Version 2.0
December 2010

Xerox® WorkCentre™ 5735/5740/5745/5755/5765/5775/5790 System Administrator Guide

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Document version 2.0: December 2010

Table of Contents

1 Introduction

2 Device Connection and Quick Setup

3 General Setup

22 Network Accounting

23 Xerox Secure Access

24 Software Upgrade

25 USB Printer Port

26 Troubleshooting

Index

1 Introduction

This guide has been created for System Administrators who need to install, set up and manage printers and other services on their network.

To use the procedures in this Guide effectively, System Administrators must have previous experience working in a network environment and must possess Supervisor, Administrator, Account Operator, or equivalent rights to the network. They must also have prior knowledge of how to create and manage network user accounts.

Xerox WorkCentre Series

Your device is not simply a conventional copier, it is a digital device capable of copying, faxing, printing and scanning, dependent on your model and configuration.

There are two configurations available:

- **WorkCentre Copier/Printer** - a multi-functional digital device capable of copying, printing, faxing (optional), e-mailing and network scanning (optional).
- **WorkCentre Copier/Printer/Scanner** - an advanced multi-functional device offering a high specification of features and functions. This model is capable of copying, printing, scanning, e-mailing and faxing (optional).

Each model has seven configurations available which provide either 35, 40, 45, 55, 65, 75, or 90 copies/prints a minute. All configurations are fully upgradeable so as to meet any future requirements you may have.

The following are supplied as standard:

- **Document Feeder**
- **Paper Trays 1 and 2** - fully adjustable and can be used for media sizes 5.5x8.5” to 11x17” (A5 to A3).
- **Paper Trays 3 and 4** - are high capacity paper trays used for media size 8.5x11” (A4).
- **Bypass Tray** - used for non-standard printing media.

The following are optional hardware, which are available for your device:

- **Tray 5** - a high capacity paper tray used for media size 8.5x11” (A4). Optional kits are available to accommodate 11x17” or 8.5x11” (A3 or A4) short edge feed media.
- **Tray 6 (Inserter)** - a paper tray for use with the High Volume Finisher. It is used to insert pre-printed sheets into copy sets.
- **High Volume Finisher (HVF)** - a finisher which can collate, offset, stack and staple your output. Booklet Maker, Trifold, Hole Punch and Post Process Inserter (PPI) kits can be installed with this finisher.
- **Booklet Maker and Trifolder** - these are devices which can be installed with HVF to staple and fold booklets or leaflets.
- **Convenience Stapler** - this provides manual stapling of up to 50 sheets. The Convenience Shelf must also be fitted.
- **Offset Catch Tray** - this delivers output collated or uncollated, each set or stack will be offset from the previous to enable easy separation.
- **Basic Office Finisher** - this device stacks, collates, staples and offsets your output.
- **Office Finisher** - this device stacks, collates, staples and offsets your output. Hole punch kits are also available for this finisher.

Related Information Sources

Information available for this product series consists of:

- The *System Administrator Guide* (this guide)
- The *User guides*
- The Xerox website http://www.xerox.com

Customer Support

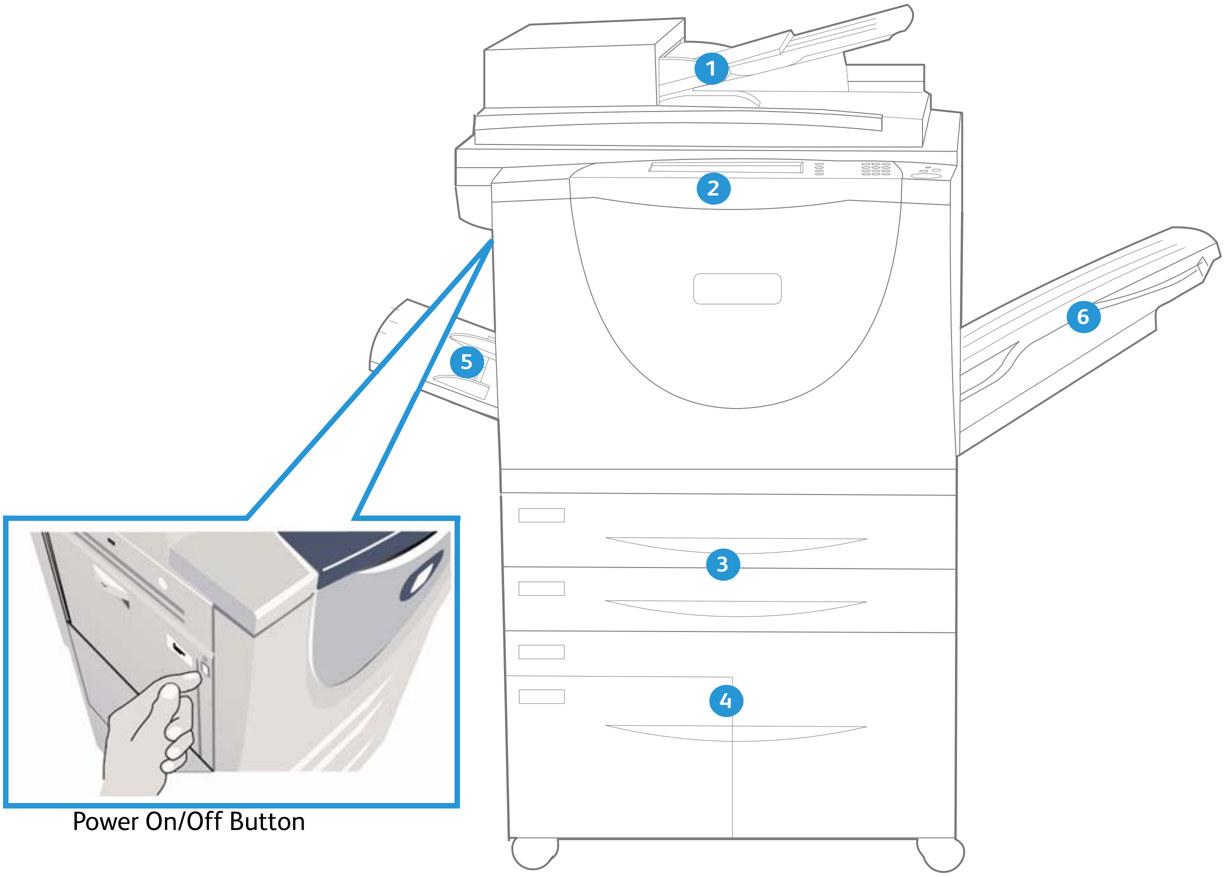
If you need assistance during or after product installation, please visit the Xerox website for online solutions and support, http://www.xerox.com

Device Connection and Quick Setup

2

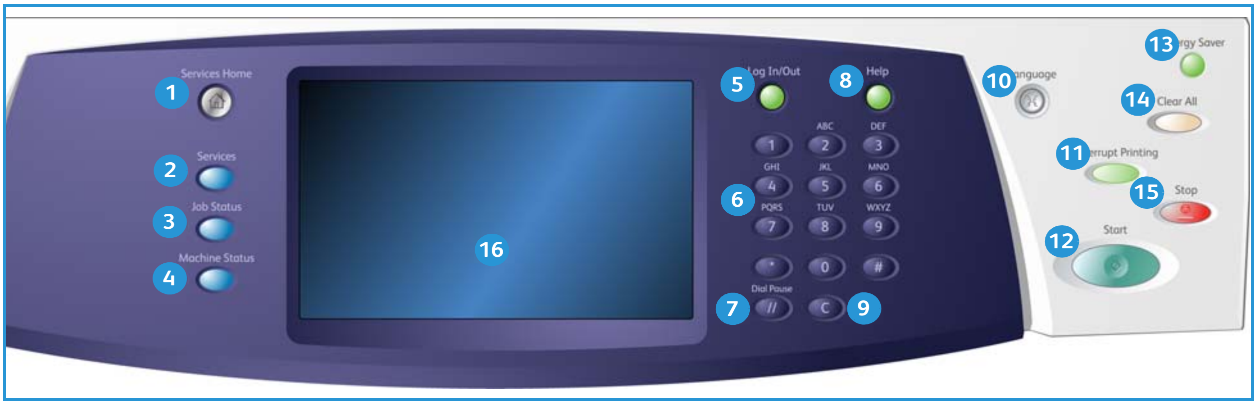
This chapter describes how to connect your device to a network and configure Ethernet settings.

Front View



1. **Document Feeder and Document Glass**: Used for scanning single or multiple documents. The *document glass* can be used for scanning single, bound, custom size or damaged documents.
2. **Control Panel:** Touch Screen and Numeric Keypad.
3. **Paper Trays 1 and 2:** These trays are standard on all models. Trays 1 and 2 are fully adjustable and can be used for media sizes 5.5x8.5” to 11x17”(A5 to A3).
4. **Paper Trays 3 and 4:** These trays are high capacity paper trays. Trays 3 and 4 are dedicated trays used for 8.5x11” or A4 size media.
5. **Bypass Tray:** Used for non-standard printing media.
6. **Offset Catch Tray:** Delivers output collated or uncollated. Each set or stack will be offset from the previous to allow easy separation.

Device Control Panel Overview



1 **Services Home** Provides access to the services available on the device.

2 **Services** Returns the display to the previous copy, fax, or scan feature screen when the **Job Status** screen or **Machine Status** screen is selected.

3 **Job Status** Use to check the progress of active jobs, or display the detailed information of completed jobs.

4 **Machine Status** Use to check the device status, the billing meter, and the status of consumables, or print various reports. Use this button also when accessing the System Administrator mode.

5 **Log In/Out** Provides access to device setups for the Administrators.

6 **Numeric Keypad** Use to enter alphanumeric characters.

7 **Dial Pause** Use to insert a pause when dialing a fax number.

8 **Help** Displays help messages for device features.

9 **‘C’ Cancel Entry** Cancels the previous entry made on the Numeric Keypad.

10 **Languages** Use to select the required language.

11 **Interrupt Printing** Interrupts the current job to run a more urgent job.

12 **Start** Use to start a job.

13 **Energy Saver** Use to select energy saver mode or perform a quick restart.

14 **Clear All** Press once to clear a current entry. Press twice to return to default settings.

15 **Stop** Stops the job in progress.

16 **Display and Touchscreen** Device display and touchscreen.

Initial Connection

Follow these steps to physically connect your device to the network.

1. Connect the Power Cable
   Ensure the device is connected to a suitable power supply and that the power cord is fully plugged in to the electrical outlet.
2. Connect the Ethernet Cable
   Connect a 10/100/1000 BaseT Ethernet cable to the Ethernet port at the rear of the device and the other end of the cable to your network port.
3. Power On the Device
   The Power On button is located on the left-side of the device.

Power Management

Power On/Off Button and Energy Saver Button

The **Power On/Off** button (located on the left hand side of the device) and the **Energy Saver** button (located on the control panel on the top right) control the application of standby operating power to each of the system modules and initiates the sequences required to bring the device to an operational state. If the **Power On/Off** button is pressed when the device is operational, the following can be initiated:

- **Energy Saver** - ends the current session and keeps the device running on low power. When in Energy Saver Mode, press any key or touch the screen to wake the device up.
- **Quick Restart** - the system powers down followed by an automatically initiated Power On sequence. Any jobs in progress will be lost. Quick Restart may be helpful if experiencing problems with the operation of the device.
- **Power Down** - the system ends the current session and powers itself off in an orderly manner.

Power On

At the Device:

1. Ensure that your device is connected to a suitable power supply and that the power cord is fully plugged in to the electrical outlet of the device.
2. Press the **<Power On/Off>** button. The entire powering on process (to power on all installed options) takes less than three minutes.

Power Down

At the Device:

1. Press the **<Power On/Off>** button, the **Power Down Options** screen displays.
2. Touch **[Power Down]**.
3. The **Power Down Confirmation** screen displays.

   Note: If the are any jobs in the queue, confirming power down will result in the deletion of any currently in the queue.

4. Touch **[Confirm]** to confirm the selection.
   The device will begin a controlled power down sequence. It remains on for approximately 45 seconds before switching off.

Energy Saver Options

The device is designed to be energy efficient and automatically reduces its power consumption after periods of inactivity. The System Administrator can set up Energy Saver options. For details, refer to Energy Saver on page 47.

At the Device:

1. Press the **<Energy Saver>** button on the control panel. The **Power Down Options** screen displays.
2. Touch **[Energy Saver]**. The device will immediately enter **Low Power Mode**.
3. To re-activate the device when in this mode, touch a button on the control panel or touch screen.

Quick Restart

At the Device:

1. Press the **<Energy Saver>** button on the control panel. The **Power Down Options** screen displays.
2. Touch **[Quick Restart]**.
3. The **Power Down Confirmation** screen displays.

   Note: Any jobs in progress will be lost.

4. Touch **[Confirm]** to confirm the selection. The device will restart.

Installation Wizard

If this is the first time the device has been powered on, the **Installation Wizard** will run. If this screen does not appear, proceed to Configure Network Connectivity Protocols with Internet Services on page 25.
The install wizard will prompt you with questions to help with the configuring of your device.

1. When the device is powered on the **Language Selection** screen displays, select the preferred language and touch **[OK]** to begin.
2. The **Welcome** screen displays, this will guide you through the short series of steps required to setup your device. Touch **[Next]**.
3. The **Activation Code** screen displays, using the on-screen keyboard enter the Activation Code supplied with the device. Touch **[Next]**.
4. The **Customer Support Telephone Numbers** screen displays, verify that the **Customer Support Telephone Number** and **Supplies Telephone Number** are correct. If either number are incorrect or missing, touch the appropriate type-in region and enter the correct number using the keypad. Touch **[Next]**.
5. The **Date Settings** screen displays, select one of the following for **Date Format**:
   - **MM/DD/YY** (default)
   - **DD/MM/YY**
   - **YY/MM/DD**

   a. Using the **left** and **right** arrow buttons select the required date settings for **Month**, **Day** and **Year**.
   b. Touch **[Next]**.

6. The **Time Settings** screen displays;
   a. For **Time Format**, select either **[12 Hour Format]** or **[24 Hour Format]**.
   b. Touch the type-in region for **[Hours]** and **[Minutes]** and enter the current hour and minute.
   c. Touch either **[AM]** or **[PM]** if a 12 Hour format was chosen earlier.
   d. Touch **[Next]**.
7. The **Time zone** tab displays, use the drop-down menu to select the correct time zone for your device locale. Touch **[Next]**.
8. The **Setup Complete** screen displays, touch **[Finish]** to restart the device for the changes to take effect.

Print a Configuration Report

A Configuration Report is a summary report of the system data for example, device configuration, serial number, software version and network data.

A Configuration Report will automatically print when the device is powered off, then on, during Power Cable and Ethernet Cable installation. The Configuration Report will list the device settings. If necessary, perform the following steps:

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

If you want to disable automatic printing of a Configuration Report at Startup, refer to To Prevent the Configuration Report to Print at Power On on page 30.

Access Tools Pathway as a System Administrator

Your device is designed to enable the device and customize feature default settings to meet your requirements. Most of the features will require you to access the Tools pathway. The Tools pathway will require you to log in to the device as the Key Operator or System Administrator.

Administrator access is required to change settings for:

- **Device Settings**
- **Service Settings**
- **Network Settings**
- **Accounting Settings**
- **Security Settings**
- **Troubleshooting**

To access the Tools pathway, you must log in as a System Administrator as follows:

1. At the device, press the **<Log In/Out>** button on the Control Panel.
2. The **Authentication Login Required** screen displays. Touch **[Keyboard]**.
3. The **Authenticated Required - Step 1 of 2** screen displays, enter the Administrator's username **[admin]** using the on-screen keyboard, touch **[Next]**.
4. The **Authenticated Required - Step 2 of 2** screen displays, enter the Administrator's password **[1111]** using the on-screen keyboard, touch **[Done]**.
5. Press the **<Machine Status>** button.
6. The **Pathway Options** screen display, touch the **[Tools]** tab for Tools pathway.

Ethernet Configuration

Ethernet Port

The Ethernet Interface is set to auto-detect the speed of your network. The device supports the following selectable speeds:

- **Auto**
- **10Mbps Half-Duplex**
- **10Mbps Full-Duplex**
- **100 Mbps Half-Duplex**
- **100 Mbps Full-Duplex**
- **1000 Mbps (1 Gbps) Half-Duplex**
- **1000 Mbps (1 Gbps) Full-Duplex**

Note: If your network has hubs that have Auto-Sensing enabled and the device Ethernet speed is set to Auto, it is possible that the hub will not arbitrate to the correct speed.

Setting the Ethernet Speed at the Device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Ethernet Physical Media]**.
3. Select the required **Ethernet Physical Media** speed to match the speed set on your hub or switch.
4. Touch **[Save]**.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools Pathway.

Enable TCP/IP and HTTP at the Device

Look at the Configuration Report, verify whether the addressing shown under TCP/IP Settings will enable this device to communicate over your network. Also, verify that HTTP is enabled under HTTP

Settings, to enable the use of the device web user interface for network and options configuration. If necessary, reset TCP/IP Addressing (including DHCP and DNS settings) and enable HTTP as follows:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch the **[Network Setup]** button,
3. Touch **[TCP IP]**.
4. From the **TCP/IP** screen, touch **[HTTP/IPP Enablement]**.
   a. For **Protocol** touch **[Enable]**.
   b. Touch **[Save]**, to return to the TCP/IP screen.
5. Touch **[TCP/IP Settings]**.
6. Configure TCP/IP settings, including DHCP (Dynamic Addressing) and DNS, touch **[Save]**, touch the **[Close]** button to return to the Network Setting screen.

   Note: This device supports IPv6 Addressing, with an automatically-built Link Local Address for broadcasting to routers that can supply the network-layer configuration parameters. See Configure Network Connectivity Protocols with Internet Services on page 25.

Quick Setup

When your device is configured with an IP Address and HTTP is enabled, you can configure network information from your web browser via Internet Services. Enter the IP Address of the device in your web browser to access Internet Services. For further information, refer to Internet Services on page 21.

Internet Services

Internet Services is the embedded HTTP server application that resides in the device. Internet Services allows Administrators to change network and system settings on the device from the convenience of their desktops.

Many of the features available within Internet Services will require an Administrator User Name and Password. The default User Name is **admin** and the default Password is **1111**. A user will only be prompted for an Administrator's User Name and Password once in a single browser session.

System Configuration

To use Internet Services, you need to enable both TCP/IP and HTTP on the device. See To Add or Change a Static IP Address when there is no DHCP Server Available on page 21.

How to Verify the IP Address

The device is configured by default to request an IP Address from a DHCP server. If your DHCP server provides a valid IP Address you will not need to configure the device with an IP Address. HTTP is also enabled by default. Print a Configuration Report to verify the IP Address.

To print a Configuration Report on demand, refer to Print a Configuration Report on page 18.

To Add or Change a Static IP Address when there is no DHCP Server Available

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[Dynamic Addressing]**.
   a. Touch **[Disable]** to disable DHCP, and touch **[Save]** to return to the **TCP/IP Settings** screen.
6. Touch **[IP Address/Host Name]**, the **IP Address/Host Name** screen displays.
   a. Touch **[IPv4 Address]** and enter the IPv4 Address using the numerical keypad.
   b. Touch **[Save]** to return to the **IP Address/Host Name** screen.
   c. Touch **[Host Name]**
   d. Touch **[Clear Text]** and enter the Host Name using the on-screen keyboard.
   e. Touch **[Save]** to return to the **IP Address/Host Name** screen.
   f. Touch **[Close]** to return to the **TCP/IP Settings** screen.
7. Touch **[Subnet and Gateway]**.
   a. Touch **[IP Gateway]**, and enter a valid IP gateway address using the numerical keypad.
   b. Touch **[Save]** to return to the **Subnet and Gateway** screen.

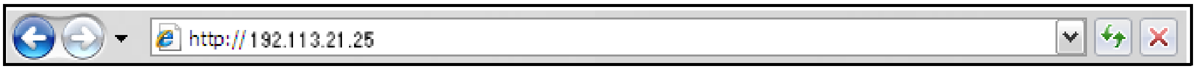
   c. Touch **[Subnet Mask]**, and enter a valid subnet mask address using the numerical keypad.
   d. Touch **[Save]** to return to the **Subnet and Gateway** screen.
   e. Touch **[Close]** to return to the **TCP/IP Settings** screen.

8. Touch **[TCP/IP Enablement]**.
9. For **IPv4**, touch **[Enable]**.
10. Touch **[Save]**.
11. Touch **[Close]**.
12. Press the **<Log In/Out>** button.
13. Touch **[Logout]** to exit the Tools pathway.

To Access Internet Services

To view the **Internet Services Welcome** screen:

1. Enter the device IP Address in the web browser.
2. Press **<Enter>** or click on the **[Go]** button. For example:



http://192.113.21.25

The Internet Services Welcome Page

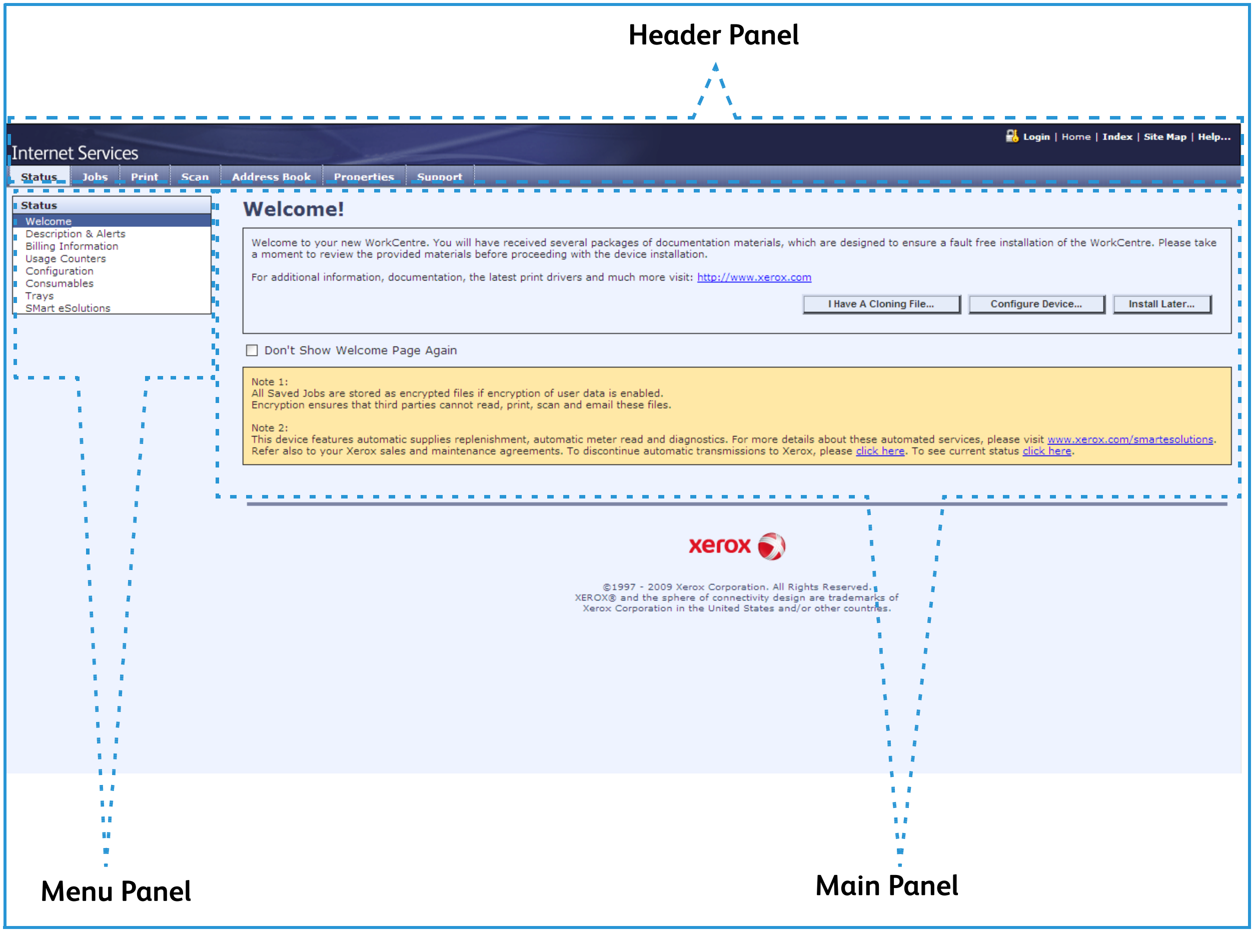
A **Welcome** page is enabled as the opening page of the device's Internet Services web pages. You can click on **[Configure Device]** on the Welcome page, or click on the **[Configuration Overview]** link on the **Properties** tab, to go directly to the Install Wizards for configuring protocols and optional services.

The **[I Have a Cloning File...]** button on the **Welcome** page lets you copy configuration settings from a compatible Xerox system and apply them to this system.

To stop displaying the **Welcome** page, check the **[Don't Show Welcome Page Again]** checkbox.

To access the **Welcome** page or **Properties** tab of Internet Services, TCP/IP and HTTP must be enabled on the device as described in the Introduction on page 9 of this guide.

The **Welcome** screen displays.



Welcome!

Welcome to your new WorkCentre. You will have received several packages of documentation materials, which are designed to ensure a fault free installation of the WorkCentre. Please take a moment to review the provided materials before proceeding with the device installation.

For additional information, documentation, the latest print drivers and much more visit: http://www.xerox.com

☐ Don't Show Welcome Page Again

Note 1:
All Saved Jobs are stored as encrypted files if encryption of user data is enabled.
Encryption ensures that third parties cannot read, print, scan and email these files.

Note 2:
This device features automatic supplies replenishment, automatic meter read and diagnostics. For more details about these automated services, please visit www.xerox.com/smartesolutions.
Refer also to your Xerox sales and maintenance agreements. To discontinue automatic transmissions to Xerox, please click here. To see current status click here.

©1997 - 2009 Xerox Corporation. All Rights Reserved.
XEROX® and the sphere of connectivity design are trademarks of
Xerox Corporation in the United States and/or other countries.

The **Internet Services** home page contains three panels without visible boundaries.

- **Header Panel:** displays the header for all pages. The header includes the Internet Services logo and model of the device. The header for the WorkCentre series also includes a user mode icon, and the name or type of a logged-in user. Below this panel on most pages is the tab bar which corresponds to the seven functions or tabs. These are **Status**, **Jobs**, **Print**, **Scan**, **Address Book**, **Properties**, and **Support**. You can navigate through the pages when you click on the text on each tab.
- **Menu Panel:** Displays a navigation tree, listing the items available within each category, with the currently displayed item highlighted.
- **Main Panel:** Displays information and settings for an item selected on the Menu Panel.

When you open Internet Services, a **Welcome** screen is displayed. If you click on the **[Configure Device...]** button, a **Configuration Overview** screen opens which provides links to the printing protocols and services that you can configure on the device.

If you click on the **[I have a Cloning File...]** button, you can copy settings from one device and transfer them to another device with the same version of system software.

Access Internet Services as System Administrator

Many settings can be configured and setup using the Internet Services. By default the **Properties** tab and many features are locked, you will need to log in as a System Administrator.

1. At your Workstation, open the web browser, enter the IP Address of the device in the Address bar.
2. Press **<Enter>**.
3. Click on the **[Properties]** tab.
4. If prompted, enter the System Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.

Login in as a System Administrator

1. At your Workstation, open the web browser, enter the IP Address of the device in the Address bar.
2. Press **<Enter>**.
3. Click on the **[Login]** link at the top right of the page.
4. In the **Login** area, enter the System Administrator details in the **[User ID]** and **[Password]** field. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.

Changing the System Administrator Password

Xerox recommends that you change the default System Administrator password after you configure the device for security reasons.

To change the System Administrator password:

At Your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[User Information Database]** link and select **[Setup]** in the directory tree.
3. In the user list, click on the [Edit...] button on the **Admin** user row. The **Edit User** page is displayed.
4. In the **User Identification** area:
   a. Enter the new password in the **[Password]** field.
   b. Retype the password in the **[Retype Password]** field and click **[Edit User]**, the **Security Confirmation** page is displayed.
   c. Enter the previous admin password and click **[Save].**

   Note: The **User Name 'Admin'** is not editable and is reserved for the Device Administrator Account.

   Note: Do not forget the password, or you could be locked out of the system requiring a service call. Be sure to keep it in a secure location.

To Setup HTTP

The Internet Services HTTP screen allows the System Administrator to specify the Keep Alive Timeout, Maximum Connections, Port Number and Secure HTTP (SSL) settings.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[HTTP]** in the directory tree.
4. In the **Configuration** area:
   a. For **Connection**, select **[Enabled]** to enable the protocol.
   b. For **Secure HTTP (SSL)**, select **[Enabled]** to set the HTTP Security Mode.
   c. Change the **Port Number** if required. The default is 443.
   d. The **[Keep Alive Timeout]** setting determines how long the device's Internet Services pages will wait for a response from a connected user before terminating the connection. Enter the required number of seconds (1 - 60) in the **[Keep Alive Timeout]** field.

   Note: Generally, user connections will be adversely affected (slow or kept busy) if the Keep Alive Timeout is set for a long period of time.

   Physical Connection will display the current physical connection in use.

   The **[Maximum Connections]** setting is the maximum number of simultaneous connections that can occur at any given moment to Internet Services. Enter a number from 8 - 32 to indicate the maximum number of clients that can be connected (for example, with open sockets) to the HTTP server at any one time in the **[Maximum Connections]** field.

   Note: In order for the device to operate in Secure HTTP (or HTTPS/SSL) mode, the device must possess a correctly configured Machine Digital Certificate. For information on Machine Digital Certificate, refer to Security Certificate Management on page 179.

   e. Click on the **[Apply]** button to accept the changes.

Configure Network Connectivity Protocols with Internet Services

Internet Services is a series of web pages, hosted on the embedded HTTP server of the device, allowing configuration of services and settings using a web browser.

Refer to Network Installation on page 69, of this guide and follow the instructions to configure protocols.

To configure individual protocols only, using your web browser, from the **Properties** tab perform the following steps:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.

2. Click on the **[Protocols]** link.

   Note: To see IPv6 Addressing parameters, if desired, click **[IP (Internet Protocol)]** in the list of Protocols, then click on **[IPv6]** tab.

3. Select your individual protocol of interest from the displayed list and modify settings to your requirements. For further information refer to Network Installation on page 69.

Set a Description for the Device

The **Internet Services Properties Description** page contains information that identifies a specific device model, name and physical location.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, select **[Description]** in the directory tree.
2. In the **Identification** area:
   a. Type a name of your choice for the device in the **[Device Name]** field.
   b. Type the site location for the device in the **[Location]** field.
   c. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.

To Enable Services

Services are pre-installed on the device, and must be enabled from the **Optional Services** screen within the device **Tools** pathway.

The Optional Services are:

- ID Card Copy
- Workflow Scanning
- E-mail
- Internet Fax
- Image Overwrite Security
- Network Accounting
- Color Scanner Enablement
- Immediate Image Overwrite
- Server Fax
- Embedded Fax
- Save Job For Reprint
- Searchable File Formats
- Smart Card

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Use the **Up** and **Down** scroll button and touch **[Optional Services]**.

   Note: If you do not see the required service, you may need to install additional hardware on your device.

3. Touch the required service you wish to enable.
4. Touch **[Enable]**.
5. Touch the **[Save]** button.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools Pathway.

The service should now be available from the **All Services** area of the device user interface screen.

To View the Service Status on the Internet Services

To view the service status on the Internet Services.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Configuration]** in the directory tree.
3. Scroll to the **Installed Options** area.
   All the installed options on the device will be listed displaying if the options are enabled or disabled, installed or not installed.

To Install Print Drivers

Refer to Print Drivers on page 141 of this guide and follow the instructions provided.

Configure Services

If you have installed one or more optional service on your device you can configure the service from Internet Services.

If you need more specific information about services and how to configure them, refer to the following chapters for each service:

- Workflow Scanning on page 201.
- Scan to Home on page 239.
- Scan to Mailbox on page 227.
- E-mail on page 243.
- Internet Fax on page 261.
- Embedded Fax on page 271.
- Server Fax on page 289.
- LAN Fax on page 299.
- Reprint Saved Jobs on page 305.
- Network Accounting on page 325.

General Setup 3

Administrator Tools Password

The Administrator password is required to access the administrator tools function both from the device touch screen and Internet Services. Access to the administrator tools is necessary to configure the device, network connectivity and optional settings.

> Note: Certain areas on the web user interface (Internet Services) are protected by the Administrator password, this will require you to log in with the User ID and Password (the default is **admin** and **1111**) BEFORE modifying any settings. After working with settings, make sure to log out by clicking on **[admin-Logout]** in the upper-right corner of the Internet Services screen, then click on the **[Logout]** button.

We recommend that you change the Administrator password immediately after device installation. A password of at least nine characters in length should be sufficient. When changed, ensure the password is kept in a secure place for future use.

Configuration Page

The Configuration page allows you to view device setup details, for example Network Setup and Workflow Scanning Setup.

> Note: These details can also be printed by clicking on the **[Print Configuration Page]** button.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Configuration]** in the directory tree.
4. To view information about a setting select the required configuration setting from the list.
5. To print the Configuration details, click on the **[Print Configuration Page]** button.

Configuration Report

> Note: The following instructions are assuming that printing a Configuration Report is open to all users.

The Configuration Report details the device software versions and network settings configured for the device. The Configuration Report automatically prints when the device is rebooted or switched on. You can print a Configuration Report by following the instructions below.

At the Device:

1. Press the **<Machine Status>** button on the device.

2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

To Prevent the Configuration Report to Print at Power On

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From **Tools** pathway, touch **[Device Settings]**.
2. Scroll down by touching the scroll-down button, touch **[Configuration Report]**.
   a. The **Configuration Report** screen displays, for **At Power On**, touch the **[Do Not Print Report]** button.
   b. Touch **[Save]**.
3. Press the **<Log In/Out>** button.
4. Touch **[Logout]** to exit the Tools pathway.

Configure Print Protocols

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. At the welcome page, click on the **[Configure Device]** button.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. If you want to use the checklist, click on the **[View Checklist]** button and click on the **[Print]** button. Scroll to the bottom of the screen and click on the **[Close]** button.
6. Click on the **[Settings]** button next to **Print Protocols**.
7. Click on the **[Configure]** button next to **General Settings** to configure general print settings.
8. In the **General** area:
   a. For **Device Start-Up Page**, check the **[Enabled]** checkbox to enable a start-up page to print at device start-up.
   b. Enter the time to pass, in minutes, for the device to timeout in the **[Timeout]** field. The range is 0-7200, the default is 30 minutes.
9. In the **Banner Sheet** area:
   a. For **Use Generic User Name and Job Name**, check the **[Enabled]** checkbox, to print the generic user and job names on the banner sheet for the print jobs instead of the names submitted with the jobs.
   b. For **Banner Sheets**, check the **[Enabled]** checkbox to allow a banner sheet to print with every print job.
   c. For **Allow Print Driver to Override**, check the **[Enabled]** checkbox to allow the Print Driver to override the banner sheet option.
10. In the **Defaults** area, select the required settings for the following options:

- **Copies** - allows you to set the default number of copies output by the device, the range is 1-9999.
- **Job Type** - allows you to select the default job type.
- **Paper Size** - allows you to specify the default paper size from the drop-down menu.
- **Paper Color** - allows you to specify the default paper color from the drop-down menu.
- **2 Sided Printing** - allows you to select either 1-Sided Print, 2-Sided Print or 2-Sided Print Flip on short edge.
- **Collate** - allows you to enable or disable the collation.

11. Click on the **[Save]** button to return to the **Print Protocols** screen.
12. Click on the **[Configure]** button next to the **IP (Internet Protocol)**, to allow the device to support your network environment.
13. Enter the information for your chosen protocol. If you need more information on how to configure protocol information refer to Network Installation on page 69.
14. Click on the **[Save]** button.
15. You have finished configuring the protocol information, click on the **[Close]** button.
16. To print to the device, install the Print Drivers on your workstation. If you need more information refer to Print Drivers on page 141.

