify a total of up to 100 addresses, using either Address Numbers or by manual input (New Recipient).
12. **Send as iFAX** – Specify the E-mail address. You can specify the address using either the Address Book, or by manual input (New Recipient).
13. **Send as E-mail** – Specify the E-mail address. You can specify the address using either the Address Book, or by manual input (New Recipient).
14. **Transfer via FTP (1) and (2)** – Specify transfer to an FTP server. You can specify the address using either the Address Book, or by manual entry into the boxes supplied.
15. **Transfer via SMB (1) and (2)** – Specify transfer to an SMB server. You can specify the address using either the Address Book, or by manual entry into the boxes supplied.
16. **Print** – Select **On** (if desired), then specify Print and Finishing settings. This prints a copy of your document after it has been scanned.
17. When done with setting selections, touch **Save**.
18. Touch Close or Exit to exit the Setup Menu screen and return to the Tools tab screen.
19. Wait several seconds for the Auto Clear service to log you out.



## Creating a Mailbox and linking to a Job Flow Sheet (for automatic processing)

Before you can link a job flow sheet to a mailbox, you need to create at least one mailbox for your use. In the process of creating the mailbox, you can link to your newly created Job Flow Sheet.

To create a mailbox and link it to a Job Flow Sheet (for automatic processing), perform the following steps.

1. Press the **Log In / Out button** on the Device's Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times.
3. Press the rectangular **Enter** button on the touch screen.
4. Press the **Machine Status button** on the Control Panel, then touch the **Tools tab**.
5. Select the **Setup & Calibration** button.
6. Press the **Create Mailbox** button.
7. When the numbered list of Mailboxes is shown on screen, use the supplied arrow keys to scroll through the list to locate an unassigned Mailbox number.
8. Select an unassigned Mailbox number from the displayed list.
9. Press the rectangular **Create & Delete** button in the lower right corner of the Mailbox selection screen.
10. When the **New Mailbox - Passcode** screen displays, use the **On** and **Off** buttons on the left-hand side of the screen to determine whether or not a password will be required to access the Mailbox. If On is selected, use the Device's numeric keypad to enter in a numbered passcode of up to 20 digits.
11. Press the **Save** button to save your settings. (To exit the screen, without saving settings, press the Cancel button.)
12. When the Mailbox settings screen displays (after assigning a password), note that you have five setting selections displayed on five numbered horizontal lines. The available selections include: Mailbox Name, Check Passcode, Delete Documents After Retrieval, Delete Expired Documents, and Link Job Flow Sheet to Mailbox.
13. To assign a name to the Mailbox, press the **Mailbox Name** selection line.

14. Press the rectangular **Change Settings** button.
15. Use the touch screen keyboard to enter in a name for your Mailbox.
16. When finished entering in a name, press the **Save** button in the upper right corner of the screen. (To exit the screen, without saving changes, press the Cancel button.)
17. On the Mailbox settings screen, press any other selection lines of interest and use the **Change Settings** button, as previously described, to access and make setting changes. Use the **Save** button to save your changes.
18. To link this Mailbox with your Job Flow Sheet, touch **Link Job Flow Sheet to Mailbox** and touch **Change Settings**.
19. Touch **Create/Change Link** to set the Mailbox link to a previously-created Job Flow Sheet. Note: If no Job Flow sheets are displayed, press **Create** to create one and follow the instructions supplied in the **Creating Job Flow Sheets** topic in this section.
20. Select your Job Flow Sheet from the list (clicking Refresh, if necessary) and touch **Save**.
21. Touch the **Auto Start** checkbox to place a checkmark in the box for automatic processing of documents as they are received in the Mailbox.
22. To exit the Link Job Flow Sheet to Mailbox screen, press the rectangular **Close** button in the upper right corner of the screen.
23. To exit the Mailbox settings screen, press the rectangular **Close** button in the upper right corner of the screen.
24. To exit the screen that lists all assigned and unassigned Mailboxes, returning to the Tools tab screen, press the **Close** button.
25. Wait several seconds for the Auto Clear service to log you out.

## Manually linking a Job Flow Sheet to documents in a Mailbox

1. Touch **Send from Mailbox** on the All Services screen.
2. Select a **Mailbox**, enter the password, then touch **Confirm**.
3. On the **Document List** screen, select a document.
4. Touch **Job Flow Settings**.
5. Touch **Select Job Flow Sheet**.
6. Select a job flow sheet and press the on-screen **Start** button.

## Testing Job Flow Sheet operation (for automatic processing)

1. Touch **Scan to Mailbox** on the All Services screen.
2. Select your Mailbox, enter the password, then touch **Confirm**.
3. Place a document in the document handler.
4. Select your scanning options.
5. Press the Control Panel's large, green **Start button**.
6. Check the destination that was specified on your Job Flow Sheet to verify that the document was received.

# Scan to PC Desktop

## Overview

Scan to PC Desktop is now a core element of the Xerox FreeFlow Digital Workflow collection for the office.

What was once called Scan to PC Desktop Deluxe is now known as Scan to PC Desktop Professional. The components in this solution include: PaperPort Professional 10, OmniPage Professional 14 Office, and Image Retriever Professional 5.2.

What was once called Scan to PC Desktop Standard is now known as Scan to PC Desktop SE. The components in this solution include: PaperPort 10 SE, OmniPage SE 3.0, and Image Retriever SE 5.2.

With either solution, the purpose of PaperPort is to create a program on the networked PC, providing a windows-style desktop for the management of scanned image and text items.

The purpose of OmniPage is to quickly turn PDF files into easily editable word processing and spreadsheet documents.

The purpose of Image Retriever 5.2 is to provide a method to monitor a specified server folder for incoming scanned items. Monitoring of E-mail can also be added in the case of the Professional program edition.

The Scan to PC Desktop solution is typically sold in 25 user licenses packages. For enterprises requiring more than 100 licenses, however, special pricing is available. Consult your Xerox Representative for details.

## Preparations

Perform the procedures for setting up this device to Scan to SMB, as stated in the **Scan to PC (FTP/SMB)** section of this guide.

## Software Installation Procedure

To install Scan to PC Desktop components on networked workstations, refer to the Scan to PC Desktop Network Installation Guide, Version 7.0. This document should have come with your software license package, and is also available from [www.support.xerox.com](http://www.support.xerox.com). If you go to the website, type Scan to PC Desktop in the upper right corner Search box and press **Enter**. Select **Support** under FreeFlow Scan to PC Desktop. Select your language and click **Go**.

*Note: The software manufacturer requires PaperPort to be installed before Image Retriever in all cases. Also, during the installation of PaperPort Professional 10, PDF Create! 2.0 must be installed.*

## Configure Image Retriever 5.2 on Networked Workstations

Referring to the **Scan to PC Desktop: Image Retriever 5.2** documentation, configure Image Retriever 5.2 on the networked workstations.

## Testing Scan to PC Operation

1. Perform a scan at the multifunction device.
2. Go to a networked workstation running Image Retriever 5.2.
3. Right click on the **Image Retriever icon** in Windows.
4. Click the **Settings** command to display the Image Retriever Settings dialog.
5. Verify that the SMB Repository (server) UNC is pointing correctly to the server and shared folder.
6. Click **Get Now**.
7. Start the PaperPort program and verify that the scanned item appears on the PaperPort desktop.

# Network Scanning (using templates)

## Overview

Network Scanning is an optional feature for this multifunction device, available for purchase from your Xerox Sales Representative.

Network Scanning allows a user to scan an original document and convert it to an electronic file. The final destination of the electronic file depends on the template chosen by the user at the device's User Interface.

The template may reside on the device, or may be cached on the device from a pool of templates pulled from a remote server.

The set up of templates, template pool servers, and file repositories is accomplished using Centware Internet Services (the device's internally-contained web pages) as stated in this section.

Once the scanned file is stored on the pre-determined server, the file can be redirected and manipulated with such software as the following:

### **SMARTsend scanning services**

Built on the Microsoft .NET platform, this server-based software works with new and legacy Multifunction Systems to enable hardcopy documents to be scanned in black and white or color, and converted into such standard digital formats as PDF, JPEG, and TIFF. This Web-based application requires no additional client software installation and uses wizards to simplify workflow (template) creation. Once a workflow, or distribution process, is created, it can be saved as a paper or electronic cover sheet. The cover sheet can be set up to direct the scanned file to a wide variety of destinations. Such destinations include an email address or distribution list, network folder, FTP folder, remote printer, Web URL, Domino.doc, Domino, Microsoft SharePoint and Xerox DocuShare.

### **Scan to PC Desktop**

For information regarding the use of Scan to PC Desktop, including Paperport, OmniPage, and ImageRetriever applications, see the **Scan to PC Desktop** topic in the **Options** section of this guide.

## Additional Notes

### Network Scanning User Authentication

Authentication can be enabled to prevent unauthorized access to the Network Scanning feature. If Authentication is enabled, users will be prompted to enter a 4 to 12 digit pass code before they can access the Network Scanning feature. For a full description of the Authentication feature refer to the **Security - Authentication** topic in this guide.

### Multifunction Device Authentication

If using a SMARTsend server, a valid Windows account must be created on the SMARTsend Server for the device's authentication. The account enables each device to communicate with the SMARTsend server to exchange template information and other configuration data. For account creation instructions, refer to the FreeFlow SMARTsend Installation and Administration Guide.

### Template Considerations when using SMARTsend

A single Xerox multifunction device cannot use both CentreWare Network Scanning services and SMARTsend. If legacy CentreWare Network Scanning Services templates need to be utilized within SMARTsend, use the SMARTsend Template Importer to import the desired templates, as stated in the FreeFlow SMARTsend Installation and Administration Guide.

### Use of a Validation Server

If you will be communicating with HTTPS to servers using SSL/TLS encryption, you can set the host name and directory (which might be a cache on a Repeater) of the Validation Server used to validate Digital Certificates over the enterprise network. To set these parameters, enter the IP Address of the multifunction device into your web browser and press **Enter**. Click the **Properties** tab of displayed Internet Services (the device's web pages), then click the **Services** folder. Select **Network Scanning**, then **Validation Server**. Select HTTP or HTTPS, enter the host name of the server, then enter the directory name (if required) specified by the Validation Server manufacturer. Click **Apply**.

## Installation Checklist

Please ensure that the following items are available or have been performed.

1. Ensure the machine is fully functioning on the network prior to installation.
2. Enable the purchased Scanning option. For instructions, refer to the **Enabling Options with Software Keys** topic, in the **Options** section of this guide. Contact your Xerox Sales Representative if you have not purchased the Scanning option.
3. Ensure that the TCP/IP and HTTP protocols are configured on the device and are fully functional. This is required to access CentreWare Internet Services to configure Network Scanning. The Internet Services function is accessed through the embedded HTTP server on the machine and allows System Administrators to configure scan settings by using an Internet browser.

To verify that the TCP/IP and HTTP protocols are correctly configured, print a Configuration Report as stated in the **Configuration Report** topic in the Network Connectivity section of this guide.

To configure TCP/IP, refer to the **TCP/IP Configuration** topic in the NOS Selection section of this guide.

To enable HTTP, refer to the **Enable Internet Services (HTTP)** topic in the Network Connectivity section of this guide.

4. Ensure that the **FTP Client** and **SMB** port are enabled on the device. To verify this, print a Configuration Report as stated in the **Configuration Report** topic in the Network Connectivity section of this guide.

To enable SMB, refer to **Enabling the SMB Setting at the Device** in the Microsoft (NetBIOS over IP) Networks topic of this guide. To enable FTP, use the same SMB enabling procedure, and simply choose FTP as the port to enable.

5. Note that after configuring a scan filing location (file repository) you need to create at least one template for users to select to scan their documents to the pre-configured repository.



## Configure a Scan Filing Location

Scanning with the machine is accomplished through user selection of templates on the device that route scanned jobs to network servers. After storage on the server, the files can be retrieved at any properly configured networked workstation. A dedicated file server is not required to receive scans. A dedicated server is required, however, for the installation and use of SMARTsend software to remotely manage the pool of templates (workflows), displayed locally to device users, if so desired. Scanning is configured on the machine using one of the file transfer options below. Select your method by clicking one of the buttons, below.

**FTP (File Transfer Protocol):** Requires an FTP service running on a server or a workstation.

**SMB (Server Message Block):** Available for filing to an environment that supports the SMB protocol.

*Note: As other filing methods become available, their configuration will be similar to the procedures for configuring scan filing repositories using FTP and SMB described in this section.*

## Configure a Scan Filing Repository using FTP

### Installation Checklist

1. Ensure that a File Transfer Protocol (FTP) service is running on the server or workstation where images scanned by the machine will be stored. Write down the IP address or host name.
2. Create a user account and password for the machine. When a document is scanned, the machine logs in using the account, transfers the file to the server or workstation and logs out. Write down the user account and password.
3. Create a directory (folder) within the FTP root to be used as a scan filing location (repository). Write down the directory name.

### Enter the Scan Repository Details via Internet Services

4. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
5. Click the **Properties** tab.
6. Click the **Services** folder, then the **Network Scanning** file folder.
7. Click the **File Repository Setup** link.
8. Select **Edit**, or a File Repository Setup number in the **Default File or Alternate File Destinations** list, then click Edit.
9. Enter a **Name** to describe the File Repository.
10. Select **FTP** for **Protocols**.
11. Enter either an IP Address or Host Name for the server.
12. Enter **21** for **Port Number**.
13. For **Document Path**, type in the name of the folder on the remote server that has been set up to receive device scans. Do not use forward slashes as the device will add them by default.
14. Supply the **Login Name** and **Password** for the machine to log into the file server. Note that the default login method is System (for automatic device log in).
15. Re-enter the password in the **Retype Password** box.
16. Click **Apply**.
17. Enter the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.
18. Test the FTP connection by logging into the scan directory from a remote PC using the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function, check the user account access rights and FTP service setup.

## Configure General Settings

19. Click the **General** hot link.
20. To print a Confirmation Sheet after every scan job, select **On** from the Confirmation Sheet drop-down menu.
21. Check the **User Name** and **Domain Name** boxes if you want these items to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
22. Click **Apply**.
23. Enter the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.

## Configure a Scan Filing Repository using SMB

### Installation Checklist

1. Create a shared folder to be used as a scan filing location (repository) for scanned documents. Note the Share Name of the folder and the Computer Name or Server Name.
2. Create a user account and password for the machine with full access rights to the scan directory. Write down the user account and password.
3. Test the settings by attempting to connect to the shared folder from another PC by logging in with the user account and password. Create a new folder within the directory and then delete the folder. If you cannot perform this function check the user account access rights.

### Enter the Scan Repository Details via Internet Services

4. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
5. Click the **Properties** tab.
6. Click the **Services** folder, then the **Network Scanning** file folder.
7. Click the **File Repository Setup** link.
8. Select **Edit**, or a File Repository Setup number in the **Default File or Alternate File Destinations** list, then click Edit.
9. Enter a **Name** to describe the File Repository.
10. Select **SMB** for **Protocols**.
11. Enter either an IP Address or Host Name for the server.
12. Enter **445** for **Port Number**.
13. Enter the Share Name in the **Share** box.
14. For **Document Path**, type in the name of the folder on the remote server that has been set up to receive device scans. Do not use back slashes as the device will add them by default.
15. Supply the **Login Name** and **Password** for the machine to log into the file server. Note that the default login method is System (for automatic device log in).
16. Re-enter the password in the **Retype Password** box.
17. Click **Apply**.
18. Enter the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.

## Configure General Settings

19. Click the **General** hot link.
20. To print a Confirmation Sheet after every scan job, select **On** from the Confirmation Sheet drop-down menu.
21. Check the **User Name** and **Domain Name** boxes if you want these items to appear on the Job Log. The Job Log works with the Document Management Fields feature and is filed with the scan job.
22. Click **Apply**.
23. Enter the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.

## Configure Scan to HTTP

The device can be configured to scan to either an HTTP or an HTTPS destination. To set up a remote template pool repository, see the next procedure.

### To configure the Scan Repository Details using CentreWare Internet Services:

1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Services** folder, then the **Network Scanning** folder.
4. Click the **File Repository Setup** link.
5. On the File Repository Setup page, in the **Default File Destination** box, click **Edit**.
6. On the File Destination page, in the **Settings** area:
  - a. On the **Friendly Name** line, type the name of the file destination.
  - b. In the **Protocol** drop-down box, click **HTTP** or **HTTPS**.  
The **Settings** area refreshes and displays more options.
  - c. If you are using HTTP:
    - On the **Host Name / IP Address & Port** line, type either an IP Address or Host Name for the server.
    - In the Port Number box (unlabeled), type **80** for the port number.
  - d. If you are using HTTPS:
    - On the **Host Name / IP Address & Port** line, type either an IP Address or Host Name for the server.
    - In the Port Number box (unlabeled), type **443** for the port number.
    - If you are using SSL, click the **Validate Repository SSL Certificate (trusted, not expired, correct FQDN)** check box.
  - e. For either HTTP or HTTPS, if you are using a proxy server:
    - Click **View HTTP Proxy Server Settings**.
    - On the Proxy Server page, verify that the settings match those in your proxy server environment. Make changes as needed, then click **Apply**.
  - f. On the **Document Path** line, type the HTTP address.  
Example: /Inetpub/wwwroot/scans/
  - g. In the **Login Credentials to Access the Destination** area, click your choice of log in credentials to be used.
  - h. Type the **Login Name** and **Password** for the machine.
  - i. Type the password in the **Retype Password** box.
  - j. Click **Apply**.
7. If prompted, type the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.
8. To set up a remote template pool repository, see the next procedure, **Setting up a Remote Template Pool Repository**.

### Setting up a Remote Template Pool Repository (optional)

1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Services** folder, then the **Network Scanning** file folder.
4. Click the **Advanced** folder, then click the **Template Pool Setup** link.
5. On the Template Pool Setup page, in the **Remote Template Repository** area:
  - a. In the **Protocol** drop-down box, click **HTTP** or **HTTPS**.  
The **Remote Template Repository** area refreshes and displays more options.
  - b. If you are using HTTP:
    - On the **Host Name / IP Address & Port** line, type either an IP Address or Host Name for the server.
    - In the Port Number box (unlabeled), type **80** for the port number.
  - c. If you are using HTTPS:
    - On the **Host Name / IP Address & Port** line, type either an IP Address or Host Name for the server.
    - In the Port Number box (unlabeled), type **443** for the port number.
    - If you are using SSL, click the **Validate Repository SSL Certificate (trusted, not expired, correct FQDN)** check box.
  - d. For either HTTP or HTTPS, if you are using a proxy server:
    - Click **View HTTP Proxy Server Settings**.
    - On the Proxy Server page, verify that the settings match those in your proxy server environment. Make changes as needed, then click **Apply**.
  - e. On the **Script path and filename (from HTTP root)** line, type the script path and filename (from HTTP root).  
Example: /xerox.asp
  - f. On the **Document Path** line, type the HTTP address.  
Example: /inetpub/wwwroot/scans/
  - g. Type the **Login Name** and **Password** for the machine.
  - h. Type the password in the **Retype Password** box.
  - i. Click **Apply**.
6. If prompted, type the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.

## Configuring the Default Template with Internet Services

You need to create at least one template for users to select to scan their documents to the pre-configured repository. This template is often referred to as the Default Template. The template can be created with either Internet Services or SMARTsend software running on a remote template pool server. Once a default template has been created, users can use the Scan tab of Internet Services to create individual templates, using the default template as a base.

**To create and configure the default template with Internet Services, perform the following steps:**

1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Services** folder, then the **Network Scanning** file folder.
4. Click the **Default Template** link.
5. To edit the filing destinations, on the **Default Template** page, in the **File** area, click **Edit**.
6. In the **Filing Destination** area:
  - a. Select a filing policy from the drop-down list. Note that you can simply accept the default policy (Rename New File).
  - b. For File Destination, note that the displayed destination should match the information previously entered when you configured your Scan Filing Repository. If you have more than one repository, the drop-down list allows you to choose your repository.
  - c. To add a scanning destination subdirectory, in the **Add (Optional)** box, type the name of the subdirectory to be added.
  - d. Click **Apply** to save any changes, or **Undo** to exit without saving changes. If you clicked **Apply**, be prepared to enter the administrator User Name (default of 11111) and Password (default of x-admin), if prompted.
7. Document Management Field (Optional)

Click **Add** to add data fields to the template. Note that if the box contains listings, you can make individual selections, then click Edit instead. This information is filed with your scanned document in the Job Log. The Job Log can then be accessed by third-party software and the information retrieved and associated with the scanned file.

  - a. Click **Add**.
  - b. Refer to the displayed descriptions to set your parameters as desired.
  - c. Click **Apply** when done.
8. To set parameters for the default template, select **Edit** for any of the available categories of settings. These include: Network Scanning, Advanced Settings, Layout Adjustment, Filing Options, Report Options, Network Scanning Image Settings, and Compression Capability. Click **Apply** to save your settings.
9. Linearized PDF files allow the first page of a large PDF file to be displayed in a user's Web browser, before the entire file is downloaded from the Web server. This fast first page display helps to alleviate Internet user frustration in waiting for an entire file to download before displaying the file's contents.

**To set the device to create linearized PDF files:**

- a. On the Default Template page, in the **Network Scanning Image Settings** area, click **Edit**.
  - b. In the **Fast Web Viewing Options** area, click **Linearized PDF**.
  - c. Click **Apply**.
10. **Searchable PDF and PDF/A.** The Searchable Format provides a second layer of data with the text of the scanned document. The second layer is converted to an optical character readable format,



enabling the text of the document to be searched on, copied, and pasted, as desired.

**To set the device to create searchable PDF files:**

- a. On the Default Template page, in the **Network Scanning Image Settings** area, click **Edit**.
- b. In the **Searchable PDF Defaults** area, click **Searchable**.
- c. Click **Apply**.