Secure Print

Secure Print requires a user to be authenticated as the owner of a print job using a passcode or by logging in to the machine. Printing will only begin when the secure passcode is entered or when the user logs in at the device. To configure secure print:

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. At the welcome page, click on the **Properties** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **Services** link.
6. Click on the Printing link and click **Secure Print**.
7. For **Method**, select one of the following:
    - **User ID**-The print job will require the user to log in at the device in order to be released for printing.
    - **Passcode** - A passcode, specified when sending the job to the printer, must be entered at the device in order to release the job for printing.
8. For **Secure Print Passcode Length**, enter the minimum required length of the Secure Print Passcode. The range is from 4 - 10 digit.
9. The device can be set to conceal the names of print jobs using asterisks on the local user interface. In the **Conceal Job Names** area, select one of the following:
    - **Conceal Secure Print Job Names Only** - Only secure print jobs will have their names concealed. Non-secure jobs names will be visible.
    - **Conceal All Job Names** - All secure and non-secure jobs will have their names concealed
    - **Show All Job names** - All secure and non-secure print jobs' names will be visible.

Hold All Jobs

The Hold All Jobs functionality allows jobs submitted to the printer to be held in a public or private queue until the user releases the job at the machine. This saves paper by preventing unwanted jobs being printed automatically. Jobs held in a private queue require the user to use their smart card or user login to release jobs for printing.

The Hold All Jobs functionality does not affect system print jobs such as:

- Fax Confirmation Report
- Configuration Sheet
- Email confirmation report
- IFAX confirmation report
- Reprint Saved Jobs
- Information Pages

The Administrator can also decide how to handle jobs that are submitted with no associated user name.

To enable and configure Hold All Jobs:

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. At the welcome page, click on the **Properties** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **Services** link.
6. Click on the **Printing** link and click **Hold All Jobs**.
7. In the **Enablement** area, select one of the following:
   - **Off** - Submitted jobs are printed immediately (unless submitted as a secure job).
   - **Hold Jobs in a Private Queue** - All identified jobs are held in a queue that is only accessible by the user who originated the job. All unidentified print jobs are held in the Unidentified Held Jobs queue.
   - **Hold Jobs in a Public Queue** - All submitted non-secure jobs are held in a public queue and can be released for print by any user. Secure print jobs require the user to be logged in or to enter the passcode to access the folder. All unidentified print jobs are held in the Unidentified Held Jobs queue.
8. The **Unidentified Job Policies** area allows you to configure how the printer manages jobs submitted without a user ID. Select one of the following:
   - **Hold Jobs; All users can manage jobs** - Jobs without a user ID will be held and any user can release them for printing unless they are submitted as a secure print job.
   - **Hold Jobs; Only Administrators can Manage Jobs** - Jobs without a user ID will be held but only Administrators can view them or release them for printing.
   - **Delete Jobs immediately** - All jobs submitted without a user ID will be deleted.
   - **Print Jobs immediately** - Jobs submitted without a user ID will be released immediately for printing unless they are submitted as a secure print job.

Cloning

Cloning allows you to copy the settings and web generated scan templates of one device and transfer them to other devices operating with the same version of system software. Depending on the optional features installed on the device, groups of settings can be cloned. For example, scan settings will be available for cloning only if the Workflow Scanning optional feature is already installed on the source device.

After selecting the settings to be cloned, a configuration cloning file is created and saved with the extension .dlm (downloadable module).

The configuration cloning file can then be submitted to other devices using Internet Services via a web browser. The settings are transferred and applied to the recipient device.

Note: Optional features must be installed on the recipient device in order to accept cloned settings. It is not possible to install an optional feature (for example, Workflow Scanning or E-mail) through the process of cloning.
The cloning feature creates a .dlm file script that can be used to configure other devices. All devices must have the same version of software for the .dlm file to be accepted.

To Verify the Software Version

Note: To verify the software version on the device access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Configuration]** in the directory tree.
3. Scroll down to the **Printer Setup** area and view the system software version.

To Clone a Device

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Cloning]** in the directory tree.
3. In the **Create Clone File** area:
    a. By default all features are selected, click on the **[Clear All]** button, and check the following feature checkboxes to select the features that you wish to clone:

        - Accounting
        - Audit Log
        - E-mail
        - Internationalization
        - SMart eSolutions
        - Print Settings
        - Device Upgrade
        - System Disk
        - Workflow Scanning
        - Web Services
        - Public Address Book
        - Connectivity Settings
        - Internet Fax
        - Security

- Administration
- Authentication & Authorization Configuration
- Fax
- Power Saver
- Templates
- Job Management

b. To select all the features, click on the **[Select All]** button.

c. Click on the **[View feature Details]** link to view the specific parameters that can be cloned for any of the feature.

d. Click on the **[Clone]** button.

4. In the **Cloning Instructions** area:

a. Right-click on the **[“Cloning.dlm”]** link that appears and select **[Save Target As]**.

b. A dialog box will prompt you to specify a name and location for the cloned file. Ensure the extension reads **‘.dlm’**.

c. Click on the **[Save]** button. The .dlm file can now be used to clone other devices.

To Install the Clone File on Another Device

Note: This procedure will cause the device to reboot and will be unavailable over the network for several minutes.

1. Click on the **[Status]** tab.
2. Select **[Welcome]** in the directory tree.
3. Click on the **[I Have A Cloning File]** button.
4. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
5. Click on the **[Login]** button.
6. In the **Install Clone File** area, click on the **[Browse]** button.
7. Locate your file and click on the **[Open]** button.
8. Click on the **[Install]** button.

The device will be unavailable over the network for several minutes. When rebooted a Configuration Report will print, if enabled.

Date and Time

This feature allows the System Administrator to set the Date and Time (including Time Zone for Daylight Saving Time) for the system. It can be set up using NTP, or it can be manually set on the device interface.

Manual Setup at the Device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Device Settings]**.
2. Touch **[General]**.
3. Touch **[Date and Time]**.

4. When the warning dialog appears, touch **[Close]**.

   Note: Any changes to these settings will require the device to reboot.

5. Select **[Date]** tab.
   a. For **Date Format**, select one of the following:
      - **mm/dd/yy**
      - **dd/mm/yy**
      - **yy/mm/dd**
   b. Touch the **Left** and **Right** arrow, select the required value for the following:
      - **Day (dd)** - the range will be dependant on the selected month.
      - **Month (mm)** - the range is from 1 to 12.
      - **Year (yy)** - the range is from 00 to 40.
6. Select the **[Time]** tab.
   a. Select one of the following time format:
      - **AM**
      - **PM**
      - **24 Hour**
   b. Touch the **Left** and **Right** arrow, select the required value for the following:
      - **Hours** - for a 12 hour format the range is 1 to 12 and for a 24 hour format the range is 0 to 23.
      - **Minutes** - the range is 00 to 59.
      - If the 12 hour format is selected, select either **[AM]** or **[PM]** from the drop-down menu.
7. Select the **[Time Zone]** tab.
8. Touch the **Time Zone** drop down menu and select the correct time zone for your device's locale. The machine time is automatically adjusted if daylight savings is in effect in your time zone.
9. Touch **[Reboot]**, the system will reboot.

Using NTP

NTP (Network Time Protocol) is designed to synchronize the clocks of computers over a network. This feature will ensure that the device's internal clock stays synchronized with the NTP server you specify.

Note: If you set up using **NTP**, the date and time of the system can be set using a network time server (NTP). The system will check the server at boot time, every subsequent 24 hours, and any time the NTP parameters are modified.
If the device is configured to use DHCP, and an NTP server, or the GMT offset is provided by the DHCP server, then the data entered here will be overwritten by the corresponding DHCP retrieved items. Enabling NTP or modifying NTP settings will cause a system reset.

At Your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.

3. Select **[NTP]** in the directory tree.
4. In the **Offset of Local Time Zone** area select the time offset (in hours) from the **[Offset of Greenwich Mean Time]** drop-down menu. The default is 0.0.
5. In the **Network Time Protocol** area:
   a. For **NTP Enabled**, check the **[Enabled]** checkbox to enable NTP on the device.
   b. Select one of the following:
      - **IPv4 Address** and enter the **IP Address** and **Port** and the **Backup IP Address** and **Port** details in the required fields. The default port number is 123.
      - **Host Name** and enter the **Host Name** and **Port** and the **Alternate Host Name** and **Port** details in the required fields. The default port number is 123.

   Note: Any changes to these settings will require the device to reboot.
6. Click on the **[Apply]** button, the system will reboot.

Image Settings

The Image Settings screen allows you to set preferences for the various file formats that the device is capable of creating when features such as E-mail and Internet Fax are used at the device.

To Configure Image Settings

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Image Settings]** in the directory tree, the **Image Setting** screen will display.
3. In the **PDF & PDF/A Settings** area:
   a. For **Optimization for Fast Web Viewing**, check the **[Enabled]** checkbox.
   If enabled, this option will create linearized PDF files. Linearized PDF files allow the first page of the 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.
   This option will produce relatively small files with a very short encoding delay per page, however the image detail may appear more grainy when printed.

   Note: Regarding Searchable PDF and PDF/A: If this option is available, by enabling the selection you will provide Workflow Scanning, E-mail, and Internet Fax users with the ability to choose **[Searchable]** as an option for their PDF and PDF/A file formats. 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.

   b. **JBIG2** is a standard algorithm for lossless compression of bi-level images (two color images), specializing in the preservation of thin lines. JBIG2 compression is usually used for text and halftone documents, and is claimed to be able to compress scanned documents up to 10 times smaller than with TIFF G4. A further claim is that it allows scanned manuals, books, check images, and other document types to be viewed and manipulated efficiently over the Internet. This method yields a very small black and white file size with fast viewing performance. This compression format requires Acrobat 5, with PDF version 1.4 or greater. There are two encoding methods for JBIG2, check both of the following checkboxes for optimal compression:

- **Enable Arithmetic Encoding**
- **Enable Huffman Encoding**

Note: Select one option for good compression and improved speed, if neither is selected, there will be no compression or optimal speed.

c. For **Flate Compression**, check the **[Enabled]** checkbox.
Flate Compression is a lossless compression format that combines LZ77 (the first LZW) and adaptive Huffman encoding (RFC 1951). Huffman compression is a lossless algorithm ideal for compressing text. LZ77 works well with files containing lots of repetitive data, such as text and monochrome image (TIFF and GIF) files. When used for PDF documents, Flate compression is applied after JPEG compression. It is also used in place of G3 compression for monochrome PDF images in Photo and Magazine mode.

d. For **MRC Compression**, check the **[Enabled]** checkbox 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.

e. When MRC Compression is enabled, select one of the following **MRC Compression Format** options:

4. XPS is Microsoft's 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. Windows vista uses the XPS format as a document format, a windows spool file format, and a page description language for printers.
In the **XPS Setting (Email Only)** area, for **MRC Compression**, check the **[Enabled]** checkbox.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Accessing Image Settings for Workflow Scanning

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Default Template]** in the directory tree.
4. Scroll to the **Workflow Scanning** area, click on the **[Edit]** button.
5. In the **Workflow Scanning** area:
   a. For **Content Type**, select either the **[Photo & Text]**, **[Photo]** or **[Text]**.
   b. Select **[for OCR]** option for **Scan Presets**.
   c. Click on the **[Apply]** button.
6. Scroll to the **Filing Options** area, click on the **[Edit]** button.
7. Within the **Filing Options** area:
   a. For **File Format**, select either **[TIFF]**, **[mTIFF]**, **[PDF]**, **[PDF/A]** or **[XPS]**.
   b. For **Searchable Options**, select **[Searchable]**.

   c. Click on the **[Apply]** button.

8. Scroll to the **Workflow Scanning Image Settings** area, click on the **[Edit]** button.
9. In the **Searchable XPS PDF & PDF/A Defaults** area:
   a. For **Searchable Options**, select **[Searchable]** and then select one of the following correct languages for your device options:
      - **Use Language Displayed on the Device User Interface**.
      - **Use this Language** - select the language used at the device from the drop-down menu.

   b. Click on the **[Apply]** button.

Accessing Workflow Scanning, E-mail, or Internet Fax Settings

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on either the **[Workflow Scanning]**, **[E-mail]**, or **[Internet Fax]** link.
3. For Workflow Scanning, select **[Default Template]** in the directory tree, then click on the **[Edit]** button within the **Filing Options** area. Select the **[Searchable]** radio button under **Searchable Options**.
4. For E-mail or Internet Fax, select **[Defaults]**, then select the **[Edit]** button within **Filing Options**. Select the **[Searchable]** radio button under **[Searchable Options]** within **Document Format** as the user presented scanning default.
5. When done, click on the **[Apply]** button to save changes or **[Undo]** to remove changes and refresh the page.

Job Management

The System Administrator can use this page to restrict **Job Deletion** features to one of the following:

- **All Users** - this option allows all users to delete any job in the jobs list. No authentication is required when deleting a job.
- **Administrators Only** - this option only allows the System Administrator to delete any job in the jobs list. The System Administrator must provide a username and password when deleting a job.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Job Management]** in the directory tree.
3. For **Job Deletion**, select either **[All Users]** or **[Administrators Only]**.
4. Click on the **[Apply]** button.

Job Operation Rights

The Job Deletion page allows you to set permissions that allow System Administrators or non-administrator users to delete jobs from the device’s active print queue.

> Note: System Administrators can always delete any job, regardless of the setting selected on the **Job Operation Rights** screen.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, select **[Device Settings]**.
2. Touch the **Scroll Down** arrow button, touch **[Job Operation Rights]**.
3. For **Delete Job Rights**, touch one of the following:
   - **All Users** - allows any user to delete any job in the active print queue. No authentication is required when the user clicks on a job in the job list and selects **Delete**.
   - **System Administrators Only** - allows only logged-in users with System Administration privileges to delete jobs from the active queue.
4. Touch **[Save]**.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

Internationalization

Internationalization allows administrators to specify the locale where the device is situated. This is used to determine the type of encoding used by the device to interpret data, such as print jobs.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Internationalization]** in the directory tree.
3. In the **Data Submission Encoding** area, if you want to specify the locale, select the required setting from the **[Selected Locale]** drop-down menu. The device will use the most appropriate type of encoding.
4. If you want to enter specific encoding, select **[Custom]** from the **[Select Locale]** drop-down menu. Select the required encoding priority order using the **Increase Priority** or **Decrease Priority** buttons.
5. Click on the **[Apply]** button to save changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Sleep Mode Settings

Sleep Mode Settings allows the System Administrator to manage network energy saving options.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Sleep Mode Settings]** in the directory tree.
3. The **Sleep Mode Settings** screen displays, in the **Sleep Mode Network Settings** area, check the following checkboxes:

- **Resume Network Controller Briefly to Poll Novell Print Queues During Sleep Mode** - when selected you must specify the interval of time (in seconds) between the polling of the print queues in the **Poll Interval during Sleep Mode** field. The range is 60 - 1200 seconds.
- **Resume Network Controller Briefly to Broadcast Service Advertising Protocol (SAP) During Sleep Mode** - when selected you must specify the interval of time (in seconds) between advertisements of service in the **SAP Interval during Sleep Mode** field. The range is 60 - 65535 seconds.

4. Click on the **[Apply]** button.

Advanced Settings

The Advanced setting page allows you to designate up to four types of broadcast packets that allows the network controller to briefly resume activity and respond when the machine is in sleep mode.

1. From the **Sleep Mode Settings** page, click on the **[Advanced Settings]** button.
2. In the **Packet Priority** area, select a broadcast packet from the Packet Priority list. Use the **[Increase Priority]** and **[Decrease Priority]** buttons to increase or decrease the selected broadcast packet's priority.
   The **Packets that Briefly Resume Network Controller** area displays packet priorities for up to four packet types.
3. Click on the **[Apply]** button.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   Note: When you click on the **[Apply]** button the system processes the Packet Priority list, and applies the four packet types with the highest priorities for which the corresponding protocols are enabled. Packet types associated with disabled protocols are skipped. The lower list then displays the packet types that, when received by the machine in Sleep Mode, will cause the Network Controller to briefly resume activity.
   Enabling the IPv6 ND broadcast filter will only wake the machine from Sleep Mode when the machines IPv6 Link Local address is used.

Custom Services Setup

This feature allows the System Administrator to set up Custom Services on the device. Custom Services allows independent software vendors and partners to develop customized programs accessible directly from the device control panel. Users can enter their authentication login at the device, and access a set of features and options designed specifically for their business need.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network.
- TCP/IP and HTTP protocols must be enabled on the device so that the device's web browser can be accessed.
- Custom Service Registration (HTTP: Web Services) must be configured.

To Enable Custom Services

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Custom Service Setup]** in the directory tree.
3. In the **Setup (Required)** area, ensure HTTP (SSL) and Custom Service Registration have been configured to enable Custom Services. If they have not been enabled, click on the **[Configure]** button, configure the settings and click on the **[Save]** button.
4. In the **Enable Custom Services** area check the following checkboxes:
   - **Export password to Custom Services** - send passwords to Custom Services.
   - **Display Custom Services Selection Button at the local user interface** - displays the Custom Service selection icon in the **Services Home** screen on the device.
5. In the **Browser Settings** area, check the following required checkboxes to enable options for Custom Services:
   - **Enable the Custom Services Browser** - allows the service to be selected at **Services Home** screen at the device.
   - **Verify server certificates** - if this option is enabled, Custom Services will check and require valid server certificates.

   Browser Version displays the current browser version.
6. In the **Proxy Server** area, from the drop-down menu select either **[No Proxy]** or **[Manual Configuration]**.
7. If **Manual Configuration** is selected:
   a. In the **HTTP, HTTPS** area, check the **[Enabled]** checkbox to enable the protocol.
   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter details of the server in the **[IP Address: Port]** or **[Host Name]** field.
   d. Check the **[Use settings for all protocols]** checkbox.
   e. Repeat the above steps **a** to **c** for **HTTPS** if you require secure HTTP.
   f. In the **Bypass Proxy Rules** area, enter the proxy server that can not be bypassed.
8. Click on the **[Apply]** button to save your changes.
9. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

SMart eSolutions Setup

SMart eSolutions allows the device to automatically send data to Xerox to be used for billing (Meter Assistant), toner replenishment (Supplies Assistant) and remote diagnostics (Maintenance Assistant).

SMart eSolutions provides the following features:

- **Meter Assistant™** - submits meter readings to Xerox from network connected devices. This eliminates the need to collect and report meter read information manually.

Meter Assistant provides detailed information including total counts of impressions, collection times and dates. The meter data is recorded in the Xerox meter readings system and is used for the invoicing of equipment on metered service agreements. The automatic collection of the meter readings will ensure quality and reliability of the data used to manage your service agreements.

- **Supplies Assistant™** - manages ink supplies for network connected equipment, and also monitors actual usage.

  Eligible devices will automatically be enabled for Supplies Assistant when the device is registered with Xerox. Supplies Assistant manages supply orders to ensure the right supplies are provided at the right time.
- **Maintenance Assistant™** - submits device performance information for network connected equipment to assist in remotely determining corrective actions required to resolve equipment performance issues.

There are three ways to register the device for SMart eSolutions:

- **Device Direct registration** - this is available as a standard feature on the device and is accessible via the Web UI using CentreWare internet Services (CWIS).
- **SMart eSolutions Windows Client** - this is an optional feature and the Windows Client can be downloaded by visiting: www.xerox.com/smartesolutions.
- **CentreWare Web (CWW)** - this is a device management software application that manages, configures, installs and provides reports for network connected devices. For further information, see www.xerox.com/centrewareweb.

  Note: SMart eSolutions is not available in all countries. Contact your Xerox Representative for further information.

Information Checklist

Before registering the device for Smart eSolutions, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the customer's network.
- If the device direct method is to be enabled, TCP/IP and HTTP protocols must be enabled on the device and setup so that internet access is provided to the device.
- If the Smart eSolutions client or CWW is to be used to enable Smart eSolutions, enable SNMP on the device. Visit www.xerox.com/smartesolutions for further instructions and to download the software.

SMart eSolutions Information

Note: The following instructions will provide the steps required to enable Smart eSolutions via the Device Direct method. To configure this feature access the Properties tab as a System Administrator.

For further details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[SMart eSolutions]** in the directory tree.
3. In the **Enrollment** area, for **SMart eSolution Enrollment** ensure **[Enrolled]** is selected.

4. In the **Communication Setup** area:
   a. For **Daily Transmission Time**, click in the time box and enter the time (hour and minute) of day you want the device to perform its daily communication with Xerox.
   b. For **HTTP Proxy Server**, click on the **[Configure]** or **[Edit]** buttons to configure or update the internet proxy settings.
5. In the **HTTP Proxy Server** area:
   a. Check the **[Enabled]** checkbox to enable the protocol.
   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter the details of the Server address **[IP Address: Port]** or **[Host Name: Port]** field.
   d. Click on the **[Save]** button to return to the **SMart eSolution Setup** page.
   e. Click on the **[Apply]** button, the **SMart eSolutions Enrollment** screen displays.
   f. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   Note: HTTP Proxy Server settings are used for the following features:

   - SMart eSolution Setup
   - HTTP(S) File Destinations
   - HTTP(S) Template Pool

Opting out of SMart eSolutions

If you wish to discontinue participation in the Smart eSolutions services, it is possible to opt out via the devices web UI using CentreWare Internet Services.

1. From the Properties tab, click on the **[General Setup]** link.
2. Select **[SMart eSolutions]** in the directory tree.
3. In the Enrollment area, for SMart eSolution Enrollment ensure **[Not Enrolled]** is selected.

Meter Assistant

Meter Assistant is a feature of SMart eSolutions. It provides detailed information, including dates, times, and counts of impressions sent in the last billing meter transmission.

The meter data is recorded in the Xerox service management system. It is used for the invoicing of metered service agreements, and also for evaluating consumable usage against printer performance. The automatic collection of the meter reads will ensure quality and reliability of the data we use to manage your service agreements.

To Enable Meter E-mail Alert:

Up to three groups can be sent e-mail alerts regarding the device status.

Sending device data to Xerox immediately:

1. At your Workstation, open the Web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[SMart eSolutions]** in the directory tree.

4. Click on the **[Meter Assistant]** tab.
5. For **Meter E-mail Alerts**, click on the **[Configure]** button (initial use) or **[Edit]** button (subsequent use).
6. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
7. Click on the **[Login]** button to display the **E-mail Alerts** screen.
   a. In the **[Recipient Group Addresses]** area, check the required **Group** checkbox.
   b. Click the field under **E-mail Addresses**, and enter the e-mail address or addresses.
   c. Continue to add e-mail addresses to create your Alert Notification group, as required.
   d. In the **[“Reply to:” E-mail Address]** field, enter the address of the administrator or user who is designated to receive any reply e-mails that are sent by users listed in the Alert Notification group.

   Note: This is normally set to the System Administrator’s e-mail address.

   e. In the **Recipient Group Preferences** area, by default, a group will be notified of all device alerts. If you want to select specific alerts, select the alerts checkbox you want the **Group** to be notified of.
   f. Enter how many minutes (0 - 60) in the field for **Set jam timer for release of status to selected groups** to wait after a jam has been detected before an e-mail status is sent. If the jam is cleared before the timer completes, no jam message will be sent.
   g. Click on **[Apply]** to save the changes.
8. The **Settings Confirmed. Send Test e-mail?** window will appear. Click **[OK]** if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the **Alert Notification** page.

Supplies Assistant

Eligible devices will automatically be enabled for Supplies Assistant when the device is registered with Xerox. Supplies Assistant manages supply order to ensure the right supplies are supplied on the right time.

Supplies Assistant provides data from the device to be used to order supplies.

Alert Notification

In the Alert Notification section you can set up groups to notify (by e-mail) when problems occur on the device. Alert notification is configured via Internet Services.

Customers can set the Xerox device to notify users or operators of problems as they occur on the device. Alert Notification is configured via Internet Services.

E-mail Alerts

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Alert Notification]** link.
3. Select **[E-mail Alerts]** in the directory tree.
4. In the **[Recipient Group Addresses]** area:
   a. Check the required Group checkbox.
   b. Click the field under **E-mail Addresses**, and enter the e-mail address or addresses.
   c. Continue to add e-mail addresses to create your Alert Notification group, as required.
   d. In the **["Reply to:" E-mail Address]** field, enter the address of the administrator or user who is designated to receive any reply e-mails that are sent by users who are listed in the Alert Notification group.

   Note: This is normally set to the System Administrator's e-mail address.

   e. Click on **[Apply]** to save the changes.
   f. If prompted, enter the **User ID** and **Password** of the Administrator's account. The default is **[admin]** and **[1111]**.
   g. Click on **[Login]**.
   h. The **Settings Confirmed. Send Test e-mail?** window will appear. Click **[OK]** if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the **Alert Notification** page.
   i. If you want to create more than one Alert Notification group, select the group number and add e-mail addresses to the group.
5. To Assign Notification Alerts to a Group:
   a. Scroll down to the **Recipient Group Preferences** area. By default, a group will be notified of all device alerts. If you want to select specific alerts, check the alerts checkbox that you want Group 1 to be notified of.
   Alerts that can be selected are:
      - **Billing meter reads reported:** An alert is generated when billing meter readings have taken place. You can set up your device so that it will automatically offer meter readings when requested by the Xerox Communication Server.
      - **Machine is stopped:** An alert is generated when the device has stopped all functions or has been turned off.
      - **Potential persistent problems exist:** An alert is generated when a problem area in the device does not receive proper attention.

- **Machine requires administrator assistance:** An alert is generated when an authorized System Administrator is needed to address a problem.
- **Machine is operational, but degraded:** An alert is generated when device is running at reduced efficiency and needs immediate attention.
- **Paper supply is low:** An alert is generated when paper is running low or wrong size is allocated.
- **Paper jam is detected:** An alert is generated when a paper jam is in need of attention in specified area if you have been notified.
- **Supplies or CRUs are low:** An alert is generated when any Customer Replaceable Units (CRUs) have reached their low marker.
- **SMart eSolution enrollment is cancelled:** An alert is generated when the state is changed from “Enrolled” to “Not Enrolled.” Clicking this link will take you to the SMart eSolution page to get more information about the enrollment state.

b. **Set jam timer for release of status to selected groups:** In this field enter how many minutes (0 - 60) to wait after a jam has been detected before an e-mail status is sent. If the jam is cleared before the timer completes, no jam message will be sent.

c. Click the **Glossary** link next to **Status Codes** in the **Recipient Group Preferences** area for further information about the Status Codes, as below:
   - **Machine is stopped:** The device has stopped all functions or has been turned off.
   - **Potential persistent problems exist:** If the area specified does not receive attention problems may re-occur.
   - **Machine requires administrator assistance:** An Authorized System Administrator must address problem.
   - **Machine is operational, but degraded:** The device is running at reduced efficiency, needs immediate attention.
   - **Paper supply is low:** Paper is running low or wrong size is allocated.
   - **Supplies or CRUs are low:** CRU/Toner/Fuser or other usable items needs attention (see LUI).
   - **Paper jam is detected:** A paper jam is in need of attention in specified area.

d. If you have created more than one group, repeat this exercise for each group.

e. Select **[Apply]** to save your settings.

f. The **Settings Confirmed. Send Test e-mail?** window will appear. Click **[OK]** if you wish to send a test e-mail to the Alert Notification recipient(s), or **[Cancel]** to return to the Alert Notification page.

Local UI Alerts

You can configure the device to display a notice on the user interface screen when the scan disk memory is low. The scan disk memory decreases according to the number of pages scanned with the Workflow Scanning, Internet Fax, E-mail or Server Fax features (when these features are installed on the device).

When the scan disk memory is low, scan jobs may slow down or the device may cancel the job.

When a user attempts to scan more pages than the Scan Job Memory Notification setting, the device will display a message to show how many pages can be scanned before the device will slow down or be forced to cancel the job. The default is 30 scanned pages.

To Set up the Local UI Alert

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Alert Notification]** link.
3. Select **[Local UI Alerts]** in the directory tree.
4. In the **Scan Disk Memory Warning** area, select one of the following options to display a warning when it is estimated that the scan disk cannot hold more than:
    - **10 scanned pages**.
    - **30 scanned pages**.
    - **Custom** - when selected, enter an amount between 0 - 75 in the **[Custom]** field.

    Note: The higher the page number, the more frequent the warnings will appear.
5. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Billing Information and Usage Counters

The Billing and Counters page provides the Billing information for the device, including number of impressions printed or copied.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Billing Information]** in the directory tree to view Current Billing information. Click on the **[Refresh]** button to refresh the Billing information.
4. Select **[Usage Counters]** in the directory tree to view the counts from the Usage Counters. Click on the **[Refresh]** button to refresh the Usage Counters.

Energy Saver

This feature allows you to set the device to save energy when not in use. This feature is set at the device.

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

At the Device:

1. From the **Tools** pathway, touch **[Device Settings]**.
2. Touch **[General]**.

3. Touch **[Energy Saver]**.
4. The **Energy Saver** screen displays, select one of the following options:
   - **Intelligent Ready** - this option allows the device to wake up and sleep automatically based on previous usage.
   - **Job Activated** - this option allows the device to wake up when any activity is detected.

   Note: If you select **Job Activated** option, the following options are available:

     - **From Standby Mode to Low Power Mode** - this option allows you to change the time in minutes. The range is 1 - 120.
     - **From Low Power Mode to Sleep Mode** - this option allows you to change the time in minutes. The range is 5 - 120.
     - **Auto Presets** - there are three automatically preset settings to choose from.
5. If you select the **Job Activated** option, either customize the minutes, using the **Left** and **Right** scroll button under each option or select one of the three preset settings.
6. Click on **[Save]**.
7. Press the **<Log In/Out>** button.
8. Touch **[Logout]** to exit the Tools pathway.

Banner Sheet

When documents are sent to print at the device, a banner sheet is printed identifying the PC that sent the print job. It is possible to disable this setting both within the Print Driver and from the device administrator tools.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Job Sheets]**.
3. Touch **[Banner Sheets]**.
4. The **Banner Sheets** screen displays, the following options are available:
   - **Print Banner Sheets**
   - **Print Driver Override**
5. To print a Banner Sheet with each Print Job, for **Print Banner Sheets**, touch **[Enable]**.
6. To allow the Print Driver to produce Banner Sheets when required, for **Allow Print Driver Override**, touch **[On]**.
7. Touch **[Save]**.
8. Press the **<Log In/Out>** button,
9. Touch **[Logout]** to exit the Tools pathway.

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Printing]** link.
3. Select **[General]** in the directory tree.
4. In the **Banner Sheet** area:
   a. For **Banner Sheet**, check the **[Enabled]** checkbox to print a Banner Sheet with each job.
   b. For **Allow the Print Driver to Override**, check the **[Enabled]** checkbox to allow your Print Driver to override this option.
5. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Service Default

The Service Default function allows the System Administrator to select the service that will display as the default on the machine's user interface screen. This function is useful where machines have more than one service installed.

Features that are used most by users will be displayed first on the screen. The rest of the features can be accessed when the user presses the **<Services Home>** button.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Device Settings]**.
2. Touch **[General]**.
3. Touch **[Entry Screen Defaults]**.
4. Touch **[Service Default]**, the **Service Default and Priority** screen displays.
5. Select an item from the list and touch the **Promote** button until the item is at the top of the list. The highest priority item will display by default service on the device **Services** screen.
6. Touch **[Save]**.
7. Press the **<Log In/Out>** button.
8. Touch **[Logout]** to exit the Tools pathway.

Job Status Default

The Job Status Default function allows the System Administrator to select the job status view that will display as the default on the machine's user interface screen when the user presses the **<Job Status>** button.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Device Settings]**.
2. Touch **[General]**.
3. Touch **[Entry Screen Defaults]**.
4. Touch **[Job status default]**, the **Job Status Default** screen displays.
5. Set the tab that will be shown by default when the user presses the **[Job Status]** button:
   - **Active Jobs** - displays the **Active Jobs** tab by default.
   - **Held Print Jobs / Secure Print Jobs** - displays the **Held Print Jobs** or **Secure Print Jobs** tab by default.
6. Select the default view for the **Active Jobs** tab.
7. Select the default view for the **Completed Jobs** tab.
8. Touch **[Save]**.
9. Press the **<Log In/Out>** button.
10. Touch **[Logout]** to exit the Tools pathway.

Saving and Reprinting Jobs

The Save Job for Reprint feature allows users to store print jobs on the device from their Print Driver, or the Print page of Internet Services, then select the job from the device's user interface for reprinting.

This feature can be enabled and configured by the System Administrator from the **Properties** tab of Internet Services (the series of web pages, hosted on the embedded HTTP server of the device).

Enabling the Feature at a TCP/IP Networked Workstation

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Reprint Saved Jobs]** link.
3. Select **[Enablement]** in the directory tree.
4. In the **Enablement** area, select **[Enabled]** to enable the feature, and click on the **[Apply]** button.

Backup Saved Jobs

1. Select **[Backup Jobs]** in the directory tree to back up saved jobs stored on the system.
2. In the **Settings** area:
   a. Select **[FTP]** from the **[Protocol]** drop-down menu.

   Note: Only FTP is available.

   b. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button for your FTP server.
   c. Enter details of the repository server in the **IP Address: Port** or **Host Name: Port** field.
   d. For **[Document Path]**, specify the path to the file repository.
   e. For **[File Name]**, type the file name for the backup. This name will be appended onto the end of the document path.
   f. For **[Login Name]**, if you selected System for Login Credentials (referring to FTP repository in the Workflow Scanning topic), then you must specify the system login name here.
   g. For **[Password]** and **[Retype Password]**, if you selected System for the login credentials, then you can specify and confirm the system password here. The password may be blank.
   h. Check the **[Select to save new password]** checkbox for an existing Login Name.
3. Click on the **[Start]** button at the bottom of the page to implement the password change, or **[Undo]** to cancel any changes.

Restore Saved Jobs

1. Select **[Restore Jobs]** in the directory tree to restore saved jobs stored on a repository.

   Note: When Saved Jobs are restored, all current Saved Jobs data will be immediately deleted. The restore process may take some time to complete depending on how many files were backed up. The restored Saved Jobs data is not appended to the existing Saved Jobs. If the restore is aborted, the Default Public Folder will be empty.

2. In the **Settings** area:
   a. Select **[FTP]** from the **[Protocol]** drop-down menu.

   Note: Only FTP is available.

   b. Select either the **[IP Address]**, **[IPv4 Address]** or **[Host Name]** radio button for your FTP server.
   c. Enter details of the repository server in the **[IP Address: Port]** or **[Host Name: Port]** field.
   d. For **[Document Path]**, specify the path to the file repository.
   e. For **[File Name]**, type the file name for the backup to restore. This name will be appended to the document path.
   f. For **[Login Name]**, if you selected System for Login Credentials (referring to FTP repository in the Workflow Scanning topic), then you must specify the system login name here.
   g. For **[Password]** and **[Retype Password]**, if you selected System for the login credentials, then you can specify and confirm the system password here. The password may be blank.
   h. Check the **[Select to save new password]** checkbox for an existing Login Name.
3. Click on the **[Start]** button at the bottom of the page to implement the password change, or **[Undo]** to cancel any changes.

Online/Offline

The Online/Offline window allows the System Administrator to stop and resume the system from receiving or sending jobs over the network.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Online/Offline]**.
3. To stop the device receiving or sending jobs over the network touch **[Offline]**. Any installed optional features using the network (for example Workflow Scanning) will not be available until the device is set to Online.

   Note: To enable the device to receive or send jobs over the network touch the **[Online]** button.

4. Touch **[Save]**.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

Foreign Interface Device

A third party access and accounting device, such as a coin operated device or a card reader can be attached to the device. To enable this option, the Foreign Device Interface Kit must be installed. After the kit is installed the System Administrator must enable Foreign Interface Device as the Accounting Mode from the Tools pathway of the device.

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Accounting Settings]**.
2. Touch **[Authentication]**, the **Accounting Mode** screen displays.
3. For **Foreign Interface Device**, touch **[On]** to enable the feature.
4. Touch **[Save]**.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

For further information regarding the setup of the third party device, refer to the third party instruction manual.

Software Upgrade via Network Connection

⚠ **WARNING:** This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software. All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Prepare for the Upgrade

Obtain the new software upgrade file for your device from the www.xerox.com website or from your Xerox Customer Support Representative. Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.