**XPS** is Microsoft's new electronic paper format, an alternative to PDF. XPS is currently supported as a saved file format in Microsoft Office 2007, with an XPS viewer built into Windows Vista. Microsoft states that Windows Vista uses the XPS format as a document format, a windows spool file format, and a page description language for printers.

Note regarding **Searchable XPS**: If this option is available, the Searchable Format provides a second layer of data with the text of the scanned document. The second layer is converted to an optical character readable format, enabling the text of the document to be searched on, copied, and pasted, as desired.

Select **MRC Compression**, if available, to use Mixed Raster Content (MRC) compression. MRC is used to divide the scanned image based on content, and then compress each area in the optimal manner for that image area. This option allows for smaller output files with better image quality.

## Setting up a Remote Template Pool Repository (optional)

1. At your workstation, open your Web browser and enter the IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Services** folder, then the **Network Scanning** file folder.
4. Click the **Advanced** folder, then click **Template Pool Setup**.
5. For **Protocol**, use the drop-down menu to select the protocol you will be using to communicate with the template pool server. Current selections are FTP, NewWare, SMB, HTTP, and HTTPS. Other selections, when available, will be set up similarly.
6. Supply the **Host Name / IP Address** (and Share Name, in the case of SMB).
7. Supply the **Port Number**. The default is 21 for FTP, 445 for SMB, and 80 for HTTP and HTTPS.
8. For **Document Path**, type in the name of the folder on the remote server containing the pool of templates. Do not use forward slashes with FTP or back slashes with SMB.
9. Supply the **Login Name** (account name) and **Password** for the device to access the remote server.  
*Note: For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide.*
10. Re-enter the password in the **Retype Password** box.
11. If available, check the Polling Settings checkbox to set up automatic, timed polling with the template pool server. This will help to assure that the latest scanning templates are available to users of the machine.
12. Click **Apply**.
13. Enter the administrator User Name and Password and click **OK**. The default is 11111 and x-admin.

## Testing Network Scanning (using templates)

1. Go to the machine and press the **All Services button**.
2. Press the **Network Scanning** button.
3. See if the template you created is displayed on screen.
4. If it is, press it. If it is not, return to the beginning of this section and repeat the required procedures.
5. Place a document in the document handler and press the **Start button** located to the immediate right of the Control Panel's numeric keypad.
6. On a network-connected PC, open a connection to the repository server, log in, and see if the document arrived in the repository folder.

## Web Service (if available)

The Web Service button on the machine, if available, enables users to view Internet or Intranet web servers on the machine's User Interface, and to send scanned files to web servers through job flow sheets, if the server login and password are valid as entered on the job flow sheet. In addition to performing the set up procedure described here, make sure to refer to the **Proxy Server Settings** topic, in the **Network Connectivity** section of this guide, for instructions on setting up Proxy Server parameters (similar to setting up connections for a standard web browser). To set up and use Job Flow Sheets with Mailboxes, refer to that topic in the Options section of this guide.

1. Press the **Log In / Out** button to enter System Administration Mode.
2. On the keypad enter [11111] or the current password. Touch **Enter** when finished.
3. Press the **Machine Status button** on the Control Panel, then touch the **Tools tab**.
4. Use the arrow control in the **Group** menu to scroll to **Web Browser Setup**.
5. Touch **Web Browser Setup**.
6. Touch **Access to Web Sites**, then touch **Change Settings**.
7. Touch **Enabled**, then touch **Save**.
8. Select any other settings of interest and use the **Change Settings** and **Save** buttons, as required.
9. Touch **Close** to return to the Tools tab screen.

### Enable the WebDAV port (for name space management)

1. Use the arrow control in the **Group** menu.
2. Touch **Connectivity & Network Setup**.
3. Touch **Port Settings**.
4. Scroll to **WebDAV**, touch the selection line, then touch **Change Settings**.
5. Touch **WebDAV – Port Status**, then touch **Change Settings**.
6. Touch **Enabled**, then touch **Save**.
7. Touch **Close** repeatedly until the Tools tab screen is displayed, then wait for the Auto Clear service to reboot the machine.
8. Return to the WebDAV settings screen and verify that the **Port Number** is set to 80 and that a **Timeout** value (30 or more seconds) has been set.
9. Make any changes desired, then touch **Close** repeatedly until the Tools tab screen is displayed.
10. Wait several seconds for the Auto Clear service to log you out.

# Security – Authentication

## Overview

### Users Controlled by Authentication

#### Authenticated Users

These are users who are registered with the machine. When using a restricted service, authenticated users are prompted to type their user IDs on the authentication screen.

#### Guest Users

These are users who are permitted to use the machine using the Guest password set by the System Administrator.

### Authentication Configuration and related Types

**No Login Required** – Users can access any service without restriction. This is the default type for the machine.

**Login to Local Accounts** – This type uses the user information registered on the machine to manage authentication.

**Login to Remote Accounts, matched with Network Accounting as Accounting Type** – Network Access (authentication) uses the user information managed on a remote accounting service to manage authentication.

User information, managed on the remote accounting service, is sent to be registered on the machine. When the user information on the remote accounting service is updated, the updated information must be sent from the remote accounting service to the machine.

Network Access allows a unified management of user information for multiple devices.

**Login to Remote Accounts, with Accounting Type set to Off or Disabled** – Remote authentication uses a remote authentication server to manage user access to the machine. User information is not required to be registered locally on the machine. Note that with remote authentication you cannot have as much individual service restriction as you have with Local machine authentication. To increase control over individual service access, with a system such as Kerberos, for example, you need to use an Authentication Agent (which, as of February 2007 was still available from the Authentication System hot link of the Remote Authentication / Directory Service folder of Internet Services).

*Note: When registering user information on a remote authentication server, use up to 32 characters for a user ID and up to 128 characters for a password. Note, however, for SMB the password limit is 32 characters.*

**Login Type set to Xerox Secure Access with Accounting Disabled** – When the Login Type is set to Xerox Secure Access, you will also need to configure a networked Authentication Server to supply credentialing information to the Secure Access Server. The Authentication Server can be running Kerberos, SMB, or LDAP and is configured as stated in the Configuring Remote Authentication topics of this guide section. Note that the Accounting Type can also be set to Network Accounting, to work with a networked accounting package, as stated in the Configuring Xerox Secure Access topic, in this section of this guide.

Refer to the Equitrac™ documentation for further setup instructions.

## Services Managed by User ID Authentication

The services that can be managed by user ID authentication vary depending on the selected Authentication mode. The following tables provide a summary of these managed services for each mode.

### When Local Machine Access is enabled

Service	Manageable by Authentication?
Copy	Yes
Print	Yes
Charge Print, Private Print	Yes
Scan Service	Yes
Fax, iFAX	Yes
Direct Fax	Yes
Report/List	No

### When Network Access is enabled

Service	Manageable by Authentication?
Copy	Yes
Print	Yes
Charge Print, Private Print	Yes
Scan Service	Yes
Fax, iFAX	Yes
Direct Fax	Yes
Report/List	No

### When Remote Access is enabled

Service	Manageable by Authentication?
Copy	Yes
Print	No
Charge Print, Private Print	Yes
Scan Service	Yes
Fax, iFAX	Yes
Direct Fax	No
Report/List	No

## Effects of Authentication on Job Flow Sheets and Mailboxes

When Login to Local Accounts is enabled, even if authentication is not enabled for the copy, fax, scan, or print services, authentication will be required for mailbox and job flow sheet operations.

For full details on the effects of Authentication on Job Flow Sheets and Mailboxes, refer to that topic in the Device's User Guide.

## Configuring Local machine authentication

When Login to Local Accounts is enabled, the System Administrator can define pass codes for authorized users (and guests, when the selection is available) to use to authenticate to the system and access restricted services.

### Preparations:

1. Ensure the machine is fully functional on the network.
2. Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional. Refer to those topics in this guide for configuring information as required. This is required to access CentreWare Internet Services to configure Authentication. The Internet Services function is accessed through the embedded HTTP server on the machine and allows System Administrators to configure Authentication settings by using an Internet browser.

### At Your Workstation:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Select the **Security** folder, then the **Authentication Configuration** hot link.
4. Select **Login to Local Accounts** from the Login Type drop-down list, then **Local Accounting** from the Accounting Mode drop-down list.
5. Place a checkmark in the **Enable** box for each service that you wish to restrict access to. For explanations of each service, click the Help button.
6. If available for selection, enable Guest User authentication from the associated drop-down list.
7. Enter the Guest Password twice in the text boxes supplied.
8. Click **Next**.
9. **To configure Authentication for each account user**, enter an Account Number in the Account Number box and click **Edit**.
10. Enter the Administrator User name (default of 11111) and password (default of x-admin) if prompted.
11. Fill in the settings for the user. For explanations of each setting, click the Help button.

*Note: Important: Set each Service Feature Access as desired. DO NOT set a Service Feature Access to "No Access," unless you wish to deny user access to that specific feature.*

12. Click **Apply**.

*Note: You can also use the User Interface at the Device to configure Local machine authentication. The menu path to follow there is: press Log In/Out, enter the Administrator password (default of 11111), press the Machine Status button, touch the Tools tab, and finally touch Auditron Administration.*

## Configuring Remote Authentication

When Login to Remote Accounts is enabled, users of the device will be asked to provide a user name and password to be validated by the designated authentication server. If this validation is successful, the machine and any restricted services will be available for individual use.

### Preparations:

1. Ensure the machine is fully functional on the network.
2. Ensure that the TCP/IP, with DNS/WINS enabled, and HTTP protocols are configured on the device and fully functional. Refer to those topics in this guide for configuring information as required. This is required to access CentreWare Internet Services to configure Authentication. The Internet Services function is accessed through the embedded HTTP server on the machine and allows System Administrators to configure Authentication settings by using an Internet browser.
3. Ensure the Authentication Server to be used is functional on your network. Refer to your manufacturer's documentation for instructions to complete this task.

### At Your Workstation:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Select the **Security** folder, then the **Authentication Configuration** hot link.
4. Select **Login to Remote Accounts** from the Login Type drop-down list, then typically **Accounting Disabled** from the Accounting Mode drop-down list.
5. Place a checkmark in the **Enable** box for each service that you wish to restrict access to. For explanations of each service, click the Help button.

*Note: If a Guest User box is available and configurable, consider whether it is advisable in your network environment to allow simple password, guest access to this restricted service device. The default setting is Off.*

6. Click **Next**.
7. Click **Configure** for Authentication System.
8. Select your system from the drop-down list and click **Apply**.



## Configure Remote Authentication for Kerberos (Windows 2000)

### At your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab and return to the Security folder.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick Kerberos (Solaris) from the drop-down list. Click **Apply**.
5. Select **Kerberos Server Settings**.
6. Enter the IP Address of the Primary Server (Domain Controller running the Key Distribution Center service).
7. Enter the IP Address of the Secondary Server (Domain Controller), if necessary.
8. Enter details of the Windows 2000 Domain in the Realm Name box. For example: example.com.
9. Enter details for up to 4 alternate Domain Controllers and backups, if required.
10. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for Kerberos (Solaris)

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab and return to the Security folder.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick Kerberos (Solaris) from the drop-down list. Click **Apply**.
5. Select **Kerberos Server Settings**.
6. Enter the IP Address of the Primary Server (the server running the Key Distribution Center service).
7. Enter the IP Address of the Secondary Server, if necessary.
8. Enter details for the Realm. For example (in upper case): EXAMPLE.COM.
9. Enter details for up to 4 alternate servers and backups, if required.
10. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for SMB

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab and return to the Security folder.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick SMB from the drop-down list. Click **Apply**.
5. Select **SMB Server Settings**.
6. From the **SMB Server Setup** drop-down menu, select your desired method. The selections include: By Domain Name, and By Domain Name and Server Address / IP Address.
7. Enter the **Domain name** (up to 15 characters) in the SMB Server – Domain Name box, for every Domain Controller specified. This entry is required regardless of the selection made from the SMB Server Setup drop-down menu.
8. Enter the **IP Address** of the Domain Controller in the SMB Server – Server Name / IP Address box (if By Domain Name and Server Address / IP Address was selected for SMB Server Setup).
9. Enter the IP Addresses of up to 4 additional Backup Domain Controllers, if applicable.
10. If you choose not to enter IP addresses, enter the **Server Name** (up to 64 characters) in the SMB Server – Server Name / IP Address box (if By Domain Name and Server Address / IP Address was selected for SMB Server Setup).
11. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for LDAP

Refer to your LDAP server documentation for the full range of information that can be entered into this LDAP dialog to fully support both E-mail applications and authentication using your LDAP server.

The path to the LDAP dialog is as follows:

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab.
4. Click the **Connectivity** folder, then the **Protocols** folder, then the **LDAP** folder.
5. Select **LDAP Directory**.
6. Click **LDAP Server**, and under Server Information, enter the IP address (or host name) in the box supplied. Note: If entering a fully qualified host name (for example, ldapserver.xerox.com), make sure that the specified domain name matches the device's TCP/IP configuration (domain name shown under DNS on the device's Configuration Report).
7. Enter the **Port Number** (default of 389).
8. If available, decide whether or not to use encryption (**Authentication with SSL**) when accessing the LDAP server.
9. Specify the LDAP Server environment from the Server Application drop-down list.
10. If desired, enter the path to the LDAP objects to limit the LDAP search in the [Search Directory Root] area. The entry should be in base DN format (for instance, ou=people, dc=xerox, dc=com).
11. For Login Name and Password, enter the machine's Login Name and Password (if required) in the boxes provided. Note that, quite often, to simply supply address information for E-mail, no login is required.

12. Enter your required number for **Maximum Number of Search Results**. This is the maximum number of addresses that will appear which match the search criteria selected by the user.
13. Enter the required time to wait for **Search Time-Out**. Alternatively, you may select Wait LDAP Server Limit.
14. Place a checkmark in the **Referral** box if you would like the server to refer to additional LDAP servers, when user information is initially unavailable.
15. If using Referral, enter the number of additional servers to check for user information (Hop Limit).
16. For **Search Name Order**, select the method that you would like LDAP to use to perform searches.
17. Click **Apply**, and supply the Administrator User name and password if prompted.

### LDAP User Mappings

You can click the **LDAP User Mappings** link to specify the attributes to search for within the LDAP database. Make sure that any entries made in the Imported Heading boxes are in LDAP nomenclature. For example, you would enter sn (surname) to search for the user's last name, and givenName to search for the users first name. Enter cn (Common Name) to search for the most commonly used attribute (given name joined to surname) to identify specific users within the LDAP system.

### LDAP Authentication

To set LDAP for authentication, click the **LDAP Authentication** link. For Authentication Method, choose either Direct Authentication or Authentication of User Attributes. **Direct Authentication** sets authentication with the LDAP server with the user name and password entered by the user. Authentication of User Attributes sets authentication with the LDAP server to the attributes listed on this dialog, such as samAccountName. Unless you are very familiar with LDAP, do not add text strings to the User Name.

### LDAP Group Access

LDAP server user groups can be used to control access to certain areas of the Xerox device. For example, the LDAP server may contain a group of users called "Admin." You can configure the "Admin" group on the device so that the members of that group will have administrator access to the device. When a user logs in at the device with their network authentication account, the device performs an LDAP look-up to determine if the user is a member of any groups. If the LDAP server confirms that the user is a member of the "Admin" group, the user will have administrator access. In the System Administrator Access Group box, enter the name of the group, defined at the LDAP server, that you want to provide with system administrator access to the device. Repeat the process for other LDAP group access boxes.

### Custom Filters

For the Email Address Filter, in the box provided, type in the LDAP search string (filter) that you wish to apply. The filter defines a series of conditions that the LDAP search must fulfill in order to return the information you seek. The form of the typed search string (filter) is LDAP objects placed inside parenthesis. For example, to find all users that have an E-Mail attribute (mail enabled), type (objectClass=user) (mail=\*). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.

## Configuring Network Authentication (by a Remote Accounting server)

Network authentication uses the user information managed on a remote Accounting server to manage authentication (access) to available machine services.

### Enable Network Authentication

To enable Network Authentication for use with this Device, at your networked workstation, perform the following steps:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Select the **Security** folder, then the **Authentication Configuration** hot link.
4. Select **Login to Remote Accounts** from the Login Type drop-down list, then **Network Accounting** from the Accounting Mode drop-down list.
5. Place a checkmark in the **Enable** box for each service that you wish to restrict access to. For explanations of each service, click the Help button.
6. Do not place a checkmark in the **Non-account Print** box if you wish to enable people without accounts to continue to print.
7. From the **Verify User Details** drop-down menu, select either Yes or No (keep logon records). The Yes selection will verify user information. When No (keep logon records) is selected, User ID and Account ID must be entered at the Device, but user information will not be checked. A logon record will be kept by the Device, however.
8. If a Guest User box is available and configurable, consider whether it is advisable in your network environment to allow simple password, guest access to this restricted service device. The default setting is Off.
9. If you wish to allow guest access, enter your guest password twice in the boxes provided.
10. Click **Apply** and enter the Administrator User name and password when prompted.
11. Click the **Reboot Machine** button, then **OK**, when prompted.
12. Refresh your web browser, then click on the **User Details Setup** link to set the Store User Details setting. Note that you can set either NVM or hard disk as the destination for saved authentication information. User Details Setup also allows you to configure the characteristics of the login prompt for User Authentication.

## **Configure communications between the Accounting server and the device**

Refer to the remote Accounting server manufacturer's documentation for the specific procedures to follow to configure communications between the server and the multifunction device.

The server will contact the device based upon Accounting service parameters set up at the server, such as the device's IP address and polling frequency.

Required network communications and server settings will be stated by the server's manufacturer.

Sample list of set up requirements for Equitrac's Accounting service

- Enable TCP/IP and HTTP on the multifunction device.
- Set up a static or reserved DHCP IP address for the device.
- Enable TCP/IP port 80 communications at the device.
- Download the Controller Interface for Xerox from the Equitrac™ web site.
- Install the Controller Interface for Xerox at the server.
- Verify that you have purchased a license for the Controller Interface for Xerox, as well as a license for each device communicating with the server.
- Register each multifunction device at the server (using the device's IP address for identification).

### **Enable the Accounting option in workstation print drivers**

Use the Windows Add Printer dialogs to add the multifunction device's print driver to individual, networked workstations. For instructions, if needed, refer to the Print Drivers section of this guide.

In the print driver default setting dialogs, locate and then enable the Accounting option. This step assures that print jobs from individual workstations will be recognized by the authentication system, rather than being unrecognized and deleted by the multifunction device.

For Windows operating systems, the default setting dialogs are accessed by right mouse clicking on the printer's icon in the Printers window for Windows 2000, or the Printers and Faxes window for Windows XP. Select **Properties** from the displayed menu, then locate and enable the Accounting option.



## Configuring Xerox Secure Access (Authentication)

Xerox Secure Access enables customers to leverage Xerox Partner Solutions to provide user authentication with an optional card reader. Users can access the features available at the device once they have been authenticated.

### Secure Access and Accounting

Secure Access can be enabled with Network Accounting or the Xerox Standard Accounting feature for accounting purposes. To configure Xerox Secure Access with Network Accounting, refer to the **Configuring Network authentication (by a remote Accounting server)** topic in this Security – Authentication section. To configure Xerox Secure Access with Xerox Standard Accounting, refer to the **Optional** information, in the Information Checklist below, then refer to the Xerox Standard Accounting section of this guide.

*Note: Secure Access cannot be enabled at the same time as Foreign Device Interface.*

### Information Checklist

1. Ensure that the device is fully functional on the network. TCP/IP and HTTP protocols must be configured so that Internet Services can be accessed.
2. Ensure that the Xerox Partner authentication solution (Secure Access Server, Controller, and Card Reader) is installed and communicating with the multifunction device. Follow the installation instructions from the manufacturer of the authentication solution to correctly set the devices up.
3. Ensure that SSL (Secure Sockets Layer) is configured on the multifunction device. The Xerox Partner authentication solution communicates with the multifunction device via HTTPS.
4. **(Optional)** Ensure that Network Accounting is configured if you want the multifunction device to send user account information to a Network Accounting server. In Internet Services (the web pages running on the multifunction device) use your web browser to enter the multifunction device's IP address, then click the **Properties** tab, then click the **Security** folder, click **Authentication Configuration**, and select Xerox Secure Access for **Login Type**, matched to Network Accounting for **Accounting Type**. For use with Xerox Standard Accounting, you select Xerox Secure Access for Login Type, then select Xerox Standard Accounting for Accounting Type. For instructions on setting up Xerox Standard Accounting, refer to the **Xerox Standard Accounting section of this guide**. For instructions on setting up your Network Accounting server, refer to the instructions that came with your accounting package, as well as the **Configuring Network authentication (by a remote Accounting server)** topic in this **Security – Authentication** section.

You may also need another Authentication Server (running LDAP in an ADS environment, for example) to communicate with the Secure Access Server providing that server with user credentialing information. A second Authentication Server may be necessary for web User Interface Authentication, if this feature is additionally desired.

5. If you have LDAP available on your network, it would be wise to configure LDAP on the multifunction device, preferably from the Remote Authentication Server / Directory Service folder, as stated in the **Configure Authentication for LDAP topic** in this section of this guide.

## Configuring Xerox Secure Access to work with Remote Authentication

### At Your Workstation:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field, then select [Enter].
2. Click the [Properties] tab.
3. Select the [Security] folder, then the [Authentication Configuration] link.  
The Properties tab refreshes and the Authentication Configuration > Step 1 of 2 area appears.
4. In the Authentication Configuration > Step 1 of 2 area:
  - a. Select [Xerox Secure Access] from the Login Type drop-down list.
  - b. Select the [Enabled] box for each service that you wish to restrict access to. For explanations of each service, select the [Help] button.  
*Note: If a Guest User box is available and configurable, consider whether it is advisable in your network environment to allow simple password, guest access to this restricted service device. The default setting is Off.*
  - c. Do not place a checkmark in the [Non-account Print] box if you wish to enable people without accounts to continue to print.
  - d. Select [Apply], then reboot the device following the prompt.
  - e. Select [Next].  
The Properties tab refreshes and the Authentication Configuration > Step 2 of 2 area appears.
5. In the Authentication Configuration > Step 2 of 2 area, on the Authentication System line, select [Configure].  
The Properties tab refreshes and the Authentication System area appears.
6. In the Authentication System area:
  - a. Settings drop-down list box, select [Authentication Agent].
  - b. Select [Apply], then reboot the device following the prompt.

## Configure Remote Authentication for Kerberos (Windows 2000)

### At your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab. Note that (as of February 2007) you can either return to the Security folder and the Authentication Configuration hot link (discussed on the previous page), or use the alternative path, stated below.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick Kerberos (Solaris) from the drop-down list. Click **Apply**.
5. Select **Kerberos Server Settings**.
6. Enter the IP Address of the Primary Server (Domain Controller running the Key Distribution Center service).
7. Enter the IP Address of the Secondary Server (Domain Controller), if necessary.
8. Enter details of the Windows 2000 Domain in the Realm Name box. For example: example.com.
9. Enter details for up to 4 alternate Domain Controllers and backups, if required.
10. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for Kerberos (Solaris)

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab. Note that (as of February 2007) you can either return to the Security folder and the Authentication Configuration hot link (discussed on the previous page), or use the alternative path, stated below.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick Kerberos (Solaris) from the drop-down list. Click **Apply**.
5. Select **Kerberos Server Settings**.
6. Enter the IP Address of the Primary Server (the server running the Key Distribution Center service).
7. Enter the IP Address of the Secondary Server, if necessary.
8. Enter details for the Realm. For example (in upper case): EXAMPLE.COM.
9. Enter details for up to 4 alternate servers and backups, if required.
10. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for SMB

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Select the **[Properties]** tab. Note that (as of February 2007) you can either return to the Security folder and the Authentication Configuration hot link (discussed on the previous page), or use the alternative path, stated below.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick SMB from the drop-down list. Click **Apply**.
5. Select **SMB Server Settings**.
6. From the **SMB Server Setup** drop-down menu, select your desired method. The selections include: By Domain Name, and By Domain Name and Server Address / IP Address.
7. Enter the **Domain name** (up to 15 characters) in the SMB Server – Domain Name box, for every Domain Controller specified. This entry is required regardless of the selection made from the SMB Server Setup drop-down menu.
8. Enter the **IP Address** of the Domain Controller in the SMB Server – Server Name / IP Address box (if By Domain Name and Server Address / IP Address was selected for SMB Server Setup).
9. Enter the IP Addresses of up to 4 additional Backup Domain Controllers, if applicable.
10. If you choose not to enter IP addresses, enter the **Server Name** (up to 64 characters) in the SMB Server – Server Name / IP Address box (if By Domain Name and Server Address / IP Address was selected for SMB Server Setup).
11. Click **Apply**, and supply the Administrator User name and password if prompted.

## Configure Remote Authentication for LDAP

Refer to your LDAP server documentation for the full range of information that can be entered into this LDAP dialog to fully support both E-mail applications and authentication using your LDAP server.

The path to the LDAP dialog is as follows:

### At Your Workstation:

1. With the Authentication Configuration web page still running, click **Configure** next to the server you wish to use for Authentication. If not still running, perform steps 2 and 3 below.
2. If the web page is not still running, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
3. Click the **Properties** tab. Note that (as of February 2007) you can either return to the Security folder and the Authentication Configuration hot link (discussed on the previous page), or use the alternative path, stated below.
4. Select the **Remote Authentication Server / Directory Service** folder in the list of hot links, select **Authentication System** and pick LDAP from the drop-down list. Click **Apply**.
5. Select **LDAP Server / Directory Service**.
6. Enter the **Primary Server IP address (or host name)** in the box supplied. Note: If entering a fully qualified host name (for example, ldapserver.xerox.com), make sure that the specified domain name matches the device's TCP/IP configuration (domain name shown under DNS on the device's Configuration Report).
7. Enter the **Primary Server Port Number** (default of 389).
8. If available, decide whether or not to use encryption (**Authentication with SSL**) when accessing the LDAP server.
9. For **Authentication Method**, choose either Direct Authentication or Authentication of User Attributes. **Direct Authentication** sets authentication with the LDAP server with the user ID and password supplied by the user. If you choose Direct Authentication, when a user presses a button at the device for a restricted service, they will be prompted for their LDAP credentials. If you select **Authentication of User Attributes**, authentication will be based on the attributes entered into this dialog, such as samAccountName or uid, for Attribute of Login User Name, or mail for Attribute of Typed User Name. Note that there are a number of other LDAP attributes that can be entered into this dialog.
10. The **Search Login Name** box can be left blank.
11. The **Search Password** and **Re-enter Search Password** boxes can be left blank.

12. Fill in the **Search Root Entry DN** (for example, ou=users, dc=xerox, dc=com), and select **All Levels below Root Entry** for Scope of Search.
13. In the Referral and Referral Hop Limit boxes, decide whether or not to perform referrals and specify the hop limit.
14. For **Server Application**, select your application from the drop-down list including Microsoft Active Directory, IBM Lotus Domino, or other Applications.
15. Enter any other attributes for LDAP to search for, such as cn, sn, givenName, mail, and telephoneNumber. Note that the default setting for Directory Service for Address Book is **Use**, which allows LDAP to be used with machine options that can benefit from LDAP address lookups (such as E-mail).
16. Click **Apply**, and supply the Administrator User name and password if prompted.

## Enable Specific Xerox Secure Access Settings

1. Open your Web browser and enter the TCP/IP address of the machine in the Address bar. Press **Enter**.
2. Select the **Properties** tab.
3. Select the **Security** folder.
4. In the **Security** folder, select the **Remote Authentication Servers** folder.
5. In the **Remote Authentication Servers** folder, select **Xerox Secure Access Settings**.
6. In the **Xerox Secure Access Settings** area:
  - a. Enter text in the **Default Prompt** and **Default Title** boxes to create the prompt and prompt title that will be displayed on the multifunction device's screen informing users how to authenticate themselves at the device.  
**Note:** If the Title and Prompt have been configured on the Secure Access Server, then that information will override the information entered here.
  - b. Select the **Enable** box for **Local Login** to allow users to log in locally at the device.
  - c. Select the **Enable** box for **Get Accounting Code** to get user accounting data from a networked Accounting Server (if used).
  - d. Click **Apply**, and provide the Administrator User name and password if prompted.



### Add the Secure Access to the Server

1. On the Windows 2000 desktop, from the **Start** menu, select **Settings**, then **Printers**. On the Windows XP desktop, from **Start**, select **Printers and Faxes**. The Vista path is Start\Control Panel\Printer(s).
2. On Windows 2000 or XP, click **Add a Printer**.
3. When the "Add Printer Wizard" screen displays, click **Next**.
4. Select **Create a new port** and choose **Secure Access Port** from the **Type** drop-down menu. (The Secure Access Port becomes available when it is installed, as above). Click **Next**.
5. When prompted, enter the **IP address** of the printer.
6. Enter a name for the print queue (such as **raw**). If you selected the Standard TCP/IP port, you can accept the default name provided by Windows. Click **Next**.
7. You will be prompted for a print driver. Select **Have Disk** and browse to the location of your print driver.
8. Select the **.INF** file, then click **Open**.
9. When the "Install from Disk" screen displays, verify that the path and file name are correct and click **OK**.
10. Select the model that corresponds to your printer and click **Next**.
11. Enter a name for your Printer and select either [Yes] or [No] for making this printer your default Windows printer. Select **Yes** if you will be printing primarily to this printer from your Windows applications. Click **Next**.
12. If the Printer Sharing Screen displays, select "Do not share this printer," unless the Printer is directly connected to your workstation and you wish to Share it with other network users. Click **Next**.
13. Select **Yes** to print a test page. Click **Next**.
14. Click **Finish**.

### Using Secure Access

1. Read the multifunction device's User Interface prompt to determine what needs to be done to be authenticated at the device. Authentication methods include swiping a card, placing a proximity card near the reader, or entering a user ID or PIN (personal identification number).
2. If the device requests further information such as accounting details, enter this information at the User Interface.
3. The device will confirm successful authentication allowing access to previously locked system features.
4. When finished using system features, press the [Clear All] button on the multifunction device's keypad to close your account.

## Configure Color Copy Access for LDAP Group

Refer to your LDAP server documentation for the full range of information that can be entered into this LDAP dialog to fully support both e-mail applications and authentication using your LDAP server.

### Set LDAP Server

To set the LDAP server:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab, click the **Connectivity** folder, click the **Protocols** folder, then click the **LDAP** folder.
3. In the **LDAP** folder, click the **LDAP Server** link.
4. On the **LDAP Directory** page, in the **Server Information** area:
  - a. On the **IP Address / Host Name & Port** line, type the IP address (or host name).  
*Note: If entering a fully qualified host name (for example, ldapserver.xerox.com), make sure that the specified domain name matches the device's TCP/IP configuration (domain name shown under DNS on the device's Configuration Report).*
  - b. Enter or verify the **Port Number** (default of 389).
  - c. If available, decide whether or not to use encryption (**Authentication with SSL**) when accessing the LDAP server.
  - d. In the **LDAP Server** drop-down list, click or verify **Microsoft Active Directory**.
5. In the **Optional Information** area:
  - a. In the **Search Directory Root** box, if desired, type the path to the LDAP objects to limit the LDAP search in the [Search Directory Root] area. The entry should be in base DN format (for instance, OU=People, DC=Xerox, DC=Com).
  - b. In the **Login Name** box, enter the machine's Login Name and Password (if required) in the boxes provided.  
*Note: Often, to simply supply address information for E-mail, no login is required.*
  - c. In the **Maximum Number of Search Results** box, type the maximum number of addresses that will appear which match the search criteria selected by the user.
  - d. In the **Search Time-Out** area, either:
    - Click **Wait LDAP Server Limit**.
    - Click **Wait** and type the required time to wait for the Search Time-Out.
  - e. To enable LDAP Referrals:
    - On the **LDAP Referrals** line, click **Enabled** to have the server refer to additional LDAP servers when user information is initially unavailable.
    - If using LDAP Referrals, enter the number of additional servers to check for user information (Hop Limit).
6. In the **Search Name Order** area, select the method that you would like LDAP to use to perform searches.
7. Click **Apply**, then reboot the device at the prompt.
8. Continue with the next procedure to set LDAP Authentication.

## LDAP Authentication

To set LDAP authentication:

9. Click the **Properties** tab, click the **Connectivity** folder, click the **Protocols** folder, then click the **LDAP** folder.
10. In the **LDAP** folder, click the **LDAP Authentication** link.
11. On the LDAP Authentication page, in the **LDAP Authentication** box:
  - a. On the **Authentication Method** line, either:
    - Click **Direct Authentication** to set authentication with the LDAP server with the user name and password entered by the user, or
    - Click **Authentication of User Attributes** to set authentication with the LDAP server to the attributes listed on this dialog, such as samAccountName.
  - b. On the **Attribute of Typed User Name** line, type "mail".
  - c. On the **Attribute of Login User Name** line, type "samAccountName".
  - d. Regarding text strings, unless you are very familiar with LDAP, do not add text strings to the User Name.
  - e. Click **Apply**, then reboot the device at the prompt.
12. Continue with the next procedure to set LDAP Group Access.

## LDAP Group Access

To set LDAP Group Access:

13. Click the **Properties** tab, click the **Connectivity** folder, click the **Protocols** folder, then click the **LDAP** folder.
14. In the **LDAP** folder, click the **LDAP Group Access** link.
15. On the LDAP Group Access page:
16. In the **Color Authorization** area, on the **Color Access Group** line, type CN=Color,CN=Users,DC=crmttrinity,DC=lab
17. Click **Apply**, then reboot the device at the prompt.
18. Continue with the next procedure to set Authentication Configuration.

## Authentication Configuration

To set Authentication Configuration:

19. Click the **Properties** tab, then click the **Security** folder.
20. In the **Security** folder, click the **Authentication Configuration** hot link.  
The **Properties** tab refreshes and the Authentication Configuration > Step 1 of 2 page appears.
21. On the Authentication Configuration > Step 1 of 2 page, in the **Authentication Configuration** box:
  - a. In the **Login Type** drop-down list, click or verify **Login to Remote Accounts**.
  - b. On the **Mailbox to PC / Server** line, click or verify the **Enabled** check box.
  - c. On the **Non-account Print** line, ensure that the **Enabled** check box is NOT checked if you wish to enable people without accounts to continue to print.
  - d. On the **Guest User** line, in the drop-down list box, click or verify **Off**.
22. Click **Apply**, then reboot the device following the prompt.
23. Continue with the next procedure to set Authentication System

## Authentication System

To set Authentication System:

24. Click the **Properties** tab, click the **Security** folder, then click the **Remote Authentication Servers** folder.
25. In the the **Remote Authentication Servers** folder, click the **Authentication System** link.
26. On the **Authentication System** page, in the **Authentication Type** box:
  - a. In the **Authentication System Settings** drop-down list box, click or verify **LDAP**.
  - b. Click **Apply**, then reboot the device at the prompt.

## Configure Color Copy Access Control at the device

To configure the device:

1. Press the **Log In / Out** button on the device Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times. (This is the factory default "password."). Touch **Enter**.
3. Press the **Machine Status** button on the Control Panel.
4. Touch the **Tools** tab.
5. Touch **Authentication / Security Settings**.
6. In the **Group** column, touch **Authentication**.
7. In the **Features** column, touch **Access Control**.
8. On the Access Control screen, touch **Feature Access**.
9. On the Feature Access screen:
  - a. In the **Items** column, touch **Color Copying**.
  - b. Touch the **Change Settings** button.
10. On the Color Copy screen, touch **Locked**, then touch **Save**.
11. Reboot the device.
12. On the All Services screen, touch the **Copy** icon, then the **Color** button.  
The Login screen appears.  
The device is configured for Color Copy Access for LDAP Group.

## 802.1X Authentication

The multifunction device supports 802.1X authentication based on the Extensible Application Protocol (EAP). 802.1X can be enabled for devices connected through both wired and wireless Ethernet networks. As described here, the 802.1X configuration is used to authenticate the multifunction device, rather than individual users. After the device has been authenticated, it will be accessible to users on the network.

The administrator can configure the machine to use one EAP type. EAP types currently supported on the device are:

EAP-MD5

PEAPv0/EAP-MS-CHAPv2

EAP-MS-CHAPv2

### Information Checklist

Create a user name and password on your authentication server which will be used to authenticate the Xerox device.

Ensure your 802.1X authentication server and authentication switch are available on the network.

### Configure 802.1X with Internet Services

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Select the **Security** folder.
4. Select the **802.1X** link.
5. Select (place a checkmark in) the **Enabled** box.
6. Select the required **Authentication Method**.
7. Enter the **User Name** and **Password** required by your authentication switch and server.
8. Click **Apply**.
9. If prompted, enter the administrator user name and password. The 11111 and x-admin.

# Security – Encryption

## Encryption Service Overview

*Note: You may have to purchase the Security Kit option to enable encryption with your Device. If you cannot generate a self-signed certificate, or enable SSL/TLS Communication, as stated under Configuration of HTTP Communication Encryption, in this section, contact your Xerox Representative to purchase the option.*

### Types of Encryption Services Available

The communication data between the machine and computers on a network can be encrypted.

Encryption for the machine, as described in this section, is set up using Internet Services. Internet Services are a series of Web (HTML) Pages located within the Device enabling network communication settings to be conveniently configured from a web browser running on a remotely located workstation.

For help with specific terminology as encryption is being set up on the machine, refer to the CentreWare Internet Services online help.

Note that the quickest and easiest, although not the most “trusted,” method to use to set up initial HTTP communication encryption is the generation of a self-signed certificate (as stated under Configuration of HTTP Communication Encryption, in this section).

Click the **Machine Digital Certificate Management** hot link in the **Security** folder on the Properties page of Internet Services. Use this link to manage all the digital certificates, of various types, stored on the machine.

#### Encryption of HTTP Communications from a Client to the Machine (Server Certificate)

The SOAP port, Internet service (HTTP) port, IPP port, and WebDAV port use the HTTP server of the machine.

The SSL/TLS suite of protocols is used in the encryption of HTTP communications from a client to the machine. A user of a client workstation accesses the machine's HTTP server by typing **https://**, followed by the IP address of the machine, into the Address box of a web browser application. The machine then offers the client a Digital Certificate, which the client accepts (after reviewing the validity of same). Upon acceptance of the Digital Certificate, a Public Key exchange takes place, encryption algorithms are agreed upon between the two parties, and the client uses the server's Public Key to communicate with the server using digitally signed and encrypted data.

Digital certificates imported from a Certificate Authority, or self-signed certificates created with CentreWare Internet Services, can be used as SSL/TLS certificates on the machine's HTTP server.

#### Encryption of HTTP Communications from the Machine to a Remote Server (Client Certificate)

The SSL/TLS suite of protocols is used to encrypt HTTP communications with a remote server.

No client certificate is typically required for this activity. However, if a remote server is set to require an SSL client certificate, an SSL/TLS client certificate must be registered on the machine.

Digital certificates imported from a Certificate Authority can be used as SSL/TLS certificates on the machine's HTTP server.

*Note: When Remote Server Certificate Validation is enabled, under SSL/TLS Settings in Internet Services, the root certificate of the remote server must be registered to the machine (imported with Internet Services) to verify the Digital certificate of same.*

## E-mail Encryption/Digital Signature

S/MIME certificates, imported from a Certificate Authority (in PKCS7 format), can be used on the machine's HTTP server for E-mail Encryption.

*Note: **To import S/MIME certificates**, use the Machine Digital Certificate Management hot link in the Security folder on the Properties Page of CentreWare Internet Services.*

### Encryption/Digital Signature of Scanned Files (PDF/XPS Documents)

While no digital signatures are required to encrypt PDF and XPS documents, these documents can be signed with imported PKCS12 Digital signatures.

When adding digital signatures to PDF or XPS documents, scan file certificates imported to the machine from a Certificate Authority, are typically used.

**To import PKCS12 scan file certificates**, use the Machine Digital Certificate Management hot link in the Security folder on the Properties Page of CentreWare Internet Services (accessed by entering the IP address of the multifunction device into the Address line of any web browser).

**IP Sec** (typically used to encrypt FTP) can be enabled from the **Security** file folder on the Properties page of Internet Services (the device's web pages available by entering the IP of the device into a standard web browser).

**802.1x** can be enabled for devices connected through both wired and wireless Ethernet networks. It is used to authenticate the multifunction device on the 802.1x network, rather than individual users.. 802.1x can be enabled from the **Security** file folder on the Properties page of Internet Services (the device's web pages available by entering the IP address of the device into a standard web browser).

# Configuration of HTTPS (SSL/TLS) Communication Encryption

## Installation Overview

### Configuration on the Machine

Two methods are available depending on the type of certificate.

- Create a self-signed certificate on the machine with Internet Services, and enable HTTPS. This method is used primarily for Server certificates.
- Enable HTTPS, and import a signed certificate from a Certificate Authority, using the Machine Digital Certificate Management hot link in the Security folder on the Properties Page of CentreWare Internet Services.

**Note:** To see this hot link, at least one certificate must have been created and stored on the machine. This is one of the purposes for creating a self-signed certificate.

**Note:** The Trusted Certificate Management folder does not appear under the Security folder until you enable HTTPS(SSL/TLS) Communication.

### Configuration on a Computer

Use IP addresses beginning with "https" in web browser applications.



## Configuring certificates with CentreWare Internet Services

Two methods are available to configure certificates with CentreWare Internet Services: creating a self-signed certificate (for SSL server), and importing a signed certificate from a Certificate Authority.

This section describes how to create a self-signed certificate (for SSL server).

### *Important*

*When performing SSL communication using a self-signed certificate created on the machine, or a certificate with which the character code is indicated by UTF-8, the following phenomena occur.*

*If Internet Explorer is used with Windows 98E or earlier, the issuer/issuing place of the certificate will not be displayed correctly.*

*SSL connection will not be made if Internet Explorer is used with Mac OS X 10.2 or later. This is because the operating system cannot recognize the character code (UTF-8) of the certificate. Use Netscape 7 in the above-mentioned OS environments.*

For information on how to import created certificates, refer to the CentreWare Internet Services online help.

### *Important*

*When importing a certificate, if the same certificate has been already registered in [Local Device] or [Others], the certificate cannot be imported. Delete the registered certificate before importing.*

1. Start a web browser.
2. Enter the machine's IP address, beginning with "https," into the Address box of your web browser, and press the **Enter** key.

Example:

https://192.168.1.1/

3. Click the **Properties** tab.
4. Click [+] on the **Security** folder to display the items in the folder.
5. Click on **Machine Digital Certificate Management**.
6. Generate a certificate.
  - a. Click the **Create Self-Signed Certificate** button.
  - b. Set the size of the Public Key as necessary.
  - c. Set Issuer as necessary.
  - d. Click the **Apply** button. When a screen to enter the user name and password appears, enter the System Administrator user ID and password into User Name and Password, and then click **OK**.

*Note: The default user ID is "11111" and the default password is "x-admin".*

7. Refresh the web browser.
8. Click [+] on the left of the **Security** folder to display the items in the folder.
9. Click **SSL/TLS Settings**.
10. Select the **Enable** check box for **SSL / TLS Server Communication**.
11. Check the **SSL / TLS Port Number**.

*Note: The correct port to use is 443. Do not use the numbers of any other ports.*

12. Apply the settings.
  - a. Click **Apply**.
  - b. The right frame on the web browser will change to the machine reboot display.
  - c. Click **Reboot Machine**. The machine will be unavailable for a short period of time.

## **Configuration on a Computer**

The following describes the configuration for a computer.

When encrypting communication between a web browser and the machine, enter an address beginning with "https" instead of "http" into the address column in the web browser.

Example of the IP address entry

https://192.168.1.1/

When encrypting IPP communications (Internet printing), enter an address beginning with "https" instead of "http" as the URL of a printer that is selected from [Add Printer].