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

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Configuration]** in the directory tree, scroll down to the **Printer Setup** section to see your System Software Version.

Upgrades

The Software Upgrade feature allows the customers to upgrade the device software as requested by a Xerox Customer Support Center Representative, without needing a Customer Service Representative to be present.

To enable or disable software upgrades on the device, follow the procedure below:

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Machine Software]** link.

3. Select **[Upgrades]** in the directory tree.
4. In the **Upgrades** area, check the **[Enabled]** checkbox to enable Machine Software upgrades.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Manual Upgrade

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Machine Software]** link.
3. Select **[Manual Upgrade]** in the directory tree.

   Note: Note the current software version and the date installed in the **Last Successful Upgrade** area. The **Auto Upgrade** area displays the status of the Auto Upgrade. If Auto Upgrade is enabled, the screen displays the time at which the Auto Upgrade will take place and the Server details.

4. In the **Manual Upgrade** area:
   a. Click on **[Browse]** to locate the software upgrade file obtained earlier.
   b. Select the file and click **[Open]**.
   c. Click on the **[Install Software]** button to proceed with the upgrade. The file will be sent to the printer and will disable the printing functionality. The web browser will become inactive and you will not be able to access the device via this method until the upgrade has completed and the device has rebooted. The upgrade should take no longer than 15 minutes.
5. When the device has completed the upgrade it will reboot automatically. The configuration report will print (if it was enabled in the Tools set up). When the device is accessible from a web browser, view the software version on the **Internet Services Manual Upgrade** page, or check the configuration report to verify that the software level has changed.

   Note: Your device can be set to automatically schedule device software upgrades from a central server at a specific time on a regular basis. For instructions click on the **[Software Upgrade]** link to the left of the page and select **[Auto Upgrades]** in the directory tree.

You have completed the steps to perform a manual software upgrade.

Software Upgrade: Auto

Your device can be set to automatically schedule device software upgrades from a central server.

WARNING: This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software. All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Determine your current System Software Version number.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Configuration]** in the directory tree, scroll down to the **Printer Setup** section to see your System Software Version.

3. Contact your Xerox Customer Support Representative to make certain that Auto Upgrading is appropriate for your device. Otherwise, refer to Upgrades on page 53 for manual upgrade instructions.
4. Press the **<Log In/Out>** button.
5. Touch **[Logout]** to exit the Tools pathway.

Set the Auto Upgrade Time

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Machine Software]** link.
3. Select **[Auto Upgrade]** in the directory tree.
4. In the **Auto Upgrade** area, for **Schedule Upgrade**, check the **[Enabled]** checkbox to enable the upgrade.
5. For **Refresh Start Time**, select either **[Hourly]** or **[Daily]** to activate the feature accordingly. If **[Daily]** has been selected, enter the required time for the upgrade to be performed.
6. For **Protocol**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
7. Enter details of the server where the software upgrade file is located at in the **[IP Address]** and **[Port]** or the **[Host Name]** and **[Port]** field (the default port number is 21).
8. Enter the path to the upgrade file on the server in the **[Directory Path]** field.
9. Enter the **[Login Name]** and **[Password]** for the server, retype the password.
10. Click on the **[Apply]** button to accept the changes.
11. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

The upgrade will now be performed automatically on the device at the time specified. When the upgrade process starts network connectivity with the device will be unavailable, including access from Internet Services. The upgrade progress can be monitored from the device screen interface.

You have completed the steps to automatically upgrade the device software.

Internet Services 4

This chapter explains how to enable and use the Internet Services feature of the device.

The Internet Services feature uses the embedded HTTP Server on the device. This allows you to communicate with the device through a web browser and gives you access to the Internet or intranet. Entering the IP Address of the device as the URL (Universal Resource Locator) in the browser provides direct access to the device.

Internet Services not only allow you to change basic settings on the Control Panel, but also allows you to change more specialized settings for the device.

Information Checklist

Before accessing Internet Services, please ensure the following items are available or have been performed:

- The device must be physically connected to the network with TCP/IP enabled so that Internet Services can be accessed from a web browser.
- An existing operational workstation with TCP/IP Internet or Intranet accessibility is required.
- HTTP (HyperText Transfer Protocol) should be enabled on the device. HTTP is enabled by default. If you need to enable HTTP, see Enable HTTP on the device on page 57.

Enable HTTP on the device

HyperText Transfer Protocol (HTTP) must be enabled on the device in order to access the embedded HTTP server.

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. From the **TCP/IP** screen, touch **[HTTP/IPP Enablement]**.
   a. For **Protocol** touch **[Enable]**.
   b. Touch **[Save]**, to return to the **TCP/IP** screen.
5. Touch **[Close]**.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools pathway.

Access Internet Services

Instructions to access Internet Services:

1. Open the web browser from your Workstation.
2. In the URL field, enter **http://** followed by the IP Address of the device. For example: If the IP Address is 192.168.100.100, enter the following into the URL field: **http://192.168.100.100**.
3. Press **<Enter>** to view the **Home** page.
4. Click a tab to access the desired page, or click on the **Index** icon at the top of the device web page to access the index and contents list.

Many of the features available within Internet Services will require the **System Administrator** log in using their **User ID** and **Passcode**. The default being **[admin]** and **[1111]**. A user will only be prompted for the Administrator User ID and Password once in a single browser session.

Status

Description and Alerts

Device Description

The **Device Description** area displays the following information:

- **Machine Model**
- **Location**
- **Status**
- **Name**
- **IP Address**

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Description and Alerts]** in the directory.

Alerts

The **Alerts** area displays all current alert messages. Each alert will specify what the problem is and a solution to the problem.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Description & Alerts]** in the directory tree.

The following information is displayed in the **Alerts** field:

- **Severity** - the importance or impact of the problem.
- **Status Code** - if the problem needs a Service Representative to fix it then let them know this code when you talk to them.
- **Description** - displays a warning or the problem and how to fix it.
- **Skill Level** - Displays the suggested skill level needed to fix this problem. The levels are:
  - **Trained** - System Administrator needed to fix this problem.
  - **Untrained** - normal user can fix this problem.
  - **Field Service** - Xerox support needed to fix this problem.
  - **Management** - network administrator needed to fix this problem.
  - **No intervention required** - a normal device status.

To set Alert Notification, refer to E-mail Alerts on page 45.

To Reboot the Device

It is possible to reboot the device from Internet Services.

1. Click on the **[Status]** tab.

2. Select **[Description & Alerts]** in the directory tree.
3. Click on the **[Reboot Machine]** button and click **[OK]** to reboot the device. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Billing Information and Usage Counters

The **Internet Services Billing Information** page displays the total number of impressions copied, printed, scanned or faxed by the device. The **Usage Counters** page shows you the number of impressions and images sent by the device.

Billing Information

The **Billing Information** page provides current readings of all device counters.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Billing Information]** in the directory tree.
4. Click on the **[Refresh]** button to view the current billing information in the **Total Impressions** area.

Usage Counters

The **Billing Meter** area shows the date and number of impressions that were notified to the Xerox Communication Server, if this has been set up.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Click on the **[Usage Counters]** link.
4. Click on the **[Refresh]** button to view the current usage in the **Usage Counters** area.

Consumables

The **Consumables** page allows you to view the status of the Customer Replaceable Units (CRUs) within the device.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Consumables]** in the directory tree.
4. The **Consumables** screen displays consumable information for:
   - **Toner Cartridges**
   - **Waste Container**
   - **Xerographic Module**
   - **Fuser**

For each unit, the **Life Remaining** icon describes the current supply level as a percentage and provides a bar graph visual display.

Trays

The **Trays** page allows you to view paper supply setup and paper output.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Status]** tab.
3. Select **[Trays]** in the directory tree.
4. The **Trays** page displays the current paper supply.

Instructions for changing the paper stock are contained in the **User guides** on your device.

Jobs

The **Jobs** tab displays a list of active and completed jobs. You can also delete jobs in this tab.

Note: The details displayed may differ from those shown on the device's touch screen.

Active Jobs

The **Active Jobs** page displays information about the active job list on the device:

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Jobs]** tab, **Active Jobs** will display.
3. Click on the **[Refresh]** button to update the information in the table.
   The following information is shown:
   - **Job Name** - the title of the print job.
   - **Owner** - the person submitting the job.
   - **Status** - the current status of the job.
   - **Type** - displays whether the job is print, scan or fax.
   - **Copy Count** - displays the number of copies requested for the job.

Saved Jobs

Within the **Jobs** tab screen select the **[Saved Jobs]** tab.

The screen will display the Saved Jobs, the available hard disk space on the device. You can also create new saved job folders and manage saved job folders.

Create a New Folder

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Jobs]** tab, click on **[Saved Jobs]** tab.
3. **Saved Jobs** screen displays. In the **Folder Operations** area, click on **[Create New Folder]** link.
4. In the **New Folder** area, enter details in the **[Name]** field.
5. Select the type of permission from the **[Folder Permissions]** drop-down menu. There are three types of folder permissions as follows:
   - **Public Folder** - allows any user to access the folder and the folder contents.
   - **Read Only** - allows access to read any of the contents of the folder, but the contents of the folder can not be deleted or have their settings changed.
   - **Private** - allows only the creator of the folder or the System Administrator to access the folder and its contents.
6. Click on the **[Apply]** button to create the folder. The folder will appear in the **Folders** list.

Manage Folders

The **Manage Folders** screen allows you to manage folders on the device; you can rename a folder, delete a folder and change folder permissions.

1. In the **Folders Operations** area, click on the **[Manage Folder]** link.
2. **To Delete**:
    a. Check the checkbox for the folder you want to delete.
    b. Click on the **[Delete Folder]** button.
3. **To Rename a folder or and change Folder Permission**:
    a. Click on the **[Pencil]** ✏ icon next to the folder you want to rename.
    b. In the **Folder properties** area, enter a new name in the **[New name]** field.
    c. Select the type of permission required for the folder from the **[Folder Permissions]** drop-down menu.
    d. Click on the **[Apply]** button to accept the changes.
4. **To Print**, **Copy**, **Move or Delete a file within a folder**:
    a. Click on the required folder in the **Folders** area.
    b. Check the checkbox for the file you want to Print, Copy, Move or Delete.
    c. From the drop-down menu select either **[Print Job]**, **[Copy Job]**, **[Move Job]** or **[Delete Job]**.
        - If you select **[Print Job]**, enter how many prints you require in the **[Copies]** field and click on the **[Go]** button.
        - If you select **[Delete Job]**, click on the **[Go]** button, click on the **[OK]** to delete or **[Cancel]** to return to the previous page.
        - If you select **[Copy Job]** or **[Move Job]**, click on the **[Go]** button. Select the folder you want the Job to be copied or moved to, click on the **[Copy Job]** or **[Move Job]** button.
5. To refresh the page, click on the **[Refresh List]** button.

Print

Print-ready documents can be quickly and easily submitted for printing using the **Job Submission** page.

A print-ready document is a file that has been formatted and saved for printing from the source application or the **Print to File** checkbox was selected in the Print Driver.

The following file formats can be printed from the **Job Submission** page:

- **PCL® 5**
- **PCL® 6**
- **PostScript®**
- **PDF**

Large print jobs need adequate space on your hard drive when printing through Internet Services.

1. At your Workstation, open the web browser from your Workstation. Enter the IP Address of the device in the Address bar. Press **<Enter>**.
2. Click on the **[Print]** tab.
3. In the **File Name** area, click on the **[Browse]** button to locate the document on your workstation.
4. When the document is located, select it and click **[Open]**.
5. In the **Printing** area:
    a. For **Copies**, select either **[Auto]** or **[Copies]**. If **Copies** is selected, enter the number of copies required (between 1 - 9999) in the field.
    b. Select the required **[Job Type]**:
        - **Normal Print**.
        - **Secure Print** - you will need to enter a 4 - 10 digit number which you will use at the device user interface to release the document for printing.
        - **Proof Print**- if several copies of the document have been selected, one copy only will print to allow the reader to check for errors. When validated, the remaining copies can be released from the device user interface.
        - **Save Job for Reprint** - the document will be saved for reprinting.
        - **Delay Print** - specify a time for your document to print.

    c. For **Paper**, click **[Paper Selection]** and select the required option.
    d. Select the required Printing options from the drop-down menu for **2 Sided Printing**, **Collate**, **Orientation** and **Output Destination**.
    If Network Accounting is installed, then enter your Account and User ID for accounting purposes. (The Accounting fields are only visible if accounting is enabled on your device).

    Note: Printing options are only valid for jobs that do not contain the settings already.
6. When finished with your selections, click on the **[Submit Job]** button to send your document to the printer. Wait for the **Job Submission** confirmation window to appear before exiting or navigating to a different screen, so your print job will not be deleted.
    Retrieve the printed document(s) from the device.

Address Book

This tab allows you to view and setup an address book on the device. This tab also allows you to import external address book, export the device address book. You can download a sample of the address book. For further information, refer to Public Address Book on page 254.

Properties

This tab allows you to view and set the device properties. These include the device details and configuration, Internet Services settings, the port settings, protocol settings, emulation settings, and the memory settings. The items displayed will depend on the model and configuration of the device.

Configuration Overview

This page displays the device configuration overview, displays information on Connectivity and Printing, if Services are configured or not, if Cloning is configured or not.

1. At your Workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Configuration Overview]** link.
6. In the **Before you Begin** area, click on the **[View Checklist]** button.

Description

This page displays the following information and allows you to set and view information related to the device, such as the name and installation location of the device:

- **Machine Model**
- **Product Code/Serial Number**
- **Device Name**
- **Location**

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Description]** link.
2. If **[Device Name]** and **[Location]** are changed, click on the **[Apply]** button, to accept the changes.

General Setup

Configuration Report

The Configuration page displays the following information:

- **Configuration**
- **Report Profile**
- **Machine Profile**
- **Installed Options**
- **Printer Setup**
- **Interpreter Profiles**
- **Network Setup**
- **Custom Service Setup**
- **Workflow Scanning Setup**
- **Port Setup**
- **Server Fax Setup**
- **Media Trays**
- **Network Authentication Setup**
- **Accounting Setup**

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Configuration]** in the directory tree.
3. To print a configuration report from this screen, click on the **[Print Configuration Report]** button.

Ethernet Configuration using Internet Services

The Ethernet can be configured from the Internet Services as well as at the device.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Physical Connections]** link.
3. Select **[Ethernet]** in the directory tree.
4. In the **General** area, select the speed from the **[Rated Speed]** drop-down menu.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Note: When you change the settings, you must restart the device to see the new values. If you return to this page before the device has been restarted, the old setting will display.

Support

The Internet Services Support page provides easy access to the Xerox website. The page can also be set up to show Xerox support telephone numbers and the contact details for the System Administrator.

To Edit Xerox Support or System Administrator Contact Details.

1. Open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Support]** tab.
3. Click on the **[Edit Settings]** link.
4. In the **System Administrator** area, to edit or add details, enter the details in the following fields:
   - **Administrator**
   - **Phone Number**
   - **Location**
5. In the **Xerox Support** area, to edit or add details, enter details in the following fields:
   - **Customer Support**
   - **Service**
   - **Supplies**
6. When completes, click on the:
   a. **[Save]** button to accept the settings If prompted, enter the **User ID** and **Password** of the Administrator's account and click on **[Login]**.
   b. **[Undo]** button to revert back to previous details.

Other features and Services

Other features and services that can be configured supported by Internet Services are explained throughout this guide.

Network Installation 5

This chapter explains how to set up the device to operate in different network environments and configure network protocols.

Windows 2000/2003/XP/Vista Environment

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

For Static IP Address	For Dynamic IP Address
• Existing operational network utilizing the TCP/IP protocol. • Ensure that the device is connected to the network. • Static IP Address for the device. • Subnet Mask Address for the device. • Gateway Address for the device. • Host Name for the device. • Ethernet Cable. • Print and Fax Drivers CD (delivered with your device).	• Existing operational network utilizing the TCP/IP protocol. • A DHCP, BOOTP or RARP Server should be available on the network. • Ensure that the device is connected to the network. • Ethernet Cable. • Print and Fax Drivers CD (delivered with your device).

For Static IP Address

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[TCP/IP Enablement]**, the **TCP/IP Enablement** screen displays.
    a. Touch **[Enable]** for **IPv4** and **IPv6**.

    Note: Any changes to the IPv6 feature will result in a reboot of the Network Controller.

    b. Touch **[Save]**.
6. Touch **[Automatic Addressing]**.
    a. Touch **[Disabled]** to disable Automatic Addressing.
    b. Touch **[Save]**.
7. Touch **[IP Address/Host Name]**, the **IP Address/Host Name** screen displays.
    a. For **IPv4 Address**, touch each octet and enter the IP address using the numerical keypad.
    b. For **Host Name**, touch the detail bar.
    c. Enter Host Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
    d. Touch **[Save]**, then touch **[Save]** to return to the **TCP/IP Settings** screen.

8. Touch **[Subnet and Gateway]**, the **Subnet and Gateway** screen displays.
   a. For **IP Gateway**, touch each octet under the title and enter IP Gateway address using the numerical keypad.
   b. Repeat this process for the **Subnet Mask**. When you are finished, touch **[Save]** to accept the changes and return to the **TCP/IP Settings** screen.
   c. Touch **[Close]** to return to the **TCP/IP** screen.
9. Touch **[HTTP/IPP Enablement]**, the **HTTP/IPP Enablement** screen displays.
   a. For **Protocol**, ensure **Enable** is selected. If not, touch **[Enable]**.
   b. Touch **[Save]**, then touch **[Close]** to return to the **Tools** pathway.
10. Touch **[TCP/IP-Line Printer]**, the **TCP/IP - Line Printer** screen displays.
   a. Touch **[Enable]**, to enable the option.
   b. If you wish to change the LPR port for your device, touch the port number area and enter the desired port number using the numerical keypad.

   Note: You can change the port number at which your device will accept LPR print jobs. It is recommended that you do this ONLY with extreme caution as most LPR spoolers are set to send print jobs to the default port of 515.

   c. Touch **[Save]** to return to the **TCP/IP** screen.
   d. Touch **[Close]** to return to the **Tools** pathway.

For Dynamic IP Address

Installation via DHCP (Dynamic Host Configuration Protocol)

DHCP is enabled on the device by default. If the device is connected to the network the TCP/IP information will be configured when the device is powered on and no further configuration is required.

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.

   Note: All options under the **IP Address/Host Name** section will be grayed out until DHCP is deselected in the Dynamic Addressing section. Follow the next step to disable DHCP and access these options if required.

5. Touch **[Automatic Addressing]**, by default, DHCP will be selected. Select the required dynamic addressing method **[BOOTP]**, **[DHCP]**, or **[RARP]**.

   Note: To give the device a static IP Address, touch **[Disabled]** to disable Automatic Addressing.

   a. Touch **[Enabled]**.
   b. Touch **[Save]**.
6. Touch **[HTTP/IP Enablement]**, the **HTTP/IP Enablement** screen displays.
   a. For **Protocol**, ensure **Enable** is selected. If not, touch **[Enable]**.

b. Touch **[Save]**, then touch **[Close]** to return to the **Tools** pathway.

DNS/DDNS Configuration

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[DNS Configuration]**, the **DNS Configuration** screen displays.
   This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.
   a. Touch the **[Domain Name]** button.
   b. Touch the bar under **Domain Name**.
   c. Touch the **[Clear Text]** button to remove the default name before entering the new name using the on screen keyboard.
   d. Touch **[Save]**.
   e. Touch **[Save]** to return to the **DNS Configuration** screen.
6. Touch **[Preferred DNS Server]**.
   a. Touch each octet under the title and enter the Preferred DNS IP server address using the numerical keypad.
   b. Touch **[Save]**, then touch **[Close]**.
7. Touch **[Alternate DNS Servers]** if required.
   a. Touch the button under **Alternate DNS Server**, enter the Alternate DNS Server IP Address using the on-screen keypad.
   b. Touch **[Save]** to return to the **DNS Configuration** screen.

   Note: If DHCP is enabled, the Alternate DNS server information is not available as a feature summary.

   c. Touch **[Close]** to return to the **DNS Configuration** screen.

Enable Dynamic DNS Registration

Note: If your DNS server does not support dynamic updates, then this function does not need to be enabled.

8. Touch **[Dynamic DNS Registration]**, touch **[Enable]**, then **[Save]** to return to the **DNS Configuration** screen.
9. Press the **<Log In/Out>** button.
10. Touch **[Logout**] to exit the Tools pathway.

Install Print Drivers

Create a New Print Queue (for Windows 2000/2003/XP)	Verify that LPR Port Monitor is Loaded (for Windows Vista)
1. At your workstation, load the **Print and Fax Drivers CD** into your CD drive. If the CD auto runs, click on **[Exit]**. 2. Verify that Print Services for Unix is loaded: from the **[Start]** menu, then **[Control Panel]**. 3. Double-click on **[Add or Remove Programs]**. 4. Select **[Add/Remove Windows Components]** (in the column on the left). 5. Scroll down until you see **[Other Network File and Print Services]** and select it. 6. Click on the **[Details]** button. 7. Check the box to add **[Print Services for Unix]** and click on **[OK]**. Click on **[Next]**. If Print Services for Unix is not installed, refer to instructions from Microsoft to install this service. 8. Click on **[Finish]**.	1. At your workstation, click on **[Start]**, **[Control Panel]** and double-click on **[Programs and Features]**. 2. Double-click on **[Windows Features]**. 3. In the **[Turn Windows Features on and off]** window expand the **[Print Services]** menu. 4. Click on **[LPR Port Monitor]** to enable the service. 5. Click on **[OK]**. Your computer may need to restart.

Add the Printer

1. At your workstation:
   - **Windows XP** - from the **[Start]** menu select **[Printers and Faxes]**.
   - **Windows 2000/2003** - from the **[Start]** menu select **[Control Panel]** then select **[Printers]**.
   - **Windows Vista** - from the **[Start]** menu select **[Control Panel]**, then double-click on **[Printers]**.
2. Click on **[Add Printer]**.

   a. For **Windows 2000/2003/XP**, click on **[Next]**.
3. For the following select:
   - **Windows 2000/2003/XP - [Local Printer attached to this computer]**.
   - **Windows Vista - [A printer attached to my computer]**.
4. If already selected, deselect **[Automatically detect and install my Plug and Play printer]**.
5. Click on **[Next]**.
6. Select **[Create a new port]**.
7. Select **[LPR Port]** from the **Type of Port** drop-down menu and click on **[Next]**.

   Note: NOTE: LPR port is only available when Print Services for Unix is installed.
8. Enter the IP Address of the device.
9. Enter the device name.
10. Click on **[OK]**.
11. You will be prompted for a Print Driver. Select **[Have Disk]** and click on **[Browse]**. Locate the **Drivers** folder on the CD.

12. Select the required driver.
13. Click on **[Open]** and then **[OK]**.
14. Select the model of your machine from the list. Click on **[Next]**.
15. The **Name your Printer** screen displays. Enter a printer name and click on **[Next]**.
16. The Printer Sharing Screen appears. If you will be sharing this printer with other clients select **[Share As]** (Windows 2000) or **[Share Name]** (Windows 2003) and enter a share name. Click on **[Next]**.
17. For Windows 2000/2003/XP, enter a name and comment if required. Click on **[Next]**.
18. Select:
    - **Windows 2000/2003/XP**: Select **[Yes]** to print a test page. Click on **[Next].**
    - **Windows Vista**: Select **[Print a test page]** to verify the device is installed, and select **[Make this my default]**, if required.
19. Click on **[Finish]**. The Print Driver will install.

Configure the Print Driver - Automatically

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

At your Desktop

1. Select **[Start]**, (**[Control Panel]**) and then **[Printers]/[Printers and Faxes]**.
2. Right-click on the appropriate printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Bi-Directional Setup]**.
   If you have given the device a valid IP Address or host name the Print Driver can provide Bi-Directional capabilities. Bi-directional communication automatically updates the Print Driver with the printer's installed options. The driver Printing Preferences will report information about the printer's operational status, active jobs, completed jobs and paper status.
5. Click on **[Automatic]** to have the driver automatically configure the IP Address of the device or click on **[Manual]** and enter the IP Address or host name of the device.

If you want to change the default SNMP settings, click on **[SNMP Community Name]** and enter the required information.

6. Click on **[OK]**.
7. Click on the **[General]** tab.
8. Click on **[Print Test Page]**. Close the **Test Page** window if necessary.
9. Click on **[OK]** to close the **Properties** box.
10. Right-click on the printer icon in the Printers folder and select **[Printing Preferences]**.
11. Ensure the **Paper/Output** tab is selected and click on the **[More Status]** button at the bottom of the window. Current information about the printer is available. Click on **[Close]** to close the window.
12. For **Default Settings**, select any required default settings in the Print Driver and click on **[OK]**.

Verify the Test Page printed at the machine.

Configure the Print Driver - Manually

To configure the Print Driver without using bi-directional communication return to the **Configuration** tab within the Properties of the Print Driver.

1. Click on **[Installable Options]**.
2. Select the options that are installed on the device.
3. Click on **[OK]**.
4. Click on the **[General]** tab.
5. Click on **[Print Test Page]**.
6. Click on **[OK]** to close the Properties box.
7. Right-click the printer icon within the Printers folder and select **[Printing Preferences]**.
8. For **Default Settings**, select any required default settings in the Print Driver.

Verify the Test Page printed at the machine.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word **cloning** in the search tool.

Windows 2000/2003 using AppleTalk

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational AppleTalk network with Macintosh workstation computers equipped with Ethernet network interface cards.
- The AppleTalk Name you wish to assign to your printer.
- The AppleTalk Zone (if used) in which your printer will reside.
- Ethernet Cable.
- The Internet Services Print and Fax Drivers CD (delivered with your device). Review any README file contained with the Print Drivers.

At the Device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[AppleTalk Settings]**, the **AppleTalk (R) Settings** screen displays.
4. Touch **[AppleTalk (R) Enablement]**.
5. Touch **[Enable]** for Protocol.
6. Touch **[Save]** to return to **AppleTalk (R) Settings** screen.
7. Touch **[Name and Area]**.
8. Touch **[Printer Name]** field and enter the desired text using the on-screen keyboard, touch the **[Save]** button.
9. Touch **[Area Name]** field, enter the desired text using the on-screen keyboard, (the printer default is * which means the printer will appear in ALL areas). Use the **C** hard button to clear out the default name prior to entering your new name).
10. Touch **[Save]**.
11. Touch **[Save]** again, touch **[Close]**.
12. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools pathway.
13. Wait few minutes for the machine to reboot. Press the **<Machine Status>** button.
    a. Touch the **[Machine Information]** tab.
    b. Touch **[Print Reports]**.
    c. Touch **[Print Report]**.
    d. Touch **[Close]**.
    The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.

At your Workstation

1. Right-click on **[My Network Places]**.
2. Select **[Properties]**.
3. Right mouse click on the network connection you want to configure AppleTalk on, and then click on **[Properties]**. The **Connection Properties** dialog box opens.
4. On the **General** tab, if the AppleTalk Protocol is in the list of installed protocols, make sure that it is selected. If the AppleTalk protocol is not listed, install it using the documentation provided by Microsoft. Then return to the next step in this document.
5. Select **[Start]**, (**[Settings]**) and then **[Printers]**/**[Printers and Faxes]**.
6. Double-click on **[Add Printer]**.
7. Click on **[Next]**.
8. Click on **[Local Printer]** (Windows 2000) or **[Local Printer attached to this computer]** (Windows 2003). Deselect the **Automatically detect and install my Plug and Play printer** option.
9. Click on **[Next]**.
10. Click on **[Create a New Port]**.
11. Select **[AppleTalk Printing Devices]** and click on **[Next]**.
12. In the **Available AppleTalk Printing Devices** box, click on the printer you want to connect to. It may be necessary to double-click on the required Zone to locate the printer. Click on **[OK]**.

    Note: You may be asked whether you want to capture the AppleTalk print device. If you are prompted to do this and you are unsure how to respond, click on the **[Help]** button and read the help file for an explanation of capturing AppleTalk print devices.

    Note: Capturing the printer may prevent other computers from printing to this printer. For more information refer to Microsoft.
13. Click on **[Have Disk]**. Load the CentreWare Print and Fax Drivers CD into your CD drive.
14. Click on **[Browse]** and locate the CD drive.
15. Locate the folder containing Print Drivers on the CD and select the required Windows Print Driver.
16. Select **[Open]**.
17. Select **[Open]** again, if necessary.
18. Select **[OK]**.
19. Select your printer model from the list and click on **[Next]**.
20. Type a name for the printer (or accept the default name), and then click on **[Next]**.
21. If you want this to be your default printer click on **[Yes]**.
22. Click on **[Next]**.
23. If you want to share this printer from your computer, click on **[Share As:]** (Windows 2000) or **[Share Name]** (Windows 2003). Enter a share name (or accept the default name), then click **[Next]**.
24. Click on **[Yes]** to print a test page.
25. Click on **[Next]**.
26. Click on **[Finish]**.

Configure the Print Driver

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

At your Desktop

1. Select **[Start]**, (**[Settings]**) and then **[Printers]**/**[Printers and Faxes]**.
2. Right-click on the appropriate printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Installable Options]**.
5. Select the options that are installed on the device.
6. Click on **[OK]**.
7. Select **[Printing Preferences]**.
8. For **Default Settings**, select any required default settings in the Print Driver.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word cloning in the search tool.

Windows using Microsoft $^{(R)}$ Networking

NetBIOS over IP

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational network utilizing the TCP/IP protocol.
- A Static IP Address for the machine.
- A Subnet Mask Address for the machine.
- A Gateway Address for the machine.
- A Host Name for the machine.
- Ensure device is connected to the network with an Ethernet Cable.
- The CentreWare Print and Fax Drivers CD (delivered with your machine).

At the Machine

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP/IP]**.
4. Touch **[TCP/IP Settings]**.
5. In the **TCP/IP Settings** screen:
   a. Touch the **[Automatic Addressing]** button.
   b. Touch **[Disabled]**.
   c. Touch **[Save]**.
6. Touch **[IP Address/Host Name]**, in the **IP Address/Host Name** screen:
   a. For **IPv4 Address**, touch each octet and enter the IP address using the numerical keypad.
   b. For **Host Name**, touch detail bar.
   c. Enter Host Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
   d. Touch **[Save]**, then touch **[Save]** to return to the **TCP/IP Settings** screen.
7. Touch **[Subnet and Gateway]**, in the **Subnet and Gateway** screen:
   a. For **IP Gateway**, touch each octet under the title and enter IP Gateway address using the numerical keypad.
   b. Repeat this process for the **Subnet Mask**. When you are finished, touch **[Save]** to accept the changes and return to the **TCP/IP Settings** screen.
   c. Touch **[Close]** to return to the **TCP/IP** screen.

8. Touch **[TCP/IP-Line Printer]**, in the **TCP/IP - Line Printer** screen,
   a. Touch **[Enable]**, to enable the option.
   b. If you wish to change the LPR port for your device, touch the port number area and enter the desired port number using the numerical keypad.

   Note: While you can change the port number at which your machine will accept LPR print jobs it is recommended that you do this ONLY with extreme caution as most LPR spoolers are set to send print jobs to the default port.
9. Touch **[Save]**, then touch **[Close]**.
10. Touch **[Microsoft Networks]**, the **Microsoft (R) Networks** screen displays.
    a. Touch **[Microsoft Enablement]**.
    b. Touch **[Enable]** to enable the Microsoft Network protocols.
    c. For **Transport**, select **[IP/Ethernet]**. Touch **[Save]** to return to the **Microsoft (R) Network** screen.
11. Touch **[Workgroup and Host]**, in the **Workgroup and Host** screen:
    a. For **Workgroup Name**, touch detail bar.
    b. Touch **[Clear Text]** to clear the default name, enter Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
    c. Touch **[Save]**, to return to the **Workgroup and Host** screen and repeat for **SMB Host Name**.
    d. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
12. Touch **[Printer Description]**. In the **Printer Description** screen:
    a. For **Printer Name**, touch detail bar.
    b. Touch **[Clear Text]** to clear the default name, enter description using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
    c. Touch **[Save]**, to return to the **Printer Description** screen and repeat for **Printer Description**.
    d. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
13. Touch **[Connections]**, in the **Connections** screen:
    a. For **Maximum Connections**, touch the detail box, enter the desired maximum simultaneous connections using the numerical keypad.
    b. For **Connection Timeout**, touch the detail box, enter the desired number of seconds for timeout using the numerical keypad.
    c. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
14. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools pathway.

    Wait for the device to reboot.
15. Press the **<Machine Status>** button.
    a. Touch **[Machine Information]** tab.
    b. Touch **[Print Reports]**.
    c. Touch **[Print Report]**.
       The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.
    d. Touch **[Close]**.
16. Install Print Drivers on your network or client workstation using the instructions on the following pages.

At your Workstation

1. Select **[Start]**, (**[Settings]**) and then **[Printers]**/**[Printers and Faxes]**.
2. Double-click on the **[Add Printer]** button and click on **[Next]**.
3. The **Add Printer Wizard** displays. Select **[A network printer, or a printer attached to another computer]**.
4. Click on **[Next]**.
5. Select **[Browse for a printer]** (Windows XP) or **[Connect to this Printer...]** (Windows 2003) and click on **[Next]**.
6. Double-click on the name of the **[SMB Host Name]** for the printer as shown on the Configuration Report.
7. Select the **[Printer Share Name]** of the printer as shown on the Configuration Report.
8. Click on **[OK]**.
9. Click on **[Next]**.
10. You will be prompted for a Print Driver. Select **[Have Disk]** and browse to the location of your Print Drivers. Select the relevant Print Driver then click on **[OK]**. Click on **[OK]** again.
11. Select the printer then click on **[Next]**.
12. Enter the printer name or keep the default.
13. To select as the Default Printer click on **[Yes]**.
14. Click on **[Next]**.
15. Click on **[Yes]** to Print a Test Page. Verify that it prints at the machine.
16. Click on **[Finish]**.

Configure the Print Driver - Automatically

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

At your Desktop

1. Select **[Start]**, (**[Control Panel]**) and then **[Printers]**/**[Printers and Faxes]**.
2. Right-click on the appropriate printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Bi-Directional Setup]**.
   If you have given the device a valid IP Address or host name the Print Driver can provide Bi-Directional capabilities. Bi-directional communication automatically updates the Print Driver with the printer's installed options. The driver Printing Preferences will report information about the printer's operational status, active jobs, completed jobs and paper status.
5. Click on **[Automatic]** to have the driver automatically configure the IP Address of the device or click on **[Manual]** and enter the IP Address or host name of the device.
6. If you want to change the default SNMP settings, click on **[SNMP Community Name]** and enter the required information.
7. Click on **[OK]**.
8. Click on the **[General]** tab.
9. Click on **[Print Test Page]**. Close the **Test Page** window if necessary.

10. Click on **[OK]** to close the **Properties** box.
11. Right-click on the printer icon in the Printers folder and select **[Printing Preferences]**.
12. Ensure the **Paper/Output** tab is selected and click the **[More Status]** button at the bottom of the window. Current information about the printer is available. Click on **[Close]** to close the window.
13. For **Default Settings**, select any required default settings in the Print Driver and click on **[OK]**.

Verify the Test Page printed at the machine.

Configure the Print Driver - Manually

To configure the Print Driver without using bi-directional communication return to the **Configuration** tab within the Properties of the Print Driver.

1. Click on **[Installable Options]**.
2. Select the options that are installed on the device.
3. Click on **[OK]**.
4. Click on the **[General]** tab.
5. Click on **[Print Test Page]**.
6. Click on **[OK]** to close the Properties box.
7. Right-click on the printer icon within the Printers folder and select **[Printing Preferences]**.
8. For **Default Settings**, select any required default settings in the Print Driver.

Verify the Test Page printed at the machine.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word cloning in the search tool.

NetBEUI over IP

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational network utilizing the TCP/IP protocol.
- Ensure device is connected to the network with an Ethernet Cable.