Note: You will typically be presented with a Digital Certificate, which you need to accept in order to send encrypted files to the device. Digital Certificates represent the Public Key of the device to which you are sending and must be accepted in order to allow the encryption process to take place.

No settings are needed to use the SOAP port and WebDAV port.

# Configuration of E-mail Encryption/Digital Signature

## Installation Overview

### Configuration on the Machine

Import an S/MIME certificate from a Certificate Authority (in PKCS7 format), then configure the certificate on the machine using CentreWare Internet Services.

### Configuration on a Computer

No special configuration is needed for remote computer **receipt** of encrypted e-mail. For sending encrypted e-mail to the machine, however, you will need a copy of the device's S/MIME certificate on your workstation to allow you to encrypt email being sent to the device. The S/MIME certificate represents the Public Key of the device, allowing encryption to take place.

## Configuring S/MIME certificates with CentreWare Internet Services

To configure S/MIME certificates with CentreWare Internet Services, first enable HTTP communications (as stated under **Configuration of HTTP Communication Encryption** in this section). Next, import an S/MIME certificate from a Certificate Authority (in PKCS7 format). Finally, enable S/MIME.

1. Start a web browser.
2. Enter the machine's IP address, beginning with "https," into the Address box of your web browser, and press the **Enter** key.

Example:

https://192.168.1.1/

3. Click the **Properties** tab.
4. Confirm that the **Machine's E-mail Address**, under the **Description** hot link, is filled in. Also note that to use E-mail with this machine, E-Mail has to be enabled and configured as stated in the Scan to E-mail section of this guide.
5. Click [+] on the left of the **Security** folder to display the items in the folder.
6. Click **Machine Digital Certificate Management**.
7. Click **Upload Signed Certificate**.

*Note: Important: When importing a certificate, if the same certificate has been already registered in [Local Device] or [Others], the certificate cannot be imported. Delete the existing certificate before importing the new one.*

- a. Enter the **Password**.
- b. Enter the **Re-enter Password**.
- c. Enter a file name for the file you want to import, or select the file to be imported by clicking the **Browse** button.
- d. Click the **Import** button. When a screen to enter the user name and password appears, enter the System Administrator user ID and password into **User Name** and **Password**, and then click **OK**.

*Note: The default user ID is "11111" and the default password is "x-admin".*

8. Refresh the web browser.
9. Click [+] on the left of **Security** to display the items in the folder.
10. Configure the certificate.
  - a. Click **Trusted Certificates Management**.
  - b. Select [Local Device] for **Category**, [S/MIME] for **Certificate Purpose**, and then click the **Display the List** button. If necessary, enter the System Administrator User Name and Password and click OK.
  - c. Place a check mark in the box in front of the Certificate you wish to view details for.
  - d. Click the **Certificate Details** button.
  - e. Click the **Use this certificate** button.
  - f. Click **Reboot**. The machine will reboot and the setting values will be reflected.
11. Refresh the web browser.
12. Click [+] on the left of **Security** to display the items in the folder.
13. Click **SSL/TLS** Settings.
14. Select the **Enable** check box for **S/MIME Communication**.

15. Apply the settings.
  - a. Click **Apply**.
  - b. The right frame on the web browser will change to the machine reboot display.
  - c. Click **Reboot Machine**. The machine will be unavailable for a short period of time.

16. Configure the settings for S/MIME.

- a. Refresh the web browser.
- b. Click [+] on the left of **Security** to display the items in the folder.
- c. Click **S/MIME Settings** and set the following items.

**Message Digest Algorithm**

Select a message digest algorithm from [SHA1] or [MD5].

**Contents Encryption Method**

Select a contents encryption method from [3DES], [RC2-40], [RC2-64], or [RC2-128].

**Certificate Auto Store**

Click the checkbox to automatically save an S/MIME certificate attached to an e-mail received from an address registered in your address book.

**Receive Untrusted E-mail**

Decide whether or not you wish to receive untrusted E-mail.

**Receive Untrusted iFAX**

Decide whether or not you wish to receive untrusted iFAXes.

**Digital Signature - Outgoing E-mail**

Decide whether or not to add a digital signature to outgoing E-mail, and the method to use if a signature is desired.

**Digital Signature - Outgoing iFAX**

Decide whether or not to add a digital signature to outgoing iFAXes, and the method to use if a signature is desired.

- d. Click the **Apply** button.

## **Configuration on a Computer**

The following describes the configuration for a remote, networked computer.

Sending scanned data by S/MIME encrypted E-mail from the machine to a computer

An S/MIME certificate **MUST** be imported, configured, and stored on the machine as stated in this section under Configuring S/MIME certificates with CentreWare Internet Services.

When importing the S/MIME certificate, make sure that a root certificate is included for use with the Supported E-mail applications shown below.

### **Receiving E-mail with S/MIME digital signature from the machine**

No settings are required on a recipient computer.

### **Sending S/MIME encrypted e-mail by E-mail printing from a computer to the machine**

It is necessary to register the S/MIME certificate of the machine on the computer.

There are two methods to set an S/MIME certificate of the machine on the computer:

Sending e-mail with S/MIME digital signature from the machine to the computer

To send e-mail with an S/MIME digital signature from the machine, configure to attach the digital signature when sending E-mail in the [Digital Signature - Outgoing E-mail] settings.

Exporting an S/MIME certificate to the computer using CentreWare Internet Services and registering the exported S/MIME certificate in the certificate storage location of the E-mail application.

Note that the exporting of certificates is accomplished using the Trusted Certificates Management hot link under Security folder on the Properties page of Internet Services. For information on how to export a certificate, refer to the CentreWare Internet Services online help. For information on how to register a certificate in an E-mail application, refer to the manuals provided with the E-mail application.

### **Sending E-mail with S/MIME digital signature from a computer to the machine**

It is necessary to register a personal certificate of a sender's E-mail address, an intermediate certificate authority certificate of the personal certificate, and a root certificate on the machine.

For information on how to import a certificate, refer to the CentreWare Internet Services online help.

## **Supported E-mail applications**

E-mail applications that can send and receive E-mail to and from the machine are as follows:

Outlook 2000/2002/2003

Outlook Express 6

Netscape 7.x

# Configuration of Scan File Signatures (PDF/XPS Documents)

## **Installation Overview**

### **Configuration on the Machine**

Import a certificate from a Certificate Authority (in PKCS12 format), then configure the certificate on the machine using CentreWare Internet Services.

### **Configuration on a Computer**

Prepare for verification of the PDF or XPS signature.



## Configuring Scan File certificates with CentreWare Internet Services

To configure certificates with CentreWare Internet Services, first enable HTTP communications (as stated under **Configuration of HTTP Communication Encryption** in this section). Next, import a certificate from a Certificate Authority (in PKCS12 format). Finally, set the certificate as a scan file certificate.

1. Start a web browser.
2. Enter the machine's IP address, beginning with "https," into the Address box of your web browser, and press the **Enter** key.

Example:

https://192.168.1.1/

3. Click the **Properties** tab.
4. Click [+] on the left of **Security** to display the items in the folder.
5. Click **Machine Digital Certificate Management**.
6. Click on **Upload Signed Certificate**.

*Important: When importing a certificate, if the same certificate has been already registered in [Local Device] or [Others], the certificate cannot be imported. Delete the existing certificate before importing the new one.*

- a. Enter the **Password**.
- b. Enter the **Re-enter Password**.
- c. Enter a file name for the file you want to import, or select the file to be imported by clicking the **Browse** button.
- d. Click the **Import** button. When a screen to enter the user name and password appears, enter the System Administrator user ID and password into **User Name** and **Password**, and then click **OK**.

*Note: The default user ID is "11111" and the default password is "x-admin".*

7. Refresh the web browser.
8. Click [+] on the left of **Security** to display the items in the folder.

9. Configure the certificate.
  - a. Click on **Trusted Digital Certificate Management**.
  - b. Select [Local Device] for **Category**, [Scan File] for **Certificate Purpose**, and then click the **Display the List** button.
  - c. Place a check mark in the box in front of the Certificate you wish to view details for.
  - d. Click the **Certificate Details** button.
  - e. Click the **Use this certificate** button.
  - f. Click **Reboot**. The machine will reboot and the setting values will be reflected.

10. Configure the settings for PDF/XPS Signatures.

- a. Refresh the web browser.
- b. Click [+] on the left of **Security** to display the items in the folder.
- c. Click **PDF/DocuWorks Security Settings** and then set the following items.

**PDF Signature**

Select the setting for PDF Signature from [Do not add signature], [Always add visible signature], [Always add invisible signature], or [Select during send].

**XPS Signature**

Select the setting for XPS Signature from [Do not add signature], [Always add signature], or [Select during send].

- d. Click the **Apply** button.

**Configuration on a Computer**

Confirm that the digital certificate being used by the machine to encrypt PDF and XPS files has been imported and is registered on the recipient's computer. This will assure the ability to conduct two way digital signing of files, should this capability be desired or needed.

## IP Sec

IP Sec (IP Security) is comprised of the IP Authentication Header and IP Encapsulating Security Payload protocols, that secure IP communications at the network layer of the protocol stack, using both authentication and data encryption techniques. The ability to send IP Sec encrypted data to the printer is provided by the use of a public cryptographic key, following a network negotiating session between the initiator (client workstation) and the responder (printer or server). To send encrypted data to the printer, the workstation and the printer have to establish a Security Association with each other by verifying a matching password (shared secret) to each other. If this authentication is successful, a session public key will be built and used to send IP Sec encrypted data over the TCP/IP network to the printer.

Providing additional security during the Public Key negotiating process, Digital Certificates can alternatively be used in place of the Shared Secret, to encrypt the Public Key information being exchanged between communicating parties. The Digital Certificate resides on the multifunction device (managed as stated in this Encryption section in the Configuring Scan File certificates topic) and **MUST** also have been imported and stored on the computer that is encrypting data being sent to the device.

Certificates add digital signatures (individualized checksums verifying data integrity) to datagrams during the public key negotiating process, greatly assisting in securing that data from network sniffers.

### To enable IP Sec:

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the symbol to the left of the **Security** folder.
4. Select **IP Sec** in the directory tree.
5. Enable the Protocol by placing a checkmark in the **Enabled** box.
6. Select **Pre-Shared Key** to use the Shared Secret (between this device and remote computers also possessing the secret). Note that if you select Digital Signature, the Shared Secret boxes will be grayed out and you will have to supply a Certificate stored on this device to the remote computer that wishes to send IP Sec encrypted data to this device. Refer to the Configuring certificates with CentreWare Internet Services topic in this Encryption section for full information.
7. Enter the Shared Secret (a password) in the **Shared Secret** and **Verify Shared Secret** boxes.
8. Select **Enabled** (default setting) for the **Communicate with Non-IP Sec Device** setting, so that computers not set up for encryption can still communicate with this device.
9. Use the on line Help for assistance with other available settings.
10. Click **Apply** when done and supply the Administrator User Name and Password, if prompted. The default is 11111 and x-admin.

# Scheduled Image Overwrite

A TCP/IP network-connected device can be set to overwrite image data on a scheduled basis.

*Note: The Image Overwrite will delete all image data from the hard disk!*

To enable a scheduled image overwrite, perform the following steps:

1. At your workstation:
  - a. Open your Web browser.
  - b. Enter the IP address of the machine in the Address or Location field.
  - c. Press Enter.
2. Click the [Properties] tab.
3. If prompted, type or enter your System Administrator user name and password.
  - user name (default): 11111
  - password ( default): x-admin
4. Click the [Security] folder.
5. Click the [Scheduled Image Overwrite] link.

*Note: The Image Overwrite will delete all image data from the hard disk!*

6. In the Scheduled Image Overwrite area, in the Advanced Settings box, on the Schedule Image Overwrite line, click [Enabled].
7. Configure the Frequency, Day, Week, Hour, and Minute settings.

*Note: The machine will be taken off line each day at the time specified to perform the overwrite.*
8. Click [Apply]. Restart the device at the prompt.

# Security – Secure Watermark

This procedure enables the System Administrator to set parameters for the inclusion of a Secure Watermark as the background for any documents that are copied or printed on this, or another identical model machine.

Secure Watermark works with copy job, client print, mailbox print, media print, incoming fax prints and reports.

*Note: It is assumed that you have purchased the Security option to enable this feature. If you did not, contact your Xerox Representative to purchase the option.*

Secure Watermark configuration items include:

- Default Watermark Effect
- Default Watermark
- Font Size
- Background Pattern
- Date Format
- Font Color
- Density
- Watermark / Background Contrast
- Force Watermark – Copy Job
- Force Watermark – Client Print
- Force Watermark – Mailbox Print
- Custom Watermark 1
- Custom Watermark 2
- Custom Watermark 3

## To configure Secure Watermark:

1. Press the **Log In / Out** button on the Device's Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times. (This is the factory default "password."). Touch **Enter**.
3. Press the **Machine Status** button on the Control Panel.
4. Touch the **Tools** tab.
5. Touch **System Settings**.
6. Touch **Common Service Settings**.
7. Touch **Watermark**. If not visible, use the scrolling arrow in the **Features** column.
8. On the **Watermark** screen, in the **Items** column, touch the item to be configured, then touch **Change Settings**. The screen for the item will open.
9. On the selected item screen, make your change and touch **Save**.
10. Touch **Close** to return to the **Tools** tab.
11. Wait several seconds for the Auto Clear service to log you out.
12. Place a copy in the document handler of the machine and press the **Start** (large green) button.

13. Place the copy just made into the document handler of the same, or an identical model, machine, and attempt to make a copy. Note that copying of this document is prohibited.

# Security – Secure Print

Supported by the device's print driver, or Internet Services print page, this feature directs the printing of confidential documents, or documents which should not be seen by third parties, to a User Account on the machine. The user can then access his or her Account, with a numeric password, at the device, and privately print out the stored documents.

**To use the Secure Print feature from the print driver**, installed on a networked workstation, perform the following steps.

1. Open a document to print from the workstation.
2. Select print in your software application, select the Printer, then select **Properties**.
3. On the **Paper / Output** tab, select **Secure Print** as your **Job Type**.
4. Click **Setup...** and enter a User ID (such as 001) and a numeric password.
5. Click **OK** on successive driver screens until the job prints.
6. Go to the printer and press the **Job Status** button.
7. Press the **Secure Print Jobs & More** tab.
8. Press **Secure Print**.
9. Select your job and press **Document List**.
10. Enter your password when prompted and press **Confirm**.
11. Select your job, press **Print** and respond to the on-screen prompt.
12. Press **Close** several times, when done, to return to the Job Status screen.
13. Press the **All Services** button on the Control Panel to return to the All Services screen.



**To use the Secure Print feature from Internet Services**, a series of web pages installed on the printer, perform the following steps.

1. On a TCP/IP networked workstation, start your web browser.
2. Enter the IP address of the printer in the address box of the browser and press **Enter**.
3. Click the **Print** tab.
4. Scroll down to the bottom of the page to see the Secure Print radio button.
5. Click on the **Secure Print radio button** to enable it.
6. Enter a User ID (such as 001).
7. Enter your desired, numeric passcode in the two boxes provided.
8. Use the **Browse...** button to locate your PRINT READY file.
9. Click **Submit Job**. Then go to the printer and press the **Job Status** button.
10. Press the **Secure Print Jobs & More** tab.
11. Press **Secure Print**.
12. Select your job and press **Document List**.
13. Enter your password when prompted and press **Confirm**.
14. Select your job, press **Print** and respond to the on-screen prompt.
15. Press **Close** several times, when done, to return to the Job Status screen.
16. Press the **All Services** button on the Control Panel to return to the All Services screen.

# Xerox Standard Accounting

## Overview

When enabled, Xerox Standard Accounting (XSA) tracks the numbers of Copy, Print, Network Scanning, E-mail, Server Fax, Internet Fax and Embedded Fax jobs (when these features are installed on the machine), for each user. Usage limits can also be applied to users to restrict the total numbers of copy, print, fax and scan jobs that a user can perform. Administrators can print a report which contains all XSA data.

XSA is set up through CentreWare Internet Services, the machine's HTTP pages displayed on your web browser. Administrators must create accounts and specify limits before users are authorized to access the machine.

When XSA is set up, users must enter their account details at the machine to use the device. When they have finished their job, their XSA allocation is reduced by the number of prints, copies or scans performed. When XSA is enabled, users must enter their account details in the printer driver to print documents from their workstations.

The XSA feature is mutually exclusive from any other accounting feature. If XSA is enabled at the device, you cannot enable Foreign Device Interface, Auditron or Network Accounting.

Each device supports unique XSA User IDs and Group Accounts.

All user IDs must be assigned to one or more group accounts.

*Note: The XSA settings and account data are stored in the machine. It is strongly recommended that you back up the settings and data regularly using the Cloning hot link available under the XSA folder of Internet Services as described in this section. Should the machine lose your XSA data and settings you can restore them from the backup file that you produced by the Cloning process.*

## Installation Checklist

Before starting the installation procedure, please ensure the following items are available or have been performed.

1. Ensure that your device is fully functioning on the network.
2. Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functioning. This is required to access CentreWare Internet Services to configure Xerox Standard Accounting. The Internet Services function is accessed through the embedded HTTP server on the machine and allows System Administrators to configure XSA with a web browser.

To verify that the TCP/IP and HTTP protocols are correctly configured, print a Configuration Report as stated in the **Configuration Report** topic in the Network Connectivity section of this guide.

To configure TCP/IP, refer to the **TCP/IP Configuration** topic in the NOS Selection section of this guide.

To enable HTTP, refer to the **Enable Internet Services (HTTP)** topic in the Network Connectivity section of this guide.

## Enable Xerox Standard Accounting (from Internet Services)

### At your Workstation

1. Open your Web browser and enter the TCP/IP address of the machine in the Address bar. Press **Enter**.
2. Click the **Properties** tab.
3. Select the **Accounting** folder, then click the **Accounting Configuration** hot link.
4. Select **Xerox Standard Accounting** from the **Accounting Type** drop-down list. Note: It is also possible to select Xerox Accounting for use with an Authentication Server, as described in the Security – Authentication section of this guide.
5. Place a checkmark in the Enable box for each service that you wish to restrict access to. For explanations of each service, click the Help button.
6. Click **Apply** and enter the Administrator User name and password when prompted (default of 11111 and x-admin).
7. Click **OK**.
8. Click the **Reboot Machine** button when it displays on screen.

## Create a Group Account

1. On the Properties tab of Internet Services, click the **Accounting** folder, then the **Xerox Standard Accounting** folder in the directory tree.
2. Click the **Group Accounts** link to create a new group account.
3. In the Group Accounts Account ID box, enter an ID for the new group account (for example 001). The Group Account can be numeric values up to a maximum of 32 characters. Group Account ID's must be unique.
4. Enter a name for the group account in the Account Name box (for example Xerox). The group name can be alphanumeric characters to a maximum of 32 characters. The Group Account name must be unique.
5. Click **Apply**. The account will now be available in the Group Accounts list. Note that you may have to refresh your browser, or click another link, then click on Group Accounts again, to see the new group.

## Create a User Account and Set Usage Limits

*Note: At least one group account must be created before you create user accounts.*

1. On the Properties tab of Internet Services, click the **Accounting** folder, then the **Xerox Standard Accounting** folder in the directory tree.
2. Click the **Manage Accounting** link.
3. Click the **Add New User** button.
4. Enter an ID for the user. The user ID can contain alphanumeric characters to a maximum of 32 characters (for example: A10). User ID's must be unique.
5. Enter the user name (for example Jane Smith). The user name can contain alphanumeric characters to a maximum of 32 characters. User names must be unique.
6. Enter a passcode in the Passcode box.
7. Specify the usage limits for this account in the User Limits boxes. The maximum value for each limit is 9999999.
8. Click the **Apply** button when you have finished setting the usage limits.

## Maximum Usage Limits and Resetting Individual Usage Limits

The first time a user logs into the device after they have reached their maximum usage limit, a message displays on the user interface. The message notifies the user that they have reached their limit for the feature. Users will not be unable to use the feature until their limit is reset.

If the user performs a copy job at the machine, and mid way through the job their limit is exceeded, the job will not continue.

If the user performs a scan job at the machine, and mid way through the job their limit is exceeded, the job will be cancelled.

If the user's limit is reached before a print job is completed, the machine will notify the user that their limit has been reached. The job will be deleted from the print queue. The job may run over due to sheets committed to the paper path.

*Note: The system administrator has unlimited access to the machine.*

### To Reset User Limits (if necessary)

1. On the Properties tab of Internet Services, click the **Accounting** folder, then the **Xerox Standard Accounting** folder in the directory tree.
2. Click the **Manage Accounting** link.
3. Place a checkmark in the box for the desired User ID.
4. Click **Limits and Access**.
5. Enter the new **User Limits**, check the **Reset** box, and click **Apply**.

## Using XSA at the machine

When you enable XSA, users must enter a valid user name at the machine to access any services to which access restriction has been applied. Refer to **Enable Xerox Standard Accounting** in this section for the specific service restricting procedure.

### At the Machine

1. Press the **All Services** button, if necessary, to display all the available service buttons.
2. Press any button representing a service to which restricted access has been applied.
3. When the “Press the Log In / Out button” message displays on screen, press the **Log In / Out button**.
4. Enter a User ID and touch **Confirm**.

*Note: If the User is a member of more than one Group Account, he or she will be asked to select the account that they wish to log into.*

5. When the User is logged in, the selected service screen will be displayed. The User can now use that service, with usage tracked by XSA.

## Resetting Usage Data

At your Workstation

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Accounting** folder, then the **Xerox Standard Accounting** folder in the directory tree.
4. Click the **Report and Reset** link.
5. To reset all usage data to zero, click the **Reset Usage Data** button.
6. Click **OK** to confirm.

**WARNING! Do not click the Reset to Default button** unless you intend to delete all users, accounts and usage data from your machine.