At the Machine

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch the **[Network Setup]**.
3. Touch **[Microsoft Networks]**. In the Microsoft (R) Networks screen:
    a. Touch **[Microsoft Enablement]**.
    b. Touch **[Enable]** to enable the Microsoft Network protocols.

   c. For **Transport**, select **[NetBEUI/Ethernet]**. Touch **[Save]** to return to the Microsoft (R) Network screen.

4. Touch **[Workgroup and Host]**. In the **Workgroup and Host** screen:
   a. For **Workgroup Name**, touch detail bar.
   b. Touch **[Clear Text]** to clear the default name, enter Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
   c. Touch **[Save]**, to return to the **Workgroup and Host** screen and repeat for **SMB Host Name**.
   d. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
5. Touch **[Printer Description]**, in the Printer Description screen:
   a. For **Printer Name**, touch detail bar.
   b. Touch **[Clear Text]** to clear the default name, enter description using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
   c. Touch **[Save]**, to return to the **Printer Description** screen and repeat for **Printer Description**.
   d. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
6. Touch **[Connections]**, in the Connections screen:
   a. For **Maximum Connections**, touch the detail box, enter the desired maximum simultaneous connections using the numerical keypad.
   b. For **Connection Timeout**, touch the detail box, enter the desired number of seconds for timeout using the numerical keypad.
   c. Touch **[Save]** to return to the **Microsoft (R) Networks** screen.
7. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools pathway.

   Wait for the device to reboot.
8. Press the **<Machine Status>** button.
   a. Touch **[Machine Information]** tab.
   b. Touch **[Print Reports]**.
   c. Touch **[Print Report]**.
      The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.
   d. Touch **[Close]**.
9. Install Print Drivers on your network or client workstation using the instructions on the following pages.

At your Workstation

1. Select **[Start]**, (**[Settings] (Windows 2000)**) and then **[Printers]**/**[Printers and Faxes]**.
2. Double-click on the **[Add Printer]** button and click on **[Next]**.
3. The **Add Printer Wizard** will appear. Select **[A network printer, or a printer attached to another computer]**.
4. Click on **[Next]**.
5. Select **[Browse for a printer]** (Windows XP) or **[Connect to this Printer...]** (Windows 2003) and click on **[Next]**.
6. Select the plus symbol to the left of **[Entire Network]** to expand it if applicable.

7. Double-click on the name of the **[WorkGroup]** for the device as shown on the Configuration Report.
8. Double-click on the name of the **[SMB Host Name]** for the printer as shown on the Configuration Report.
9. Select the **[Printer Share Name]** of the printer as shown on the Configuration Report.
10. Click on **[OK]**.
11. Click on **[Next]**.
12. You will be prompted for a Print Driver. Select **[Have Disk]** and browse to the location of your Print Drivers. Select the relevant Print Driver then click on **[OK]**.
13. Select the printer then click on **[Next]**.
14. Enter the printer name or keep the default, to select as the Default Printer click on **[Yes]**.
15. Click on **[Yes]** to print a Test Page. Verify that it prints at the machine.
16. Click on **[Finish]**.

Configure the Print Driver

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

At your Desktop

1. Select **[Start]**, (**[Settings] (Windows 2000)**) and then **[Printers]**/**[Printers and Faxes]**.
2. Right-click on the appropriate printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Installable Options]**.
5. Select the options that are installed on the device.
6. Click on **[OK]**.
7. Click on the **[General]** tab.
8. Click on **[Print Test Page]**.
9. Click on **[OK]** to close the Properties box.
10. Right-click on the printer icon within the Printers folder and select **[Printing Preferences]**.
11. For **Default Settings**, select any required default settings in the Print Driver.

Verify the Test Page printed at the machine.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word **cloning** in the search tool.

IP Configuration in a Mac Environment

Apple LPR Printing

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational network utilizing the TCP/IP protocol.
- If you want to use dynamic IP addressing a DHCP, BOOTP or RARP dynamic IP addressing server should be available on the network.
- If you want to use static IP addressing you will need a valid IP Address, subnet mask, gateway address and DNS server address (if necessary) to assign to the device.

Installation via DHCP (Dynamic Host Configuration Protocol)

DHCP is enabled on the device by default. If the device is connected to the network the TCP/IP information will be configured when the device is powered on and no further configuration is required.

Dynamic IP Addressing via DHCP, BOOTP or RARP

If your device is not configured correctly, or if you want to configure the device for BOOTP or RARP, follow these instructions:

At the Machine

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]** button.
4. Touch **[TCP/IP Settings]**.

   Note: All options under the Name/Address section will be grayed out until DHCP is deselected in the Dynamic Addressing section. Follow the next step to disable DHCP and access these options if required.
5. Touch **[Automatic Addressing]**. By default, **DHCP** will be selected. Select **[BOOTP]**.
6. Touch **[Save]**.
7. Touch the **[Close]** button.
8. Touch **[TCP/IP-Line Printer]**. in the **TCP/IP - Line Printer** screen:
   a. Touch **[Enable]**, to enable the option.

b. If you wish to change the LPR port for your device, touch the port number area and enter the desired port number using the numerical keypad.

Note: While you can change the port number at which your machine will accept LPR print jobs it is recommended that you do this ONLY with extreme caution as most LPR spoolers are set to send print jobs to the default port.

c. Touch **[Save]**, then touch **[Close]**.

9. Touch **[HTTP/IPP]**.
   a. Touch **[Enable]**.
   b. Touch **[Save]** to return to the **TCP/IP** screen.

DNS Configuration

1. From the **TCP/IP** screen, touch **[TCP/IP Settings]**.
2. Touch **[DNS Configuration]**, the **DNS Configuration** screen displays.
   This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.

   Note: If DHCP or DHCP Autonet is enabled, the Domain Name, Preferred DNS Server and Alternate DNS Server menu buttons will be grayed out and unselectable, but their feature summaries will be visible. If you need to change the Domain Name select **[Close]** to close the DNS Configuration screen. Select **[Automatic Addressing]** and select **[Disabled]**. Select **[Save]**. Now touch **[DNS Configuration]** button to make the required changes.

   a. Touch the **[Domain Name]** button.
   b. Touch the field under **Domain Name**.
   c. Touch the **[Clear Text]** button to remove the default name before entering the new name using the on-screen keyboard.
   d. Touch **[Save]**.
   e. Touch **[Save]** to return to the **DNS Configuration** screen.
3. Touch **[Preferred DNS Server]**.
   a. Touch each octet under the title and enter the Preferred DNS IP server address using the numerical keypad.
   b. Touch **[Save]**, then touch **[Close]**.
4. Touch **[Alternate DNS Servers]** if required.
   a. Touch the button under **Alternate DNS Server**, enter the Alternate DNS Server IP Address using the on-screen keypad.
   b. Touch **[Save]** to return to the **DNS Configuration** screen.

   Note: If DHCP is enabled, the Alternate DNS server information is not available as a feature summary.
5. To enable **Dynamic DNS Registration**, touch **[Dynamic DNS Registration]**.

   Note: If your DNS server does not support dynamic updates, then this function does not need to be enabled.

   a. Touch **[Enable]**, then **[Save]** to return to the **DNS Configuration** screen.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout**] to exit the Tools pathway.

Static IP Addressing

At the Machine

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[TCP/IP Enablement]**, in the **TCP/IP Enablement** screen
   a. Touch **[Enable]** for **IPv4** and **IPv6**.

   Note: Any changes to the IPv6 feature will result in a reboot of the Network Controller.

   b. Touch **[Save]**.
6. Touch **[Automatic Addressing]**.
   a. Touch **[Disabled]** to disable Automatic Addressing.
   b. Touch **[Save]**.
7. Touch **[IP Address/Host Name]**, the **IP Address/Host Name** screen displays.
   a. For **IPv4 Address**, touch each octet and enter the IP Address using the numerical keypad.
   b. For **Host Name**, touch the **detail** bar.
   c. Enter Host Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
   d. Touch **[Save]**, then touch **[Save]** to return to the **TCP/IP Settings** screen.
8. Touch **[Subnet and Gateway]**, the **Subnet and Gateway** screen displays.
   a. For **IP Gateway**, touch each octet under the title and enter the IP Gateway address using the numerical keypad.
   b. Repeat this process for the **Subnet Mask**. When you are finished, touch **[Save]** to accept the changes and return to the **TCP/IP Settings** screen.
   c. Touch **[Close]** to return to the **TCP/IP** screen.
9. Touch **[HTTP/IP Enablement]**, the **HTTP/IP Enablement** screen displays.
   a. For **Protocol**, ensure **Enable** is selected. If not, touch **[Enable]**.
   b. Touch **[Save]**, then touch **[Close]** to return to the **Tools** pathway.
10. Touch **[TCP/IP-Line Printer]**, on the **TCP/IP - Line Printer** screen displays.
   a. Touch **[Enable]**, to enable the option.
   b. If you wish to change the LPR port for your device, touch the port number area and enter the desired port number using the numerical keypad.

   Note: You can change the port number at which your device will accept LPR print jobs. Do this ONLY with extreme caution as most LPR spoolers are set to send print jobs to the default port of 515.

   c. Touch **[Save]** to return to the **TCP/IP** screen.
   d. Touch **[Close]** to return to the **Tools** pathway.

DNS Configuration

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[DNS Configuration]**, the **DNS Configuration** screen displays.
   This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.
   a. Touch the **[Domain Name]** button.
   b. Touch the bar under **Domain Name**.
   c. Touch the **[Clear Text]** button to remove the default name before entering the new name using the on screen keyboard.
   d. Touch **[Save]**.
   e. Touch **[Save]** to return to the **DNS Configuration** screen.
6. Touch **[Preferred DNS Server]**.
   a. Touch each octet under the title and enter the Preferred DNS IP server address using the numerical keypad.
   b. Touch **[Save]**, then touch **[Close]**.
7. Touch **[Alternate DNS Servers]** if required.
   a. Touch the button under **Alternate DNS Server**, enter the Alternate DNS Server IP Address using the on-screen keypad.
   b. Touch **[Save]** to return to the **DNS Configuration** screen.

   Note: If DHCP is enabled, the Alternate DNS server information is not available as a feature summary.

8. To enable **Dynamic DNS Registration**, touch **[Dynamic DNS Registration]**.

   Note: If your DNS server does not support dynamic updates, then this function does not need to be enabled.

   a. Touch **[Enable]**, then **[Save]** to return to the **DNS Configuration** screen.
9. Press the **<Log In/Out>** button.
10. Touch **[Logout**] to exit the Tools pathway.

Install Print Drivers

Information Checklist

- Ensure TCP/IP settings are correctly configured on the device.
- Locate the Print and Fax Drivers CD delivered with your device.

At your Workstation

1. Load the Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and select the required language, if necessary.
3. Double-click to open the **[Drivers]** folder.
4. Double-click to open the **[Mac]** folder.

5. Double-click to open the folder containing the drivers for your Mac OS version.
6. Double-click to open the **[machine model.dmg]** file.
7. The **Xerox Printer Installer** dialog box appears. Click on **[Continue]**.
   a. Click on **[Continue]** and then **[Agree]** to accept the License Agreement.
   b. Select the volume (if necessary) where you want to install the printer. Click on **[Continue]**.
   c. Click on **[Install]**.
   d. When **Installation Complete** displays, Click on **[Finish]**.
8. Click on the **Printer Setup Utility** on the Dock and go to step 14, or:
9. Double-click on the hard drive icon on the desktop.
10. Double-click to open **[Applications]**.
11. Double-click to open **[Utilities]**.
12. Double-click to open **[Printer Setup Utility]**.
13. Click on the **[Add]** button to add a new printer or click on the **[Printers]** menu and click on **[Add Printer]**.
14. Select **[IP Printing]** from the top menu.
15. Select **[Internet Protocol Printing]** or **[LPD/LPR Printing]** from the next menu.
    a. Enter the IP Address of the printer.
    b. Enter a name for the print queue. (You may leave this blank if you prefer).
    c. Select **[Xerox]** from the **Printer Model** list.
    d. Select your printer model from the **Model Name** list.
    e. Click on **[Add]**. The device will appear in the **Printer List**.
    f. Select the printer and click on the **[Show Info]** button.
16. Click on **[Installable Options]**.
17. Select the options as installed on your device. If you want to use the Save Job for Reprint feature, ensure **Job Storage** is set to **[Installed]**.
18. Click on **[Apply Changes]**.
19. Close the Printer Info box.
20. Print a document to verify that the printer is installed correctly.

You have completed the steps.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word **cloning** in the search tool.

Apple Print Queue

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational AppleTalk® network.
- The AppleTalk Name you wish to assign to your printer.
- The AppleTalk Zone (if used) in which your printer will reside.
- Ethernet Cable.
- The CentreWare Print and Fax Drivers CD (delivered with your machine). Review any README file contained with the Print Drivers.

At the Machine

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[AppleTalk Settings]**. The **AppleTalk (R) Settings** screen displays.
   a. Touch **[AppleTalk (R) Enablement]**.
   b. Touch **[Enable]**.
   c. Touch **[Save]** to return to the **AppleTalk (R) Settings** screen.
   d. Touch **[Name and Area]**.
   e. Touch the text field for **[Printer Name]**. Touch **[Clear Text]** to clear default name (the printer default is * which means the printer will appear in ALL zones) and enter the desired text using the on-screen keyboard. When finished touch **[Save]**.
   f. Repeat previous step for **Area Name**.
   g. Touch **[Save]**.
   h. Touch **[Close]**.
4. Press the **<Log In/Out>** button.
5. Touch **[Logout**] to exit the Tools pathway.

   Wait five minutes for the machine to reboot.
6. Press the **<Machine Status>** button.
   a. Touch **[Machine Information]** tab.
   b. Touch **[Print Reports]**.
   c. Touch **[Print Report]**.
   The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.
   d. Touch **[Close]**.

Install Print Drivers

Information Checklist

- Ensure TCP/IP settings are correctly configured on the device.
- Locate the Print and Fax Drivers CD delivered with your device.

At the Mac

At your Workstation

1. Load the Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and select the required language, if necessary.
3. Double-click to open the **[Drivers]** folder.
4. Double-click to open the **[Mac]** folder.
5. Double-click to open the folder containing the drivers for your Mac OS version.
6. Double-click to open the **[machine model.dmg]** file.
7. The **Xerox Printer Installer** dialog box appears. Click on **[Continue]**.
    a. Click on **[Continue]** and then **[Agree]** to accept the License Agreement.
    b. Select the volume (if necessary) where you want to install the printer. Click on **[Continue]**.
    c. Click on **[Install]**.
    d. When installation Complete displays, click on **[Finish]**.
8. Click on the **Printer Setup Utility** on the Dock and go to step 14, or:
9. Double-click on the hard drive icon on the desktop.
10. Double-click to open **[Applications]**.
11. Double-click to open **[Utilities]**.
12. Double-click to open **[Printer Setup Utility]**.
13. Click on the **[Add]** button to add a new printer or click the **[Printers]** menu and click **[Add Printer]**.
    a. Select **[AppleTalk]** from the menu.
    b. Select the required AppleTalk area from the menu.
    c. Select the print queue from the **Name** list.
    d. Select **[Xerox]** from the **Printer Model** list.
    e. Select your printer model from the **Model Name** list.
    f. Click on **[Add]**. The device will appear in the Printer List.
    g. Select the printer and click on the **[Show Info]** button.
14. Click on **[Installable Options]**.
15. Select the options as installed on your device. If you want to use the Save Job for Reprint feature, ensure **Job Storage** is set to **[Installed]**.
16. Click on **[Apply Changes]**.
17. Close the Printer Info box.
18. Print a document to verify that the printer is installed correctly.

You have completed the steps.

Configuration Cloning

If you are installing multiple machines on your network you may find the Cloning feature useful. This feature allows you to copy configuration settings from one machine to another. For further information enter the word cloning in the search tool.

Network Configuration

This section explains how to set up the device to operate in a Windows TCP/IP environment. The following information is provided:

Note: The device supports IP versions 4 and 6. IPv6 can be used instead of or in addition to IPv4. IPv4 Settings can be configured directly at the device user interface, or remotely, via a web browser using Internet Services. IPv6 can only be configured using Internet Services. To configure TCP/IP Settings using Internet Services, see Configure IP Settings using Internet Services on page 96.

Configure Static IP Address using the Device

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Existing operational network utilizing the TCP/IP protocol.
- Ensure that the device is connected to the network.

- Static IP Address for the device.
- Subnet Mask Address for the device.
- Gateway Address for the device.
- Host Name for the device.
- Ethernet Cable.
- Print and Fax Drivers CD (delivered with your device).

Enter a Static IP Address

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[TCP/IP Enablement]**, the **TCP/IP Enablement** screen displays.
   a. Touch **[Enable]** for **IPv4** and **IPv6**.

   Note: Any changes to the IPv6 feature will result in a reboot of the Network Controller.

   b. Touch **[Save]**.
6. Touch **[Automatic Addressing]**, the **Automatic Addressing** screen displays.
   a. Touch **[Disabled]** to disable Automatic Addressing.
   b. Touch **[Save]**.
7. Touch **[IP Address/Host Name]**, the **IP Address/Host Name** screen displays.
   a. For **IPv4 Address**, touch each octet and enter the IP Address using the numerical keypad.
   b. For **Host Name**, touch **detail** bar.
   c. Enter Host Name using the on-screen keyboard. To access more characters, touch **[123]** on the user interface.
   d. Touch **[Save]**, then touch **[Save]** to return to the **TCP/IP Settings** screen
8. Touch **[Subnet and Gateway]**, the **Subnet and Gateway** screen displays.
   a. For **IP Gateway**, touch each octet under the title and enter IP Gateway address using the numerical keypad.
   b. Repeat this process for the **Subnet Mask**. When you are finished, touch **[Save]** to accept the changes and return to the **TCP/IP Settings** screen.
   c. Touch **[Close]** to return to the **TCP/IP** screen.
9. Touch **[Advanced Settings]**.
10. Touch **[Continue]**.
11. Touch **[HTTP/IP Enablement]**, the **HTTP/IP Enablement** screen displays.
    a. For **Protocol**, ensure **Enable** is selected. If not, touch **[Enable]**.
    b. Touch **[Save]**, then touch **[Close]** to return to the **Tools** pathway.

DNS/DDNS Configuration

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Network Setup]**.
3. Touch **[TCP IP]**.
4. Touch **[TCP/IP Settings]**.
5. Touch **[DNS Configuration]**, the **DNS Configuration** screen displays.

   Note: This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.

   a. Touch the **[Domain Name]** button.
   b. Touch the bar under **Domain Name**.
   c. Touch the **[Clear Text]** button to remove the default name before entering the new name using the on screen keyboard.
   d. Touch **[Save]**.
   e. Touch **[Save]** to return to the **DNS Configuration** screen.
6. Touch **[Preferred DNS Server]**.
   a. Touch each octet under the title and enter the Preferred DNS IP server address using the numerical keypad.
   b. Touch **[Save]**, then touch **[Close]**.
7. Touch **[Alternate DNS Servers]** if required.
   a. Touch the button under **Alternate DNS Server**, enter the Alternate DNS Server IP Address using the on-screen keypad.
   b. Touch **[Save]** to return to the **DNS Configuration** screen.

   Note: If DHCP is enabled, the Alternate DNS server information is not available as a feature summary.

Enable Dynamic DNS Registration

Note: If your DNS server does not support dynamic updates, then this function does not need to be enabled.

8. Touch **[Dynamic DNS Registration]**.
   a. Touch **[Enable]**, then **[Save]** to return to the **DNS Configuration** screen.
9. Press the **<Log In/Out>** button.
10. Touch **[Logout**] to exit the Tools pathway.

Configure Dynamic Addressing

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Existing operational network utilizing the TCP/IP protocol.
- DHCP or BOOTP Server should be available on the network.
- Device must be connected to the network via Ethernet Cable.

Installation via DHCP (Dynamic Host Configuration Protocol)

DHCP is enabled on the device by default. If the device is connected to the network, the TCP/IP information will be configured when the device is powered on and no further configuration is required.

Print a Configuration Report to verify that TCP/IP information is correct.

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.

Installation via BOOTP or DHCP

Ensure your device is connected to the network with Ethernet cabling.

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[TCP IP]**.
3. Touch **[TCP/IP Settings]**.
4. Touch **[Automatic Addressing]**. By default, DHCP is selected.
5. Select one of the following required Dynamic Addressing methods:
   - **BOOTP**
   - **DHCP**
   - **RARP**
6. Touch **[Save]**.
7. Touch **[Close]**.
8. Press the **<Log In/Out>** button.
9. Touch **[Logout**] to exit the Tools pathway.

Configure IP Settings using Internet Services

Note: TCP/IP and HTTP should have been initially configured, refer to Enable TCP/IP and HTTP at the Device on page 19 of this guide.

IPv4

Note: To configure TCP/IP Settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[IP (Internet Protocol)]** in the directory tree, the **IP (Internet Protocol)** page displays.
4. Ensure that **[IPv4]** is selected.
5. In the **General** area:

   a. For **Protocol**, the **[Enabled]** checkbox be enabled.

Note: If the **[Enabled]** checkbox for **Protocol** is not checked, you will not be able to access Internet Services. TCP/IP must then be enabled from the device's user interface.

⚠ **CAUTION:** Disabling TCP/IP or changing the IP address will affect SLP, SNMP, NetBIOS/IP, Raw TCP/IP Printing, SMTP, LDAP, POP3, HTTP and NTP. If TCP/IP is disabled, Internet Services will not be available until TCP/IP is enabled from the device control panel. If you change the IP Address, you must reference the new address within your web browser to locate the device.

   b. **Physical Connection** will display the physical network connection. This will display **“Ethernet”**.

   c. Select one of the following methods for obtaining a Dynamic IP address from the **[IP Address Resolution]** drop-down menu:

   - **DHCP** (Dynamic Host Configuration Protocol).
   - **RARP** (Reverse Address Resolution Protocol).
   - **BOOTP** (Bootstrap Protocol).
   - **STATIC** (fixed, User-defined), this is the default selection.

   d. Enter a name which corresponds to the IP Address of the device in the **[Host Name]** field.

   e. If you select **[Static]**, type the IP Addresses that applies in **[Machine IP Address], [Subnet Mask]**, and **[Gateway Address]** fields.

Note: If **BOOTP** or **DHCP** address resolution mode is selected, you cannot change the IP Address, Subnet Mask, or default gateway. If RARP address resolution mode is selected, you cannot change the IP Address. Select **[Static]** if you wish to disable dynamic addressing.

   f. Enter details of an identifier of the IP site to which the device is connected in the **[Domain Name]** field.

   g. If DNS configuration is required, enter IP Address for the **[Preferred DNS Server]**. Enter an IP Address for **[Alternate DNS Servers 1]** and **[Alternate DNS Servers 2]**.

Note: If DHCP or BOOTP is the IP Address Resolution setting, you cannot change the Domain Name, Primary DNS Server, Alternate DNS Server 1, and Alternate DNS Server 2 settings.

h. For **Dynamic DNS Registration**, check the **[Enabled]** checkbox to enable **Dynamic DNS Registration (DDNS)**.

Note: If your DNS Server does not support dynamic updates there is no need to enable DDNS.

6. In the **DHCP/DDNS** area:

a. For **Release Registration**, check the **[Enabled]** checkbox, ONLY if you wish to release this device's IP Address upon reboot. Default is unchecked.

7. In the **Zero-Configuration Networking** area.

a. For **Self Assigned Address**, check the **[Enabled]** checkbox, to support 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). Refer to the IETF website for zeroconf details.

b. For **Multicast DNS**, check the **[Enabled]** checkbox to resolve host names to IPv4 addresses without using a conventional DNS server.

8. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.

9. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Note: Changing the device IP Address will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. These protocols will need to reference the new IP Address. Disabling TCP/IP will impact other protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. This web user interface will be disabled until TCP/IP is re-enabled from the local user interface.

IPv6

Note: IPv6 is optional. It may be used in addition to, or in place of IPv4.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[IP (Internet Protocol)]** in the directory tree, the **IP (Internet Protocol)** page displays.
4. Ensure that **[IPv6]** is selected.
5. In the **General** area:

a. For **Protocol**, check the **[Enabled]** checkbox to enable the TCP/IP protocol.

Note: If you do not check the **[Enabled]** checkbox for **Protocol,** you will not be able to access Internet Services. TCP/IP must then be enabled from the device's user interface.

Note: If you uncheck the **[Enabled]** checkbox for **[Protocol]**, the Network Controller will reboot. This may require several minutes, during which time all network services will be unavailable.

b. Enter a name which corresponds to the IP Address of the device in the **[Host Name]** field.

c. **[Physical Connection]** will display the physical network connection. This will display **"Ethernet"**.

d. Enter details of an identifier of the IP site in which the device is connected in the **[Domain Name]** field.

6. In the **Stateless Addresses** area:
   a. The **Link-Local Address** is automatically populated.
   This is a network address which is intended only for use in a local data link layer network, and not routed beyond that network. Link-local addresses are often used for network address auto-configuration where no external source of network addressing information is available. The printer's IPv6 Link-local address is automatically generated, and displayed here. Link-local addresses always begin with **"fe80"**.
   b. Check the **[Use Router Supplied Prefixes]** checkbox if router advertisements are used.
   A router-supplied prefix is the 64-bit (sub-) network address. If routers are present, they will periodically send Router Advertisement packets containing address prefixes. These prefixes determine what sort of auto configuration can be done by the device. Select this setting to use Router Supplied Prefixes. When enabled, Global Addresses associated with this device are displayed. If there are no routers on the network, this setting can be disabled.
   c. The **[Global Addresses]** will display any global addresses associated with the device. Global addresses are equivalent to public IPv4 addresses. They are globally routable and reachable on the IPv6 internet.
7. The device performs auto-address DHCP configuration every time it powers up. This is used for neighbour discovery and address resolution on the local IPv6 subnet.
   However, you can choose to use manual configuration, automatic configuration or a combination of automatic and manual configuration.
   Default Dynamic Host Configuration Protocol (DHCP) Settings area:
   a. Select one of the following options:
      - **Use DHCP as directed by a router** - this option is fully automatic. The DHCPv6 Address will be obtained and displayed on the screen.
      - **Always Enable DHCP for address assignment and other configuration data** - this option is fully automatic. The DHCPv6 Address will be obtained and displayed on the screen.
      - **Always Enable DHCP for other configuration data only** - this is the semi-automatic configuration. The DHCPv6 Address will be obtained and displayed on the page.
      - **Never use DHCP** - when this option is selected, you must configure the Manual Address Options and DNS separately.
   b. If you select either **[Use DHCP as directed by a router]** or **[Always Enable DHCP for address assignment and other configuration data]** you have the option to enable the release of DHCPv6 Address at Power Down. This option instructs the printer to send a DHCP release message to the router when the device is powering-down. This releases the current DHCP configuration and discards the printer's IP Address configuration.
   To select this option check the **[Release DHCPv6 Address at Power Down]** checkbox for **DHCPv6 Address**.
8. In the **DNS Configuration** area:
   a. Enter an IP Address for the **[Preferred DNS Server]**. Enter an IP Address for **[Alternate DNS Server 1]** and **[Alternate DNS Server 2]**.
   b. Check the **[Prefer IPv6 Address over IPv4]** checkbox to enable this option.
   By default, the printer will prefer an IPv4 address over IPv6 address if both are enabled. For example, when querying the DNS, the printer will normally use the IPv4 address if an IPv6 address is also provided. By selecting this checkbox, this will change the preference to IPv6.

9. The **Default Gateway** will display the link-local address of the router (known in IPv4 as the default gateway).
10. The device can be configured with up to 4 manual IPv6 addresses, in the **Manual Address Options** area:
    a. Check the **[Enable Manual Address]** checkbox to enable **Router Prefix** attachment.
    b. The **Router Prefix** is derived from router advertisements. Select a router address prefix from the list supplied in the **[Router Prefix]** drop-down menu to populate the prefix for manual entry address.
    c. Click on the **[Add]** button to add your address.
11. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
12. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Configure SLP

Configure Service Location Protocol (SLP) if needed to support CUPS, Mac OS, and NetWare.

SLP is used to announce and look up services on a local network. When SLP is enabled, the device becomes a Service Agent (SA) and announces its services on the network to User Agents (UA), who search for services, using SLP.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SLP]** in the directory tree.
4. In the **General** area:
   a. For **Protocol,** check the **[Enabled]** checkbox to enable Service Location Protocol (SLP).
   b. Enter an IP Address for the **[Directory Agent]**, if required. This will specify the address of a single Directory Agent (DA) to be added to the list of Directory Agents in the device’s DA list.
   c. Enter the required name(s) for **[Scope 1,2,3]**, this allows the System Administrator to set one of the three manually configurable scope names. A scope is a searchable group or container to which an agent may be associated. The default scope is called **“DEFAULT”**.
   d. For **Message Type**, select either **[Multicast]** or **[Broadcast]** from the drop-down menu. This setting defines whether SLP will use multicast or broadcast in communications. Multicast packets are routed between subnets as needed, but broadcast are not.
   e. Enter a value for **Multicast Radius** (0-255), the default is 255. This allows the System Administrator to reconfigure the Multicast Radius for SLP. This is similar to the Time To Live (TTL) in the TCP/IP parameter, and defines how many routers the multicast packet may cross.
   f. Enter a value for **MTU** to set the Maximum Transmission Unit (484 - 32768), with 1400 as the default. This allows the System Administrator to set the maximum packet size for SLP.
   g. **Version** will display the SLP version number supported by the device.
   h. **Port Number** will display the socket (port) that all SLP communications will use. All devices are required to listen on port 427 for UDP and TCP packets.
   i. **Character Set** will display the character set in use. The default is US-ASCII.
5. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Configure FTP

This page allows you to set the File Transfer Protocol (FTP) mode when FTP is selected as the protocol to be used for network filing services. The following features use network filing services:

- **Workflow Scanning**
- **Reprint Saved Jobs**
- **Software Upgrades**

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[FTP]** in the directory tree.
4. In the **Mode** area, select one of the following required modes:
   - **Passive** - this option allows the device to act as an FTP client. The FTP server specifies a random port number to be used for data transport.
   - **Active** - this option allows the device to specify the return port to be used for data transport.

   Note: Some network firewalls may not support Active mode.
5. Click on the **[Apply]** button to accept the changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

SNMP (Simple Network Management Protocol)

The System Administrator uses this page to enable or disable Simple Network Management Protocol (SNMP).

You can also enable or disable Authentication Failure Generic Traps on the device. SNMPv3 can be enabled to create an encrypted channel for secure device management.

SNMP is a set of protocols designed to help manage complex networks. SNMP compliant devices store data about themselves in MIBs and return this data to the SNMP requesters. The SNMP Configuration pages provide control over SNMP security, including methods to configure:

- Administrative and Key User accounts with privacy and authentication protocols and key associated with each account.
- SNMP user account read or read/write access.
- An access control list that limits SNMP access to the printer to specific hosts.

To Configure SNMP v1/v2

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SNMP]** in the directory tree.

   Note: For security purposes, Xerox recommends that the administrator changes the SNMP v1/V2c public/private community strings from their default string names to random string names.

4. In the **SNMP Properties** area:
   a. Check the **[Enable SNMP v1/v2c Protocols]** checkbox to select the protocol, then click on the **[Edit SNMP v1/v2c Properties]** button.
   The System Administrator uses the **Edit SNMP v1/v2c Properties** page to edit the **GET**, **SET**, and **TRAP** community names for the device.
   b. In the **Community Names** area, enter a name in the **[GET Community Name]** field. The default is **public**.
   c. Enter a name in the **[SET Community Name]** field. The default is **private**.

   Note: Changes made to the GET or SET community names for this device will require corresponding GET or SET community name changes for each application which uses the SNMP protocol to communicate with this device (for example, Xerox PrinterMap, Xerox Internet Services, any 3rd party network management applications).

   d. In the **Default Trap Community Name** area, enter a name in the **[TRAP Community Name]** field. The default is **SNMP_trap**.

   Note: The Default TRAP community name is used to specify the default community name for all traps generated by this device. The Default TRAP community name can be overridden by the TRAP community name specified for each individual TRAP destination address. The TRAP community name for one address may not be the same TRAP community name specified for another address.

   e. Click on the **[Save]** button to accept the changes and return to the SNMP page.

5. In the **Authentication Failure Generic Traps** area, check the **[Enable]** checkbox to enable Authentication Failure Generic Traps to generate a trap for every SNMP request by the device which contains an invalid community name.

   Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

6. Click on the **[Apply]** button to save changes, or click on the **[Advanced Settings]** button to add or edit an IP or IPX Address. For further information refer to SNMP Advanced Settings on page 104.
7. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

To configure SNMP v3

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.

   Note: SSL (Secure Socket Layer) must be enabled before you can configure SNMP v3. Click the **[Configure HTTPS]** link on the SNMP Internet Services screen to complete this task. When SSL is enabled, return to the **SNMP** screen.

   Before, enabling the HTTP Security Mode, the device **must** have a Machine Digital Certificate configured. For information on Machine Digital Certificate, refer to Security Certificate Management on page 179.

3. Select **[HTTP]** in the directory tree.
   a. Select enable for the **[Secure HTTP (SSL)]** option.
   b. Change the **[Secure HTTP (SSL) Port Number]** if required. The default is 443.
   c. Click on the **[Apply]** button to accept the changes.
4. Select **[SNMP]** in the directory tree.
5. To configure **SNMP v3**, in the **SNMP Properties** area:
   a. Check to ensure the **[Enable SNMP v3 Protocols]** checkbox is selected.
   b. Click on the **[Edit SNMP v3 Properties]** button.
   System Administrator uses the **Edit SNMP v3 Properties** page to configure Authentication Password and Privacy Password for the Administrator Account.
6. In the **Administrator Account** area:
   a. Check the **[Account Enable]** checkbox to create an administrator account that can be used to provide more extensive access to the objects on the device.
   b. Enter the required data in the **[Authentication Password]** and **[Confirm Authentication Password]** fields.
   c. Enter the required data in the **[Privacy Password]** and **[Confirm Privacy Password]** field.
7. In the **Print Drivers/Remote Clients Account** area:
   a. Check the **[Account Enabled]** checkbox to Create an account for bi-directional Print Drivers and Xerox remote clients.

b. If you want to reset to the default Password, click on the **[Reset]** button.

Note: This account allows Xerox Clients and Drivers a limited amount of access to objects on the device. If the device does not have SNMP v1/v2c enabled, and does not have this account enabled, Xerox SNMP based clients will not be able to communicate with it. The default passwords should be used, unless the passwords have been changed on the client.

c. Click on the **[Save]** button to save changes and return to the SNMP page.

8. In the **Authentication Failure Generic Traps** area:

   a. Check the **[Enable]** checkbox to enable Authentication Failure Generic Traps to generate a trap for every SNMP request by the device which contains an invalid community name.

   Note: When the Authentication Failure Generic Trap is enabled, this machine will generate a trap for every SNMP request that is received by the machine which contains an invalid community name.

9. Click on the **[Apply]** button to save changes, or click on the **[Advanced Settings]** button to add or edit an IP or IPX Address. For further information refer to SNMP Advanced Settings on page 104.
10. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

SNMP Advanced Settings

To Add or Edit an IP Address:

The System Administrator can add or delete IP and IPX Addresses for the Network Management Workstations that receive Traps from the device.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SNMP]** in the directory tree.
4. From the **SNMP** page, click on the **[Advanced Settings]** button.
5. To add or edit an IP Address, in the **Trap Destination Addresses** area, click on the **[Add IP Address]** button or the **[Edit]** button for the required address.
6. In the **Required Information** area:
   a. For **[IP Address]**, enter the IP destination address of the SNMP manager that you are setting up to receive traps for.
   b. For **[UDP Port Number],** enter port number for the UDP destination port of the SNMP manager that you are setting up to receive traps for.
   c. For **[SNMP Version]**, select the SNMP version that matches the SNMP manager with which the device is communicating with.
7. In the **Traps** area:
   a. The **[TRAP Community Name]** will display the default value for the TRAP Community Name.
   b. For **[Traps to be Received]**, check the checkbox for the type of traps sent by this device to the Destination Address indicated by the IP Address and UDP port number entered by the user. The choices are:

- **Printer Traps**
- **Job Monitoring Traps**
- **Cold Start Generic Traps**
- **Warm Start Generic Traps**
- **Authentication Failure Generic Traps (Status: Enabled)**

Note: When **Authentication Failure Generic Traps** is disabled, traps of this type will not be sent by this device. To enable Authentication Failure Generic Traps, go to **SNMP Properties** from the main **SNMP Configuration** page.

8. Click on the **[Save]** button to save settings and return to the **Advanced Settings** page.
9. Click on the **[Back]** button to return to the **SNMP** page.
10. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
11. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

To Add or Edit an IPX Address:

The System Administrator uses this page to add or edit an Internetwork Packet Exchange (IPX) trap destination address for this printer. IPX is a routing protocol used in Novell NetWare environments. Default values are shown when adding an address.

1. From the **SNMP** page, click on the **[Advanced Settings]** button.
2. To add an IPX Address or edit, in the **Trap Destination Addresses** area, click on the **[Add IPX Address]** button or the **[Edit]** button for the required address.
3. In the **Required Information** area:
   a. For **[IPX External Network Number]**, enter the IPX number of the device that is set to receive traps.
   b. For **[Physical MAC Address]**, enter the MAC address of the printer that is receiving the trap.
   c. For **[IPX Socket Number]**, enter the socket number of the running application that is listening for the information.
   d. For **[SNMP Version]**, select the SNMP version that matches the SNMP manager with which the device is communicating.
4. In the **Traps** area:
   a. The **[TRAP Community Name]** will display the default value for the TRAP Community Name.
   b. For **[Traps to be Received]**, check the checkbox for the type of traps sent by this device to the Destination Address indicated by the IP Address and UDP port number entered by the user. The choices are:
      - **Printer Traps**
      - **Job Monitoring Traps**
      - **Cold Start Generic Traps**
      - **Warm Start Generic Traps**

- **Authentication Failure Generic Traps (Status: Enabled)**

Note: When **Authentication Failure Generic Traps** is disabled, traps of this type will not be sent by this Device. To enable Authentication Failure Generic Traps, go to **SNMP Properties** from the main **SNMP Configuration** page.

5. Click on the **[Save]** button to save settings and return to the **Advanced Settings** page.
6. Click on the **[Back]** button to return to the **SNMP** page.
7. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
8. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

SSDP (Simple Service Discovery Protocol)

Allows you to configure the SSDP (Simple Service Discovery Protocol) for Universal Plug and Play settings on the device. SSDP provides a mechanism where by network clients, with little or no static configuration, can discover network services. SSDP accomplishes this by providing for multicast discovery support as well as server based notification and discovery routing.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SSDP]** in the directory tree.
4. In the **[General]** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable SSDP.
   b. Enter the discovery expiration Cache Control in minutes in the **[Cache Control]** field. The range is from 1 to 43200 and default is 1440.
   c. Enter the discovery advertisement Time to Live, measured in router hops in the **[Time to Live]** field. the range is from 1 to 60 and the default is 4.
5. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Microsoft Networking

Configure Microsoft Networking

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[Microsoft Networking]** in the directory tree.
4. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable Microsoft Networking.
   b. Enter the device workgroup in the **[Workgroup]** field.
   c. Enter the device SMB (Server Message Block protocol) host name in the **[SMB Host Name]** field.
   d. Enter a descriptive host name comment in the **[SMB Host Name Comment]** field (if required).
   e. Enter the device share name in the **[Share Name]** field.
   f. Enter a descriptive share name comment in the **[Share Name Comment]** field.

   Physical Connection displays the physical network connection, and will display **"Ethernet"**.

   Transport displays the current transport layer protocol, and will display **"TCP/IP"**.

   g. Enter the maximum number of simultaneous connections the server is allowed in the **[Maximum Connections]** field. The range is 10 - 30, and the default is 30.
   h. Enter the timeout value for outgoing connection attempts in the **[Connection Timeout]** field. The range is 1 - 32767 seconds, and the default is 600 seconds.
5. If you do not need to configure WINS, then click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Configure WINS (if used)

When running WINS the device registers its IP Address and NetBIOS Hostname with a WINS server. WINS allow the device to communicate using hostname only, removing a significant overhead from the Systems Administrators.

WINS server address is stored in the file:
/smart/etc/wins.name

It is possible to manually enable WINS and configure primary and secondary WINS servers through Internet Services.

1. In the **Microsoft Networking** page, scroll down to the **WINS** section.
2. In the **Server Information** area for **WINS**:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable WINS.
   b. Enter the IP Address in the **[Primary Server IP Address]** of a Primary Server.

c. Enter the IP Address in the **[Secondary Server IP Address]** of a Secondary Server.

Note: If DHCP is configured, WINS IP Address(es) will be overridden.

Note: WINS may be used for Address Resolution in addition to DNS. Microsoft Networking needs to be enabled for the device to register services with WINS.

3. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
4. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

LPR/LPD

This page allows the System Administrator to select and edit LPR/LPD (Line Printer Remote/Line Printer Daemon) options. LPR/LPD is a common TCP/IP printing protocol in Unix environment to establish connections between the device and the workstations on a network.

Note: TCP/IP and HTTP should have been initially configured, refer to Enable TCP/IP and HTTP at the Device on page 19 of this guide and follow the steps provided.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[LPR/LPD]** in the directory tree.
4. In the **General** area:
    a. For **Protocol**, check the **[Enabled]** checkbox to enable LPR/LPD.

    Note: Disabling LPR/LPD will affect clients printing to the device over TCP/IP using the LPR printing port.

    b. **Physical Connection** displays the physical network connection, this will always display **"Ethernet"**.

    c. In the **Port Number**, enter an LPR/LPD port number. The default is 515.
5. In the **Advanced Settings** area:
    a. For **PDL Switching**, check the **[Enabled]** checkbox to enable **PDL Switching**.
    PDL switching allows the device to process print jobs which contain two or more printer languages, for example: PCL and PostScript, or ASCII and PostScript.

    b. For **PDL banner page attributes override LPR control file attributes for job name and owner**, check the **[Enabled]** checkbox to enable this option. This feature allows you to replace the standard information displayed on a banner page, and substitute the user name and job name taken from the print job.

    Note: Banner pages print if banners are set to **On** at the file server, even if banners are set to **Off** in the device.

    c. Select the required option from the **[Place temporary hold on which jobs:]** drop-down menu. This feature allows you to set the device to hold certain jobs before printing, until the complete job is received. This delay helps to ensure that the banner page information prints correctly. Some banner sheet information is contained in the job's control file which may not always be the first part of a print job the device receives. The following options are available:
    - **None (Use printer's default banner sheet job name if data file 1st)** - The device will not wait to receive the job control information. This selection may cause banner sheet information to print incorrectly.
    - **All (consistent with older implementations)** - This option puts all jobs on hold. All data is received before a job begins to print. This setting can cause jobs to print slowly but will result in accurate banner sheet information.
    - **Only those with data file received 1st** - The device holds the job if the job's data file is received first. This ensures the device waits to receive the job's control file information so that the banner sheet contains accurate information.

6. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
7. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Raw TCP/IP Printing

Note: TCP/IP must be enabled before Raw TCP/IP Printing is enabled.

Raw TCP/IP is a printing method used to open a TCP socket-level connection, over Port 9100, to stream a print-ready file to the printer's input buffer, and then to close the connection after sensing an End Of Job indicator in the Page Description Language, or after expiration of a preset timeout value. Port 9100 printing does not require a Line Printer Request (LPR) from the workstation, or the use of a Line Printer Daemon (LPD) running on the printer. Raw TCP/IP printing is selected in Windows 2000 as the Standard TCP/IP port.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[Raw TCP/IP Printing]** in the directory tree, the **Raw TCP/IP Printing** page displays.
4. In the **General** area:
   a. For **Protocol,** check the **[Enabled]** checkbox to enable Raw TCP/IP Printing. **Physical Connection** displays the physical network connection, this will always display **"Ethernet"**.
5. Up to three ports may be enabled and configured, in the **Port Information** area:
   a. For **Port 1** Leave the **TCP Port Number** set to 9100. If two additional ports are available, click on the **[Default All]** button to check if they are set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
   b. Leave the **Bidirectional** (**[Enabled]**) checkboxes and **Maximum Connections per Port** settings at their default values.
   c. Set the **[End of Job Timeout]** to the number of seconds to wait before processing a job without an End Of Job indicator. The range is from 1 to 65535, and the default is 300.
   d. Leave the **PDL Switching** (**[Enabled]**) checkbox at its default value.

   Note: Do not check the **[Enabled]** checkbox for **PDL Switching**, when Windows clients print is using port 9100. this prevents each print job from generating a banner page.
6. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
7. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   To add additional options, from the **Raw TCP/IP Printing** screen, click on the **[Advanced]** button.
8. In the **Connections** area:
   a. For **Maximum Concurrent Connections per Port (1-32)**, enter a value between 1 and 32 to specify the maximum number of concurrent connection allowed.
   b. For **Maximum Concurrent Jobs per Connection (0-500)**, enter a value between 0 and 500 to specify the maximum number of concurrent jobs per connection allowed.
   c. For **Total Job Limit per Connection (0 - 32768)**, enter the required job limit that can be active per port between 1 and 32768. This setting limits the total number of jobs accepted on a single connection. After the limit is reached and all jobs complete printing, port 9100 loses the connection.

9. In the **Job Boundary Determination** area:
   a. For **End of Job Timeout**, enter the required time between 0 and 1800, for the device to wait for the data received through the port before terminating the job.
   b. For **Control D Marks End of PostScript Job**, check the **[Enabled]** checkbox, when enabled, the "Ctrl-d" character indicates the end of a PostScript print job.
10. In the **Backchannel Data** area:
    a. For **Backchannel Data Transmission to Client**, check the **[Enabled]** checkbox to allow backchannel information to transmit back to the client, such as PDL interpreter and PJL status messages.
    b. For **Out of Order Backchannel Data**, check the **[Enabled]** checkbox to allow bidirectional information from multiple print jobs to return to the client out of order. This option also ensures communication between the printer and client.
11. In the **Banner Page Printing** area:
    a. For **Banner Page Enabled**, from the drop-down menu, select one of the following to allow banner sheets to print:
       - **No Jobs**
       - **First Jobs Only**
       - **All Jobs**

    b. If required, for **Banner Page for Each Document of Job**, check the **[Enabled]** checkbox to generate a banner page for each document in a job. This only applies to PDL switched PJL jobs. When disabled, banner sheet is printed for the first document only.
    c. For **Banner Page for Job Containing only PJL Commands**, check the **[Enabled]** checkbox, to allow banner pages to print only for jobs that are specifically requested through PJL commands.
12. In the **Miscellaneous** area:
    a. For **Language (PDL) Switching within PJL Job**, check the **[Enabled]** checkbox to allow the port to handle PJL print jobs consisting of more than one language, for example PCL and PostScript. Each language is spooled as a separate document which creates a multiple document job.
    b. If required, for **Job Data Parsing Override**, check the **[Enabled]** checkbox to force the parsing job data. Job data is not parsed when bidirectional and PDL switching are disabled.
13. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
14. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

SMTP (Simple Mail Transfer Protocol)

The SMTP (Simple Mail Transfer Protocol) page allows you to configure this option, This is required for E-mail and Internet Fax features. E-mail and Internet Fax features use the same SMTP information for outgoing jobs.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click the **[Connectivity]** link.

2. Click on the **[Protocols]** link.
3. Select **[SMTP Server]** in the directory tree.
   a. In the **Required Information** area, select one of the following:
      - **Use DNS (to identify SMTP Server)** - Use this to allow the DNS to automatically find an IP address of the mail server.
      - **Specify SMTP Server Manually** - Select this option to map to a specific SMTP server.

   a. If you select **Specify SMTP Server Manually**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**. Enter the **[IP Address]**and **[Port]**, or the **[Host Name]** and **[Port]** of the SMTP Server.

   b. Enter a valid e-mail address in the **[WorkCentre E-mail Address]** field (matching the account set up on the SMTP Server) which the device will use as a default E-mail From and Reply To address.
4. In the **Optional Information** area:
   a. Enter the maximum allowable size for an e-mail with an attachment in the **[Maximum Message Size (Message and Attachment]** field. The range is from 512Kb to 20480 Kb.

   b. Enter the allowable number of fragments in the **[Number of Fragments]** field. The range is from 1 to 500; the default is 1.

   c. Enter allowable size to control the size of e-mail jobs sent to the SMTP server in the **[Total Job Size]** field. The range is from 512Kb to 2,000,000Kb (2Gb); the default is 512Kb.

   d. For **[Login Credentials for the WorkCentre to Access the SMTP Server to send automated emails]**, select one of the following authentication method that the printer will use to access the SMTP server for any automated e-mail messages that it sends for notification or confirmation:
      - **None** - if no authentication is required.
      - **System** - Select this option to have the printer authenticate itself using the credentials you provide for the Login Name and Password.
        Enter details for the SMTP server account in the **[Login Name]**, **[Password]** and **[Retype Password]** fields.
        Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

   e. For **Login Credentials for the Walkup User to send Scanned E-mails**, select how walkup users can be authenticated by the SMTP server. Users can be prompted to log in or users can be authenticated using the system credential specified on the SMTP Server configuration screen, select one of the following:
      - **Authenticated User** - when selected the device will prompt to log in using their own network credentials.
      - **Same as Automated E-mails:** - when selected, each user will need to enter the system credentials specified on the SMTP Server configuration screen.
5. Click on the **[Apply]** button to implement any changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

LDAP

Note: LDAP support is only available on the device. Configuration of the LDAP directory settings requires the network to support LDAP services.

LDAP (Lightweight Directory Access Protocol) is a popular protocol used by large accounts to access large quantities of data including corporate address books. The local system will need to know where the LDAP server is located on the network and may need a login name and password if the LDAP server is not configured to allow NULL names and passwords.

The Internet Services **LDAP** page allows you to configure Lightweight Directory Access Protocol information.

LDAP is used for the following activities:

- To access the corporate address book to locate e-mail addresses for use with the E-mail and Internet Fax services.
- To authenticate users when configured as the method of Authentication.
- To authorize users to gain access to device features, when configured as the method of Authorization.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the E-mail feature is functional on the device and your network supports LDAP services.
- Obtain the IP Address (or Host Name) of your LDAP Server. The device may also need a login name and password if the LDAP server is not configured to allow NULL names and passwords.
- Use an LDAP client to validate your settings before inputting them into the Internet Services menus. LDAP clients include Microsoft Outlook Express, Microsoft Outlook and Netscape Communicator.
- To use host names, DNS must be configured on the device.

To Configure LDAP Server

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[LDAP]** in the directory tree, the LDAP page displays.
4. To add a new LDAP directory, click on the **[Add New]** button.
5. In **Server Information** area:
   a. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
   b. Enter details in the **[Friendly Name]** field.
   c. Enter the **IP Address** and **Port** or the **Host Name** and **Port** of the Primary and Backup LDAP Server.

d. Select the server type from the **[LDAP Server]** drop-down menu.

6. In the **Optional Information** area:
   a. Enter the search directory location of the server where the LDAP information is stored in the **[Search Directory Root]** field.
   b. For **Login Credentials to Access LDAP Server**, select one of the following:
      - **None** - If no login is required.
      - **Authenticated User** - The device will use the login details entered by the user to access the LDAP server. This option requires Authentication to be configured on the device.
      - **System** - If selected the device will specify the LDAP server login details and enter the required information in the **[Login Name]** and **[Password]** fields. Format for the login name may be login name or domain/login name.
   c. **Enter a Login Name** and **Password**, if required, for the device to access the LDAP server. Format for the login name may be login name or domain/login name.
   d. For **SSL**, check the following checkbox:
      - **Enable SSL** - To enable SSL (Secure Socket Layer).

   Note: SSL requires a server certificate to be available to the device.

      - **Validate Repository SSL Certificate** - If you want the device to verify that the server certificate is trusted, valid and has a fully qualified domain name (FQDN).
   e. Click on the **[View Trusted SSL Certificates]** link to view secure certificates that have been uploaded to the device. (Click the browser **[Back]** button to return to the LDAP Settings screen).
   f. For **Maximum Number of Search Results** select either **[Use LDAP Server Maximum]** or **[Maximum Number of Search Results]**. If you select the latter, enter the maximum number of addresses that will appear which match the search criteria selected by the user. Set the search results to one less than the server will allow. For example, if the LDAP server limit is 75, set the search results to 74 or less. The range is between 5 and 100.
   g. **Search Timeout:** There are two options. You can let the server use its timeout limit by selecting the **[Use LDAP Server Timeout]**, or select **[Wait]** and specify how many seconds the search should last (between 5 and 100). If the search takes longer than the time specified in the **[Wait... seconds]** box the user will be notified that the search failed.
   h. For **LDAP Referrals**, check the **[Enabled]** checkbox if the primary LDAP server is connected to additional servers, the search will continue on those servers as well.
   i. The **Perform Query on** option will help control the returns by allowing the LDAP query to be either on **[Mapped Name Field]** or **[Surname and Given Name Fields]**. Netscape and Lotus Domino will typically require a setting of Surname to allow returns of “lastname, firstname”.
7. Click on the **[Save]** button to implement the changes.

To Figure Contexts for LDAP

1. From the **LDAP** screen, click on the **[Contexts]** tab under the LDAP title at the top of the screen.

   Contexts are used with the Authentication feature. Contexts speeds up searching through the LDAP tree by specifying where to look in the tree. The administrator can configure the device to automatically add an authentication context to the Login Name provided by a user.

2. Enter the default login information in the **[Default Login Context]** field, this is the first context that will be searched.

   Note: The word LDAP should appear in the login context, for example, cn=LDAP, o=xerox, c=us.

3. Click on the **[Apply]** button.

To Define User Mappings

Fields contained within LDAP structures are not standardized. This section allows you to find out what results you will get when searching for a name using one of the LDAP servers. Editing the mapping will give some control over your LDAP server results, therefore improving name searches for the user.

To map the LDAP fields:

1. From the **LDAP** screen, click on the **[User Mappings]** tab under the LDAP title at the top of the screen.
   a. The **Server Information** area will display a summary of the LDAP server settings assigned in the **LDAP Server** screen.
   b. In the **Search** area, enter details in the **[Enter Name]** field and click on the **[Search]** button this lets you test the LDAP name search and field matching capability.
   c. The information about this user is then displayed against the fields shown on the device. By using the drop-down menu under **Imported Heading** boxes re-map any fields you require against the device properties.

   Note: Internet Fax users should ensure that the **Internet Fax** field is NOT set to **"No Mappings Available"** in the drop-down menu. This setting will prevent the LDAP Address Book appearing on the Internet Fax screen at the device. Select the field that contains the Internet Fax addresses, in many cases, there is no unique Internet Fax address, therefore, a regular e-mail address is used.

2. When you have finished making your selections click on the **[Save]** button.

At the Device:

1. Select the **[E-mail]** or **[Internet Fax]** icon, then touch **[OK]**. It may be necessary to press the **<Services Home>** button.
2. Touch the **[To]** button.
3. Enter a name which corresponds with an entry in your company's e-mail address list, using the on-screen keyboard touch screen, for example: *lastname*, *firstname*.
4. Touch **[Enter]**. The **Search Results** screen displays.
5. Select the required name from the list (if there is more than one match).
6. Touch the **[Add]:** button to select the name as a recipient for your e-mail.
7. Touch **[Done]**. The e-mail address will appear in the Address List.
8. Place a document to e-mail in the document handler and press the green start button.
9. Verify that the recipient received the scanned document in his/her e-mail inbox.

To Configure Authorization 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, (LDAP server will find members nested down five levels of a group. For example, if LDAP searches for a user within the Admin Group, it may not find that user, but may find another group. It will also look for the user in that group as well and so on). If the LDAP server confirms that the user is a member of the 'Admin' group, the user will have administrator access to the device.

There are three ways to configure access to various group accounts:

- **User Roles**
- **Device Access**
- **Service Access**

Setup User Role Access At Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.
2. Select the **[User Roles]** tab. Use this tab to define the access groups that are authorized for the following roles:
   - For the **System Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with System Administrator access to the device.
   - In the **Accounting Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with accounting administrator access to the device.
3. To verify either group, enter the name of one of the members of the LDAP server group in the **[User Name box]**, then click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist.

   Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When no access group is listed, all members will have access.
4. When done, click on the **[Close]** button.

Setup Device Access at Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.
2. Select the **[Device Access]** tab.
   a. For **Services Pathway [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with Service access to the device.
   b. Repeat the process for **Job Status Pathway** and **Machine Status Pathway**.

c. To verify any of these groups, enter a name of one of the members of the LDAP server groups in the **[Enter User Name]** field, then click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When two or more groups are entered, they must be separated by commas. When no access group is listed, all members will have access

d. When done, click on the **[Close]** button.

Setup Service Access at Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.
2. Select the **[Service Access]** tab, use this tab to define the groups that are authorized to access various device functions and services.
   a. Enter the names of LDAP groups, as required in the **Access Group** field, to allow access to individual device services.

Note: By default everybody has access to all of the services on the device. By entering a group name in any of the services, access is then restricted to those users belonging to that group.

b. Verify each group by entering a group user in the **Enter User Name** field, and click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When no access group is listed, all members will have access.

c. When done, click on the **[Close]**.

Configure Custom Filters

This feature allows the System Administrator to specify custom filter information for LDAP servers. These filters, for example, allow you to filter out non-users such as machines.

1. From the **LDAP** screen, click on the **[Custom Filters]** tab under the LDAP title at the top of the screen.
2. In the **LDAP Authentication** area, check the **[Append base DN]** checkbox to enable. This will specify the distinguished name(s) that will lead to the entry in the LDAP directory under which all users and groups will be retrieved. Distinguished name is a unique name for an entry in your LDAP directory. For example: cn=USERID, o=xerox, c=us.

   Note: Many UNIX/Linux LDAP servers require this attribute to be set and is used frequently when **Login Credentials to Access LDAP Server** is set to **[Authenticated User]**.

3. In the **Email Address Book Filter** area:
   a. Check the **[Enable Custom Filter]** checkbox.

b. In the field 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 parentheses. 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.

4. In the **User ID Query Filter** area:
    a. Check the **[Enable Custom Filter]** checkbox.
    b. In the field 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 attributes placed inside parentheses. For example, to find the user with a sAMAccountName of Bob, type (objectClass=user) (sAMAccountName=Bob). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.
5. Click on the **[Apply]** button to implement any changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Configure POP3 Setup

The POP3 (Post Office Protocol version 3) allows retrieval of mail with the Internet Fax feature from remote servers over TCP/IP on network port 110. Internet Fax must be installed on your device to access POP3 information.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[POP3]** in the directory tree.
4. In the **Server Information** area:
    a. Select either **[IPv4 Address]** or **[Host Name]**. Enter the **[IP Address]** and **[Port]**, or the **[Host Name]** and **[Port]** of the POP3 server. The default port number is 110.
    b. Enter the username of the account on the POP3 server in the **[Login Name]** field.
    c. Enter a password for the username in the **[Password]** field.
    d. Enter the password in the **[Retype password]** field.
    e. Check the **[Select to save new password]** checkbox.
5. In the **POP3 Settings** area:
    a. Check the **[Enable receipt of E-mail via POP3]** checkbox to allow the device to check the POP3 server and retrieve the e-mail receipt.
    b. Type in the e-mail server polling interval in minutes in the **[Polling Interval]** field. The range is from 1 to 60, and the default is 15.
6. Click on the **[Apply]** button to implement any changes.
7. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Configure HTTP

Hyper text transfer protocol, **HTTP** is a protocol (utilizing TCP) to transfer hypertext requests and information between clients and servers.

Enable HTTP at the Device

By default HTTP is enabled. If disabled, you will need to enable it at the device before accessing Internet Services.

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch the **[Network Setup]** button.
3. Touch **[TCP IP]**.
4. From the **TCP/IP** screen, touch **[HTTP/IPP Enablement]**.
   a. For **Protocol** touch **[Enable]**.
   b. Touch **[Save]**, to return to the TCP/IP screen.
   c. Touch **[Close]**.

Configure HTTP at your Workstation

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[HTTP]** in the directory tree.
4. In the **Configuration** area:
   a. For **[Connection]**, if required change the HTTP Port Number. The default is 80.
   b. The **Keep Alive Timeout** setting determines how long the device's Internet Services pages will wait for a response from a connected user before terminating the connection. Enter the required number of seconds (1 - 60) in the **[Keep Alive Timeout]** field.

   Note: Generally, user connections will be adversely affected (slow or kept busy) if the Keep Alive Timeout is set for a longer period of time.

   Maximum Connections displays the maximum number of simultaneous connections that can occur at any given moment to the web server.

   Note: In order for the device to operate in Secure HTTP (or HTTPS/SSL) mode, the device must possess a correctly configured Machine Digital Certificate. For information on Machine Digital Certificate, refer to Security Certificate Management on page 179.

   c. For **Secure HTTP (SSL)**, select **[Enabled]** to set the HTTP Security Mode.
   d. Change the **Port Number** if required. The default is 443.
   e. Click on the **[Apply]** button to accept the changes.

Proxy Server

A proxy server is a server that acts as a go-between for requests from clients seeking resources from other servers.

A client connects to the proxy server and requests service. The proxy server filters the request against its filtering rules and if it meets the rule it allows the connection.

A proxy server has two purposes:

- For security, keeps the device behind it anonymous.
- Speeds up access to a resource (via caching). It is commonly used to cache web pages from a web server.

The **Internet Services Proxy Server** page allows you to enter the address of the Proxy Server which the device can use. If your network does not use a proxy server you do not need to enable the proxy server setting.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[Proxy Server]** in the directory tree.
4. In the **HTTP Proxy Server** area:
   a. Check the **[Enabled]** checkbox to enable the protocol.
   b. Select either **[IPv4 Address]**, **[IPv6]** or **[Host Name]**.
   c. Enter either the IP Address and Port or Host Name and Port in the **[IP Address: Port]** or **[Host Name: Port]**. The default port number is 8080.
5. Click on the **[Apply]** button to implement any changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

NTP

NTP (Network Time Protocol) is used to set the date and time of the system at start and every subsequent 24 hour period, as well as any time the NTP parameters are modified. This feature ensures that the device's time stays synchronized with the NTP server specified.

If the device is configured to use DHCP, an NTP server, or the GMT offset is provided by the DHCP server, then the data entered here will be overwritten by the corresponding DHCP retrieved items.

> Note: Enabling NTP or modifying NTP settings will cause a system reset.

At Your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[NTP]** in the directory tree.
4. In the **Offset of Local Time Zone** area:
   a. From the drop-down menu, select the **[Offset of Greenwich Mean Time]** value. The default is 0.0 (Greenwich Mean Time).
5. In the **Network Time Protocol** area:
   a. For **NTP Enabled**, check the **[Enabled]** checkbox to enable the protocol.
   b. Select either **[IPv4 Address]** or **[Host Name]**.
   c. Enter details in the **[IP Address: Port]** or **[Host Name: Port]** field. The default port number is 123.
   d. Enter details in the **[Backup IP Address: Port]** or **[Backup Host Name: Port]** field.
6. Click on the **[Apply]** button to implement any changes.
7. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

WSD

WSD (Web Services for Devices) is a technology from Microsoft, which provides a standard method for discovering and using network connected devices, and is supported in Windows Vista and Windows Server 2008 environments. WSD is one of the several supported communication protocols.

WSD (Web Services for Devices) specifies a lightweight subset of the overall Web services protocol suite that is appropriate for network-connected devices. The device profile prescribes how to use elements of core Web services specifications to enable these functions.

Enabling WSD at Your Workstation

Note: To configure this feature or setting access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[WSD (Web Services for Devices]** in the directory tree.
4. In the **WSD Services** area, check the **[Enabled]** checkbox to enable the protocol.
5. Click on the **[Apply]** button to implement any changes.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Apple Talk

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational AppleTalk network with Macintosh workstation computers equipped with Ethernet network interface cards.
- The AppleTalk Name you wish to assign to your printer.
- The AppleTalk Zone (if used) in which your printer will reside.
- Ethernet Cable.
- The Internet Services Print and Fax Drivers CD (delivered with your device). Review any README file contained with the Print Drivers.

Enabling AppleTalk on the device

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[AppleTalk]** in the directory tree.
4. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable the AppleTalk.
   b. Type a name for the device in **[Printer Name]**. The default name is based on the device Ethernet MAC address.
   c. Enter details in the **[Zone Name]** filed. An AppleTalk zone is a logical group of nodes or networks. Zones are assigned according to a logical scheme such as organizational departments or physical locations.

   Note: The default local zone is identified as “*”. This should only be changed if you have defined zones on your network.

   d. **Physical Connection** displays physical network connection. This will display **“Ethernet”**.
   e. **Printer Type** displays the current assigned printer type. This will display **“LaserWriter”**.
5. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

NetWare

NetWare is a network operating systems developed by Novell that supports DOS, Windows, OS/2 and Mac. NetWare is the most widely-used LAN control program. It is a stand-alone operating system that runs in the server.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An existing operational NetWare network.
- Login to a NetWare file server/tree as Supervisor/Administrator or have the equivalent privileges.
- Ensure the device is connected to the network via Ethernet cable.
- Set up a print server object using NWADMIN. Refer to the documentation supplied by Novell to complete this task. Record precisely (observe upper and lower case, dot notation) the NDS Tree, NDS Context Name, frame type, Print Server Name and the Print Server password assigned. If your printer services queues on multiple file servers, the Print Server name and password must be the same on all file servers.

Configure NetWare Settings

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[NetWare]** in the directory tree.
4. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable NetWare protocol.
   b. If FIPS 140-2 encryption is enabled on the device a widow is displayed requesting that you acknowledge that Netware is not FIPS compliant. Click the **[Confirm]** button to continue.
   c. Select the required **[Filing Transport]** from the drop-down menu.
   d. Select the required **[Frame Type]** from the drop-down menu. Selections for the frame type are dependent upon the Physical Connection.
   e. For **[Queue Poll Interval]**, enter the queue poll interval in seconds. The range is from 1 - 240 seconds, and the default is 5.
   f. **Physical Connection** displays physical network connection. This will display **"Ethernet"**.
   g. **External IPX Number** displays the current IPX number.
   h. Enter the NetWare logical name associated with the device in the **[Printer Server Name]** field. The default name is based on the Ethernet MAC address.
   i. Enter the print server password in the **[New Print Server Password]** field, then re-enter it in the **[Retype New Print Server Password]** field.
   j. Check the **[Select to save new password]** checkbox.

5. In the **Service Advertising Protocol (SAP)** area:
   a. For **Protocol**, check the **[Enabled]** checkbox if you wish to enable SAP protocol.
   SAP is used to inform other network devices about the device's available services. If SAP is disabled, the device will not send out periodic SAP broadcast messages
   b. Set the SAP periodic broadcast frequency in the **[SAP Frequency]** field. The range is from 15 - 300 seconds, or enter 0 for none. The default is 60.

   SAP allows service-providing nodes, such as file servers, print servers, gateway servers and application servers to advertise their services and addresses. The Service Advertising Protocol (SAP) is included in the Internetwork Packet Exchange (IPX) protocol. SAP makes the process of adding and removing services on an IPX internetwork dynamic.
6. In the **Bindery Settings** area, if using NetWare in Bindery mode (when NDS tree and NDS context are not used), you can set which file server the device will use for the Binder service. You can enter the names of up to four primary **[File Servers]** for the device in the Bindery Settings field.
7. NetWare Directory Services (NDS) is a system designed to make management of large networks easier for Administrators. NDS allows users, groups, files, directories, and other local and remote resources to be displayed in a hierarchical tree structure.
   In the **NetWare Directory Services (NDS)** area:
   a. If **IP** is selected for the **[Filing Transport]** in the **General** area, select either **IPv4 Address** or **Host Name**.
   b. In the **[NDS Server (For Server FAX and Workflow Scanning only)]** fields, if you selected **[IPv4 Address]**, enter the IP Address of the NDS server. If you selected **[Host Name]**, enter the host name of the NetWare server.
   c. In the **[NDS Tree]** field, enter the name for the NDS tree.

   Note: If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank. The default tree name is “Xerox_DS_Tree”.

   d. In the **[NDS Context]** field, enter the name for the NDS context.

   Note: If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank. The default context name is “Xerox_DS_Context”.
8. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
9. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

NDPS/NEPS

For The Xerox NDPS/NEPS Agent, documentation, and Print Drivers visit the Xerox website at www.xerox.com.

Novell Distributed Print Services (NDPS)/Novell Enterprise Print Services (NEPS) are products built on Novell's printing architecture.

These products allow System Administrators to take advantage of built-in printer intelligence to centrally manage network printing resources from anywhere on the network, improve network printing performance, and reduce the difficulty of network printing for end users.

The Xerox NDPS/NEPS Solution allows you to use Novell NDPS/NEPS with many of the latest Xerox printers. It includes administrative tools that snap-in to NWAdmin that allows users to easily configure and manage their network print services. It also has a set of NetWare Loadable modules that run on the NetWare server.

NetWare users can automatically create a printer object in the NDS tree and have automatic driver download capability. This eliminates individual driver installation by downloading the driver as users connect to a printer. Network users can perform remote, up-to-the-minute status checks or define meaningful notifications for their Xerox network printers.

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

This is the procedure to set up printing to a device from an AS400 using the SNMP drivers.

This procedure is intended for users familiar with the AS400 system, especially those experienced with printing in an AS400 environment.

The AS400 must run V4R5 of OS400 so that the SNMP drivers are present (or V4R3/V4R4 with the most current PTFs installed).

The device must have port 9100 enabled.

Procedures to Enable Port 9100

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[Raw TCP/IP Printing]** in the directory tree.
4. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable Raw TCP/IP Printing.
   b. **Physical Connection** displays the physical network connection, this will always display **“Ethernet”**.
5. Up to three ports may be enabled and configured, in the **Port Information** area:
   a. For **Port 1** Leave the **TCP Port Number** set to **9100**. If two additional ports are available, click on the **[Default All]** button to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
   b. Leave the **Bidirectional** checkboxes and **Maximum Connections per Port** settings at their default values.
   c. Set the **End of Job Timeout** to the number of seconds to wait before processing a job without an End Of Job indicator. The range is from 1 to 65535, and the default is 300.
   d. Leave the **PDL Switching**, **[Enabled]** checkbox at its default value.

   Note: Do not check the **[Enabled]** checkbox for **PDL Switching**, when Windows clients print using port 9100. this prevents each print job from generating a banner page.
6. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
7. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Create a Device Description

Create a device description from your AS400 terminal 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 the default value, 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. Press **<Enter>**, A message indicates that you have created the device Xerox printer.
7. Power on the device and start a print writer. Place a spool file in the appropriate queue to test the printer.

AS400 Printing using LPR (CRTOUTQ) - Optional

Creating a remote queue (LPR) on the AS400

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

   Note: ONLY CHANGE THE PARAMETERS IN BOLD.

   - 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****

   Note: The 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**

2. Press **<Enter>** to create.

   Note: The Workstation Customizing Object is the file that was created in the Create a Device Description on page 130, step 2.

3. At this point, a spool file (document) can be sent to the WorkCentre device.

   Note: If printing PCL, set this parameter to HPIIID, 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).

UNIX

HP-UX Client (Version 10.x)

HP-UX workstations require specific installation steps to communicate with the machine. The machine is a BSD-style UNIX printer, whereas HP-UX is a System Vstyle UNIX.

> Note: All UNIX commands are case-sensitive, so enter the commands exactly as they are written.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the device.

  At the Device:

  a. Press the **<Machine Status>** button on the device.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.

The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.

- Ensure the machine is connected to the network with Ethernet cabling.
- Ensure you can PING the machine IP address from the UNIX workstation.

Configure the Client

- Add the machine hostname to the etc/hosts file on the HP-UX workstation or DNS server.
- Ensure that you can PING the machine from the HP-UX workstation, using the hostname found in the **/etc/hosts** file.
- Use either the **GUI** method or the **tty** Method as follows:

GUI Method

1. Open a command window from the desktop.
2. Type **[su]** to become super user.
3. Type **[sam]** to start the System Administrator Manager (SAM).
4. Select the **[Printers and Plotters]** icon.
5. Select **[lp]** spooler.
6. Select **[Printers and Plotters]**.
7. Select **[Actions: Add Remote Printer/Plotter...]**.
8. Enter the following information into the Add Remote Printer/Plotter form:
   - **[Printer Name: printer name]**. Where printer name is the name of the queue being created.