## Print a Usage Report

At your Workstation

1. Open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Accounting** folder, then the **Xerox Standard Accounting** folder in the directory tree.
4. Click the **Report and Reset** link.
5. Click the **Generate Report** button.
6. Follow any additional displayed prompts to save the XSA Report.csv (comma separated value) file to your workstation.

## Enable XSA in your Print Drivers

Refer to the driver documentation for the steps to follow to enable XSA in your print drivers.

## Backing Up XSA data and settings and Cloning to another device

The Cloning feature enables you to copy settings, including Xerox Standard Accounting (XSA) settings and account information, to a file on your workstation or Server. You can then use this file to restore the data and settings on the same machine or to clone other machines. You can only clone XSA settings to another Xerox device that supports the XSA feature.

The Clone feature will create a .dat file script that can be used to configure other machines. All machines must have the same version of software for the .dat file to be accepted.

The software version is located on the Properties tab, under General Setup.

### Check that the device you want to clone settings to supports XSA

1. At a networked workstation, open your web browser and enter the TCP/IP address of the machine that you want to clone to. Press **Enter**.
2. Click the **Properties** tab.
3. See if the Xerox Standard Accounting is shown in the directory tree (under the Accounting folder). If it is not, then you cannot clone XSA settings to this machine.
4. Click the **General Setup** folder.
5. From the display of available hot links, verify that **Cloning** is among them.

### To clone a machine

1. At your workstation, open your web browser and enter the TCP/IP address of the machine with the settings that you want to copy, in the Address bar. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **General Setup** folder, then **Cloning**.
4. In the **Cloning** area, in the **Create Clone File** box, select the settings that you wish to clone.
  - a. To clone all features, verify that all features are checked and then click **Clone**.
  - b. To customize the configuration file, disable any of the features by clearing the check boxes next to the feature(s), then click **Clone**.
  - c. To see a detailed listing of the feature details, click **View Feature Details**.
5. Enter the current administrator User name and password, if prompted. The default is 11111 and x-admin.
6. Right-click on the .dat link that appears and select **Save Target As**.
7. A dialog box will prompt you to specify and name and location for the cloned file. Ensure the extension reads .dat.
8. Click **Save**. The .dat file can now be used to restore the information to the same machine or to clone other machines.

## To Restore Settings or Clone Settings to another Machine

*Note: This procedure will cause the machine to reboot and will be unavailable over the network for several minutes.*

*Note: All machines must have the same version of software for the .dat file to be accepted*

1. Open your web browser and enter the TCP/IP address of the machine that you wish to restore or clone the settings to. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **General Setup** folder, then **Cloning**.
4. In the **Cloning** area, in the **Install Clone File** box:
  - a. Click **Browse** and move through your file system to the .dat file.
  - b. Click **Open**.
  - c. Click **Install**.
5. If prompted, enter the current administrator User name and password. The default is 11111 and x-admin.

*Note: The machine will be unavailable over the network for several minutes.*

6. Once rebooted a Configuration Report should automatically print, if enabled. If the Configuration Report does not automatically print, manually print the list by referring to the instructions in the Configuration Report topic in the Network Connectivity section of this guide. Looking at the Configuration Report, verify that some or all of your settings have been cloned to the new machine. Also, note that it may be necessary for you to use your web browser to view the Xerox Standard Accounting set up of Users and Groups on the new machine.

# Audit Log

## Overview

With TCP/IP and HTTP-based processes running on the device, exposure to access attacks, eavesdropping, file tampering, service disruption, and identity (password) theft is significantly increased.

The Audit Log, regularly reviewed by the Security Administrator, often with the aid of third party analyzing tools, helps to assess attempted security breaches, identify actual breaches, and prevent future breaches.

The Audit Log is enabled or disabled from the **Audit Log** hot link on the **Properties tab** of Internet Services, accessed from a networked workstation running a web browser. To enable Internet Services, if necessary, refer to the **Enable Internet Services** topic in the **Network Connectivity** section of this guide.

Access to logged data is also accomplished from the **Audit Log** hot link on the **Properties tab** of Internet Services, but additionally requires the enabling of SSL/TLS encryption. To enable this encryption, refer to the **Security – SSL/TLS Encryption** topic in the **Options** section of this guide.

Events tracked in the Audit Log, include: Starting and Stopping of the device, Login/Logout events, Changes to system settings, and job completions.

## Accessing the Audit Log feature

The Audit Log feature is accessed through Internet Services as follows:

1. On a networked workstation, open your Web browser and enter the TCP/IP address of the machine in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Audit Log** hot link.
4. Supply the Administrator User Name and Password (defaults of 11111 and x-admin), when prompted.
5. Select the On-Line Help for additional help, as required.

# Annotation (Bates Stamping)

## Overview

Adding notes to scanned and copied pages (annotation) is primarily a user-controlled feature. An Annotation button is accessed by pressing the Copy button on the device's Main (All Services) screen, then by pressing the Output Format tab. Bates Stamping is one of the selections available by pressing the Annotation button.

Bates Stamping is used in the legal profession to sequentially number or date/time-mark documents as they are scanned and copied by the system. A number of parameters are available for selection, as specified below.

*Note: Other forms of annotation are available, with default parameters set by the System Administrator using the same button-pressing sequence stated in this section under **Configuring a precise bates stamp location**. For these other forms of annotation, note that you will need to press the Copy Defaults button, after pressing Copy Service Settings on the Tools tab, to modify stamp settings.*

## Configuring Bates Stamp Settings

1. Insert a document in the device's document handler.
2. Press **Copy** on the Main (All Services) screen.
3. Press the **Output Format** tab.
4. Press the **Annotations** button.
5. Select **Bates Stamp**.
6. Set Bates Stamping to on.
7. Press the **Prefix** text box, and press Edit if necessary, to use the displayed keyboard to specify the Prefix to use.
8. Press **Save**.
9. Press the **Number of Digits** button to assign the number of digits for printed page numbers. Press **Save** to save setting changes.
10. Press **Apply To** in order to specify the pages on which to print the Bates Stamp. Press **Save** to save changes.
11. Press **Position** to specify the relative position on the page for the printed Bates Stamp. Note that, if available, a precise location can be set by the System Administrator as stated in this section. Press **Save** to save changes.
12. Press **Format & Style** to specify the size and color of type for the Bates Stamp. Press **Save** to save changes.
13. Press **Save** when done, then press **Save** again.
14. Press the **Start** button.

## Configuring a precise Bates Stamp location (if available)

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press the rectangular **Enter button** on the touch screen.
4. Press the **Machine Status button**.
5. Touch the **Tools tab**.
6. Press **Copy Service Settings**.
7. Press **Copy Control**.
8. Press the down arrow to scroll to the Bates Stamping selection lines.
9. Press the applicable Bates Stamp position lines to set the precise location for your Bates stamp, using x and y axes.
10. Press **Change Settings** to change settings.
11. Press **Save** to save your changes.
12. Press **Close** until the System Settings screen is displayed.
13. Press **Exit** on the System Settings screen to return to the Main (All Services) screen.

*Note: If you press the Copy Defaults button, after pressing Copy Service Settings on the Tools tab, many annotation settings are available for selection and modification.*

# Media Card Reader

## Overview

The Media Card Reader is available as an optional kit for the WorkCentre 328/7335/7345.

If the Media Card Reader is installed on the WorkCentre 7328/7335/7345, image data (Exif) taken by digital cameras and document files (PDF, TIFF) can be printed by the WorkCentre 7328/7335/7345.

For further information, refer to the *Media Card Reader User Guide*.

*Note: "Exif" is a file format that embeds information required to print data in an image taken by digital cameras.*

The WorkCentre 7328/7335/7345 uses two media printing modes:

- Media Print – Text – prints data stored in document format. It is helpful to think of the word "text" as synonymous with "document."
- Media Print – Photos – prints data stored in the standard format of most digital cameras.

## Media Card Reader Hardware

- Access Indicator – this light illuminates when the media card is inserted.
- Eject Button – press this button to eject the media card.
- Media Slot – insert the media card into this slot.

## Supported Media and File Formats

The Media Card Reader supports **CompactFlash** media only. To use media other than CompactFlash, insert the media into a CompactFlash adaptor.

*Note: The media and the CompactFlash adaptor are optional.*

The media and file formats that can be used are as follows.

### Supported Media

- SmartMedia
- CompactFlash
- CompactFlash (MicroDrive)
- SD Card
- Memory Stick
- xD-Picture Card

### Supported File Formats

- Media Print - Photos
  - JPEG
  - TIFF - DCF1.0-compliant JPEG/TIFF (Exif2.0, Exif2.1, Exif2.2) are supported.
- Media Print - Text
  - PDF Extension: .pdf, PDF1.3 or later
  - TIFF Extension: .tif, gray scale 4 bit/8 bit uncompressed, 4 bit/24 bit compressed by JPEG, compressed by MH/MMR



## Important Notes and Restrictions

- MagicGate Memory Stick is not supported.
- Image files other than files in Exif format (JPEG and TIFF files created on computers) cannot be printed.
- If an image file in Exif format is edited or saved on a computer, the file format is changed and no longer remains in Exif format.
- Do not save image files and document files in the same medium.
- A media card containing over 900 files may not be detected properly.
- In Media Print - Text mode, PDF files or TIFF files stored in folders cannot be printed.
- PDF files stored on Mac OS cannot be printed and displayed on the screen.
- If characters not supported by the machine are used in file names, the file names will not be displayed on the screen.
- Characters up to 255 can be recognized as a file name. However, not more than 100 characters will be displayed.
- Use media formatted by digital cameras or computers (FAT12, 16, 32 only).
- Only use media recommended by Xerox. For the information on recommended media, contact our Customer Support Center.
- If anything is wrong with a media card, the process aborts within a few minutes and an error message appears.
- Before powering off the WorkCentre 7328/7335/7345, be sure to eject the media card.

## Inserting and Ejecting Media

To insert or eject a media card, follow the procedure below:

*CAUTION: Do not press the Eject Button, pull out the USB cable, or power off the machine when the Access Indicator light is illuminated. Data stored on the media card may be damaged.*

1. Before ejecting the medium, touch the antistatic label.
2. Press the Eject button, and then pull out the media card.

## Selecting and Printing Text Files

### To Select and Print Text Files:

1. Insert the media card into the Media Slot of the Media Card Reader.
2. Press the All Services button.
3. Touch the Media Print – Text icon.
4. After the files are imported, touch the appropriate button. You can choose from:
  - Select All
  - Select from List
  - Select Range
5. Touch the Media Print Text and Advanced Settings tabs as required to change any appropriate print settings.
6. Press the Start button.

## **Media Print Text Tab**

The Media Print Text tab allows you to select from a variety of printing options.

The options for the Media Print Text tab include:

- Output Color – you can choose Color or Black & White.
- Paper Supply – choose the paper tray to be used as a source when printing.
- 2 Sided Printing – choose 1 Sided, 2 Sided (Flip on long edge), or 2 Sided (Flip on short edge).
- Multiple-Up – choose from Off, 2 Pages Up, or 4 Pages Up.

## **Index Print**

The Index Print button allows you to print a collection of miniature (30mm x 40mm) images onto one page from the files on the media card.

When you select the Index Print button, you will only be able to specify the number of copies printed. All other printing options remain at their previous settings.

## **Advanced Settings**

The Advanced Settings tab allows you to select from a variety of printing options.

You can choose to set Bitmap Smoothing to On or Off on this tab. Selecting the On option smoothes out rough and jagged edges within your document.

## **Selecting and Printing Photo Files**

1. Insert the media card into the Media Slot of the Media Card Reader.
2. Press the All Services button.
3. Touch the Media Print – Photos icon.
4. After the files are imported, touch the appropriate button. You can choose from:
  - Select All
  - Select from List
  - Select Range
5. Touch the Media Print Photos and Advanced Settings tabs as required to change any appropriate print settings.
6. Press the Start button.

## **Media Print Photos Tab**

The Media Print Photos tab allows you to select from a variety of printing options. The Media Print Photos tab is shown below. The options for the Media Print Photos tab include:

- Output Color – you can choose Color or Black & White.
- Paper Supply – choose the paper tray to be used as a source when printing.
- 2 Sided Printing – choose 1 Sided, 2 Sided (Flip on long edge), or 2 Sided (Flip on short edge).
- Output Photo Size – choose from Full Page Print, any available Output Size, or anywhere from 2 to 8 Pictures per Page.

## Index Print

The Index Print button allows you to print a collection of miniature (30mm x 40mm) images onto one page from the files on the media card. When you select the Index Print button, you will only be able to specify the number of copies printed. All other printing options remain at their previous settings.

## Advanced Settings

The Advanced Settings tab allows you to select from a variety of printing options.

You can choose to set Bitmap Smoothing to On or Off on this tab. Selecting the On option smooths out rough and jagged edges within your document.

## Problem Solving

If one of the following symptoms occurs, or if an error message appears on the screen, follow the remedy to solve the problem.

**Symptom 1.** The access indicator light of the Media Card Reader does not illuminate.

- **Cause:** The USB cable may not be connected correctly.
- **Remedy:** Power off the machine, pull out the USB cable, and then insert the cable into the connector securely.

**Symptom 2.** The **Media Print - Photos** and **Media Print - Text** icons are not displayed on the **All Services** screen.

- **Cause:** The machine does not recognize the media card reader properly.
- **Remedy:** Power off the machine, pull out the USB cable, and then insert the cable into the connector securely.

**Symptom 3.** Blank sheets are output.

- **Cause:** Files that cannot be printed by the machine (image files not saved in Exif format) are included in the selected files.
- **Remedy:** Image files not saved in Exif format cannot be printed by Index Print. Delete the image files that cannot be printed by Index Print, and then print files again.

*Note: If an image file in Exif format is edited or saved on a computer, the file format is changed and no longer remains in Exif format.*

# USB Printing

## Overview

The USB Printing is available as an optional kit for the WorkCentre 7328/7335/7345.

If the Media Card Reader is installed on the WorkCentre 7328/7335/7345, image data (Exif) taken by digital cameras and document files (PDF, TIFF) can be printed by the WorkCentre 7328/7335/7345.

*Note: "Exif" is a file format that embeds information required to print data in an image taken by digital cameras. If an image file in Exif format is edited or saved on a computer, the file format is changed and no longer remains in Exif format.*

The WorkCentre 7328/7335/7345 uses two media printing modes:

- Media Print – Text – prints data stored in document format. It is helpful to think of the word "text" as synonymous with "document."
- Media Print – Photos – prints data stored in the standard format of most digital cameras.

*Note: The USB Printing option is similar to the Media Card Reader option, but there are several important differences.*

## USB Printing Hardware

- USB slot

## Supported Media and File Formats

USB Printing supports typical USB flash drives.

### Supported File Formats

- Media Print - Text
  - PDF Extension: .pdf, PDF1.3 or later
  - TIFF Extension: .tif, gray scale 4 bit/8 bit uncompressed, 4 bit/24 bit compressed by JPEG, compressed by MH/MMR
  - XPS
- Media Print - Photos
  - JPEG
  - TIFF - DCF1.0-compliant JPEG/TIFF (Exif2.0, Exif2.1, Exif2.2) are supported.

*Note: The photo files MUST be in the format that they were stored in on the camera. Copy the folder, (for instance, a DCIM folder) to the USB drive.*

## Important Notes and Restrictions

- Image files other than files in Exif format (JPEG and TIFF files created on computers) cannot be printed.
- If an image file in Exif format is edited or saved on a computer, the file format is changed and no longer remains in Exif format.
- Do not save image files and document files in the same medium.
- In Media Print - Text mode, PDF files or TIFF files stored in folders cannot be printed.
- PDF files stored on Mac OS cannot be printed and displayed on the screen.

- If characters not supported by the machine are used in file names, the file names will not be displayed on the screen.
- Characters up to 255 can be recognized as a file name. However, not more than 100 characters will be displayed.

# Selecting and Printing Text Files

## To Select and Print Text Files:

1. Insert the USB drive into the USB slot.
2. Press the All Services button.
3. Touch the Media Print – Text icon.
4. After the files are imported, touch the appropriate button. You can choose from:
  - Select All
  - Select From List
  - Select Range
5. Touch the Media Print Text or Advanced Settings tabs as required to change any appropriate print settings.
6. Touch the file to be printed.
7. Press the Start button.

## Media Print Text Tab

The Media Print Text tab allows you to select from a variety of printing options.

The options for the Media Print Text tab include:

- Output Color – you can choose Color or Black & White.
- Paper Supply – choose the paper tray to be used as a source when printing.
- 2 Sided Printing – choose 1 Sided, 2 Sided (Flip on long edge), or 2 Sided (Flip on short edge).
- Output – choose stapling options as needed.
- Index Print
  - The Index Print button allows you to print a collection of miniature (30mm x 40mm) images onto one page from the files on the media card.
  - When you select the Index Print button, you will only be able to specify the number of copies printed. All other printing options remain at their previous settings.

## Advanced Settings Tab

The Advanced Settings tab allows you to select from a variety of printing options.

- Multiple-Up – choose from Off, 2 Pages Up, or 4 Pages Up.
- Bitmap Smoothing – Selecting the On option smoothes out rough and jagged edges within your document.

## Selecting and Printing Photo Files

### To Select and Print Photo Files:

*Note: The photo files MUST be in the format that they were stored in on the camera. Copy the folder, (for instance, a DCIM folder) to the USB drive.*

1. Insert the USB drive into the USB slot.
2. Press the All Services button.
3. Touch the Media Print – Photos icon.
4. After the files are imported, touch the appropriate button. You can choose from:
  - Select All
  - Select From List
  - Select Range
5. Touch the Media Print Photos or Advanced Settings tabs as required to change any appropriate print settings.
6. Touch the file to be printed.
7. Press the Start button.

### Media Print Photos Tab

The Media Print Photos tab allows you to select from a variety of printing options. The Media Print Photos tab is shown below. The options for the Media Print Photos tab include:

- Output Color – you can choose Color or Black & White.
- Paper Supply – choose the paper tray to be used as a source when printing.
- 2 Sided Printing – choose 1 Sided, 2 Sided (Flip on long edge), or 2 Sided (Flip on short edge).
- Output Photo Size – choose from Full Page Print, any available Output Size, or anywhere from 2 to 8 Pictures per Page.
- Index Print
  - The Index Print button allows you to print a collection of miniature (30mm x 40mm) images onto one page from the files on the media card.
  - When you select the Index Print button, you will only be able to specify the number of copies printed. All other printing options remain at their previous settings.

### Advanced Settings Tab

The Advanced Settings tab allows you to select from a variety of printing options.

You can choose to set Bitmap Smoothing to On or Off on this tab. Selecting the On option smoothes out rough and jagged edges within your document.

# Thumbnail Preview

Thumbnail Preview is an optional feature and may not be available on your machine. Review the instructions that are included in the Thumbnail kit.

## To view a thumbnail preview and print a document

1. At the device, select [All Services].
2. Select [Send from Mailbox] icon.
3. Select [Mailbox Name].  
A list of Mailbox Names are displayed with a number association. The numbers are used as identifiers for commonly used mailboxes. You may identify the mailbox by the name or number, depending on how you choose to identify the mailbox.
4. Select the document name from the Document List.  
The document selected will be used to send to the printer. When a document is identified and selected, a check mark will be placed in the Order field. More than one document can be selected.
  - In the Mailbox, a document to be previewed may be any print, scan, or fax job
  - On a thumb drive, a document may only be a JPEG in the Exchangeable image file format (Exif). Exif JPEGs are JPEGs as they are stored on a digital camera. A JPEG produced by Photoshop or any other image modification and storage software will not work properly.
5. Select Thumbnail.  
The Thumbnail feature will open a preview window of the selected document. A small, thumbnail-sized image will display on your screen. This option is useful in determining if you have chosen the correct document.
6. Select Print.  
The mailbox print settings will display.
7. Select the Paper Supply, Output, and 2 Sided Printing Options.
  - Paper Supply: Select the paper to be used with this document.
  - Output: Select the desired output destination for this document.
  - 2 Sided Printing: Select the appropriate 2 Sided Printing option for this document.
8. Select Print.  
The selected document will be printed to the specified location.



# Hard Disk Data Encryption

The controller hard disk data encryption is enabled by default on your WC 7300 series product. This encryption feature provides an additional level of data security on the device, while operating at a low level within the operating system. The impact on performance is very small.

*Note: Enabling or disabling disk encryption will result in a system reboot and a hard disk initialization. During hard disk initialization, all customer information, mailboxes, templates, and other information stored on the disk will be lost.*

## To verify or change hard disk data encryption

1. Press the Log In / Out button on the Device's Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times.
3. Press the Machine Status button on the Control Panel.
4. Touch the Tools tab.
5. Touch Common Service Settings.
6. Scroll to Other Settings.
7. Scroll to Data Encryption. The current setting appears in the Current Settings column. Data Encryption should appear to be ON.
8. To change the setting, touch Data Encryption, touch Change Settings. Touch On or Off, then touch Save.

*Note: Enabling or disabling disk encryption will result in a system reboot and a hard disk initialization. During hard disk initialization, all customer information, mailboxes, templates, and other data stored on the disk will be lost.*

## Encryption Key For Confidential Data

When enabling Data Encryption, the system administrator may also create an Encryption Key For Confidential Data. The system administrator may either verify the default encryption key, or enter a new alpha-numeric string of up to 12 characters to be used by the encryption algorithm.

# Internet Services

## Enable Internet Services (HTTP)

Internet Services are a series of Web (HTML) Pages located within the Device enabling network communication settings to be conveniently configured from a web browser running on a remotely located workstation.

*Note: If Authentication is enabled, as stated in the **Security – Authentication** topic in the **Options** section of this guide, you will have to supply the Administrator User Name and Password when first accessing Internet Services, rather than supplying these credentials after configuring individual features with Internet Services.*

### To access Internet Services Settings at the Device

1. Press the **Log In / Out button** on the Control Panel.
2. Press the **"1" key** on the numeric keypad five consecutive times. (This is the factory default "password.")
3. Press **Enter** on the touch screen.
4. Press the **Machine Status** button on the Control Panel.
5. Press the **Tools tab**.
6. Press **Connectivity & Network Setup**.
7. Press **Port Settings**.
8. When the Port Settings menu displays, press the down arrow key to view additional selections.
9. Press the **Internet Services (HTTP)** selection line.
10. Press the **Change Settings** button in the lower right corner of the Port Settings menu screen.
11. When the Internet Services (HTTP) menu displays, note that you have two settings available for selection. The Port Settings menu selections are **Port Status** and **Internet Services Port Number**. After pressing the selection line, to access available settings press the Change Settings button in the lower right corner of the touch screen.

## Internet Services (HTTP) Enablement

1. Press the selection line labeled **Port Status**.
2. Press the **Change Settings** button.
3. On the Port Status screen, note which of the two buttons is highlighted as the current setting for Internet Services Enablement. The available settings are Enabled or Disabled. In order to use Internet Services, this setting **MUST** be enabled.
4. To change settings, press your setting of choice, then press the **Save** button.
5. To exit the screen, without making any changes, click the **Cancel** button.

### Internet Services Port Number

1. Press the selection line labeled **Internet Services Port Number**.
2. Press the **Change Settings** button.
3. On the Port Number screen, use the supplied keypad to enter the appropriate port number (default of 80).
4. To change settings, press the **Save** button.
5. To exit the screen, without making any changes, press the **Cancel** button.

### Exiting the Internet Services Selection Menu

To exit the Internet Service Selection Menu, which returns you to the Port Settings menu, press the rectangular **Close** button in the upper right corner of the touch screen.

### Exiting the Port Settings Menu and returning to the Tools tab screen

1. To exit the Port Settings menu, returning to the **Tools tab** screen, press the rectangular **Close** button in the upper right corner of the Port Settings menu screen.
2. Wait several seconds and the Auto Clear service should log you out.

*Note: If you changed any settings in the Port Settings menu, the Device will automatically reboot to register and enable your new settings.*

# Overview

**Internet Services** is the embedded HTTP server application that resides in the Device. Internet Services allows you to access Device configuration and connectivity tools using a web browser.

To access the Device's Internet Services from your workstation, **set your browser so that it will not try to access the Device through a proxy server**.

With your Internet Browser program running on your workstation, enter the Device's **IP Address** (as seen on the Configuration Report) into the Address or Location field of the browser. Press the **Enter** key on your keyboard.

Internet Services contains the following main menu tabs:

- **Status:** Allows you to review the status of the Device's Trays and Consumables.
- **Jobs:** Allows you to view the current job queue, as well as a history of processed jobs.
- **Print:** Features the **Job Submission** hot link. **Job Submission** allows you to send print-ready jobs to the Device. This tab also includes the feature known as **Secure Print**, which is covered in this guide in the topic of the same name. Note: The print-ready jobs must be in a file format that the Device recognizes (PostScript files with a **.ps** file extension, for example). Delivery methods include Immediate Print, Proof Print, Delayed Print, and Secure Print. For information on Secure Print, refer to the Security – Secure Print topic in this guide.
- **Scan:** Includes the **Mailbox**, **Job Templates**, and **Job Flow Sheets** hot links. The **Mailbox** link lets you create individual mailboxes into which you can direct scanned documents. These documents can then be retrieved and printed, either at the device or locally at your workstation, as explained in the Scanning to the Device's Hard Drive (Mailbox) topic. In addition, by using **Job Flow Sheets**, as explained in the Set Up and Use of Job Flow Sheets topic, you can perform a number of actions on the documents residing in your mailbox. **Job Templates** enables the creation and editing of individual Job Templates, used to direct scanned jobs to Network Servers.
- **Properties:** Allows you to configure the Device for job processing, options support, and network communications.
- **Support:** Provides a Software Upgrade hot link, and displays System Administrator and Xerox Support information. By clicking on Change Settings, the displayed System Administrator information can be modified as desired. Note that Machine Software is best upgraded using the Machine Software folder, contained in the Services folder of the Properties tab.

# Status Tab

The **Status** tab allows you to retrieve the status of the Device's Trays and Consumables.

Click either the **Trays** or **Consumables** hot link to view the status of the desired item.

Click the **General** hot link for a general description of the machine currently being communicated with.

Click the **Refresh** button at any time to refresh the status screens.

Note that this Tab also contains a handy **Reboot Machine** button, enabling remote rebooting of the Device, when needed.

# Jobs Tab

Clicking the **Jobs** tab allows you to view the current job queue, as well as a history of processed jobs.

Click on the **Active Jobs** hot link to view the current job queue.

If you click on the folder labeled **Job History List** you will see the Job History hot link which, when clicked, displays a list of jobs that have been processed from the dates indicated on the screen. The list includes jobs that have been printed, copied, and scanned.

# Print Tab

The **Print** tab features the **Job Submission** hot link.

**Job Submission** allows you to send print-ready jobs to the Device. Note: The print-ready jobs must be in a file format that the Device recognizes (PostScript files with a **.ps** file extension, for example). Delivery methods include Immediate Print, Proof Print, Delayed Print, and Secure Print. For information on **Secure Print**, refer to the Security – Secure Print topic in this guide. Use the **Browse...** button to locate your print-ready job. Click **Submit Job** when you are ready to submit your job.

# Scan Tab

Includes the **Mailbox**, **Job Templates**, and **Job Flow Sheets** hot links. The **Mailbox** link lets you create individual mailboxes into which you can direct scanned documents. These documents can then be retrieved and printed, either at the device or locally at your workstation, as explained in the **Scanning to the Device's Hard Drive (Mailbox)** topic.

In addition, by using **Job Flow Sheets**, as explained in the **Set Up and Use of Job Flow Sheets** topic, you can perform a number of actions on the documents residing in your mailbox.

**Job Templates** enables the creation and editing of individual Job Templates, used to direct scanned jobs to Network Servers.

For complete instructions on how to create the default template (upon which user templates are based), how to configure a scan filing repository, or how to set up a remote template repository, refer to **Network Scanning (using templates)** in the **Options** section of this guide.



# Properties Tab

The **Properties** tab allows you to configure the Device's numerous job processing, options support, and network communications settings.

The **Directory Tree** on the left side of the screen consists of individual **hot links**, mixed in with a number of **file folders**, including nested folders and links.

*Note: Internet Services is being enhanced to make it more consistent with similar Xerox products. As of the published date of this guide, the list of individual links and folders on this tab is as stated below. If a link has been moved, however, simply click the individual file folders on this tab to view their contents and locate the described link.*

## Descriptions of the folders and hot links in the Directory Tree

The **Configuration Overview** hot link provides a convenient method for locating key Connectivity and Services settings. Clicking Settings, then Configure, takes you directly to the pages of interest, allowing you to quickly configure the items selected.

The **Description** hot link displays basic Device identification information.

### General Setup folder

#### Overview

The General Setup folder contains the Configuration, Job Management, Paper Tray Attributes, Paper Settings, Power Saver Settings, Stored Document Settings, Memory Settings, Internet Services Settings, Pool Server Settings, and Cloning.

Subfolders in the General Setup folder include Alert Notification, Billing & Counters, and Smart eSolutions.

#### Description of links

The **Configuration** hot link provides coverage of such subjects as Memory allocation; available Page Description Languages and their version numbers; Firmware (Software) versions for the Controller and Device components; Hard Disk partition information; and Hardware information (indicating the availability of the Ethernet Port and Hard Disk, for example).

The **Job Management** hot link allows you to set permissions that allow System Administrators or general (non-administrator) users to delete jobs from the machine's print queue.

The **Paper Tray Attributes** hot link provides a display of the available Trays (including bypass), their media settings, and tray selection order. To have the Device register changes made to any settings, click the rectangular Apply button.

The **Paper Settings** hot link displays Paper Settings, which can be manipulated and set for installed trays, per the Device's User Guide. To have the Device register changes made to any settings, click the rectangular Apply button.

**The Power Saver Settings** hot link displays the settings for low power mode and sleep mode. **Low Power Mode** is selectable from 1 to 240 minutes. **Sleep Mode** is selectable from 1 to 240 minutes. To have the Device register changes made to any settings, click the rectangular **Apply** button.

The **Stored Document Settings** hot link enables you to set a minimum passcode length for jobs stored on the device.

The **Memory Settings** hot link enables you to view or change the amount of memory allocated on the hard drive for spooling incoming jobs into buffers (dedicated to specific ports or protocols). To have the Device register changes made to any settings, click the rectangular **Apply** button.

*Note: When making setting changes you may be prompted for the Administrator password.*

The **Internet Services Settings** hot link displays such Internet Services settings as the Auto Refresh Interval in seconds, and the Display Language (if available). To have the Device register changes made to any settings, click the rectangular **Apply** button.

The **Pool Server Settings** hot link is used to set up the login details from this device to a remote template pool server. For details, refer to the **Setting up a Remote Template Pool Repository** topic in the Network Scanning section of this guide.

**Cloning** enables you to conveniently copy the settings and web-generated scan templates of one machine and transfer them to other machines operating with the same version of system software. Groups of settings can be cloned, depending on the optional features installed on the machine.

#### **Alert Notification subfolder**

This folder contains two links. The **Billing Meter Read Alerts** link is used to set up an e-mail notification to the designated Billing Administrator whenever billing meters are automatically read by the Meter Assistant. The **Supplies Data Sent Alerts** link is used to set the receiving email address for alerts from the Supplies Assistant. For more information on both the Meter and Supplies Assistants, see the **Smart eSolutions (Meter Assistant and Supplies Assistant)** topic in this guide.

#### **Billing & Counters subfolder**

The **Billing & Counters** folder contains links which display a tally of the total number of pages, images, or jobs processed by the device.

#### **The Smart eSolutions subfolder**

The Smart eSolutions folder contains all the hot links you need to set up automatic billing meter reading and supplies reporting. For more information on both the Meter and Supplies Assistants, see the **Smart eSolutions (Meter Assistant and Supplies Assistant)** topic in this guide.

#### **Connectivity folder**

The **Port Settings** hot link displays a table with check boxes to enable or disable specific ports. Note that if any selections, such as Port 9100 for example, are unavailable for setting using the Device's Control Panel, they can be set here. To have the Device register changes made to any settings on this Table, click the rectangular **Apply** button, then click the **Reboot Machine** button (always available on the Status Tab) to remotely reboot the Device.

The **Port Settings** hot link selections include:

- EtherTalk
- NetWare (for Novell networks)
- SNMP
- SMB
- LPD
- Port 9100
- Send E-mail

- Receive E-mail
- E-mail Notification Service
- Internet Services
- FTP Client
- IPP
- UPnP Discovery
- WebDAV
- Bonjour
- WSD
- SOAP

## Physical Connections subfolder

The file folder, labeled **Physical Connections**, contains Ethernet, Parallel Port (if available), and USB (if available) hot links. Note that the Parallel Port and USB hot links need an optional kit installed before they can be displayed.

Click on the **Ethernet** hot link to view or change **Ethernet (speed) Settings** from a drop-down selection list. Selections include: Auto (auto sensing), 10 Base-T (Half Duplex), 10 Base-T (Full Duplex), 100 Base-TX (Half Duplex), and 100 Base-TX (Full Duplex). The MAC Address of the machine is also displayed, but not editable. To have the Device register changes made to any settings, click the rectangular Apply button.

Click on the **Parallel** hot link to view or change the enablement settings for **Bi-Directional Communications** (a check box) and **Auto Eject Time** (Parallel Port Timeout), with a range of 5 to 1275 seconds. To have the Device register changes made to any settings, click the rectangular Apply button.

Click on the **USB** hot link to view or change the **Auto Eject Time**, which is the length of time the Controller will wait for an end of job command before processing the job. Refer to the On-Line Help for assistance in configuring the Adobe Communication Protocol (if available).

## Protocols subfolder

The subfolder, labeled **Protocols**, contains a list of hot links for viewing or modifying the communications protocols used by the Device.

Note that the previously displayed hot link for **E-mail** has been moved to the **Services** folder in the main directory tree. The remaining links for **SMTP Server**, and **POP3 Setup** allow you to configure E-mail server addressing, for support of E-mail scanning with the machine. For complete information on the required E-mail settings, refer to the **Scan to E-mail topic in the Options section of this guide**. To have the Device register changes made to any settings, click the rectangular **Apply** button.

The **Proxy Server Settings** hot link allows you to set your proxy server parameters in support of such services as the Meter Assistant and Web Service (if available).

## LDAP nested subfolder

The LDAP nested folder contains the same settings available under Authentication Configuration in the Security folder. This allows you to configure authentication for the device using LDAP, or to independently configure LDAP for use with the device, such as in address book support for E-mail.

## Services Folder

This folder contains several subfolders.

The **Printing subfolder** contains a hot link labeled **Print Mode**, and another sub-folder labeled **Language Emulations**.

Click on the **Print Mode** hot link to set the Page Description Language emulation used by the Printer's Input Ports displayed on the screen. Depending upon the Ports enabled at the Device, the list of Ports will include: Parallel, AppleTalk (with PostScript), SMB, LPD, IPP and Port 9100. Typical Page Description selections for each Port include: Auto (auto select), PostScript, HP-GL/2, PCL, and TIFF/JPEG. To have the Device register changes made to any settings, click the rectangular Apply button.

Click on the **Language Emulations** folder, then on a Page Description language to access the Printer's default preferences for processing that Page Description Language. To have the Device register changes made to any settings, click the Apply button.

The **E-mail subfolder** contains a **Default** link to set up default E-mail parameters and a **Public Address Book** link. For complete information on REQUIRED E-mail settings, refer to the **Scan to E-mail topic in the Options section of this guide**. The **Public Address Book** hot link enables you to import an address book in Comma Separated Value (CSV) format. This address book can be used by such system options as E-mail, Fax, and iFAX. Click the **Browse...** button to locate your CSV formatted file, then click **Import Now**.

The **Fax subfolder** is used to set the machine to support embedded fax (Scan to Fax) or Server Fax (Scan to Fax Server). The **Defaults** hot link is used to enable or disable the printing of a Transfer Report in support of Server Fax operations. Refer to the **Server Fax topic** of this guide for full information.

## Services Folder (continued)

The **Network Scanning subfolder** is used to set up **Network Scanning using Templates**, as stated in this guide in the topic of the same name.

The **Machine Software Subfolder** currently contains two hot links: Upgrades and Manual Upgrade.

The **Upgrades** hot link provides the Enabling control for software upgrades.

The **Manual Upgrade** hot link provides the ability to manually perform software upgrades, after enabling through the Upgrades link.

The **Xerox Services subfolder** contains a link to setting up the **Xerox Communication Server**. This is the Xerox server that supports automatic billing and supplies reporting, set up as stated in the **Smart eSolutions (Meter Assistant and Supplies Assistant) topic** in this guide.

The **Custom Services subfolder** contains the **Validation Options** and **Custom Services** links. The **Validation Options** link is meant to work with a validation server, which is used in an enterprise network to certify the authenticity of Digital Certificates used for file encryption. Note that Digital Certificates typically work with SSL/TLS encryption, which is set up from the Machine Digital Certificate Management link in the Security folder. The host name and path settings for a validation server are set up through the **Validation Server** hot link in the Network Scanning subfolder. For a definition of the Custom Services link, consult the on-line help.

## Accounting folder

The file folder, labeled **Accounting**, contains the **Accounting Configuration** hot link allowing you to secure machine services through Accounting methods. This was formerly the standalone Auditron Administration hot link, in the Properties tab directory tree.

## Security folder

This file folder now contains the contents found in previous products in the Security folder.

The **Authentication Configuration** hot link is used for setting up the machine with local and remote Authentication, and for the use of Authentication in conjunction with Accounting methods. The folder also contains a hot link for Audit Log settings, as well as a link for setting up the details of the log in used by users to access device services.

**User Details Setup** is used to configure the characteristics of the login prompt for User Authentication.

Remote Authentication Server / Directory Services subfolder

The **Remote Authentication Server / Directory Services** folder is meant to support machine authentication administered by a remote server. This type of authentication is first set up by selecting the **Security** folder, then **Authentication Configuration** in the list of hot links, then selecting Login to Remote Accounts from the **Login Type** drop-down list. Machine connection to the remote authentication server is then set up by either clicking **Next** and **Configure** in the Authentication Configuration dialog, or by using the hot links displayed here under the Remote Authentication Server / Directory Services folder. For complete details on the set up and use of authentication, including Remote Authentication, refer to **Security – Authentication** in the **Options** section of this guide.

The **IP Filtering** link lets you set up IP address restrictions for access to this device.

The **Audit Log** hot link allows you to enable or disable the Audit Log as explained in the Audit Log topic of this guide.

The **Machine Digital Certificate Management** link is used to manage all digital certificates, of various types, stored on the machine.

The **IP Sec** link lets you configure the settings for IP Sec encryption.

The **Trusted Certificates Management** link sets the categories for trusted certificate management (used with digital certificates).

The **802.1x** link is used to authenticate the multifunction device on the 802.1x network.

The **SSL / TLS** link lets you configure the settings for SSL / TLS encryption.

The **PDF / XPS Security Settings** hot link displays the dialog to determine whether or not to add a digital signature to PDF and XPS files.

Job Indication Limit subfolder

The Job Indication Limit subfolder contains hot links that can be used to block queue display at the device.

The **System Administrator Settings** link lets you change the Login ID and Passcode used by the System Administrator to access Tools on the device's local user interface, and to modify Properties with Internet Services.

# Support Tab

The **Support** tab provides a **Software Upgrade** hot link, and displays System Administrator and Xerox Support information. By clicking on Change Settings, the displayed information can be modified as desired.



# Additional Details of some Properties Tab features

## Setting TIFF (and other PDL) Processing Properties

To set the Printer's default TIFF / JPEG, PostScript, PCL, or HP-GL/2 processing properties, perform the following steps:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the folder in the directory tree labeled **Services**.
4. Click the folder labeled **Printing**, then on the folder labeled **Language Emulations**.
5. Click on the **TIFF / JPEG**, or **PostScript**, or **PCL**, or **HP-GL/2** hot link to access the Device's list of default settings for processing the selected Page Description Language.
6. Select a Printer number and click the **Edit** button (when available) to access a list of numerous processing settings.
7. Click the rectangular **Apply** button to have the device register changes made to any settings. To return settings to their previous values, without making changes, click the **Undo** button.

## Setting PDL Emulations

To set the PDL (Page Description Language) Emulations, used by the Device's Input Ports, perform the following steps:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the folder in the directory tree labeled **Services**.
4. Click the folder labeled **Printing**.
5. Click on the folder labeled **Language Emulations** to see the Page Description Languages currently supported by system software.
6. Click on the **Print Mode** hot link to access a list of the Device's Input Ports, displaying the Page Description Language emulations they are currently set to use.
7. Depending upon the Ports enabled at the Device, the list of displayed Ports includes: Parallel, AppleTalk (with PostScript), SMB, LPD, IPP, WSD, and Port 9100. Typical Page Description selections for each Port include: Auto (auto select), PostScript, HP-GL/2, PCL and TIFF/JPEG.
8. Make your required setting changes, and click the rectangular **Apply** button to have the device register the changes. To return settings to their previous values, without making changes, click the **Undo** button.

## Banner Sheet Printing

When documents are sent to print at the machine, a banner sheet is printed identifying the PC that sent the print job. The banner sheet is printed on paper from a selected tray. When the selected tray is empty, the device will automatically switch to another tray with the same size paper and print the banner sheet from that tray. The device will continue to print banner sheets from this secondary tray until the selected tray is refilled.

### **To set banner sheet printing and select a banner sheet paper tray:**

1. Press the Log In / Out button on the Device's Control Panel.
2. Press the "1" key on the numeric keypad five consecutive times.
3. Press the Machine Status button on the Control Panel.
4. Touch the Tools tab.
5. Touch System Settings.
6. In the Group column, touch Print Service Settings.
7. In the Features column, touch Other Settings.
8. On the Other Settings screen, in the Items column, touch Banner Sheet, then touch Change Settings.
9. On the Banner Sheet screen, select one of the following:
  - Off
  - Start Sheet (the default choice)
  - End Sheet
  - Start Sheet & End Sheet
10. Touch Save.
11. To select a banner sheet tray:
  - a. On the Other Settings screen, in the Items column, touch Banner Sheet Tray, then touch Change Settings.
  - b. Touch Tray 1, Tray 2, Tray 3, or Tray 4 to select the tray that will hold the banner sheet paper.

*Note: Tray 3 is the suggested choice, with Tray 4 as the secondary tray.*
12. Touch Save.

## Set the Ethernet Speed

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the **Connectivity** folder, then the **Physical Connections** folder.
4. Click the **Ethernet** hot link.
5. Select your network speed from the drop-down list.
6. Click the **Apply** button to accept the changes, or the **Undo** button to return the settings to their previous values.

*Note: Changes to settings are not applied until you restart the Device. A Reboot Machine button is available on the Status Tab of Internet Services.*

## Configure TCP/IP Settings

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **TCP/IP** in the directory tree.
5. Review the available selections as displayed on your screen and explained in the **TCP/IP Configuration Selection List**, below.
6. Accept the default Host Name, or type in your own unique Host Name for this Device.
7. Select the desired method for obtaining an IP Address.
8. If **Static** is selected, type in the addresses that apply for **IP Address**, **Subnet Mask**, and **Gateway**.

*Note: If DHCP or BOOTP addressing method is selected, you cannot manually change the IP Address, Subnet Mask, or Gateway. Select Manual if you wish to manually enter in these addresses.*

**Caution:** Changing the IP address for the Device will affect NetBIOS/IP, LPR/LPD, FTP, SNMP, and Port 9100 printing. It will also interrupt the ability to communicate with the device using the Internet Services (series of web pages on the Device). When you change the Device's IP Address, make sure to print out a Configuration Report (as stated in this guide) so that you have a record of the TCP/IP addresses for use with workstations that need to communicate with the Device using TCP/IP.