- **[Remote System Name: hostname]**. Where hostname is the machine hostname from the **/etc/hosts** file.
- Select **[Remote Printer is on a BSD System]** and click on **[OK]** to complete form.

9. Click on **[Yes]** at the Configure HP UX Printers Subpanel screen. This screen may be obscured by the **Add Remote Printer/Plotter** form.
10. Select **[File: Exit]**.
11. Select **[File: Exit Sam]**.
12. Type **[exit]** to exit super user mode.
13. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.

tty Method

Follow the steps below to use the HP System Administrator Manager (SAM) GUI (Graphical User Interface).

> Note: Refer to the HP-UX documentation for additional information on using the System Administrator Manager (SAM).

1. Open a command window on the desktop. From the command prompt (#), enter the information below. Remember that UNIX commands are case-sensitive.
2. Type **[su]** to become super user.
3. Type **[sh]** to run the Bourne shell.
4. Type **[lpshut]** to stop the print service.
5. Create the print queue by typing (on the same command line): **[lpadmin -pqueuename -v/dev/null -mrmodel -ocmrcmodel -osmrsmodel -ob3 -orc -ormhostname -orplp]**.

   Where queuename is the name of the queue being created and hostname is the machine hostname from the **/etc/hosts** file.
6. Type **[lpsched]** to start the print service.
7. Type **[enable queuename]** to enable the queue to print to the machine.
8. Type **[accept queuename]** to the queue accepting jobs from the HP-UX workstation.
9. Type **[exit]** to exit the Bourne shell and then **[exit]** to exit super user mode.
10. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.
11. Verify that the job is printed at the device.

Solaris 2.x

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the machine.

  At the Device:

  a. Press the **<Machine Status>** button on the device.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.

  The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.

To Configure your Solaris 2.x Client

- Ensure the machine is connected to the network with Ethernet cabling.
- Ensure you can PING the machine IP address from the UNIX workstation.
- Add the machine printer hostname to the **/etc/hosts** file.

  Note: Perform the following steps to create a machine print queue on a Solaris 2.x workstation using either the **GUI** or the **TTY** method.

GUI Method

1. Open a command window from the desktop.
2. Type **[su]** to become super user.
3. Type **[admintool]** to run the System Administrator Tool.
4. Select **[Browse:Printers]**.
5. Select **[Edit:Add:Access to Printer...]**.
6. Enter the following information into the Access to Remote Printer form:

   [Printer Name: queuename]. Where queuename is the name of the queue being created.

   [Print Server: hostname]. Where hostname is the machine hostname from the **/etc/hosts** file. Click on **[OK]** to complete the form.
7. Type **[sh]** to run the Bourne shell.
8. Type **[lpadmin -p queuename -s hostname!lp]** to modify the remote queuename.
9. Type **[exit]** to exit the Bourne shell and **[exit]** to exit super user mode.
10. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**.

tty Method

1. Type **[su]** to become super user.
2. Type **[sh]** to run the Bourne shell

3. Define the machine as a BSD style printer. Type **[lpsystem -t bsd hostname]**. Where hostname is the machine hostname from the **/etc/hosts** file.
4. Create the queue. Type **[lpadmin -p queuename -s hostname -T unknown -I any]**. Where queuename is the name of the queue being created.
5. Type **[exit]** to exit the Bourne shell and **[exit]** to exit super user mode.
6. Test the queue created. Type the command **[lp -d queuename /etc/hosts]**. Verify that the job prints at the device.

SCO UNIX Environment

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that the correct IP Address is being used for the machine. To verify this, print a Configuration Report from the machine.

  At the Device:

  a. Press the **<Machine Status>** button on the device.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Print Reports]**.
  d. Touch **[Print Report]**.
  e. Touch **[Close]**.

  The Configuration Report will print. On the report verify the details under **Network Setup** heading are correct.

Set up for a SCO UNIX Client

SCO UNIX workstations require specific installation steps to communicate with the machine. The machines are BSD style UNIX printers, whereas SCO is System V style UNIX.

- Ensure the machine is connected to the network with Ethernet cabling.
- Add the machine printer hostname to the /etc/hosts file on the SCO workstation.
- Ensure that you can PING the machine from the SCO workstation, using the hostname found in the /etc/hosts file.

  Perform the following steps to create a machine print queue on a SCO UNIX workstation using either the GUI or the TTY method.

GUI Method

1. Log in as root.
2. From the Main Desktop, select icons: **[System Administration: Printers: Printer Manager]**.
3. Select **[Printer: Add Remote: UNIX...]**.
4. Enter the following information in to the Add Remote UNIX Printer form:
5. Host: hostname (Where hostname is the machine hostname from the **/etc/hosts** file).

   Printer: name of the queue being created, i.e: dc xxxq. Select **[OK]** to complete the form.
6. Select **[OK]** at the Message window.

7. Select **[Host:Exit]**.
8. Select **[File: Close this directory]**.
9. Select **[File: Close this directory]**.
10. Click on **[Save]** at the Warning Confirmation window.
11. Type **[exit]** to log out of root account.
12. Open UNIX Window.

tty Method

1. Type **[su]** to become super user.
2. Type **[rlpconf]** to create a printer. Enter the following information:

   [Printer Name: queuename]

   [Remote Printer: r]

   [Hostname: hostname]

   If the information has been entered properly, type **[y]**.
3. Click on **[Enter]** to accept default of a non-SCO remote printer.
4. Click on **[Enter]** to accept default of non-default printer.
5. Click on **[Enter]** to start process of adding queue.
6. Type **[q]** to quit the rlpconf program.

CUPS

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 A T and T Line Printer (LP) system designed in the 1970s for printing text to line printers.

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

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 19, so that the web user interface (Internet Services) can be accessed.
- Ensure that the DNS settings are configured.

Enable Port 9100 as Additional Support for HTTP (IPP) Printing

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[Raw TCP/IP Printing]** in the directory tree.
4. In the **General** area:
   a. For **Protocol,** check the **[Enabled]** checkbox to enable Raw TCP/IP Printing.

   b. **Physical Connection** displays the physical network connection, this will always display **“Ethernet”**.

5. Up to three ports may be enabled and configured, in the **Port Information** area:
   a. For **Port 1** Leave the **[TCP Port Number]** set to 9100. If two additional ports are available, click on **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
   b. Leave the **Bidirectional** checkboxes and **Maximum Connections per Port** settings at their default values.
   c. Set the **End of Job Timeout** to the number of seconds to wait before processing a job without an End Of Job indicator. The range is from 1 to 65535, and the default is 300.
   d. Leave the **PDL Switching**, **[Enabled]** checkbox at its default value.

   Note: Do not check the **[Enabled]** checkbox for **PDL Switching**, when Windows clients print using port 9100. this prevents each print job from generating a banner page.

6. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values, or **[Default All]** to enter printer defaults for all settings (recommended).
7. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

   Note: The settings are not applied until you restart the device.

8. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
9. Click on the **[Reboot Machine]** button and click on **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

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.

An Overview of the Common UNIX Printing System, Version 1.1, and a wide range of other descriptive documentation, is also available at this site.

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 installation begins as follows:

Tar format:

After untarring the files, run the installation script with the ./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. CUPS is also the default printing system for Mandrake Linux.

Installing the Xerox PPD on the workstation

The Xerox PPD for CUPS is available on one of the CD-ROMs that came with your printer. From the CD-ROM, 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 and 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 on **[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.

Print Drivers 6

This chapter summarizes the Print Driver features and functions. You can use Internet Services to configure the Print Drivers.

- Windows 2000/2003 Server on page 142
- Windows 2000 Professional on page 144
- Windows XP on page 147
- Windows Vista on page 150
- Apple Macintosh 10.X on page 153

Windows 2000/2003 Server

Xerox Printer Installer

This section provides instructions on how to install the Print Driver manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the Internet Services Print and Fax Drivers CD-ROM delivered with your device and follow the instructions contained in the Internet Services Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.
- Locate the Print and Fax Drivers CD, load the CD into your CD drive. (This was delivered in the Internet Services Network Services Pack with your device.) Review any README file contained with the Print Driver.

Windows Add Printer Wizard

1. At the Desktop, right-click on **[My Network Places]**/**[Network Neighborhood]** icon.
2. Select **[Properties]**.
3. Click on the **[Protocols]** tab.
4. Verify that the **[TCP/IP]** protocol has been loaded and the checkbox is checked.
5. Select the **[Services]** tab and verify that **[Microsoft TCP/IP Printing]** is loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Verify that Print Services for UNIX is loaded

1. From the **[Start]** menu, select **[Settings]** (for Windows 2000).
2. Select **[Control Panel]**.
3. Double-click on **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Select **[Other Network File and Print Services]**.
6. Click on **[Details]**.

7. Check the checkbox to select **[Print Services for UNIX]**.
8. Click on **[OK]**.
9. Click on **[Next]**.
10. Close the **[Add/Remove Programs]** window.

Add the Printer

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]/[Printers and Faxes]**.
2. Double-click **[Add Printer]** and click on **[Next]**.
3. Select **[Local Printer]** (Windows 2000) or **[Local Printer attached to this computer]** (Windows 2003) and uncheck **[Automatically detect and install my Plug and Play printer]**.
4. Click **[Next]**.
5. Select **[Create a New Port]**.
6. Select **[LPR Port]** from the **Type** drop-down menu and click **[Next]**.

   Note: The LPR Port is only available when Print Services for UNIX is installed.
7. Enter the **IP Address** of the printer.
8. Enter the printer name.
9. Click on **[OK]**.
10. You will be prompted for a Print Driver. Select **[Have Disk]** and click **[Browse]**. Locate the Drivers folder on the CD.
11. Select the required driver.
12. Click on **[Open]** and then **[OK]**.
13. Select the model of your machine from the list. Click on **[Next]**.
14. The **Name your Printer** screen appears. Enter a printer name and click **[Next]**.
15. The **Printer Sharing Screen** appears. If you will be sharing this printer with other clients select **[Share As]** (Windows 2000) or **[Share Name]** (Windows 2003) and enter a share name. Click **[Next]**.
16. Enter details in the **[Location]** and **[Comment]** if required. Click **[Next]**.
17. Select **[Yes]** to print a test page and verify that it prints at the device. Click **[Next]**.
18. Click **[Finish]**. The Print Driver will install.

Configure the Print Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]/[Printers and Faxes]**.
2. Right-click on the printer icon and select **[Properties]**.
3. Click on the **[Advance]** tab, then click on **[Printing Defaults]**.
4. Select the settings you wish to set for the printer.

For further information on Configuring the Print Driver and Installation, refer to the **Print Drivers Guide for Windows CD**.

Windows 2000 Professional

Note: You can use Internet Services to configure the Print Driver in this environment.

Xerox Printer Installer

This section provides instructions on how to install the Print Drivers manually. However, you can use Xerox Printer Installer to find the printer and install drivers.

To use the Xerox Printer Installer locate the Print and Fax Drivers disc delivered with your device and follow the instructions contained in the Guide for Microsoft Windows.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Print Reports]**.
  d. Touch **[Print Report]**.
  e. Touch **[Close]**.
- Locate the Internet Services Print and Fax Drivers CD. (This was delivered in the Internet Services Network Services Pack with your device.) Review any README file contained with the Print Drivers.

To install the Print Driver on Windows 2000 Professional choose one of the following options:

- Connect to an existing print queue already created on a network server.
- Create a new print queue on the Windows 2000 Professional workstation.

Connect to an Existing Print Queue

1. At the Windows 2000 Professional Desktop, right mouse click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon.
4. Select **[Properties]**.
5. Verify that the **Internet Protocol (TCP/IP)** protocol has been loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Add the Printer

1. From the **[Start]** menu, select **[Settings]**.
2. Select **[Printers]**.

3. Double-click on **[Add Printer]** and then click **[Next]**.
4. Verify that **[Network Printer]** is selected and click on **[Next]**.
5. The **Locate Your Printer** screen will appear. Select the **[Type the Printer Name]** option or click on **[Next]** to browse for a printer.
6. Enter the path to the printer or click on **[Next]** to browse for the print queue created on your server.
7. Select the printer and click on **[Next]**. Select **[Yes]** if you wish to make it the default printer. Click on **[Next]**.
8. Click on **[Finish]**. The Print Driver will download to the Windows 2000 Professional workstation.
9. When the Print Driver has installed open an application on the workstation and print a test page to verify operation.

Create a New Print Queue

Go to the Windows 2000 Professional Workstation:

1. At the Desktop, right click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon and select **[Properties]**.
4. Verify that the [Internet Protocol (TCP/IP)] protocol has been loaded. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.

Verify that Print Services for UNIX is loaded

1. From the **[Start]** menu, select **[Settings]**.
2. Select **[Control Panel]**.
3. Double-click **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Select **[Other Network File and Print Services]**.
6. Click on **[Details]**.
7. Check the checkbox to select **[Print Services for UNIX]**.
8. Click on **[OK]**.
9. Click on **[Next]**.
10. Close the **[Add/Remove Programs]** window.

Add the Printer

1. From the **[Start]** menu, select **[Settings]** then **[Printers]**.
2. Double-click on **[Add Printer]** and then click **[Next]**.
3. Select **[Local Printer]** and deselect **[Automatically detect and install my Plug and Play printer]**.
4. Click on **[Next]**.
5. Select **[Create a new port]** and choose **[LPR Port]** from the Type pull-down menu.
6. Click on **[Next]**.

7. Enter the IP Address of the printer.
8. Enter a name for the print queue and click **[OK]**.
9. You will be prompted for a Print Driver. Select **[Have Disk]** and browse to the location of your Print Driver.
10. Select the **[.INF]** file then click on **[Open]**.
11. The wizard will return you to the previous dialog. Verify the path and file name are correct and click on **[OK]**.
12. Select the model that corresponds to your device and click on **[Next]**.
13. The **Name your Printer** screen appears. Enter a printer name. Select **[Yes]** if you wish to make this the default printer, then click on **[Next]**.
14. The **Printer Sharing** screen appears. If you will be sharing this printer with other clients select the **[Share As]** button and enter a share name. Click on **[Next]**.
15. Enter a location and comment (optional).
16. Select **[Yes]** to print a test page and verify that it prints at the device. Click **[Next]**.
17. Click on **[Finish]**.

Configure the Print Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]**.
2. Right-click on the printer icon and select **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Change the settings you wish to set for the printer.
5. Click on **[OK]**.

For further information on Configuring the Print Driver and Installation, refer to the **Print Drivers Guide for Windows CD**.

Windows XP

Note: You can use Internet Services to configure the Print Driver in this environment.

Xerox Printer Installer

This section provides instructions on how to install the Print Driver manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the Internet Services Print and Fax Drivers disc delivered with your device and follow the instructions contained in the Internet Services Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.
- Locate the Internet Services Print and Fax Drivers CD. (This was delivered in the Internet Services Network Services Pack with your device.) Review any README file contained with the Print Driver.

To install the Print Driver on Windows XP choose one of the following options:

- **Connect to an existing print queue already created on a network server.**
- **Create a new print queue on the Windows XP workstation.**

Connect to an Existing Print Queue

1. At the Windows XP Workstation verify that the TCP/IP protocol stack is loaded: select **[Start]**, right-click the **[My Network Places]** icon, and select **[Properties]**.
2. Right-click on the **[Local Area Connection]** icon. Select **[Properties]**.
3. Verify that the **Internet Protocol (TCP/IP)** protocol has been loaded. It may be necessary to scroll down the list. If this software is not present, install it using the documentation provided by Microsoft. Then return to the next step in this document.
4. From the **[Start]** menu select **[Printers and Faxes]**.
5. Select **[Add a Printer]**.
6. The **Add Printer Wizard: Welcome Page** displays. Click on **[Next]**.
7. Verify that **[A network printer, or a printer attached to another computer]** is selected, and click on **[Next]**.

8. The **Specify a Printer** screen will appear. Select one of the following:
   - **Connect to this printer** - if you know the name of the server and printer.
   - **Find a printer in the directory** - to browse for the print queue created on your server.

   Click on **[Next]**.
9. Select the printer and click on **[OK]**.
10. If you want to make this printer your default printer select **[Yes]**, then click on **[Next]**.
11. Click on **[Finish]**. The printer will download to the Windows XP workstation.
12. When the Print Driver has installed, open an application on the workstation and print a file to verify that the Print Driver has correctly installed.

Configure the Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Right-click on the printer icon and select **[Properties]**. Use the available tabs to set the printing defaults. Additional settings may be accessed by clicking on the **[Printing Preferences]** button on the **General** tab.
3. Click on the **[Apply]** button, then **[OK]**.

Create a New Print Queue on Windows XP

1. Obtain the Print Driver for your operating system.
2. Verify that Print Services for UNIX is loaded: from the **[Start]** menu, select **[Control Panel]**.
3. Double-click **[Add/Remove Programs]**.
4. Select **[Add/Remove Windows Components]**.
5. Scroll down until you see **[Other Network File and Print Services]**.
6. Click on the **[Details]** button.
7. Check the checkbox to add **[Print Services for UNIX]** if not already installed and click on **[OK]**.
8. Click on **[Next]**.

Add the Printer

1. From the **[Start]** menu select **[Printers and Faxes]**. The Vista path is Start\Control Panel\Printer(s).
2. Click on **[Add a Printer]**, then **[Next]**.
3. Select **[Local Printer attached to this computer]**.
4. If already selected, deselect **[Automatically detect and install my Plug and Play printer]**.
5. Click on **[Next]**.
6. Select **[Create a new port]**.
7. Select **[LPR]** from the Type of Port pull down menu, then click **[Next]**.
8. Enter the **IP Address** of the printer.
9. Enter a name for the print queue and click **[OK]**.
10. You will be prompted for a Print Driver. Select **[Have Disk]** and click on **[Browse]** to browse to the location of your Print Driver.
11. Select the required driver then click on **[Open]**.

12. When the **Install from Disk** screen appears, verify that the path and file name are correct, then click on **[OK]**.
13. Select the model of your device from the list. Click on **[Next]**.
14. The **Name your Printer** screen appears. Enter a printer name.
15. If you want to make this printer your default printer select **[Yes]**, then click on **[Next]**.
16. The **Printer Sharing** screen appears. If you will be sharing this printer with other clients select the **[Share Name]** button and enter a share name. Click on **[Next]**.
17. Enter a location and comment in the **[Location and Comment screen]** (optional).
18. Select **[Yes]** to print a test page. Click on **[Next]**.
19. Click on **[Finish]**. The Print Driver will install. At the device verify that the test page printed.

Configure the Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Right-click on the printer icon and select **[Properties]**.
3. Use the available tabs to set the printing defaults. Additional settings may be accessed by clicking on the **[Printing Preferences]** button on the General tab.

For further information on Configuring the Print Driver and Installation, refer to the Print Drivers Guide for Windows CD.

Windows Vista

Xerox Printer Installer

This section provides instructions on how to install the Print Driver manually. However, you can use Xerox Printer Installer to discover the printer and install drivers.

To use the Xerox Printer Installer locate the Internet Services Print and Fax Drivers disc delivered with your device and follow the instructions contained in the Internet Services Print and Fax Drivers Guide for Microsoft Windows.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Verify the device is configured with the correct IP Address, Subnet Mask, and Gateway Address information by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.
- Locate the Internet Services Print and Fax Drivers disc. (This was delivered in the Internet Services Network Services Pack with your device.) Review any README file contained with the Print Driver.

To install the Print Driver on Windows Vista choose one of the following options:

- **Connect to an existing print queue already created on a network server.**
- **Create a new print queue on the Windows Vista workstation.**

Connect to an Existing Print Queue

> Note: You will need to know the server name where the print queue is located and the printer share name.

1. At your Workstation, click on **[Start]** then select **[Control Panel]**.
2. Click on the **[Hardware and Sound]** button.
3. Open the **[Printers]** folder.
4. Click on **[Add Printer]**.
5. Select **[Add a network, wireless or Bluetooth printer]**.
6. Click on **[Next]**.
7. The **Select a printer** screen will display. Select **[The printer that i want isn't listed]**, and click on **[Next]**.
8. In the **Find a printer by name or TCP/IP Address** screen, select **[Find a printer in the directory, based on location or feature]**, and click on **[Next]**.

9. In the **Find Printers** pop-up menu, enter the name of the printer you are trying find in the **[Name]** field, and click on **[Find now]**.

   Note: Ensure **[Entire Directory]** is selected from the **In** drop-down menu.
10. Select your printer from the list and click on **[OK]**.
11. The **status bar** will display. In the **[Type a printer name]** window, check the **[Set as the default Printer]** checkbox.
12. Click on **[Next]**.
13. The **You've successfully added...** pop-up window will display. You can print a test page by clicking on the **[Print a test page]**.
14. Click on **[Finish]**.

Create a New Print Queue

- Ensure you have the Internet Services Print and Fax Drivers disc (delivered with your device).
- The device must be configured with a valid IP Address, subnet mask and gateway address.
- LPD (Line Printer Daemon) must be enabled on the device.

Verify that LPR Port Monitor is Loaded

1. Click on **[Start]**, **[Control Panel]** and double-click on **[Programs and Features]**.
2. Double-click on **[Windows Features]**.
3. In the **[Turn Windows Features on and off]** window expand the **[Print Services]** menu.
4. Click on **[LPR Port Monitor]** to enable the service.
5. Click on **[OK]**. Your computer may need to restart.

Add the Printer

1. At your Workstation, click on **[Start]** then select **[Control Panel]**.
2. Click on the **[Hardware and Sound]** button, open the **[Printers]** folder.
3. Click on **[Add a Printer]**.
4. Select **[Add a network, wireless or Bluetooth printer]**.
5. Click on **[Next]**.
6. The **Select a printer** screen will display, select **[The printer that i want isn't listed]**, and click on **[Next]**.
7. In the **Find a printer by name or TCP/IP Address** screen, select **[Find a printer in the directory, based on location or feature]**, and click on **[Next]**.
8. In the **Find Printers** pop-up menu, enter the name of the printer you are trying find in the **[Name]** field, and click on **[Find now]**.

   Note: Ensure **[Entire Directory]** is selected from the **In** drop-down menu.
9. Select your printer from the list and click on **[OK]**.
10. The **status bar** will display. In the **[Type a printer name],** check the **[Set as the default Printer]** checkbox.
11. Click on **[Next]**.

12. The **You've successfully added...** pop-up window will display, you can print a test page by clicking on the **[Print a test page]**.
13. Click on **[Finish]**.

Configure the Print Driver

If your device has any installable options fitted then these should be set in the driver, for example, a High Capacity Feeder or a Finisher.

1. At your Workstation, click on **[Start]** then select **[Control Panel]**.
2. Click on **[Hardware and Sound]** button, open the **[Printers]** folder.
3. Right click the appropriate printer icon and select **[Properties]**.
4. Click on the **[Configuration]** tab.
5. Click on **[Bi-Directional Setup]**. Bi-directional communication automatically updates the Print Driver with the printer's installed options. The driver Printing Preferences will report information about the printer's operational status, active jobs, completed jobs and paper status. If you do not want to configure Bi-directional Setup go to step 7.
6. Click on **[Automatic]** to have the driver automatically configure the IP Address of the device or click on **[Manual]** and enter the IP Address or host name of the device.

   If you want to change the default SNMP settings, click **[SNMP Community Name]** and enter the required information.
7. Click on **[OK]**.
8. Click on **[Installable Options]**.
9. If Bi-directional setup has not been enabled select the options that are installed on the device.
10. Click on **[OK]**.
11. Click on **[OK]** to close the Properties box.
12. Right click the printer within the Printers folder and select **[Printing Preferences]**.
13. Select any required default settings in the Print Driver.

For further information on Configuring the Print Driver and Installation, refer to the Print Drivers Guide for Windows CD.

Apple Macintosh 10.X

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Verify the AppleTalk settings have been configured properly on the device by printing a Configuration Report.

  To print a Configuration Report, go to the Device

  a. Press the **<Machine Status>** button.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.

  The Configuration Report will print. On the Configuration Report, check under the **AppleTalk** heading have been configured.
- Locate the Internet Services Print and Fax Drivers disc. Review any README file contained with the Print Driver.

Install the Print Driver

View the Configuration Report and note the Name given to the device under **AppleTalk Settings**.

Instructions for 10.x (OS X)

At the Macintosh Workstation

1. Load the Internet Services Print and Fax Drivers CD-ROM into your CD drive.
2. Open the CD and select the required language if necessary.
3. Double-click to open the **[Drivers]** folder.
4. Double-click to open the **[Mac]** folder.
5. Double-click to open the folder containing the drivers for version 10.x.
6. Double-click to open the **[machine model.dmg]**.
7. Double-click to open the **[machine model.pkg]** file to run the installer program.
8. When the Welcome screen displays, click **[Continue]**.
9. Click on **[Continue]**, then **[Agree]** to accept the Licence Agreement.
10. Select the required disk (if necessary) where you want to install the printer. Click on **[Continue]**.
11. Click on **[Install]**.
12. Click on **[Close]**, and restart the workstation.
13. When the workstation has restarted, double click the hard drive icon.
14. Double-click the **[Applications]** icon.
15. Double-click the **[Utilities]** folder.
16. Double-click the **[Printer Setup Utility]** icon.

17. Double-click the **[Add]** button to add a new printer or click the **[Printers]** menu and click on **[Add Printer]**.
18. Select **[IP Printing]** from the top menu.
19. Select **[Internet Protocol Printing]** or **[LPD/LPR Printing]** from the next menu.
20. Enter the IP Address of the printer.
21. Enter a name for the print queue. (You may leave this blank if you prefer).
22. Select **[Xerox]** from the **Printer Model** list.
23. Select your printer model from the **Model Name** list.
24. Click on **[Add]**. The device will appear in the Printer List.
25. Select the printer and click on the **[Show Info]** button.
26. Click on **[Installable Options]**.
27. Select the options as installed on your device. If you want to use the Save Job for Reprint feature, ensure **Job Storage** is set to **[Installed]**.
28. Click on **[Apply Changes]**.
29. Close the Printer Info box.
30. Print a document to verify that the printer is installed correctly.

View the Printer Utility on the Internet Services Print and Fax Services CD.

For further information on Configuring the Print Driver and Installation, refer to the Print Drivers Guide for Macintosh CD.

Authentication 7

Authentication Overview

This feature allows the user to be identified to the device, so that the device can then determine if the user has access to the Device, Pathway, Services and/or its Features. It also enables the device to identify the logged in user when various functions are performed, for example, sending an e-mail.

Authentication can be enabled to prevent unauthorized use of installed device options and standard features. For example, the System Administrator can configure the device to allow users to access specific services such as Machine Status Pathway, Job Status Pathway and Service Pathway such as Color Copy, Reprint Saved Jobs, Workflow Scanning, E-mail, Internet Fax and Fax.

Authentication is used to verify that a user accessing the device is a valid user. The user's authentication details are verified either remotely by a network authentication server, locally by an internal database on the device, or by a card reader or authentication solution with the Xerox Secure Access feature.

Users will be asked to provide a User Name and Password to be validated by the designated authentication server. If this validation is successful, the options which were previously locked will be available for individual use.

There are four Authentication options:

- **Username / Password Validated Remotely on the Network** - The System Administrator can select one of these environments to provide network authentication:
  - **Kerberos (Solaris)**
  - **Kerberos (Windows 2000/2003)**
  - **SMB (Windows NT/2000/2003).**
  - **LDAP (Lightweight Directory Access Protocol).**
- **Username / Password Validated Locally on the Xerox Machine**- The System Administrator defines users with Username and Password, using a web browser, allowing users to authenticate to the system and use restricted services.
- **Xerox Secure Access** - For information on this type of authentication, refer to Xerox Secure Access on page 331.
- **Smart Card**- For information on this type of authentication, please refer to the Smart Card guide supplied with your device.

Administrators who choose to enable authentication locally are required to configure user accounts in the **Local User Information Database** (**Properties > Security > User Information Database > Setup**), refer to User Information Database on page 173.

Authorization Overview

This feature works in conjunction with the Authentication feature to determine what an authenticated user is allowed to do.

When a user has been authenticated, the Authorization feature will validate the role of that user. When remote authorization is selected, not only is the 'User Role' defined, but also the user can be authorized for individual services and pathways.

Authorized Users Roles Controlled by Authentication

- **System Administrator** Access - Users who have full access to the device and the device settings.
- **Account Administrator** Access - these users have access to the accounting settings.
- **User**

There are two options for Authorization:

- **Username / Password Validated Locally on the Xerox Machine** - refers to the database included on your device.
- **Username / Password Validated Remotely on the Network** - refers to networked server/databases that will provide authentication of user login details. Supported method is:
  - LDAP (Lightweight Directory Access Protocol).

The administrator can specify the services and device pathways on a device that requires authentication. Services can be locked and/or hidden so that unauthorized users cannot use or see them. Pathways can be locked or unlocked.

Authentication Configuration

Network Authentication can be enabled to prevent unauthorized use of features and pathways (for example Machine Status Pathway, Job Status Pathway and Service Pathway such as Color Copy, Reprint Saved Jobs, Workflow Scanning, E-mail, Internet Fax and Fax).

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 options which were previously locked will be available for individual use (depending on the authorization settings).

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functional on the network.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional. This is required to access Internet Services to configure Network Authentication. Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure Authentication settings by using an Internet browser.
- Ensure the Authentication Server to be used is functional on your network and refer to your manufacturer's documentation for instructions to complete this task.

Authentication Configuration (Network Authentication)

Procedure (Initial Use)

The first time you access the Authentication Configuration screen you will be asked to change the System Administrator Password. The System Administrator password is used to access Tools at the device user interface, and change settings via Internet Services.

Use this screen to change the default System Administrator password before proceeding to any authentication configuration settings.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Device System Administrator Password** page displays. In the **User Name & Password** area, enter details in the **[New Password]** field.
4. Retype the details in the **[Retype New Password]** field.
5. Click on **[Save]**. The following steps will display.
6. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
7. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
8. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu.
9. In the **Authentication method on the machine's web user interface (Web UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu.
10. In the **Authorization information is stored** area select **[Remotely on the Network]** from the drop-down menu.
11. In the **Personalize the machine's touch interface** area, check the checkbox to allow the **From:** address to be automatically set to the logged in user's e-mail address, when they log in via Secure Access and for the Scan-to Home home directory to be automatically set to that of the logged in user.
12. Click on the **[Save]** button to save the new settings and return to the **Xerox Access Setup** page.

Procedure (Subsequent Use)

The following steps are written as subsequent use, assuming that the initial Authentication Configuration has previously been completed.

Authentication Configuration for Kerberos (Solaris)

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.

3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu and click on the **[Save]** button to return to the **Xerox Access Setup** page.
5. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Authentication Servers** row.
6. In the **Authentication Server** page, select **[Kerberos (Solaris)]** from the **Authentication Type** drop-down menu, and click on the **[Add New]** button.
7. In the **Server Information** area:
    a. Enter details in the **[Realm]** field.
    b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** button.
    c. If IPv4 or IPv6 Address is selected, enter details in the **[IP Address: Port]** and **[Backup IP Address: Port]** field.
    d. If Host Name is selected, enter details in the **[Host Name: Port]** and **[Backup Host Name: Port]** field.
8. In the **Optional Information** area, if required, you can indicate which LDAP server should be used to acquire authorization and personalization data when authenticating to the server.
    a. Click on the **[Add LDAP Mapping]** button, the LDAP page displays. To configure LDAP server, click the **[Edit]** link or to add a new LDAP server click on the **[Add New]** button.
    b. The **LDAP: Server** page displays. For details on how to configure this option refer to LDAP on page 115.
    c. When you have configured the feature, click on the **[Save]** button.
    d. Click on the **[Add Mapping]** button to return to the **Add Authentication Server** page.
9. Click on the **[Add Server]** button to save the settings and return to the **Authentication Server** page.
10. Click on the **[Save]** button to return to the **Xerox Access Setup** page.
11. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
    a. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
12. Click **[Save]** to confirm the changes and return to the Xerox Access Setup page..
13. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for Kerberos (Windows 2000/2003)

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.

3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu and click on the **[Save]** button to return to the **Xerox Access Setup** page.
5. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Authentication Servers** row.
6. In the **Authentication Server** page, select **[Windows 2000/2003]** from the **Authentication Type** drop-down menu, and click on the **[Add New]** button.
7. In the **Server Information** area:
   a. Enter details in the **[Domain]** field.
   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** button.
   c. If IPv4 or IPv6 Address is selected, enter details in the **[IP Address: Port]** and **[Backup IP Address: Port]** field.
   d. If Host Name is selected, enter details in the **[Host Name: Port]** and **[Backup Host Name: Port]** field.
8. In the **Optional Information** area, if required, you can indicate which LDAP server should be used to acquire authorization and personalization data when authenticating to the server.
   a. Click on the **[Add LDAP Mapping]** button, the LDAP page displays. To configure LDAP server, click the **[Edit]** link or to add a new LDAP server click on the **[Add New]** button.
   b. The **LDAP: Server** page displays. For details on how to configure this option refer to LDAP on page 115.
   c. When you have configured the feature, click on the **[Save]** button.
   d. Click on the **[Add Mapping]** button to return to the **Add Authentication Server** page.
9. Click on the **[Add Server]** button to save the settings and return to the **Authentication Server** page.
10. Click on the **[Save]** button to return to the **Xerox Access Setup** page.
11. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
12. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
13. Click **[Save]** to confirm the changes and return to the Xerox Access Setup page..
14. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003/2008)

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.

3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu and click on the **[Save]** button to return to the **Xerox Access Setup** page.
5. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Authentication Servers** row.
6. In the **Authentication Server** page, select **[SMB (Windows 2000/2003)]** or **[SMB (Windows NT4)]** from the **Authentication Type** drop-down menu, and click on the **[Add New]** button.
7. In the **Configuration (Required)**area:
   a. Enter details in the **[Domain]** field.
   b. Check the **Optional Information** checkbox.
   c. Select either the **[IPv4 Address]** or **[Host Name]** radio button.
   d. If IPv4 is selected, enter details in the **[IP Address: Port]** field.
   e. If Host Name is selected, enter details in the **[Host Name: Port]** field.
8. Click on the **[Add Server]** button to save the settings and return to the **Authentication Server** page.
9. Click on the **[Save]** button to return to the **Xerox Access Setup** page.
10. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
    a. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
11. Click **[Save]** to confirm the changes and return to the **Xerox Access Setup** page.
12. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Authentication Configuration for LDAP/LDAPS

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Remotely on the Network]** from the drop-down menu and click on the **[Save]** button to return to the **Xerox Access Setup** page.

   Note: LDAP can also simply be used as an Information (Personalization) server, supplying information to other Authentication servers being used on the network.

5. In the **Current Configuration** area, click on the **[Configure]/[Edit]** button for **Authentication Server**.

6. In the **Authentication Server** page, select **[LDAP]** from the **Authentication Type** drop-down menu and click on the **[Add New]** button.
7. To configure LDAP, refer to LDAP on page 115.
   a. When you have configured LDAP settings, click on the **[Save]** button to return to the **Authentication Configuration: LDAP** page.
   b. Click on the **[Save]** button and return to the **Xerox Access Setup** page.
8. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
   a. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
9. Click **[Save]** to confirm the changes and return to the Xerox Access Setup page..
10. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Configure Authorization Access (by groups) for LDAP

Used when **Remotely on the Network** is selected for **Authorization**.

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. (LDAP server will find members nested up to five levels down a group. For example, if LDAP searches for a user within the Admin Group, it may not find that user, but may find another group. It will also look for the user in that group as well and so on). If the LDAP server confirms that the user is a member of the ’Admin’ group, the user will have administrator access to the device.

1. If you have already logged out of Internet Services or closed your browser, at a networked workstation open the web browser and enter the IP Address (or Host Name) of the device in the Address bar, and press **<Enter>**.
2. Click the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. Click on the **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LDAP]** in the directory tree.
8. Click on **[Add New]**.
9. Click on the **[Authorization Access]** heading tab under the LDAP title.
   a. Select the **[User Roles]** tab. Use this tab to define the access groups that are authorized for the following roles:
      - For the **System Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with System Administrator access to the device.