*Note: When using DHCP, set a reasonably long Lease Time for the IP Address so that the Device can be restarted, when taken out of service for maintenance, without being assigned a new IP Address.*

*Note: Upon rebooting, when the system comes up, if it can't locate a DHCP server on the network it will use whatever IP address it was previously configured with.*

9. Determine the method to use to supply the DNS Server IP Addresses (to resolve Host Names with IP Addresses).
10. Determine whether or not Dynamic DNS should be enabled.
11. When finished modifying settings, click the Apply button. To exit the settings screen without making changes, click the Undo button.

*Note: Changes to TCP/IP settings will not be applied until you restart the Device. A remote Reboot Machine button is available on the Status Tab of Internet Services.*

## TCP/IP Configuration Selection List

As displayed on your screen, the following selections are available for TCP/IP Configuration.

### IP Mode

Select the IP Mode that applies to your network environment.

### General

Host Name. The default entry assures a name that is unique to this device on the network.

IP Address Resolution. Use this drop-down menu to select the method to use to assign IP Addresses. Select Static, DHCP, RARP, BOOTP, or DHCP/Autonet.

Note that with the Autonet option selected, if a Windows 2000 client can't contact the DHCP server, it will assign itself an IP address from the 169.254.0.0 class B address space. This is also known as zero configuration, or Bonjour, networking. Make sure to check the Enabled box for Self Assigned Address at the bottom of your screen.

IP Address entry box. To be filled in manually ONLY when Static addressing is selected.

Subnet Mask entry box. To be filled in manually ONLY when Static addressing is selected.

Gateway Address entry box. To be filled in manually ONLY when Static addressing is selected.

### Domain Name

Enter the fully qualified domain name here. For example: xerox.com.

### DNS Configuration

DNS Server Address Resolution check box. If enabled with a check mark, the Device will contact the DHCP Server for the IP Addresses of up to three DNS Servers. If unchecked, this information must be entered manually.

Three DNS Address boxes are supplied for the manual entry of DNS Server addresses.

Dynamic DNS Update Box. If your DNS Server does not support dynamic IP address updates there is no need to enable this checkbox. Check the Overwrite box to enable DNS information overwriting.

Generate Domain Search List Automatically. A check box is provided for enabling automatic Domain searches.

Domain Names 1,2,3. Three text boxes are provided for the entry of Domains to search (for example, Xerox.com).

Connection Timeout. An entry box is provided for entering a Timeout for searches of Domains.

### Zero Configuration Networking

Used with DHCP/Autonet selected from the IP Address Resolution drop-down menu, when this box is checked the device will assign itself an IP address from the 169.254.0.0 class B address space.

*Note: Changes to TCP/IP settings will not be applied until you restart (reboot) the Device.*

## Configure LPD

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **LPD** in the directory tree.
5. The available selections include:
  - Port Number, with a default value of 515. As this is the port for the TCP Spooler assigned by the IANA (Internet Assigned Numbers Authority), the default value should not need to be changed.
  - A TBCP Filter checkbox (displayed when PostScript is enabled).
  - Connection Time-Out entry box.
  - Maximum Number of Sessions: Enter the maximum number of simultaneously connected hosts for this interface (or accept the default value).
6. Enter a Time Out value for jobs being sent to the Device through this Port. This is the length of time that the Controller will wait for an end of job command before printing the current job.
7. Click the **Apply** button to accept the changes, or the Undo button to return the settings to their previous values.

*Note: Changes to settings are not applied until you restart the Device. A Reboot Machine button is available on the Status Tab of Internet Services.*

## Configure SNMP

It is possible to remotely define and modify GET (Read Only), SET (Read/Write), and Trap SNMP (Simple Network Management Protocol) community names for the Device. You can also enter the System Administrator's Name here for packet identification purposes.

### SNMP Community Name properties that can be configured

**Community Name (Read Only)**—This is the password for SNMP GET requests from the SNMP Manager to the Agent in the Device. Applications, such as Xerox Printer Map or CentreWare Conductor, obtaining information from the device by SNMP use this password.

**Community Name (Read/Write)**—This is the password for SNMP SET requests from the SNMP Manager to the Agent in the Device. Applications, such as Xerox Printer Map or CentreWare Conductor, which set information on the device by SNMP use this password.

**Community Name (Trap Notification)**—This is the default password for SNMP TRAPS sent from the device to the Manager by SNMP.

## Configuring SNMP Community Names with Internet Services

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **SNMP Configuration** in the directory tree, and check the **Enable** box for the version desired.
5. Enter a name for **Community Name (Read Only)**, also known as GET.
6. Enter a name for **Community Name (Read/Write)**, also known as SET.

**Caution:** If you change the GET and/or SET Community Names, you must also change the names in all network applications that are communicating by SNMP with this Device.

7. Enter a name for the **Community Name (Trap Notification)**. This is the default password for SNMP TRAPS sent from the device to the Manager by SNMP.
8. Optionally enter the System Administrator's name for packet identification purposes.
9. Select a trap and click **Edit** in the Trap Notification Settings section.
10. Select your transport method (IPX or UDP) and fill in the trap destination information for your selected method.
11. Select the event(s) that you wish to report on by checking the applicable box(es).
12. Click the **Apply** button to accept the changes, or the **Undo** button to return the settings to their previous values.

*Note: Changes to settings will not be applied until you restart the Device. A Reboot Machine button is available on the Status Tab of Internet Services.*



## Configure Microsoft Networking (also known as SMB)

For full instructions on configuring this device for Microsoft Networking, refer to the Microsoft (NetBIOS over IP) Networks topic in the NOS Selection section of this guide.

## Configure IPP

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **IPP** in the directory tree.
5. The available selections include:
  - Port Number Static Display, with a default value of 631. This is the port number assigned by IANA (Internet Assigned Numbers Authority).
  - Additional Port Number entry box. You can enter port 80 (HTTP) here as a backup port.
  - A TBCP Filter checkbox (displayed when PostScript is enabled).
  - Administrator Mode checkbox. This is disabled by default. Consult the On-Line Help for use of this feature.
  - DNS checkbox.
  - Connection Time-out entry box.
6. Verify that the **DNS** checkbox is checked (enabled) by default. If enabled, the DNS Server will be available to resolve Host Names to IP Addresses, in support of printing with IPP.
7. Enter a **Connection Time Out** value for jobs being sent to the Device through this Port. This is the length of time that the Controller will wait for an end of job command before printing the current job.
8. Click the **Apply** button to accept changes, or the Undo button to return settings to their previous values. Note: Setting changes are not applied until you restart the Device. There is a convenient **Reboot Machine** button on the Status tab of Internet Services.

## Modify the HTTP (Internet Services) Settings

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **HTTP** in the directory tree.
5. The available selections include:
  - Port Number entry box. The default value is Port 80, which is the HTTP Port number assigned by the IANA (Internet Assigned Numbers Authority). This default value should not need to be changed.
  - Maximum Connections entry box.
  - Connection Time-out entry box.
  - Secure HTTP (SSL) checkbox** – To be enabled only when you wish to set all HTTP communications with the device to encrypted communications. If you do this you will have to have a digital certificate installed on the device, as stated in the **Security – Encryption section** of this guide.
  - Secure HTTP Port Number** – HTTP traffic will be routed to this port when using HTTP with SSL encryption.
6. In the **Maximum Connections** entry box, accept the default value, or enter a number for the maximum number of hosts (networked workstations) that can be connected to the Device's HTTP Server (Internet Services web pages) at one time.
7. In the **Connection Time-Out** entry box, accept the default value, or enter the number of seconds that a browser connection can remain open without any activity.
8. Click the **Apply** button to apply setting changes, or the Undo button to return settings to their previous values.

*Note: Setting changes are not applied until you restart the Device. There is a convenient Reboot Machine button on the Status Tab of Internet Services.*

## Configure WSD (Web Services on Devices)

As stated by Microsoft, WSD is Microsoft's implementation of the Devices Profile for Web Services (DPWS) standard, a specification that enables devices, such as printers, cell phones, cameras, and home entertainment centers, to use standard Web-based protocols (HTTP and UDP) to discover one another, advertise their services over the IP (versions 4 or 6) network, and report on their operational status.

Typically, a device such as a network printer will use a small amount of flash memory to store WSD-related information. The WSD device then advertises a primary endpoint that can be located through WS-Discovery (via UDP) on a Windows Vista client.

The endpoint supplies metadata about itself through WS-Metadata Transfer. This information typically includes manufacturer, device information, and service host metadata (information on offered services).

WSD provides two way communication, enabling a printer to both receive jobs and to send status notifications to Windows clients when events occur, such as supplies running low.

To configure this multifunction device for WSD, perform the following steps.

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **WSD** in the directory tree.
5. The available selections include:

Port Number - Enter the port number between 1 and 65535. Port 80 is the recommended HTTP default. Do not use the numbers assigned to the other ports.

TBCP Filter - Check to enable TBCP Filter when PostScript data is to be processed. This is only available when the optional PostScript 3 kit is installed. When the transmission data includes binary data or EPS data, disable this. For Windows, follow the Output Protocol setting in the Device Settings tab of the Properties screen of the print driver.

Data Receive Time-Out - Enter the timeout period for receiving data from WSD clients between 1 and 65535 seconds in 1 second increments.

Notification Delivery Time-Out - Enter the timeout period for notification delivery to WSD clients between 1 and 60 seconds in 1 second increments.

Maximum TTL - The Time to Live setting (in seconds) for undelivered IP datagrams (such as UDP being used with WSD). Enter a value 1 and 10.

Maximum Number of Subscribers - Enter the maximum number of clients for reserved notification between 1 and 200.

6. Click the **Apply** button to apply setting changes, or the Undo button to return settings to their previous values.

*Note: Setting changes are not applied until you restart the Device. There is a convenient Reboot Machine button on the Status Tab of Internet Services.*

## Configure Port 9100 (Raw Printing)

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **Port 9100** in the directory tree. (1)
5. The available selections include:
  - TCP Port Number, with a default value of 9100. This does not need to be changed.
  - A TBCP Filter checkbox (displayed when PostScript is enabled).
  - Connection Time-Out entry box.
6. Enter a **Time Out** value for jobs being sent to the Device through this Port. This is the length of time that the Controller will wait for an end of job command before printing the current job.
7. Click the **Apply** button to accept changes, or the Undo button to return settings to their previous values. Note: Setting changes are not applied until you restart the Device.

*Note: (1) If Port 9100 is NOT displayed in the Properties Tab directory tree, click the Port Status hot link in the directory tree. Use your mouse to place a check mark in the checkbox on the Port 9100 line. Click the Apply button, then click the Reboot button (always available on the Status Tab) to remotely reboot the Device.*

## IP Filtering (IP Address Restriction)

Using Internet Services, access to the Device's Services can be restricted by Host IP Address.

To restrict device access, perform the following steps:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus symbol (+) to the left of the **Security** file folder.
4. Select **IP Filtering**.
5. Choose which IP Filtering to apply depending upon the address space used with your network. Note that IPv4 is the traditional (xxx.xxx.xxx.xxx) address space used with TCP/IP networks.

**IP Filter Enablement Check box.** If enabled with a check mark, access to the Device's services will be restricted to the list of IP Addresses and Subnet Masks specified by clicking the Edit button. If disabled (unchecked), host access to the Device is universal (unrestricted).

**Add or Edit button.** When this button is clicked, a list of ten lines of IP Address and Subnet Mask entry boxes is displayed. Sometimes referred to as a "restriction list," this list is used to supply the IP Addresses and Subnet Masks of up to ten hosts (individual workstations) that are authorized to access the Device's services. All other hosts, not specified in this list, will be prevented from accessing the Device's services.

6. Click **Apply** when done.

*Note: Changes to settings are not applied until you restart the Device. A Reboot Machine button is available on the Status Tab of Internet Services.*

## Configure EtherTalk (AppleTalk)

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **EtherTalk** in the directory tree.

*Note: If EtherTalk is NOT displayed in the Properties Tab directory tree, click the Port Settings hot link in the directory tree. Use your mouse to place a check mark in the checkbox on the EtherTalk line. Click the Apply button*

5. The available selections include:
  - Printer Name.
  - Zone Name.
6. Enter the name that you wish to assign to this Printer. This is the name that will appear in the Chooser.
7. Either accept the default zone of \* which lets the closest router assign the Device to a zone, or assign the Device to a zone (with a 32 character naming limit).
8. Click the **Apply** button to accept changes, or the Undo button to return settings to their previous values.

*Note: Changes to settings are not applied until you restart the Device. A Reboot Machine button is available on the Status Tab of Internet Services.*

## E-mail, SMTP, and POP3 Settings

The Protocols hot links for SMTP, and POP3, and the E-mail subfolder under the Services folder (on the Properties page of Internet Services) can be used instead of the settings at the machine's User Interface, to configure E-mail scanning with the machine.

For complete information on required E-mail settings, refer to the **Scan to E-mail** topic in the **Options** section of this guide.

To have the Device register changes made to any settings, click the rectangular **Apply** button. You can reboot the device remotely using the **Reboot Machine** button, which is available on the Status Tab of Internet Services.



## Bonjour (if available for selection)

Bonjour, also known as zero-configuration networking, supports communicating with other devices using 169.254/16 IPv4 addressing, over the same physical or logical link (such as in ad hoc, or isolated (non-DHCP) networks).

When the Bonjour protocol is enabled on ALL communicating devices, and those devices are connected, Host names of the individual devices will be resolved to IPv4 addressing, without the use of a DNS server, and IP communications can then take place.

To view the Host Name and Printer Name automatically assigned to this machine under Bonjour, do the following:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press **Enter**.
2. Click the **Properties** tab.
3. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder.
4. Select **Bonjour** in the directory tree.

*Note: If Bonjour is NOT displayed in the Properties Tab directory tree, click the Port Settings hot link in the directory tree. Use your mouse to place a check mark in the checkbox on the Bonjour line. Click the Apply button. If Bonjour is not available in the Port Settings list, click the TCP/IP link in the Protocols folder, and scroll to the bottom of the displayed page to Zero-Configuration networking.*

5. Make a note of the Host Name and Printer Name for reference in working with other Bonjour (zero-configuration) connected workstations.

*Note: You can change these names, however the Host Name must be unique on the network. The automatically generated Host Name should assure its uniqueness. The Host Name has a 32 character limit, while the Printer Name has a 62 character limit. If you change either name, be sure to click Apply. You can reboot the device remotely using the Reboot Machine button, which is available on the Status Tab of Internet Services.*

# Troubleshooting

## General Troubleshooting Procedure

1. Make sure that the machine is switched ON and that the Main screen (typically the All Services screen) is displayed.

*Note: The actual screen displayed as the Main screen is selectable. To determine the screen you would like displayed, press the Log In / Out button, enter the Administrator password (default of 11111), press Enter, and press the Machine Status button. Press the Tools tab. Press Common Service Settings, press Screen/Button Settings, select Service Screen Default, touch Change Settings, make your selection and touch Save. Touch Close until the Tools tab screen is displayed. Wait several seconds for the Auto Clear service to log you out.*

2. Make sure that the machine is plugged into a live network drop, typically with a Category 5 twisted pair cable attached to the RJ-45 socket at the rear of the Device.

*Note: You can often determine if the drop is live by looking at the link and activity (if available) light or lights at the rear of the Device. If these lights are lit and/or blinking, you have a live connection. If you cannot determine if the drop is live, plug the machine into another drop being used by another machine that is fully functioning on the network. You can use a hub to connect both machines to the live network drop so that you do not interrupt the operations of the working machine. If you do not have access to a second working drop, or a hub, connect a laptop to the RJ-45 socket at the rear of the Device using a crossover (NOT a patch) cable.*

3. Print a Configuration Report at the Device using the instructions supplied in the **Configuration Report** topic in the **Network Connectivity** section of this guide.
4. Referring to the Configuration Report, determine if the appropriate ports and protocols are enabled for your Network environment.

To support communicating with the Device's Internet Services, a series of internal Web Pages that enable the configuration of operating settings, the TCP/IP protocol stack should be enabled. The Device should also have a valid IP Address, Subnet Mask, and Gateway displayed. If this is not the case, go to the **NOS Selection** section of this guide, locate the **TCP/IP Protocol Configuration** topic, and follow the instructions supplied.

As some Network Environment settings can only be configured through use of Internet Services on the Device, if this tool is shown as "disabled" on the Configuration Report, follow the instructions in the **Enable Internet Services (HTTP)** topic in this guide.

5. At any networked workstation, or at your laptop connected to the Device with a crossover cable, open your Web browser and enter the TCP/IP address of the Device (as shown on the Configuration Report) into the Address or Location field. Press Enter. If the HTTP port is enabled at the Device, you should see the Internet Services series of web pages. Note that depending upon Authentication and Encryption settings, you might also see an Administrator Log In prompt, or a Digital Certificate prompt. With the display of these prompts or pages you have proven that the device is communicating with HTTP over the TCP/IP network. A ping command (see TCP/IP Troubleshooting), issued from the workstation's command prompt, can further verify this working connection.
6. To troubleshoot network communication problems interfering with printing or scanning to the machine's hard drive (mailboxes), refer to the specific topic, that applies to your network operating environment, within this Troubleshooting section.
7. To resolve problems with system Options, refer to the **Configuration Report** to determine if the options are installed, enabled, and properly configured on your machine.

To enable purchased options, refer to the **Enabling Options with Software Keys** topic in the Options section of this guide.

To properly configure enabled options, refer to the applicable topic in the **Options** section of this guide.

# TCP/IP Troubleshooting

Use the following check list to troubleshoot your network communication problem.

## Check Physical Media and Network Interface Cards

1. Verify that the Device is powered ON.
2. Verify that the Device and Workstation are using the correct cabling to communicate over the network. Use category 3 UTP patch (NOT crossover) cable for 10 Base T communications, category 5 UTP patch (NOT crossover) cable for 10 Base T / 100 Base TX communications, and Token Ring cabling for Token Ring networks.
3. Verify that the cable at both the Device and Workstation is fully plugged into the Network Interface Card (NIC). Check the link light, which is typically a green LED, to make sure that it is lit. Typically, but not always, a second light on the Network Interface Card will be intermittently flashing, indicating the presence of network traffic. If neither of these lights is lit, there is a problem with the NIC.

## Print a Configuration Report at the Device and perform these tasks:

1. Under the **Ethernet Rated Speed** data label on the List, verify that your communications speed is correctly set for your network and that you have a MAC address listed. The driver for your NIC works at the Media Access Control (MAC) layer of the protocol stack. If no MAC address is shown, you have either a bad NIC or no NIC at all. Replace or install the Network Interface Card.
2. Under the **TCP/IP** data label, determine the method being used to assign TCP/IP addressing to the Device. Specifically note the Mode being used. IP version 4 is the traditional mode using address formats of xxx.xxx.xxx.xxx. Verify that the IP Address, Subnet Mask, and Gateway addresses are correct for your network and have NOT changed from their previous settings. Note: The use of DHCP (the DHCP Server) with a short "lease" time can cause the Device to be assigned a new IP Address when it is powered off for an extended period of time. This will interrupt communications with workstations using the "old" IP address. If you do not want the IP address to be subject to constant changes, either increase the lease time at the DHCP Server, or use the Static IP Addressing method as described in the **TCP/IP Protocol Configuration** procedure in the NOS selection section of this guide.
3. Under the **LPD** data label, if you are communicating with the Device through an LPR port, make sure that LPD is Enabled. If it is NOT, enable it following the instructions supplied in this guide under **TCP/IP LPD Enablement**. Also verify that the displayed port number is "515." If it is NOT, set it to "515" using the instructions supplied in the **Configure LPD** procedure in the Internet Services section of this guide.
4. Under the **Port 9100** data label, to enable the Device to automatically determine the Page Description Language to use in processing jobs sent over the workstation's LPR port, make sure that this Port is enabled. This is the meaning of the word "raw" when used to name the queue during LPR port creation. Follow the instructions supplied in the **Configure Port 9100 (Raw Printing)** procedure in the NOS Selection section of this guide.
5. Under the **CentreWare Internet Services** data label, verify that this feature is Enabled. If it is NOT, enable it following the instructions supplied in the **Network Connectivity** section of this guide.

## At the workstation, perform these tasks:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press ENTER. If the Device's Internet Services (web pages) begin to display on the workstation, you are communicating with the Device. If NOT, make sure that your web browser is not set to use a proxy server and repeat the procedure. If unsuccessful, perform the next step.
2. Verify that the workstation has been assigned an IP address, subnet mask, and gateway address by running a Command (DOS) prompt, typing **ipconfig/all** (Windows 2000/XP) and pressing ENTER. If any of the addresses are incorrect or missing, right mouse click on the Network Neighborhood icon (My Network Places in Windows 2000), and make sure that the **TCP/IP protocol** is installed and properly configured for IP addressing. For XP, click Start/My Network Places/right mouse click in the open window/select Properties/right mouse click Local Area Connection/then select Properties.
3. Run a Command (DOS) prompt on the workstation and perform **ping** tests to verify successful packet transmission first to the workstation's NIC, then to the Gateway (if being used), then to the Device's NIC. To run Ping Tests, at the Command (DOS) prompt, type: ping xxx.xxx.xxx.xxx and press ENTER. Note that there is a space between the word "ping" and the first xxx. Let xxx.xxx.xxx.xxx first represent the workstation's IP address, then the IP address of the default gateway, and finally the IP address of the Device. If successful, you will receive a reply such as: "Reply from xxx.xxx.xxx.xxx: bytes=32 time<10ms TTL=128." If you receive "Time Out" or "0 bytes received" notifications, the device being pinged is incorrectly configured or malfunctioning.
4. If Web browser and Ping Tests are successful but you are still unable to print to the Device, verify that the driver is using the correct LPR Port to print through. On Windows desktops, select **Start, Settings, Printers** (Start/Printers and Faxes in XP), right click on the Printer's icon, and select **Properties**. Select the Ports Tab (Windows 2000) and verify that the LPR Port being printed through matches the IP Address of the Device. If the IP address does NOT match, you are printing to the wrong device on the network. Either select the correct port from the displayed list, or use the **Add Port** button to create a new port with an IP Address matching that of your Device.