- In the **Accounting Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with accounting administrator access to the device.

b. To verify either group, enter a name of one of the members of the LDAP server group in the **[User Name box]**, then click on the **[Test]** button.
Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist.

Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When two or more groups are entered, they must be separated by commas. When no access group is listed, all members will have access.

10. Select the **[Device Access]** tab.

a. For **Services Pathway [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with Service access to the device.

b. Repeat the process for **Job Status Pathway** and **Machine Status Pathway**.

c. To verify any of these groups, enter a name of one of the members of the LDAP server groups in the **[Enter User Name]** field, then click on the **[Test]** button.
Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When two or more groups are entered, they must be separated by commas. When no access group is listed, all members will have access.

11. Select the **[Service Access]** tab. Use this tab to define the groups that are authorized to access various device functions and services.

a. Enter the names of LDAP groups, as required in the **Access Group** field, to allow access to individual device services.

Note: By default everybody has access to all of the services on the device. By entering a group name in any of the services, access is then restricted to those users belonging to that group.

b. Verify each group by entering a group user in the **Enter User Name** field, and click on the **[Test]** button.
Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When two or more groups are entered, they must be separated by commas. When no access group is listed, all members will have access.

c. When done, click on **[Close]**.

Local Authentication

With Local Authentication enabled, the System Administrator defines passwords via a web browser, for users to use to authenticate to the system and use restricted services.

If using this method, you can only determine the User Role. You can not control individual user access to items. If authentication is successful, then the user will have access to all locked items (except System Administrator items, unless they are a System Administrator).

> Note: If users are created locally on the device using the **User Information Database**, those users will be authenticated only if the **Authentication Configuration** method is set to "**Locally on the Device**". If the authentication method is switched to "**Remotely on the Network**", those users will not be authenticated unless their credentials are also accessible remotely.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[User Name/Password Validated Locally on the Xerox Machine]** from the drop-down menu and click on the **[Save]** button to return to the **Xerox Access Setup** page.
5. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Local User Information Database** row.
6. In the **User Information Database** area, click on the **[Add New User]** button.
   a. In the **User Identification** area, enter details of the new user in the **[User Name]**, **[Friendly Name]**, **[Password]** and **[Retype Password]** fields.
   b. In the **[User Role]** area, select one of the following roles:
      - **System Administrator**
      - **Accounting Administrator**
      - **User**
   c. Click on the **[Add New User]** button to add the user.

   Note: You can also Edit user credentials, as well as Delete users, from the **User Information Database** screen. If using this method, you can only determine the user role to items if Authentication is successful. User will have access to all locked items if they have System Administrator access.

7. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
   a. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
8. Click **[Save]** to confirm the changes and return to the Xerox Access Setup page..
9. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Xerox Secure Access

System Administrators can configure the device so that users must be authenticated and authorized before they can access specific services or areas. Xerox Secure Access provides a means of authenticating users via an authentication server and optional card reader.

For further information about Xerox Secure Access, refer to Xerox Secure Access on page 331.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- 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.
- Ensure that the Xerox Partner authentication solution (Secure Access Server, Controller, and Card Reader) is installed and communicating with the device. Follow the installation instructions from the manufacturer of the authentication solution to correctly set the devices up. Make sure to securely mount any external user authenticating devices to the device.
- Ensure that SSL (Secure Sockets Layer) is configured on the device. The Xerox Partner authentication solution communicates with the device via HTTPS.
- (Optional) Ensure that Network Accounting is configured if you want the device to send user account information to a Network Accounting server. For instructions, refer to the Network Accounting section of this guide.
- You may also need another Authentication Server to communicate with the Secure Access Server providing that server with user credentialing information. A second Authentication Server will be necessary for web user interface Authentication, if this feature is additionally desired.
- You will need to configure LDAP communications on the device as stated in the LDAP/LDAPS topic in the Authentication section of this guide.

Configure Authentication

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's touch interface (Touch UI)** area select **[Xerox Secure Access Unified ID System]** from the drop-down menu.
5. Select the required option from the **[Authentication method on the machine's web user interface (Web UI)]** drop-down menu.
    a. When a user attempts to access Internet Services they are prompted to enter their login information. The option selected from the web user interface Authentication menu defines how the device will validate the user's rights to access Internet Services. This is required because if the user normally authenticates at the device with a card reader, there would be no method for the device to authenticate users who access Internet Services from their workstations.

- Select **[Locally on the Device]** to validate users listed in the Local User Information Database. This option requires you to configure accounts in the Local User Information Database.
- Select **[Remotely on the Network]** to validate users via an Authentication Server. This option requires you to have a server that will provide authentication of user login details. Authentication via Kerberos (Solaris, Windows 2000), NDS (Novell), SMB (Windows NT4/2000) or LDAP is supported.

b. Select required method from the **[Authorization]** drop-down menu. The card reader and Authentication Solution authenticates (validates) the user. The Authorization method determines which areas of the device a user is allowed to access. There are two options:

- Select **[Locally on the Device]**: if you want the device to check the Local User Information Database for levels of authorization.
- Select **[Remotely on the Network]**: if you want to use an LDAP server to determine levels of authorization.

If you selected Remotely on the Network (from the Location of Access Rights box), configure LDAP communications as stated in the Configure Authentication for LDAP/LDAPS in the Authentication section of this guide.

c. Check the **[Automatically retrieve user's e-mail address from LDAP]** checkbox under **Personalization** if you want to set the From address to the logged in user's e-mail address when they log in via Secure Access.

d. Click on the **[Save]** button to return to the **Xerox Access Setup** page.

6. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Xerox Secure Access Setup** row.

a. The **Xerox Secure Access Setup** screen displays. The device will automatically configure itself to work with the XSA remote server. Click on the **[Manually Configure]** button if the XSA remote server does not configure automatically.

b. In the **Server Communication** area, select either **[IPv4 Address]** or **[Hostname]**.

c. Enter details in the **[IP Address: Port]** or **[Host Name: Port]** fields.

d. Enter the details in the **[Path]** field.

e. Under the **Device Log In Methods** heading, select one of the following:

- **Xerox Secure Access Device Only (e.g., Swipe Cards** - if you want to allow the user to swipe their swipe cards at the UI.
- **Xerox Secure Access Device + alternate on-screen authentication method** - if you want users to authenticate using the device's control panel as well as the XSA feature. When the second option is enabled, a button labelled "Alternate Login" is displayed on the "Instructional Blocking Window" providing users with an alternate method to log in. For example, this feature can be enabled for users who are unable to use their swipe card. When the alternate button is selected, the remote server presents a series of log in screens on the local user interface. The remote server is still responsible for authenticating the user. All other Xerox Secure Access options are supported with this setting.

f. Under the **Accounting Information** heading, note that this item will be grayed out if Network Accounting is not enabled. If accounting is enabled, select **[Automatically apply Accounting Codes from the server]**, if the Secure Access Server has been configured to return the accounting User ID and Account ID login. If you want the user to enter these values at the local user interface during login, select **[User must manually enter accounting codes at the device]**.

g. Under the **Device Instructional Blocking Window** heading, enter text in the **[Window Title]** and **[Instructional Text]** fields to create the prompt that will be displayed on the device's user interface informing users how to authenticate themselves at the device.

Note: If the Title and Prompt have been configured on the Secure Access Server, then this information will override the Title and Prompt text entered here.

h. Click on the **[Save]** button when done.

7. Click on the **[Close]** button to return to the Authentication Configuration page.

Enable Web User Interface Authentication

A second, networked Authentication Server will be necessary for web user interface Authentication, if **Remotely on the Network** was selected. Full instructions for configuring network authentication, using Kerberos, NDS, SMB, and LDAP/LDAPS are contained in the Network Authentication section of this guide.

The path to the Authentication Server configuration screen is:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page is displayed. In the **Authentication, Authorization and Personalization** area click on the **[Edit...]** button.
4. In the **Authentication method on the machine's web user interface (Web UI)** area, select **[Remotely on the Network]** from the drop-down menu. Click on the **[Save]** button to return to the **Authentication Configuration** page.
5. In the table displaying a list of related configuration setting pages, click the **[Edit...]** button on the **Authentication Server** row.
6. Follow the instructions to select the required Authentication Type from the drop-down menu.
   - See Authentication Configuration for Kerberos (Solaris) on page 157.
   - See Authentication Configuration for Kerberos (Windows 2000/2003) on page 158.
   - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003/2008) on page 159.
   - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003/2008) on page 159.
   - See Authentication Configuration for LDAP/LDAPS on page 160.
7. When you have configured the required Authentication Type, click on the **[Save]** button to return to the **Xerox Access Setup** page.

Configure your LDAP Server

Configure LDAP communications on the device as stated in the LDAP/LDAPS topic. See Authentication Configuration for LDAP/LDAPS on page 160.

8. To set Authentication to control access to individual Services, In the table displaying a list of related configuration setting pages, click on the **[Edit..]** button for **Tools and Feature Access (Lock/Unlock)**.
    a. On the **Tools & Feature Access** page, in the **Presets** area, select either **[Open Access]** to allow all users access to all pathways and features or **[Custom Access]** and lock or unlock the various pathways and features as required.
9. Click **[Save]** to confirm the changes and return to the Xerox Access Setup page..
10. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Using Secure Access

1. Read the 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 device's keypad to close your account.

Security

8

This chapter describes how to configure the following Security features for the device:

Security @ Xerox

For the latest information on securely installing, setting up and operating your device see the Xerox Security Information website located at www.xerox.com/security.

Email Encryption and Signing

Email Encryption and Signing allow users to ensure that Emails sent from the device are signed and/or encrypted.

Signed e-mails can be sent to any address the user specifies and encrypted email can be sent to any recipient with a valid security certificate.

To enable and configure Email encryption

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click the **[Authentication]** link and select **[Setup]** in the directory tree.

   Note: Smart Card authentication must be set as the primary authentication method before Email encryption and signing are made available.
3. In the table of associated services at the bottom of the screen, click the **[Edit...]** button next to **E-mail Encryption and signing**.
4. In the **Email Encryption Enablement** area, select one of the following settings:
   - **Off** - Email encryption is disabled and cannot be activated by a user at the device.
   - **Always On: Not Editable By User** - Email encryption is enabled and cannot be deactivated by a user at the device.
   - **Editable by User** - Email encryption is enabled but can be activated or deactivated by a user at the device. The default state can be set by selecting one of the following:
     - **Off** - Email encryption is deactivated by default but can be activated by the user.
     - **On** - Email encryption is activated by default but can be deactivated by the user.
5. Select the required **Encryption Algorithm** to be used.
6. In the **Email Signing Enablement** area, select one of the following settings:
   - **Off** - Email signing is disabled and cannot be activated by a user at the device.
   - **Always On: Not Editable By User** - Email signing is enabled and cannot be deactivated by a user at the device.
   - **On: Editable by User** - Email signing is enabled but can be activated or deactivated by a user at the device. The default state can be set by selecting one of the following:
     - **Off** - Email signing is deactivated by default but can be activated by the user.
     - **On** - Email signing is activated by default but can be deactivated by the user.
7. Select the required **Signing Hash Key** to be used.
8. Click the **[Save]** button.

FIPS 140-2 Encryption

The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules. Your device supports FIPS 140-2 Level 1 only.

To Enable FIPS 140-2 Encryption

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click **[Encryption]** and select **[FIPS 140-2]** in the directory tree.
3. Select the **Enabled** radio button and click the **[Run Configuration Check & Apply]** button.
4. The system runs a configuration check to ensure that all services are FIPS 140-2 compliant. If all services are compliant a confirmation page is displayed.
5. Click **[Reboot the Machine]**, the machine will restart with FIPS 140-2 enabled.

To Disable FIPS 140-2 Encryption

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click **[Encryption]** and select **[FIPS 140-2]** in the directory tree.
3. Select the **Disable** radio button and click the **[Apply]** button.
4. The machine will automatically restart with FIPS 140-2 disabled.

User Data Encryption

User Data Encryption ensures all data or job-sensitive data on the device's hard drive is protected.

User Data Encryption is automatically **enabled** on the device and no further configuration is required by the administrator.

When enabled, the data on the hard drive will not be meaningful when the hard drive has been separated from the device it was originally installed on.

If the hard disk is removed from the device then the encrypted data remains protected because the encryption key is not stored on the hard drive.

To Disable User Data Encryption

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Encryption]** link and then select **[User Data Encryption]** in the directory tree.
3. In the **[User Data Encryption Enablement]** area, select **[Disabled]**.
4. Click on the **[Apply]** button.

Note: Changing the User Data Encryption setting will reboot the Network Controller. This may result in a loss of user data and will interrupt or delete current jobs on the device.

User Information Database

User Information Database is a local database that contains user data for access by Authentication and basic Authorization.

The User Information Database allows you to add new users to the database. User information can be edited and deleted from the database.

Password Settings allow you to change password rules.

Note: If the Password rules are changed, old passwords are NOT AFFECTED by the new rules. If users are created locally on the device using the **User Information Database**, those users will be authenticated only if the **Authentication Configuration** method is set to **"Locally on the Device"**. If the authentication method is switched to **"Remotely on the Network"**, those users will not be authenticated unless their credentials are also accessible remotely. For further information on Authentication Configuration, refer to Authentication on page 155.

To Add a New User to the Database

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[User Information Database]** link.

3. Select **[Setup]** in the directory tree.
4. On the **User Information Database** page, click on the **[Add New User]** button.
5. On the **Add New User** page, in the **User Identification** area:
   a. Enter a login name that the user will enter to gain access to the device or the Internet Services in the **[User Name]** field.

   Note: The login name is case-sensitive.

   b. Enter a name that will be associated with the login name in the **[Friendly Name]** field.
   c. Enter a password in the **[Password]** field, and retype the password in the **[Retype Password]** field to confirm that it is correct.
6. In the **User Role** area, select one of the following roles for the new user:
   - **System Administrator**: This will appear in the Role column as **"SA**". This role has access to all pathways, services and features on the device.
   - **Accounting Administrator**: This will appear in the **Role** column as **"AA"**. The accounting administrator can access all pathways, services, and features on the device, as well as accounting tools and any non-secured tools features. The accounting administrator can neither edit nor create any new users for the device.
   - **User**: This will appear in the **Role** column as **"USER**".
7. Click on the **[Add New User]** button to save the new user settings.

To Edit a User on the Database

As a System Administrator

Note: Accounting Administrator cannot access this page.

Note: Any user on the database can log into the Internet Services and edit their own password.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[User Information Database]** link.
3. Select **[Setup]** in the directory tree.
4. On the **User Information Database** page, click on the **[Edit]** link next to the user you want to edit.
5. On the **Edit User** page:
   a. In the **User Identification** area, edit any relevant field.

   Note: The **[User Name]** field is not editable.

   b. In the **[User Role]** area, select the type of role for the user.
6. Click on the **[Edit User]** button to save the changes.

As an Individual User

Note: To configure this feature or these settings, you will have to access the **Properties** tab. This will require you to log in using your individual User ID and Password.

1. At your Workstation, open the web browser, enter the IP Address of the device in the Address bar.
2. Press **<Enter>**.

3. Click on the **[Properties]** tab.
4. If prompted, enter details in the **[User ID]** and **[Password]** fields.
5. Click on the **[Login]** button.
6. From the **Properties** tab, click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **Edit User** page:
   a. In the **User Identification** area, edit any relevant field.

   Note: The **[User Name]** field is not editable.

   b. In the **[User Role]** area, select to change the role of the user.
9. Click on the **[Edit User]** button to save the changes.

To Delete a User

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[User Information Database]** link.
3. Select **[Setup]** in the directory tree.
4. On the **User Information Database** page, under the **User Name** column, check the user checkbox you want to delete and click on the **[Delete]** button to delete the user.
5. A pop-up window will state **“All associated data will be lost. Delete Selected User Account?”**. Click on the **[OK]** button to confirm selection.

Password Settings

Use this page to set or change the password rules. This page is only available to users who are System Administrators

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[User Information Database]** link.
3. Select **[Password Settings]** in the directory tree.
4. On the **Password Settings** page, in the **Password Rules** area:
   a. Enter the minimum number of characters that will be accepted as a password in the **[Minimum Length]** and **[Maximum Length]** field.
   b. Optionally, you can also check to select either or all options:
      - Cannot contain **“Friendly Name”**.
      - Cannot contain **“User Name”**.
      - Must contain **“at least 1 number”**.
5. Click on the **[Apply]** button to save your changes and return to the **User Information Database** page.

IP Filtering

The IP Filtering security feature provides the ability to prevent unauthorized network access based on IP Address and/or port number filtering rules set by the System Administrator using Internet Services.

Authorized users will be able to create IP Address filtering rules.

Authorized users can enter a list of addresses that are allowed access to the device, and/or a list of addresses that are not allowed access to the device.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[IP Filtering]** in the directory tree.

   In the **IP Filter Rule List** area, the following information is displayed:

   - **Rule Number** - Display the rule order. Rule ordering is important in IP Filtering, because rules can negate each other if placed in an incorrect order.
   - **Action** - displays how IP Filtering handles incoming packets.
   - **Source IP/Mask** - displays which IP or IP range and network mask the rule has been created to handle.
   - **Source Port** - displays the originating port (if applicable) that the rule has been created to handle. If the incoming packet did not originate from this source port, the rule is not applied.
   - **Destination Port** - displays the port to which the packet was sent. If the incoming packet was not sent to this port, the rule is not applied.
   - **ICMP Message** - displays the ICMP Message the rule was created to handle. ICMP Messages are only shown when the protocol is set to ICMP.
   - **Protocol** - displays which protocols the rule handles.

To Add IP Filter Rule

1. On the **IP Filtering** page, click on the **[Add]** button to display the **Add IP Filter Rule** page.
2. In the **Define IP Filter Rule** area:

   a. From the **[Protocol]** drop-down list, select the protocol (**All**, **TCP**, **UDP** or **ICMP**) that the rule will apply to.

   b. From the **[Action]** drop-down list, select how you wish IP Filtering to handle the incoming packets the options are **Accept**, **Drop**, or **Reject**.

   c. From the **[Move This Rule To]** drop-down list, select either **End of List** or **Beginning of List** for the location of this rule. The order of the rules should be determined by the expected traffic to the device. Note that rule order is important in IP Filtering because rules can negate each other if placed in an incorrect order. For example, specific rules should be added to the top of the list, whereas blanket policies should be added to the bottom of the list

   d. Enter the **[Source IP Address]** to which this rule will apply.

e. Enter a number for the **[Source IP Mask]** to which this rule will apply. The allowable range of 0 to 32 corresponds to the 32 bit binary number comprising IP Addresses. A number of 8, for example, represents a Class A address (mask of 255, 0, 0, 0). The number 16 represents a Class B address (mask of 255, 255, 0, 0). The number 24 represents a Class C address (mask of 255, 255, 255, 0).

3. Click on the **[Apply]** button to accept the changes or on the **[Cancel]** button to exit the window without saving changes.

Audit Log

Audit Log is a log that tracks access and attempted access to the server. With TCP/IP and HTTP-based processes running on the server, exposure to access attacks, eavesdropping, file tampering, service disruption, and identity (password) theft is significantly increased. The Audit Log, regularly reviewed by the System Administrator, often with the aid of third party analyzing tools, helps to assess attempted server security breaches, identify actual breaches, and prevent future breaches. Access to the log's data is protected by enabling SSL (Secure Sockets Layer) protocols. The Audit Log, and its associated data protected by strong SSL encryption, helps to meet the Controlled Access Protection (Class C2) criteria, set by the United States Department of Defense. To enable this feature, perform the following steps.

IMPORTANT: Audit Log cannot be enabled until SSL (Secure Sockets Layer) is enabled on the device. To enable SSL on a device, the device needs a Server Certificate. For instructions on how to set up a Server Certificate, refer to Security Certificate Management on page 179.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[Audit Log]** in the directory tree.

   Note: You must enable SSL before enabling Audit Log.

3. In the **Enabling Audit Log on machine** area, check the **[Enabled]** checkbox for **Audit Log**.
4. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
5. Click on the **[Save]** button to save the Audit Log as a text file.
6. In the **Audit Log Download Form** page:

   a. Right-click on the **[Download Log]** link and select **[Save Target As]** to download file.

   b. Specify the location for the Audit Log to be saved in. The Audit Log is saved as **[Auditfile.txt.gz]**. This is a text file compressed as a GZIP file. Click on **[Save]**.

   c. Open the **[Auditfile.txt.gz]** compressed file.

   d. The Auditfile.text is a raw text file. To view the Audit Log as tab-delimited text, open the Auditfile.txt document in an application that can import text as a tab-delimited document, such as Microsoft® Excel.

To View the Audit Log

Note: Copy jobs and Embedded Fax jobs are not recorded in the Audit Log. The completion status of both types of jobs can be checked by viewing the applicable Completed Job Log entries.

Note: For a LAN Fax job, the event in the Audit Log will be recorded under the title of “print/driver fax”.

Note: To record the user’s name in the Audit Log, Network Authentication must be configured and enabled.
If **“Guest Access”** is enabled, job entries in the Audit Log will be associated with the generic identity **“Local User”**. Therefore ‘Guest Access’ is not recommended for secure configurations.

Note: There may not be an entry made in the Audit Log for a scan-to-mailbox job, although the job completion status will be reported in the Completed Job Log. If a scan-to-mailbox job is deleted from its scan-to-mailbox folder, there will be no entry created in either the Completed Jobs Log or the Audit Log for the job deletion.

Event ID

A unique value that identifies the entry. The following list shows the ID number allocated to each type of activity displayed in the Audit Log:

ID	Activity
1	System start-up
2	System shut down
3	On Demand Image Overwrite started
4	On Demand Image Overwrite complete
5	Print job
6	Network Scan Job
7	Server Fax job
8	IFAX
9	E-mail job
10	Audit Log Disabled
11	Audit Log Enabled

ID	Activity
12	Print/Fax driver LAN Fax job
13	Data Encryption
14	Scheduled ODIOD Standard started
15	Scheduled ODIO Standard complete
16	Scheduled ODIO Full started
17	Scheduled ODIO Full complete
18	Scan to Mailbox job
19	Delete File/Dir (CPSR)
20	USB
21	Scan to Home
23	System Configuration Data Changes

Event Description

The Audit Log contains a maximum list of the last 15,000 activities on the device. The activities that are displayed include:

- System start-up and shutdowns.
- On demand image overwrites completed.
- Jobs completed.

- Embedded Fax jobs.
- Store Files jobs.
- Accounting information.
- Workflow Scanning jobs - one scan to file audit log entry is recorded for each network destination within the scan job.
- Server Fax jobs - one audit log entry is recorded for each job.
- E-mail jobs - one audit log entry is recorded for each SMTP recipient within the job.

Completion Status

The Completion Status column shows the status of jobs and has the following values:

- comp-normal - the job completed correctly.
- comp-deleted - the job was deleted.
- comp-terminated - the job was cancelled.

Identify the PC or User

To record the user's name in the Audit Log, Network Authentication must be configured on the Xerox device.

IIO Status

If IIO (Immediate Image Overwrite) is enabled, this column will show the status of overwrites completed on each job.

Entry Data

This column contains any additional data that is recorded for an Audit Log entry, for example:

- Machine name
- Job name
- Username
- Accounting Account ID (when Network Accounting is enabled)

Security Certificate Management

A Machine Digital Certificate provides keys for encryption/decryption of data. It ensures the data is not tampered with and validates the source of data.

A Digital Certificate is like an ‘Electronic Driver’s License’. It contains the following:

- **Name of whom the Certificate is issued to**
- **Serial Number**
- **Expiration Date**
- **Name of the Certificate Authority that issued the Certificate**
- **A Public Key**
- **A Digital Signature of the Key from a Certificate Authority**
- **Country Code**

Other information it contains:

- **State/Province Name**
- **Locality Name**
- **Organization Name**
- **Organization Unit**
- **E-mail Address**

The device can be configured for secure access with the SSL (Secure Socket Layer) protocol via Digital Certificates. The enablement of SSL provides encryption for all workflows where the device is used as a HTTPS server.

Workflows include:

- **Administration of the device via Internet Services**
- **Printing via Internet Services**
- **Printing via IPP**
- **Scan Template Management**
- **Workflow Scanning via HTTPS**
- **Administration of Network Accounting**

The device exports the signed certificate to the client to establish an SSL/HTTPS connection.

There are two options available to obtain a server certificate for the device:

- Have the device create a Self Signed Certificate.
- Create a request to have a Certificate Authority sign a certificate that can be uploaded to the device.

A self-signed certificate means that the device signs its own certificate as trusted and creates the public key for the certificate to be used in SSL encryption.

A certificate from a Certificate Authority or a server functioning as a Certificate Authority, for example Windows 2000 running Certificate Services, can be uploaded to the device.

Note: A separate request is required for each Xerox device.

With SSL enabled (from the Connectivity/Protocols/HTTP selections of the **Properties** tab of Internet Services), and a digital certificate installed, remote users accessing the system over an HTTP-based interface are assured of having their network communications protected against eavesdropping and tampering, using strong encryption. The only action required by the workstation user is to type **https://** followed by the IP Address (or fully qualified domain name) of the system into the Address or URL box of the web browser. The subsequent acceptance of a Digital Certificate completes the exchange of the Public Key enabling the encryption process to proceed.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- An IP Address or Host Name must be configured on the device.
- DNS must be enabled and configured on the device.
- HTTP must be enabled so that Internet Services can be accessed.

- Ensure the system time configured on the device is accurate. This is used to set the start time for self signed certificates.

Enable Secure HTTP (SSL)

Security certificates cannot be configured until the secure HTTP Protocol (SSL) is enabled:

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[HTTP]** in the directory tree.
4. In the **Configuration** area:
   a. Under **Secure HTTP (SSL),** select **[Enabled]**.
   b. Enter the **[Secure HTTP Port Number]** if required.
5. Click on the **[Apply]** button.

- Close your web browser and then access Internet Services screen again. The Security warning appears. Self-signed certificates usually cause browsers to display messages which question the trust of the certificate. Click on the **[OK]** button to continue.

To Create a Digital Certificate

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[Security Certificates]** in the directory tree, the Security Certificates page displays.
3. To create a Self Signed certificate:
   a. Select the **[Xerox Device Certificate]** tab.
   b. Click on the **[Create New Xerox Device Certificate]** button.
   c. Complete the Self Signed Certificate form with details for:
      - **2 Letter Country Code**
      - **State/Province Name**
      - **Locality Name**
      - **Organization Name**
      - **Organization Unit**
      - **Subject Alternative Name** (if required)
      - **E-mail Address**
      - **Days of Validity**

   Note: **Common Name** on the form is generated by the device and cannot be changed.

   d. Click on the **[Finish]** button to continue. Values from the form will be used to establish a self-signed certificate, and you will be returned to the **Security Certificates** page.

   Note: A Xerox Device Certificate is inherently less secure than installing a certificate signed by a trusted, third party Certificate Authority (CA). However, specifying a self-signed certificate is the easiest way to start using SSL. A self-signed certificate is also the only option if your company does not have a Server functioning as a Certificate Authority (Windows 2000 running Certificate Services, for example), or does not wish to use a third party CA.

4. To create a **Certificate Signing Request:**
   a. Select the **CA-Signed Device Certificate(s)** tab.
   b. Click the **[Create Certificate Signing Request (CSR)]** button.
   c. Complete the Certificate Signing Request (CSR) form with details for:
      - **2 Letter Country Code**
      - **State/Province Name**
      - **Locality Name**
      - **Organization Name**
      - **Organization Unit**
      - **Subject Alternative Name** (if required)
      - **E-mail Address**

   Note: **Common Name** on the form is generated by the device and cannot be changed.

   d. Click on the **[Finish]** button to continue. Values from the form will be used to generate a Certificate Signing Request.
   e. When the process is complete, you will be prompted to save the Certificate Signing Request. Right-click on the **[Right-click to save this certificate for submission to a trusted certificate authority]** link and select **[Save Target As]**.
   f. Save the Certificate to your hard drive and send it to a **Trusted Certificate Authority**.
   g. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

To Upload a Signed Certificate

When a signed certificate is received from the Trusted Certificate Authority, upload the certificate to the device.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[Security Certificates]** in the directory tree.
3. Select the **CA-Signed Device Certificate(s)** tab.
4. Click the **[Install CA-signed Device Certificate]** button.
5. Click the **[Browse]** button to locate the signed certificate. Click on the **[Open]** button.
6. Click on the **[Next]** button. The details of the Certificate are displayed. Change the friendly name of the Certificate if required and click **[Next]**.
7. The digital certificate will appear in the installed certificates list.

   Note: For the upload to be successful, the signed certificate must match the CSR created by the device and must be in a format that the device supports.

   Note: The device only supports certificates of type **"Base64"**.

8. To view installed certificates:
   a. Select **[Security Certificates]** in the directory tree for **[Security]**.
   b. Click on the checkbox for the required certificate in the list.

c. Click **[View/Save].** The certificate details are displayed.

IP Sec

IP Sec (IP Security) consists of the IP Authentication Header and IP Encapsulating Security Payload protocols, that secure IP communications at the network layer of the group of protocols, 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 used to send IP Sec encrypted data over the TCP/IP network to the printer. Providing additional security in the negotiating process, SSL (Secure Sockets Layer protocols) are used to assure the identities of the communicating parties with digital signatures (individualized checksums verifying data integrity), precluding password guessing by network sniffers.

IP Sec security settings are the means by which an administrator can configure multiple groups of hosts and groups of protocols. Also this feature is used to setup IPsec and IKE (Internet Key Exchange) protocols on the printer.

The IP Sec implementation is a ‘full’ implementation that the device can initiate a connection for print, scan and administration, and fully work with other industry IPsec nodes. IPsec is necessary for securing many protocols including:

- **LPR and Port9100 printing**
- **FTP Filing**
- **Scan to E-mail**
- **LDAP**
- **Internet Fax**

Security Policies: To Enable IP Sec

Note: IP Sec cannot be enabled until SSL (Secure Sockets Layer) is enabled on the device. To enable SSL on a device, the device needs to have a Server Certificate. For instructions to set up a Server Certificate, refer to Security Certificate Management on page 179.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[IP Sec]** in the directory tree.
3. Ensure **[Security Policies]** tab is highlighted under the **IPsec** heading.
4. In the **Settings** area, check the **[Enabled]** checkbox for **Enablement** enable the IP Sec.
5. Click on the **[Apply]** button.

Note: It is recommended that IP Sec is enabled after the Host Groups, Protocol Groups and Action have been configured and defined.

Define Policy

An IPsec Policy is a set of conditions, configuration options and security settings which allows two systems to agree on how to secure traffic between them. Multiple policies can be simultaneously active, however the scope and policy list order may alter the overall policy behavior.

Note: Before creating Policies, configure Host Groups, Protocol Groups and Actions.

6. In the **Define Policy** area, there are three policy options:
   - **Hosts Groups**
   - **Protocol Groups**
   - **Action**

   This area allows you to select settings for allowing or disallowing Hosts and Protocols and what action to be taken.
7. For each individual option select settings from each drop-down menu.
8. Click on the **[Add Policy]** button.

Saved Policies

9. In the **Saved Policies** area, there will be a list of all the policies saved.
10. To delete a policy, highlight the policy and click on the **[Delete]** button.
11. Also you can prioritise an individual policy by clicking the **[Promote]** and **[Demote]** buttons.

Disable IP Sec at the device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[IP Sec]**.
3. Touch **[Disable]**, then touch **[Save]**.
4. Press the **<Log In/Out>** button.
5. Touch **[Logout]** to exit the Tools pathway.

Host Groups

Host Group page allows you to view and manage host groups. A host group is a logical grouping of hosts based on their specific IP Address or subnet address range.This option displays all the Host Groups saved and the details of each Host Group.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[IP Sec]** in the directory tree.
3. Ensure **[Host Groups]** tab is highlighted under the **IPsec** heading.
4. Host Groups can be deleted by highlighting a Host Group in the **IP Host Group** area, and clicking on the **[Delete]** button. If the Host Group selected is not being used by a security policy, then click on the **[OK]** button.

5. To add or edit a Host Group in the **IP Host Group** area, either click on the **[Add New Host Group]** button or highlight a Host Group and click on the **[Edit]** button.

   Note: If you change the name of the Host Group that is being used in the **Security policy**, then the updated host group name will also be reflected in the security policy details.

6. In the **IP Host Group Details** area:
   a. To define or modify a Host Group enter the name of the Host Group in the **[Name]** field.
   b. Enter a description or purpose of this Host Group in the **[Description]** fields.
7. In the **Address List** area select at least one set of network information.
   a. Select either **[IPv4]** or **[IPv6]**.
   b. From the **Address Type** drop-down menu, select one of the following:
      - **Specific** - to specify a single IP Address.
      - **All** - if all addresses of the IP type are to be included.
      - **Subnet** - to specify a range of IP Addresses.
   c. For the **[IP Address]** field, enter the Specific or Subnet address range. For a Subnet range, enter the lowest IP Address in the fields provided, then the final IP lower octet (for IPv4) or range (for IPv6) in the final field.
   d. Click on the **[Add]** button, to add the address range to the host group.
8. Click on the **[Save]** button to return to the **IPsec** page.
9. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"** to save changes and return to the IP Sec page.

Protocol Groups

This option displays all the Protocol Groups saved and the details of each Protocol Group.

1. From the **IP Sec** page, click on the **[Protocol Groups]** tab under **IPsec** heading.
2. Protocol Groups can be deleted by highlighting a Protocol Group in the **IP Protocol Groups** area and clicking on the **[Delete]** button. If the Protocol Group selected is not being used by a security policy, then click on the **[OK]** button.
3. To add or edit a Protocol Group in the **IP Protocol Groups** area click on either the **[Add New Protocol Group]** button or highlight a Protocol Group and click on the **[Edit]** button.

   Note: If you change the name of a Protocol Group that is being used in Security policy, then the updated protocol group name will also be reflected in the security policy entry.

   a. In the **IP Protocol Group Details** area, enter the name of the protocol group in the **[Group Name]** field.
   b. Enter description for this protocol group in the **[Description]** field.
   c. Check the required services checkboxes for this protocol group under **[Service Name]**.
4. In the **Custom Protocol** area:
   a. Check the corresponding checkboxes to select or deselect a custom protocol. Enter details in the **[Service Name]** field.
   b. From the **[Protocol]** drop-down menu select the protocol type.
   c. Enter the port number in the **[Port]** field.

d. From the **[Device is]** drop-down menu, select either **[Server]** or **[Client]**.

Note: The **Service Name**, **Protocol Type**, **Port Number** and **Device is** fields for a Custom Protocol will be disabled when its associated checkbox is unchecked.

5. Click on the **[Save]** button to return to the **IPSec** page.

Actions

This option displays the list of actions associated with the IPsec security policies. You can view and manage IP actions that can be used in the security policies.

1. From the **IP Sec** page, click on the **[Actions]** tab under **IPsec** heading.
2. To delete an Action, highlight an Action in the **IP Actions** area and click on the **[Delete]** button. If the Action selected is not being used by a security policy, then click on the **[OK]** button.
3. To add or edit an Action, in the **IP Protocol Group** area:
   a. Click either on the **[Add New Action]** button to add a new Action or highlight an Action and click on the **[Edit]** button to edit details of an Action.

   Note: If you change the name of an Action that is being used in Security policy, then the updated action name will also change in the security policy entry.
4. **Step 1 of 2** page displays, in the **IP Action Details** area:
   a. Enter a name for this IP Action in the **[Action Name]** field.
   b. Enter description for this IP Action in the **[Description]** filed.
5. In the **Keying Method** area:
   a. Select a Keying Method. This will specify the type of authentication used in an IP Sec policy. Select one of the following:
      - **Manual Keying** - this method is used if client devices are not configured for, or do not support, IKE.
      - **Internet Key Exchange (IKE)**- this is a keying protocol that works on top of IPsec. IKE offers a number of benefits including: automatic negotiation and authentication; anti-replay services; certification authority (CA) support; and the ability to change encryption keys during an IPsec session. Generally, IKE is used as part of virtual private networking.
      - **X.509 Certificate (Local Certificate)** - this is a public key certificate.
      - **Trusted Root Certificate**.
      - **Pre-shared Key Passphrase** - the use of pre-shared key authentication is not recommended because it is a relatively weak authentication method.

   b. If you select **[Internet Key Exchange (IKE)]**, enter the pre-shared key passphrase in the **[Pre-shared Key Passphrase]** field.