5. If the correct Port is being used by the driver but you are still unable to print, perform the following procedure. In Windows 2000/XP, follow the instructions for TCP/IP Peer to Peer (LPR) Printing, under the Print Drivers Tab of this guide, to verify that **Print Services for Unix** are installed in the workstation.
6. Note that access to this Device's Services can be restricted by Host IP addresses. As this feature could cause communications to appear to fail in certain instances, see the **IP Filtering** procedure in the Nos Selection section of this guide for further details.
7. To assure successful printing, make sure that the Device is configured to support the Page Description Language (PDL) being used by your driver. To check the PDL being used by the driver, print a test job "to file." Open and view the job in a program such as Notepad. The PDL being used by the driver will be displayed in the first few lines of Printer Language. Next, check the Page Description Languages being supported by the Device's ports by following the instructions supplied under the Setting PDL Emulations procedure in the Internet Services section of this guide. The PDL being used by the driver, and the PDL supported by the Port you are printing to, **MUST** match for successful printing to occur.

# NetBIOS over IP Troubleshooting

Use the following check list to troubleshoot your network communication problem.

## Check Physical Media and Network Interface Cards

1. Verify that the Device is powered ON.
2. Verify that the Device and Workstation are using the correct cabling to communicate over the network. Use category 3 UTP patch (NOT crossover) cable for 10 Base T communications, category 5 UTP patch (NOT crossover) cable for 10 Base T / 100 Base TX communications, and Token Ring cabling for Token Ring networks.
3. Verify that the cable at both the Device and Workstation is fully plugged into the Network Interface Card (NIC). Check the link light, which is typically a green LED, to make sure that it is lit. Typically, but not always, a second light on the Network Interface Card will be intermittently flashing, indicating the presence of network traffic. If neither of these lights is lit, there is a problem with the NIC.

## Print a Configuration Report at the Device and perform these tasks:

1. On the Configuration Report, verify that **"SMB" is enabled**. If it is NOT enabled, to enable SMB, follow the instructions supplied in the **Microsoft (NetBIOS over IP) Networks** procedure in the NOS Selection section of this guide.
2. On the Configuration Report, note that the default name of the Device's workgroup is **Workgroup** and that the Device has a unique **SMB Host Name**. To modify the Device's Workgroup or SMB Host Name, if required, use your workstation's Web browser to access the Internet Services (Web Pages) residing in the Device as described in the **Microsoft (NetBIOS over IP) Networks** procedure in the NOS Selection section of this guide.
3. On the Configuration Report, under the **TCP/IP** data label, note what method the Device is using to acquire its TCP/IP addresses. If the method shown is **STATIC**, make sure that the Device has a valid IP address, Subnet Mask, and Gateway address for the network.
4. On the Configuration Report, verify that **DNS is enabled**. The use of Naming Servers is REQUIRED to resolve NetBIOS device names to IP addresses for packet routing over the TCP/IP network. If in doubt as to whether DNS and WINS are enabled, verify the settings following the instructions supplied in the **TCP/IP Dynamic Addressing or Microsoft (NetBIOS over IP) Networks** procedures in the **NOS Selection** section of this guide. WARNING: If the Device is NOT informed of the addresses of the DNS/WINS Servers, you may not be able to see or use the Device's NetBIOS name on the network. Make sure that the Device is informed of the addresses of the DNS/WINS Servers, using the instructions supplied in the above mentioned procedures.
5. Under the **CentreWare Internet Services** data label, verify that this feature is Enabled. If it is NOT, enable it following the instructions supplied in the **Network Connectivity** section of this guide. You **MUST** use this tool at your workstation if you need to change the Device's Workgroup name, the SMB Host Name, the TCP/IP (internet) Host Name, or DNS settings. Note that when using DNS to resolve host names to IP addresses, the NetBIOS name (SMB Host) and the TCP/IP Host Name **MUST** be the same.

## At the DNS or WINS Server

Refer to the Server Operating System documentation for the appropriate procedure to use to enable Host name to IP address resolution on the Server. Make sure that the Device's TCP/IP (internet) Host Name and NetBIOS (SMB Host) Name (which should be identical for DNS) is being mapped to an IP Address on the Server. Refer to the Device's Configuration Report and verify that the Device's TCP/IP Host and NetBIOS (SMB Host) Names continue to match the entries in the Server's database. Also verify that the IP Address shown on the Report matches the IP address in the Server's database. If the information is incorrect on the Server, NetBIOS communications from the workstations to the Device WILL be disrupted.



At the workstation, perform these tasks:

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press ENTER. If the Device's Internet Services (web pages) begin to display on the workstation, you are communicating with the Device. If NOT, make sure that your web browser is not set to use a proxy server and repeat the procedure. If unsuccessful, perform the next step.
2. On Windows 2000 workstations, verify that the **Internet protocol (TCP/IP)** is installed and that it is configured for **DNS resolution** of the NetBIOS Host Name. Also verify that the **Client for Microsoft Networks** is installed. Finally, through Add/Remove Programs and Add/Remove Windows Components, select Other Network File and Print Services, click Details, check the box for **Print Services for Unix**, and click OK and Next.
3. Run a **Command (DOS) prompt** on the workstation and perform **ping** tests to verify successful packet transmission first to the workstation's NIC, then to the Gateway (if being used), then to the Device's NIC. To run Ping Tests, at the Command (DOS) prompt, type: ping xxx.xxx.xxx.xxx and press ENTER. Note that there is a space between the word "ping" and the first xxx. Let xxx.xxx.xxx.xxx first represent the workstation's IP address, then the IP address of the default gateway, and finally the IP address of the Device (as shown on the Configuration Report).
4. If communicating with the printer in a Peer to Peer environment, at the Workstation's Desktop double click the **Network Neighborhood** icon and see if the Printer's **SMB Host Name** appears in the **Workgroup** indicated on the Configuration Report. If it does NOT, SMB may not be enabled at the Device, or there is no Master Browser in the Workgroup. Check the Configuration Report to verify that SMB is enabled and, if necessary, enable Auto Master Mode. To enable SMB, or Auto Master Mode, following the instructions supplied in the **Microsoft (NetBIOS over IP) Networks** procedure in the NOS Selection section of this guide.

5. From your Workstation's Desktop, click Start/Settings/Printers (Start/Printers and Faxes in XP), right mouse click on the Printer's icon and select Properties. From the Ports Tab (Windows 2000) determine the Port that the driver is using to print through. For peer to peer communications, the port name should match the SMB Host name of the Device as shown on the Configuration Report. If it doesn't you are printing to the wrong port and either need to select the correct port or use the Add Port button to create a new port for the driver to print through. Follow the instructions supplied in the NetBIOS over IP Peer to Peer Printing procedure in the Print Drivers section of this guide. If the name matches, use the General Tab of the driver to print a test page to determine the status of communications between the Workstation and the Device.
6. If communicating with the device in a Client/Server environment, at the Workstation's Desktop double click the Network Neighborhood icon and see if the Printer's Server is displayed. If you double click on the Server's name, a list of Shared printers should be displayed, with the Printer being one of the devices shown. Note that since the Printer is identified as a Share name on the Server, it may NOT have the same name as the SMB Host name on the Configuration Report. If you do not recognize your Server or Printer's name in the list, perform the following step.
7. From your Workstation's Desktop, click **Start/Settings/Printers** (Start/Printers and Faxes in XP), right mouse click on the Printer's icon and select **Properties**. From the Ports Tab (Windows 2000) determine the Port that the driver is using to print through. For Client/Server communications, the port name should be in the form of a UNC (universal naming convention) such as \\Computer\_name\Share\_name. If it isn't you are printing to the wrong port and either need to select the correct port or use the **Add Port** button to create a new port for the driver to print through. If the name looks correct, use the **General** Tab of the driver to print a test page to determine the status of communications between the Workstation and the Device.
8. Note that if you have the "UNC" of the Printer, you can enter this into the text box of the **Run** command on your workstation. When you press **Enter**, the workstation will attempt to reconnect to the network Server and Printer Share that was specified by the UNC. Depending upon how the Server was configured you can then either manually or automatically reinstall the driver.
9. To assure successful printing, make sure that the Device is configured to support the Page Description Language (PDL) being used by your driver. To check the PDL being used by the driver, print a test job "to file." Open and view the job in a program such as Notepad. The PDL being used by the driver will be displayed in the first few lines of Printer Language. Next, check the Page Description Languages being supported by the Device's ports by following the instructions supplied under the **Setting PDL Emulations** procedure in the Internet Services section of this guide. The PDL being used by the driver, and the PDL supported by the Port you are printing to, **MUST** match for successful printing to occur.

# IPP Troubleshooting

Use the following check list to troubleshoot your network communication problem.

## Check Physical Media and Network Interface Cards

1. Verify that the Device is powered ON.
2. Verify that the Device and Workstation are using the correct cabling to communicate over the network. Use category 3 UTP patch (NOT crossover) cable for 10 Base T communications, category 5 UTP patch (NOT crossover) cable for 10 Base T / 100 Base TX communications, and Token Ring cabling for Token Ring networks.
3. Verify that the cable at both the Device and Workstation is fully plugged into the Network Interface Card (NIC). Check the link light, which is typically a green LED, to make sure that it is lit. Typically, but not always, a second light on the Network Interface Card will be intermittently flashing, indicating the presence of network traffic. If neither of these lights is lit, there is a problem with the NIC.

## Print a Configuration Report at the Device and perform these tasks:

1. Under the **Ethernet Rated Speed** data label on the Report, verify that your communications speed is correctly set for your network and that you have a MAC address listed. The driver for your NIC works at the Media Access Control (MAC) layer of the protocol stack. If no MAC address is shown, you have either a bad NIC or no NIC at all. Replace or install the Network Interface Card.
2. Under the **CentreWare Internet Services** data label, verify that this feature is Enabled. If it is NOT, enable it following the instructions supplied in the **Network Connectivity** section of this guide.
3. Under the **TCP/IP** data label, determine the method being used to assign TCP/IP addressing to the Device. Verify that the IP Address, Subnet Mask, and Gateway addresses are correct for your network and have NOT changed from their previous settings. Note: The use of DHCP (the DHCP Server) with a short "lease" time can cause the Device to be assigned a new IP Address when it is powered off for an extended period of time. This will interrupt communications with workstations using the "old" IP address. If you do not want the IP address to be subject to constant changes, either increase the lease time at the DHCP Server, or use the Static IP Addressing method as described in the **TCP/IP Protocol Configuration** procedure in the NOS selection section of this guide.
4. Under the **IPP** data label, verify that the IPP Port is Enabled. If it is NOT, enable the port following the procedure stated in the **IPP Configuration** topic in the NOS Selection section of this guide.
5. Under the **IPP** data label, verify that IPP is using **DNS** to resolve Host Names to IP Addresses in support of IPP printing. If it is NOT, using your workstation's Web browser enter the TCP/IP Address of the Device in the Address or Location field. Press **Enter**. Click the **Properties** tab. Click the plus (+) symbol to the left of **Connectivity**, then the **Protocols** file folder and **select IPP** in the directory tree. Verify that the DNS Enablement Checkbox is checked. If it is NOT checked, check it with your mouse and click **Apply**. Reboot the Device with the **Reboot Machine** button on the Status tab.
6. Under the **IPP** data label, verify that the Port number associated with IPP is **631**. This is the port number assigned to IPP by the Internet Assigned Numbers Authority. If the number is not 631, set it to 631 following the instructions supplied in the **Configure IPP** procedure in the Internet Services section of this guide.

## At the Windows 2000 workstation, perform these tasks:

*Note: As IPP (the Internet Printing Protocol) is supported by all Windows 2000 workstations, the following procedure is written specifically for Windows 2000. The IPP printing "service" is available for other workstation operating systems through downloads from the Microsoft web site. In general, troubleshooting procedures for other operating systems will be similar to this one.*

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press ENTER. If the Device's Internet Services (web pages) begin to display on the workstation, you are communicating with the Device. If NOT, make sure that your web browser is not set to use a proxy server and repeat the procedure. If unsuccessful, perform the next step.
2. Verify that the Internet protocol (TCP/IP) is installed in the Windows 2000 or XP workstation. On the Windows 2000 Desktop, right click the My Network Places icon and select Properties. Right click on the Local Area Connection icon and select Properties. On the Windows XP desktop, click Start, Control Panel, and double click Network Connections. Right click on the Local Area Connection icon and select Properties. Verify that the Internet Protocol (TCP/IP) has been loaded. If it has, click on (highlight) this item with your mouse and click the Properties button to verify that this workstation is using either a dynamic or static method to obtain a valid TCP/IP address, and that the workstation's host name is being resolved using DNS. If the TCP/IP protocol is not loaded, click the Install... button, then select Protocol as the type of network component that you wish to install. Click the Add... button and select Internet Protocol (TCP/IP). With your Operating System Installer Disk readily available, click the Have Disk... button and follow any remaining instructions. Once the protocol has been installed, you can click on (highlight) the item with your mouse and click the Properties button to verify or set up the method being used for TCP/IP addressing.
3. Run a Command (DOS) prompt on the workstation and perform **ping** tests to verify successful packet transmission first to the workstation's NIC, then to the Gateway (if being used), then to the Device's NIC. To run Ping Tests, at the Command (DOS) prompt, type: ping xxx.xxx.xxx.xxx and press ENTER. Note that there is a space between the word "ping" and the first xxx. Let xxx.xxx.xxx.xxx first represent the workstation's IP address, then the IP address of the default gateway, and finally the IP address of the Device. If successful, you will receive a reply such as: "Reply from xxx.xxx.xxx.xxx: bytes=32 time<10ms TTL=128." If you receive "Time Out" or "0 bytes received" notifications, the device being pinged is incorrectly configured or malfunctioning.

4. If Web browser and Ping Tests are successful but you are still unable to print to the Device, verify that the driver is using an IPP Port to print through. From the Windows desktop, select **Start, Settings, Printers** (Start/Printers and Faxes in XP), right click on the Printer's icon, and select **Properties**. Select the Ports Tab and verify that the IPP Port being printed through matches the IP Address, or fully qualified Domain Name, of the Printer. If the IP address (or fully qualified Domain Name) does NOT match, you are printing to the wrong device on the network. Either select the correct port from the displayed list, or use the **Add Port** button to create a new IPP port with an IP Address (or fully qualified Domain Name) matching that of your Device.

*Note: A fully qualified Domain Name consists of the Device's internet Host Name, followed by its internet domain name, separated by periods.*

5. Note that access to this Device's Services can be restricted by Host IP addresses. As this feature could cause communications to appear to fail in certain instances, see the **IP Filtering** procedure in the NOS Selection section of this guide for further details.
6. To assure successful printing, make sure that the Device is configured to support the Page Description Language (PDL) being used by your driver. To check the PDL being used by the driver, print a test job "to file." Open and view the job in a program such as Notepad. The PDL being used by the driver will be displayed in the first few lines of Printer Language. Next, check the Page Description Languages being supported by the Device's ports by following the instructions supplied under the **Setting PDL Emulations** procedure in the Internet Services section of this guide. The PDL being used by the driver, and the PDL supported by the Port you are printing to, **MUST** match for successful printing to occur.

# EtherTalk Troubleshooting

Use the following check list to troubleshoot your network communication problem.

## Check Physical Media and Network Interface Cards

1. Verify that the Device is powered ON.
2. Verify that the Device and Workstation are using the correct cabling to communicate over the network. Use category 3 UTP patch (NOT crossover) cable for 10 Base T communications, category 5 UTP patch (NOT crossover) cable for 10 Base T / 100 Base TX communications, and Token Ring cabling for Token Ring networks.
3. Verify that the cable at both the Device and Workstation is fully plugged into the Network Interface Card (NIC). Check the link light, which is typically a green LED, to make sure that it is lit. Typically, but not always, a second light on the Network Interface Card will be intermittently flashing, indicating the presence of network traffic. If neither of these lights is lit, there is a problem with the NIC.

## Print a Configuration Report at the Device and perform these tasks:

1. Under the **Ethernet Rated Speed** data label on the Report, verify that your communications speed is correctly set for your network and that you have a MAC address listed. The driver for your NIC works at the Media Access Control (MAC) layer of the protocol stack. If no MAC address is shown, you have either a bad NIC or no NIC at all. Replace or install the Network Interface Card.
2. Under the **CentreWare Internet Services** data label, verify that this feature is Enabled. If it is NOT, enable it following the instructions supplied in the **Network Connectivity** section of this guide.
3. Under the **EtherTalk** data label, verify that the Port is enabled, and that Device has been assigned an EtherTalk Printer Name and an EtherTalk zone. If one or more of these parameters needs to be configured, follow the instructions supplied in the **EtherTalk (AppleTalk) Configuration** topic of the NOS Selection section of this guide.
4. Under the **EtherTalk** data label and at the bottom of the Configuration Report, verify that **PostScript** is installed in the Device. If a PostScript license is installed in the Device, the PostScript logo will be clearly displayed at the bottom of the Report. NOTE: If a PostScript license is NOT installed in the Device, EtherTalk will NOT be displayed on the Configuration Report, and will be unavailable for configuration using Internet Services. Consult your Xerox Representative for assistance.

## At the Macintosh workstation

Verify that the Printer is visible in the **Chooser**. If it is NOT, install the Driver and PPD file as stated in the **EtherTalk (AppleTalk) Peer to Peer Printing** topic of the Print Drivers section of this guide.

# Scanning to Hard Drive Troubleshooting

Use the following check list to troubleshoot your network communication problem.

## Before you start

It is assumed that you purchased the Scanning option to enable Scanning to the Hard Drive with your Device. If you did not, contact your Xerox Representative to purchase this option.

## Check Physical Media and Network Interface Cards

1. Verify that the Device is powered ON.
2. Verify that the Device and Workstation are using the correct cabling to communicate over the network. Use category 3 UTP patch (NOT crossover) cable for 10 Base T communications, category 5 UTP patch (NOT crossover) cable for 10 Base T / 100 Base TX communications, and Token Ring cabling for Token Ring networks.
3. Verify that the cable at both the Device and Workstation is fully plugged into the Network Interface Card (NIC). Check the link light, which is typically a green LED, to make sure that it is lit. Typically, but not always, a second light on the Network Interface Card will be intermittently flashing, indicating the presence of network traffic. If neither of these lights is lit, there is a problem with the NIC.



## Print a Configuration Report at the Device and perform these tasks:

1. Under the **Ethernet Rated Speed** data label on the Report, verify that your communications speed is correctly set for your network and that you have a MAC address listed. The driver for your NIC works at the Media Access Control (MAC) layer of the protocol stack. If no MAC address is shown, you have either a bad NIC or no NIC at all. Replace or install the Network Interface Card.
2. Under the **CentreWare Internet Services** data label, verify that this feature is enabled. If it is NOT, enable it following the instructions supplied in the **Network Connectivity** section of this guide.
3. Under the **TCP/IP** data label, determine the method being used to assign TCP/IP addressing to the Device. Verify that the IP Address, Subnet Mask, and Gateway addresses are correct for your network and have NOT changed from their previous settings. Note: The use of DHCP (the DHCP Server) with a short "lease" time can cause the Device to be assigned a new IP Address when it is powered off for an extended period of time. This will interrupt communications with workstations using the "old" IP address. If you do not want the IP address to be subject to constant changes, either increase the lease time at the DHCP Server, or use the Static IP Addressing method as described in the **TCP/IP Protocol Configuration** procedure in the NOS selection section of this guide.

### At the Device

1. Verify that you have correctly set up your Mailbox as stated in the **Setting Up Mailboxes** section of the **Scanning to the Device's Hard Drive (Mailboxes)** topic, in the Options section of this guide.
2. Scan a test document to your Mailbox as stated in the **Scanning to Mailboxes** section of the **Scanning to the Device's Hard Drive (Mailboxes)** topic, in the Options section of this guide.

## At the Workstation

1. Open your Web browser and enter the TCP/IP address of the Device in the Address or Location field. Press ENTER. If the Device's Internet Services (web pages) begin to display on the workstation, you are communicating with the Device. If NOT, make sure that your web browser is not set to use a proxy server and repeat the procedure. If unsuccessful, perform the next step.
2. Verify that the workstation has been assigned an IP address, subnet mask, and gateway address by running a Command (DOS) prompt, typing **ipconfig/all** (Windows 2000/XP) and pressing ENTER. If any of the addresses are incorrect or missing, right mouse click on the Network Neighborhood icon (My Network Places in Windows 2000) and make sure that the **TCP/IP protocol** is installed and properly configured for IP addressing.
3. Run a Command (DOS) prompt on the workstation and perform **ping** tests to verify successful packet transmission first to the workstation's NIC, then to the Gateway (if being used), then to the Device's NIC. To run Ping Tests, at the Command (DOS) prompt, type: ping xxx.xxx.xxx.xxx and press ENTER. Note that there is a space between the word "ping" and the first xxx. Let xxx.xxx.xxx.xxx first represent the workstation's IP address, then the IP address of the default gateway, and finally the IP address of the Device. If successful, you will receive a reply such as: "Reply from xxx.xxx.xxx.xxx: bytes=32 time<10ms TTL=128." If you receive "Time Out" or "0 bytes received" notifications, the device being pinged is incorrectly configured or malfunctioning.
4. When Internet Services are successfully displayed on your monitor, retrieve your scanned test document as stated in the **Retrieving Images from Mailboxes** section of the **Scanning to the Device's Hard Drive (Mailboxes)** topic, in the Options section of this guide.

Published by:

Xerox Corporation

GKLS East Coast Operations

800 Phillips Road, Building 0845-17S

Webster, New York

14580-9791

United States of America

Translated by:

Xerox

GKLS European Operations

Bessemer Road

Welwyn Garden City

Hertfordshire

AL7 1BU

UK

Copyright 2007 by Xerox.

All rights reserved.