   Note: Only one Action may be created when selecting Internet Key Exchange (IKE) Keying Method.
6. Click on the **[Next]** button to display the **Step 2 of 2** screen.

If you Selected Manual Keying as the Keying Method:

1. In the **Mode Selections** area, select one of the **[IPsec Mode]** options from the drop-down menu:
   - **Transport Mode** - this is the default Mode for IP Sec. This only encrypts the IP payload.

- **Tunnel Mode** - this mode encrypts the IP header and the payload. It provides protection on an entire IP packet by treating it as an AH (Authentication Header) or ESP (Encapsulating Secuirty Payload) payload.
  When this mode is selected, you have the option of specifying a host IP Address

2. In the **Security Selections** area select preferred option and enter the required information.
3. Click on the **[Save]** button to return to the **IP Sec** - **Action** page.

If you Selected Internet Key Exchange (IKE) as the Keying Method:

IKE Phase 1 authenticates the IPSec peers and sets up a secure channel between the peers to enable IKE exchanges.

IKE Phase 2 negotiates IP Sec System Administrator to set up the IP Sec tunnel.

1. In the **IKE Phase 1** area:
   a. For **[Key Lifetime]** enter length of time that this key will live, either in seconds, minutes or hours.
   b. Select required option from the **[DH Group]** drop-down menu. Choose one of following:
      - **DH Group 2** - which provides a 1024 bit Modular Exponential (MODP) keying strength.
      - **DH Group 14** - which provides a 2048 bit MODP keying strength. Diffie-Hellman (DH) is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.
   c. For **Hash - Encryption**, check the required checkboxes:
      - **SHA1** (Secure Hash Algorithm 1) and **MD5** (Message Digest 5) are one-way hashing algorithms used to authenticate packet data. Both produce a 128-bit hash. The SHA1 algorithm is generally considered stronger but slower than MD5. Select MD5 for better encryption speed, and SHA1 for better security.
      - **3DES** (Triple-Data Encryption Standard) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.
      - **AES** (Advanced Encryption Standard) is a more secure method compared to 3DES.
2. In the **IKE Phase 2** area:
   a. Select from the **[IPSec Mode]** drop-down menu one of the following:
      - **Transport Mode** - this provides a secure connection between two endpoints as it encapsulates the IP payload, while Tunnel Mode encapsulates the entire IP packet.
      - **Tunnel Mode** - this provides a virtual ‘secure hop’ between two gateways. It is used to form a traditional VPN, where the tunnel generally creates a secure tunnel across an untrusted Internet.
   b. If you select **[Tunnel Mode]**, then select either **[Disabled]**, **[IPv4 Address]** or **[IPv6 Address]**.
   c. If you select **IPv4 Address** or **IPv6 Address**, enter IP Address details.
   d. From the **[IPsec Security]** drop-down menu, select either, **Both**, **ESP** or **AH**.
      AH (Authentication Header) and **ESP (Encapsulating Security Payload)** are the two main wire-level protocols used by IPsec, and they authenticate (AH) and encrypt and authenticate (ESP) the data flowing over that connection. They can be used independently or together.
   e. For **[Key Lifetime]** enter length of time that this key will be valid for, either in seconds, minutes or hours.

f. Select the preferred option from the **[Perfect Forward Secrecy]** drop-down menu. Default is '**None**'

g. Check the required checkboxes for **[Hash]** and **[Encryption]**.
Hash refers to the authentication mode, which calculates an Integrity Check Value (ICV) over the packet's contents. This is built on top of a cryptographic hash (MD5 or SHA1).
Encryption uses a secret key to encrypt the data before transmission. This hides the contents of the packet from eavesdroppers. Algorithm choices are AES and 3DES

Note: **Encryption** will not be shown if **[IPsec Security]** is set to **AH**.

3. Click on the **[Save]** button to return to the **IPSec** - **Action** page.

Security Certificates

A Trusted Certificate Authority is a Certificate Authority (CA) that is trusted to authenticate digital certificates. This page allows trusted root certificates to be uploaded to a server so that the server will 'trust' any certificates that have been signed by that CA.

Digital certificates and the enablement of SSL provides encryption for all workflows where the device is used as a HTTPS server.

Workflows include:

- Administration of the device via Internet Services
- Printing via Internet Services
- Printing via IPP
- Scan Template Management
- Workflow Scanning via HTTPS
- Administration of Network Accounting

To Access the Security Certificates Screen

The device exports the signed certificate to the client to establish an SSL/HTTPS connection.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[Security Certificates]** in the directory tree.

   The Security Certificates page shows any currently installed trusted root certificates in the **Root/Intermediate Trusted Certificate(s)** tab.

To Install a Machine Root Certificate

To complete this procedure you must have a digital certificate available. For instructions to configure a digital certificate, refer to Security Certificate Management on page 179.

1. At the **Security Certificates** screen, select the **[Root/Intermediate Trusted Certificate(s)]** tab and click on the **[Install external Root/Intermediate trusted certificates]** button.
2. Click the **[Choose File]** button to locate the signed certificate from the Trusted Certificate Authority. This file has an extension **"CER"** or **"CRT"**. Click on the **[Open]** button.
3. Click on the **[Next]** button. The details of the Certificate are displayed. Change the friendly name of the Certificate if required and click **[Next].**
4. The digital certificate will appear in the installed certificates list in the **Root/Intermediate Trusted Certificate(s)** area.

To Delete a Certificate

1. At the **Security Certificates** screen, select a certificate from the list in the **Installed Certificate** area.

2. Click on the **[Delete]** button.
3. Click on the **[OK]** button when the acknowledgement message appears.

To Request a Machine Root Certificate

If the device does not have a trusted root certificate, or if it is using a self-signed certificate, users may see an error message related to the certificate when attempting to connect to the device’s Internet Services server. To resolve this, install the generic Xerox Root CA Certificate in user's Web browsers.

1. At the **Security Certificates** screen, right-click on the **[Download the Generic Xerox Device CA]** link which appears at the bottom of the screen, under the installed Certificates list.
2. Select **[Save Target As]**.
3. Browse to the location where you want to save the **cacert.crt** file and click on **[Save]**.

   The **cacert.crt** file is now ready to be uploaded to any device needing a Machine Root Certificate.

802.1X

The device supports 802.1X authentication based on the Extensible Application Protocol (EAP). 802.1X Port Based Network Access Control is used to ensure that devices that are connected to the network have the proper authorization. The 802.1X configuration is used to authenticate the device rather than an individual user. After the device has been authenticated, it will be accessible to users on the network.

The System Administrator can configure the machine to use one EAP type. EAP types currently supported on the device are:

- **EAP-MD5** - Extensible Authentication Protocol (EAP). This method offers minimal security.
- **PEAPv0/EAP-MS-CHAPv2** - Protected Extensible Authentication Protocol (PEAP). This is an open standard authentication method and is widely supported by software vendors. EAP-MS-CHAPv2 is an inner EAP method supported by Microsoft.
- **EAP-MS-CHAPv2** - this is the Microsoft-supported EAP method, but does not include the PEAP shell.
- **EAP-TLS** - EAP-Transport Layer Security is a strong, open standard authentication method that is widely supported.

  Note: Only **EAP-TLS** type authentication is available when FIPS 140-2 is enabled on the device.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Create a user name and password on your authentication server which will be used to authenticate the machine.
- Ensure your 802.1X authentication server and authentication switch are available on the network.

To Configure 802.1X

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

Note: When FIPS 140-2 is enabled, 802.1X authentication can only be enabled at the device if the saved EAP is EAP-TLS.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[802.1X]**.
   a. Touch **[Enable]**.
   b. Select the **Authentication Method** (EAP type) used on your network by touching the **[Authentication Method]**.

   Note: The **EAP-TLS** method is not available for selection at the device. To use EAP-TLS, 802.1X must be configured at the web interface.

   c. Touch **[Username]** field and enter the user name required by your authentication switch and server using the on-screen keyboard.

   d. Touch **[Save]**.
   e. Touch the **[Password]** field and enter the password using the on-screen keyboard.
   f. Touch **[Save]**.
3. Touch **[Save]**. The network controller will now reset taking the device offline for several minutes.
4. When the device comes back online, if the Tools screen is still displayed with a message indicating that you are still logged in as Administrator, press the **<Log In/Out>** button.
5. Touch **[Logout]** to exit the Tools pathway.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[802.1X]** in the directory tree.
3. In the **Configure 802.1X** area:
   a. For **Protocol**, check the **[Enable 802.1X]** checkbox to enable this feature.
   b. Select an authentication method from the **[Authentication Method]** drop-down menu.

   Note: When FIPS 140-2 is enabled, only EAP-TLS type authentication is available.

   c. Enter a login name to use in the **[User Name (Device Name)]** field.
   d. Enter a password to use to access the account in the **[Password]** and **[Retype Password]** field.
   e. Check the **[Select to save password]** checkbox.
4. Click on the **[Apply]** button to save changes.
5. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

To Disable 802.1X

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[802.1X]**.
   a. Touch **[Disable]**.
   b. Touch **[Save]**.
3. Press the **<Log In/Out>** button.
4. Touch **[Logout]** to exit the Tools pathway.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.

2. Select **[802.1X]** in the directory tree.
3. In the **Configure 802.1X** area:
   a. For **Protocol**, uncheck the **[Enable 802.1X]** checkbox to disable this feature.
4. Click on the **[Apply]** button to save changes.
5. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

System Timeout

This feature resets the system to the default state after a set amount of time elapses without any user interface activity.

If users do not interact with Internet Services web pages within the time defined, logged in users will be logged and all unsaved settings will be lost.

When Authentication and/or Accounting is on (a user is logged in) and the System Timeout timer expires and if no partial job exists, the system shall log the user out (without warning or notification) and perform a Reset to Default.

At Your Workcentre:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Select **[System Timeout]** in the directory tree.
3. The System Timeout page displays. In the **Web System Timer** area, for **[Minutes]**, enter the time the system will wait before a logged in user will be logged out. You can enter a time from 6 to 60000 minutes.
4. Click on the **[Apply]** button.
5. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

On Demand Overwrite

Overview

The On Demand Overwrite feature provides security conscious customers with the ability to delete data from the device's hard disk.

The device's hard disk stores data similar to the way a hard drive functions on a personal computer, but with the data encrypted for extra protection. When Print, Copy, E-mail, Internet Fax and Scan jobs are submitted to the device, information is stored on the device's hard disk (if these features are installed and configured on the device).

The On Demand Overwrite feature can be used by a System Administrator to overwrite the image data.

There are two types of Image Overwrite:

- **Standard**: Standard Image Overwrite will delete all image data from the memory and hard disk, except:
  - Jobs and folders stored in the Reprint Saved Jobs feature.
  - Jobs stored in the Scan to Mailbox feature (if installed).
  - Fax Dial Directories.
  - Fax Mailbox contents.

  The process takes approximately 30 minutes to complete. The device is taken offline until the overwrite is complete and any existing jobs in the print queue are terminated. Once begun, the overwrite process cannot be cancelled.
- **Full:** Full Image Overwrite will delete all image data from the memory and hard disk, including:
  - Jobs and folders stored in the Reprint Saved Jobs feature.
  - Jobs stored in the Scan to Mailbox feature (if installed).
  - Fax Dial Directories.
  - Fax Mailbox contents.

  This will take approximately 90 minutes to complete. The device is taken offline until the overwrite is complete and any existing jobs in the print queue are terminated. Once begun, the overwrite process cannot be cancelled.

Information Checklist

Before starting the procedure, ensure the following task has been performed:

- Ensure the device is fully functioning in its existing configuration prior to overwriting.

To Verify that On Demand Image Overwrite is an Installed Option

If a Configuration Report did not print during SIM installation, at the Device print the report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.

4. Touch **[Print Report]**.
5. Touch **[Close]**.

On the Configuration Report, check under the **Installed Options** heading if **On Demand Image Overwrite** is an installed and enabled option.

To Perform an Image Overwrite at the Device

This procedure will overwrite the image data from the hard disk. This excludes Embedded Fax data, when this feature is installed on the device.

> Note: All existing jobs (excluding Embedded Fax), regardless of their state are deleted and all job submission is prohibited for the duration of the overwrite. Do not switch off the device while image overwrite is in progress.

> Note: The device must not be in diagnostics mode when the Overwrite is started. Diagnostics Mode is used by a Customer Service Representative when servicing the device.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Security Settings]**.
2. Touch **[On Demand Overwrite]**.
3. Select one of the following:
    - **Standard Image Overwrite**
    - **Full Image Overwrite**

    a. Touch **[Start Image Overwrite]** to start the Image Overwrite process.

    b. The **Image Overwrite Confirmation** screen display. Touch **[Overwrite]** to begin. The device will be taken offline and will be unable to receive any incoming jobs.

    c. Following completion of the Overwrite the On Demand Overwrite completion screen appears. Touch **[Close]**. The network controller will reboot and network functionality will be unavailable for several minutes.

    When rebooted, the Disk Overwrite confirmation report is printed. This details the status and time of the overwrite.

    To verify the overwrite has completed view the Confirmation Sheet, under Confirmation Details. The Job Information: Status ESS Disk should read '**SUCCESS**'.

To Perform an On Demand Overwrite over the Network

When the device has a network controller and is connected over the network, it is possible to run the Image Overwrite function using a web browser. This is performed using Internet Services.

> Note: All existing jobs, regardless of their state, will be deleted and all job submission will be prohibited for the duration of the overwrite. Do not switch off the device while image overwrite is in progress.

> Note: The device must not be in diagnostics mode when the Overwrite is started. Diagnostics Mode is used by a Customer Service Representative when servicing the device.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network.
- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 19, so that the web user interface (Internet Services) can be accessed.
- Ensure that no one is currently using the device.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[On Demand Overwrite]** link.
3. Select **[Manual]** in the directory tree.
4. Click on the **[Start]** button for either **Standard** or **Full** image overwrite.
5. A confirmation pop-up screen displays. Click on the **[OK]** button and the overwrite will commence. The device will be taken offline and will be unable to receive any incoming jobs. Any existing jobs in the queue will be deleted.
6. The network controller will reboot and network functionality will be unavailable for several minutes. When rebooted, the **On Demand Overwrite Confirmation Report** will print. This details the status and time of the overwrite.

   To verify the overwrite has completed, view the report. Under Confirmation Details: The Job Information: Status ESS Disk should read '**SUCCESS**'.

   Note: If you wish to backup jobs and folders prior to Full Overwrite, on the **On Demand Overwrite: Manual** page, click on the link at the bottom of the page to navigate to the **Reprint Saved Jobs** feature. For more information on Reprint Saved Jobs feature, refer to Reprint Saved Jobs on page 305.

To Schedule On Demand Overwrite

A TCP/IP network-connected device can be set to overwrite image data on a daily, weekly, or monthly basis. To schedule a daily overwrite, perform the following steps.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[On Demand Overwrite]** link.
3. Select **[Scheduled]** in the directory tree.
4. In the **On Demand Overwrite > Scheduled** page:
   a. From the **[Frequency]** drop-down menu, select the frequency for the overwrite to occur.
   b. If **[Daily]** is selected, specify the time for the Overwrite in **[Time]** (24-Hour Clock). The device will be taken offline each day at the time specified to perform the overwrite.
   If **[Weekly]** is selected, select a day in the week for **[Day of Week]**. For **[Time]** specify the

time for the overwrite to run on that day of the week.
If **[Monthly]** is selected, select a day between 1 and 28 for **[Day of Month]**, for **[Time]** specify the time for the for the overwrite to run on that date of the month.

c. Select either **[Standard]** or **[Full]** overwrite for **Type**.

d. Click on the **[Apply]** button.

e. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Immediate Image Overwrite

Overview

The Immediate Image Overwrite feature provides security conscious customers with the ability to overwrite jobs from the device’s image disk. The device's hard disk stores data similarly to the way a hard drive functions on a personal computer, but with the data encrypted for extra protection. When Print, Copy, E-mail, Internet Fax and Scan jobs are submitted to the device, information is stored on the device's hard disk (if these features are installed and configured on the device). Immediate Image Overwrite performs an overwrite on a job by job basis, immediately after each job has been processed. For devices with network connectivity, all jobs that pass through the device are immediately overwritten. For devices without network connectivity and which have Embedded Fax installed, all fax jobs are immediately overwritten.

> Note: Copy jobs are not stored on the device’s image disk, so they do not need to be overwritten.

When enabled the feature becomes immediately operational and requires no configuration by the System Administrator.

Immediate Image Overwrite and Internet Fax Jobs

> Note: Internet Fax jobs are not overwritten until the job's Delivery Status Notifications (DSN's) and Message Disposition Notifications (MDN's) have been received, or timeout occurs, i.e. the job is not overwritten until after the **Delivery Confirmed** state or **Sent state** is exited. This means that the job may not be overwritten for up to 72 hours as this is the maximum timeout setting for an Internet Fax job.

Information Checklist

Before starting ensure the following item is available or task has been performed:

- Ensure the device is fully functioning in its existing configuration prior to installation.

To Verify that Immediate Image Overwrite is an Installed Option

Print a Configuration Report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**

On the Configuration Report, check under the **Installed Options** heading if **Immediate Image Overwrite** is an installed and enabled option.

To Disable or Enable Immediate Image Overwrite

At the Device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Optional Services]**.
3. Touch **[Image Overwrite Security]**.
4. Touch **[Enable]** or **[Disable]**, then touch **[Save]**. The change in status will be immediately effective.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

Immediate Image Overwrite Status

When Immediate Image Overwrite is configured on the device any job that is overwritten will have its overwrite status displayed in the Completed Jobs queue details window.

To view Overwrite Status at the Device

1. Press the **<Job Status>** button.
2. Touch the **[Other Queues]** button (if necessary).
3. Touch the drop-down menu and select **[All Completed Jobs]**.
4. Touch a job in the queue.
5. View the **Immediate Overwrite** status under **Value**. This will appear as **Successful** or **Failed**.
6. Touch **[Close]**.

Workflow Scanning 9

Workflow Scanning enables users to scan an original document, convert it to an electronic file, and distribute and archive the file in a variety of ways. The final destination of the electronic file depends on the template chosen by the user at the device's user interface. Workflow Scanning is an automated work management feature. It automates the processes of getting large volumes of hardcopy documents into suitable scanned image formats, stored, distributed or made accessible for further processing, as needed. When workflow is optimized for purpose, and IT infrastructure considerations are taken into account, substantial benefits can be achieved in efficiency and management

Workflow Scanning is set up and controlled by templates. A template is a file that stores scanning and routing preference for a given workflow. 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 scanned file will be archived or published on a pre-determined network server called a File Repository, and then, with the help of server or desktop software:

- Routed to a user's PC desktop for viewing or editing.
- Integrated with a variety of popular document management and workflow applications.
- Sent to a network directory or filing location for later retrieval.
- Sent to an e-mail distribution list.

Workflow Scanning User Authentication

Authentication can be enabled to prevent unauthorized access to the Workflow Scanning feature. If Authentication is enabled, users will be prompted to enter a network user name and password, or a PIN, before they can access the Workflow Scanning feature. For a full description of the Authentication feature refer to the Authentication section of this guide. Authentication can be configured after Workflow Scanning has been installed.

Device Authentication

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

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network.
- Ensure you have the Scanning Kit.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

This is required to access Internet Services to configure Workflow Scanning. The Internet Services function is accessed through the embedded HTTP server on the device and enables System Administrators to configure scan settings by using an Internet browser.

- If you require color or grayscale scanning, or scan to JPEG you will need the Color Scanning Enablement Kit.
  The Kit can be purchased from your Xerox Sales Representative. Follow the instructions with the Color Scanning Enablement Kit to ensure the Kit is installed before you continue with the Network Scanning instructions.

Enable Workflow Scanning

Print a Configuration Report:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Reports]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report, check under the **Workflow Scanning Setup** heading if **Workflow Scanning Enabled** is enabled.

At the Device:

> Note: To configure this feature or setting access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Optional Services]**.
3. Touch **[Workflow Scanning]**.
4. Touch **[Enable]**.
5. Touch **[Save]**.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools Pathway.

Configure a File Repository

Scanning with the device 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 device using one of the file transfer options below.

- **FTP (File Transfer Protocol):** Requires an FTP server running on a server or a workstation.
- **NetWare NCP (NetWare Core Protocol):** Available for filing to a NetWare server.
- **SMB (Server Message Block):** Available for filing to an environment that supports the SMB protocol.

- **HTTP/HTTPS:** Supports scans to a web server using a CGI script.

  Note: The device uses two repositories:
  A **File Repository**, used by the **Workflow Scanning** service.
  A **Fax Repository**, used by the **Server Fax** service.

File Transfer Protocol (FTP)

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that File Transfer Protocol (FTP) services are running on the Server or Workstation where images scanned by the device will be stored.

  Write down the IP Address or Host Name.
- Create a folder within the FTP root. This is the Scan Repository.

  Write down the Directory Path Structure.
- Create a user account and password which has read and write access to the folder within the FTP root.

  Write down the user Account and Password details.
- Test the FTP connection by logging into the Scan Repository directory from a PC with the user account and password:
  - Create a new folder within the directory.
  - Delete the folder.

Enter the Scan Repository Details via Internet Services

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[File Repository Setup]** in the directory tree. The **File Repository Setup** page displays.
4. Click on the **[Add New]** button or the **[Edit]** button (if the default File Repository has been set).

   Note: During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.
5. The **File Destination** page displays. In the **Settings** area:
   a. Enter a descriptive name for the file repository in the **[Friendly Name]** field.
   b. Select **FTP** from the **[Protocol]** drop-down menu.
   c. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   d. Enter details of the Repository Location in the **[IP Address: Port]** or **[Host Name: Port]** field. The default port number is 21.
   e. Type in the path to the repository in the **[Document Path]** field. Enter the full path to the directory, starting at the root of FTP services. For example: **/directory name/directory name**.
   f. For **[Login Credentials to Access the Destination]**, select one of the following:

- **Authenticated User and Domain** - select this method if the user name and domain are to be authenticated via LDAP.
- **Authenticated User** - select this method if just the user name is to be authenticated via LDAP.
- **Prompt at User Interface** - select this method to have each user enter authentication credentials at the printer's control panel.
- **System** - select this method if the credentials are going to be typed in on this page and stored in the device's memory
- If you select **System**, enter details in the **[Login Name]** and **[Password]**.
- Enter the password again in the **[Retype password]** field.
- Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.

g. Click on the **[Save]** button to accept the changes.

The Next Step is to proceed to the General Settings. Refer to Configure General Settings on page 209.

NetWare NCP (NetWare Core Protocol)

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Ensure NetWare protocol is enabled on your device.

  Print a Configuration Report to verify that NetWare protocol is enabled on your device.

  a. Press the **<Machine Status>** button.

  b. Touch the **[Machine Information]** tab.

  c. Touch **[Print Reports]**.

  d. Touch **[Print Report]**.

  e. Touch **[Close]**.

  The Configuration Report will print. On the report under the **Network Setup** if **NetWare** is enabled.

  For instructions on how to enable NetWare, refer to NetWare on page 127.
- Designate or create a new directory on the NetWare server to be used as the scan filing location (repository). Note the server name, server volume, directory path, the NDS Context and Tree, if applicable.
- Create a user account and password with access to the scan directory. When a document is scanned the device logs in using the account, transfers the file to the server and then logs out. Note the user account and password.
- Test your settings 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.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[File Repository Setup]** in the directory tree. The **File Repository Setup** page displays.
4. Click on the **[Add New]** button or the **[Edit]** button (if the default File Repository has been set).

   Note: During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

5. The **File Destination** page displays. In the **Settings** area:
   a. Enter a descriptive name for the file repository in the **[Friendly Name]** field.
   b. Select **NetWare** from the **[Protocol]** drop-down menu.
   c. Enter the name of the server in the **[Server Name]** filed.
   d. In the **[Server Volume]** field, enter the path to the repository on the NetWare server.
   e. If you are using Bindery or Bindery emulation, leave the **[NDS Tree]** field blank, if you are using NDS, this field cannot be left blank. The default tree name is **"Xerox_DS_Context"**.
   f. If you are using Bindery or Bindery emulation, leave the **[NDS Context]** field blank. If you are using NDS, this field cannot be left blank. The default context name is **"Xerox_DS_Context**".
   g. Type in the path to the repository in the **[Document Path]** field. Enter the full path to the directory, starting at the root of FTP services. For example: **/directory name/directory name**.
   h. For **[Login Credentials to Access the Destination]**, select one of the following:
      - **Authenticated User and Domain** - select this method if the user name and domain are to be authenticated via LDAP.
      - **Authenticated User** - select this method if just the user name is to be authenticated via LDAP.
      - **Prompt at User Interface** - select this method to have each user enter authentication credentials at the printer's control panel.
      - **System** - select this method if the credentials are going to be typed in on this page and stored in the device's memory
      - If you select **System**, enter details in the **[Login Name]** and **[Password]**.
      - Enter the password again in the **[Retype password]** field.
      - Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.
   i. Click on the **[Save]** button to accept the changes.

The Next Step is to proceed to the General Settings. Refer to Configure General Settings on page 209.

Server Message Block (SMB)

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- 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.
- Create a user account and password for the device with full access rights to the scan directory. Note the user account and password.
- 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.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[File Repository Setup]** in the directory tree. The **File Repository Setup** page displays.
4. Click on the **[Add New]** button or the **[Edit]** button (if the default File Repository has been set).

   Note: During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

5. The **File Destination** page displays. In the **Settings** area:
   a. Enter a descriptive name for the file repository in the **[Friendly Name]** field.
   b. Select **SMB** from the **[Protocol]** drop-down menu.
   c. Select either **[IPv4 Address]** or **[Host Name]**.
   d. Enter details of the SMB server location in the **[IP Address: Port]** or **[Host Name: Port]** fields.
   e. Type in the share name in **[Share]** field that will be used for filing scanned documents.
   f. Type in the path to the repository in the **[Document Path]** field. Enter the full path to the directory, starting at the root of FTP services. For example: **/directory name/directory name**.
   g. For **[Login Credentials to Access the Destination]**, select one of the following:
      - **Authenticated User and Domain** - select this method if the user name and domain are to be authenticated via LDAP.
      - **Authenticated User** - select this method if just the user name is to be authenticated via LDAP.
      - **Prompt at User Interface** - select this method to have each user enter authentication credentials at the printer's control panel.
      - **System** - select this method if the credentials are going to be typed in on this page and stored in the device's memory.
      - If you select **System**, enter details in the **[Login Name]** and **[Password]**.
      - Enter the password again in the **[Retype password]** field.

- Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.

h. Click on the **[Save]** button to accept the changes.

The Next Step is to proceed to the General Settings. Refer to Configure General Settings on page 209.

HTTP/HTTPS

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that HTTP/HTTPS services and a web service (such as Apache) are running on the server, where POST requests and scanned data will be sent for processing by a CGI script. Note the IP address or host name.

  Note: HTTP and HTTPS protocol both require server-side scripts to allow files to be transferred to your HTTP server from your device.
  CGI (Common Gateway Interface) script: A program that is run on a web server, in response to input from a browser. The CGI script is the link between the server and a program running on the system, i.e a database.

- Download a sample script:

  At your Workstation:

  Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

  a. From the **Properties** tab, click on the **[Services]** link.

  b. Click on the **[Workflow Scanning]** link.

  c. Select **[File Repository Setup]** in the directory tree. The **File Repository Setup** page displays.

  d. Click on the **[Add New]** button or the **[Edit]** button (if the default File Repository has been set).

  e. The **File Destination** page displays. Select **[HTTP]** or **[HTTPS]** from the **[Protocol]** drop-down menu.

  f. Click on the **[Get Example Scripts]** link under **Script Path and Filename:** to download an example script in **PHP**, **ASP** or **Perl** language:

  g. Select an appropriate **Script Language** file which is supported by your HTTP Scan Repository server.

  h. Right-click on the required script and select **[Save Target As...]** to save the file to your HTTP Scan Repository server.

  i. Save the **[.zip]** or **[.gz]** file to a location on the desktop and extract it.

  j. Extract the downloaded file to the root of the **[Web Services]** home directory.
  Write down the path and filename as you will need it later.

- Create a login account for the device on the web server.

  a. Create a home directory for the device.

  b. Add a bin directory to the home directory.

  c. Place an executable CGI script in the bin directory.

d. Make a note of the complete path to the executable CGI script.
When a document is scanned, the device logs in using the account, sends a POST request along with the scanned file, then logs out. The CGI script handles the remaining details of file transfer.

- Create a directory on the web server, or an alternate server, to be used as a scan filing location (repository).
  a. Set appropriate read and write permissions.
  b. Make a note of this directory's path.
- Test the connection.
  a. Log in to the device's directory on the web server.
  b. Send a POST request and file to the web server.
  c. Check to see if the file was received at the repository.
- The script can be defined with script_name.extension or by path/script_name.extension.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[File Repository Setup]** in the directory tree. The **File Repository Setup** page displays.
4. Click on the **[Add New]** button or the **[Edit]** button (if the default File Repository has been set).

   Note: During device configuration, SMARTsend (if used) overwrites the Default Repository and Template Pool scan settings. If certain applications will use Default Repository settings, not matching SMARTsend settings, reconfigure the applications to use an Alternate Repository before configuring the device with SMARTsend's Add/Update feature.

5. The **File Destination** page displays. In the **Settings** area:
   a. Enter a descriptive name for the file repository in the **[Friendly Name]** field.
   b. Select **HTTP** or **HTTPS** from the **[Protocol]** drop-down menu.
   c. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   d. Enter details of the HTTP or HTTPS server in the **[IP Address: Port]** or **[Host Name: Port]** field. The default port number for **Host Name** and **HTTP** is 80 and for **HTTPS** is 443.
   e. The Network Scanning feature will use any proxy server settings specified. To view the settings click on the **[View HTTP Proxy Server Settings]** link.
   f. For **HTTPS** only: You can check the **[Validate Repository SSL Certificate]** checkbox to have the repository’s SSL certificate validated for the correct hostname and checked for a signature of a trusted certificate authority. Or click **[View Trusted SSL Certificates]** link to verify that the device has a digital certificate installed.
   g. Enter the script path and filename you downloaded and saved on your desktop earlier in the **[Script path and filename (from HTTP root)]** field.
   h. Type in the path to the repository in **[Document Path]** field. Enter the full path to the directory, starting at the root of HTTP or HTTPS server. For example: **/directory name/directory name**.
   i. For **[Login Credentials to Access the Destination]**, select one of the following:

- **Authenticated User and Domain** - select this method if the user name and domain are to be authenticated via LDAP.
- **Authenticated User** - select this method if just the user name is to be authenticated via LDAP.
- **Prompt at User Interface** - select this method to have each user enter authentication credentials at the printer's control panel.
- **System** - select this method if the credentials are going to be typed in on this page and stored in the device's memory
- If you select **System**, enter details in the **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
- Enter the password again in the **[Retype password]** field.
- Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.

j. Click on the **[Save]** button to accept the changes.

The Next Step is to proceed to the General Settings. Refer to Configure General Settings on page 209.

Configure General Settings

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[General]** link in the directory tree.

Note: The Confirmation Sheet specifies the success or failure of the Workflow Scanning job.

4. In the **Settings** area, select one of the following options from the **[Confirmation Sheet]** drop-down menu:
   - **Errors only** - select to prints a Confirmation Sheet only when the job is unsuccessful.
   - **On** - select to print a Confirmation Sheet after every Workflow Scanning job.
   - **Off** - when selected, turns off the Confirmation Sheet printing function.
5. In the **Distribution Templates** area:

   a. Under **Maximum Number of Job Templates**, it will display the maximum number of job templates that can be viewed from the device’s control panel.

   b. For **Allow Manual Entry of File Destinations**, check the **[Enabled]** checkbox to manually allow entry of file destination.

   c. If you want the device to automatically update templates stored in the Template Pool (a repository on the network), then enter the required time for the update in the **[Refresh Start Time]** area.

   d. To update the Template Pool List manually, click on the **[Refresh Template List Now]** button.

Note: The Refresh Template List capability only applies to templates stored in a Template Pool. Templates stored on the device are updated automatically.

6. In the **Template Distribution Repositories** area, select one of the following **Login Source** to control user access to a pool of templates stored on a remote server. Communications to the

server, including entry of the required device Login Name and Password, are set up by selecting **Advanced**, then **Template Pool Setup**, in the Internet Services directory tree:

- **Authenticated User** - to have the Authentication Server control remote template pool access.
- **Prompt at User Interface** - this works well for small offices without an Authentication server. Users are prompted to type in a user name and password at the printer's control panel when access to the template pool is requested.
- **Prompt if Authenticated User Does Not Match Template Owner** - to prompt authentication when system credentials do not match the template owner.
- **None** - if no user authentication is required.

7. In the **Job Log** area, for **Optional Information**, check on **[User Name]** and/or **[Domain]** checkboxes if you want these to appear in the Job Log when users log in to the device when Network Authentication is enabled.
8. Click on the **[Apply]** button.
9. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Configuring Validation Servers

The Validation Server's link within Internet Services enables you to configure a Validation Server that will verify metadata. Metadata is additional information that can be entered when a user scans their documents at the device. The administrator creates metadata entries when they configure Document Management Fields within a Workflow Scanning - Default Template.

A Validation Server is a service or application that is used to validate the metadata entered by the user when they scan their documents.

The Validation Server feature provides a way to reduce inconsistencies or inaccuracies in the data entered by a user.

When the user scans a document at the device and enters metadata, if one or more of the metadata objects require validation, the device will send the metadata to the validation server. The validation server checks the data against the criteria that have been set up on the validation server. The validation server either accepts the data as valid, or returns an error message which is displayed on the device.

If the validation server returns a successful validation response, then the job will proceed. If the metadata in the template or the metadata entered at the local UI is invalid, then the job will be canceled and is not transferred to the network.

Providing these levels of validation will ensure that the data entered via the system user interface will meet the requirements for that workflow.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network. TCP/IP and HTTP must be configured on the device.
- Ensure your validation server or application is installed on your network.

- Ensure Network Scanning is configured on your device.
- To communicate with the Validation server via HTTPS, SSL must be enabled on the device.

To Add or Edit a Validation Server

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Validation Servers]** in the directory tree.
   The Validation Servers page will allow you to configure the following settings:
   - **Add** - displays the **[Add Validation Server]** page, which allows you to configure a new validation server.
   - **Edit** - displays a page which allows you to edit the above settings for the selected server.
   - **Delete** - deletes the selected server.
4. In the **Validation Servers** area, click on the **[Add]** button to add a new validation server, or select an existing validation server from the list and click on the **[Edit]** button to display the **Add Validation Server** page.
5. In the **Server Information** area:
   a. For **Protocol**, select from the drop-down menu the communication protocol for the Validation Server.
   b. Select the method you want to use to specify the Validation Server. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter the IP Address and Port or Hostname and Port of the Validation Server in the **[IP Address: Port]** or **[Host Name: Port]** field.

   Note: The default port number is **80** if you select **HTTP** for **Protocol** or **443** if you selected **HTTPS** for **Protocol**.

   d. In the **[Path]** field, enter the path on the server.

   Note: The format for a directory path for FTP is **/directory/directory**, while the format for a directory path for SMB is **\directory\directory**.

   e. Specify the time in seconds after which the server will time out in the **[Response Timeout]** field. The range is from 5 to 100. The default is 8.
   f. Click on the **[Apply]** button to save settings and return to the **Validation Server** page.

To Delete a Validation Server from the list:

1. From the Validation Servers page, in the **Validation Servers** area:
   a. Highlight the Validation Server and click on the **[Delete]** button.
   b. Click on the **[OK]** button when you see the confirmation message **‘Are you sure you want to delete the selected validation server?’**.

Scanning Web Service

Use this page to examine the status of services required for Scanning Web Services.

The following services must be enabled and/or configured for Scanning Web Services to be available:

- **HTTP (SSL)**
- **Scan Template Management**
- **Scan Extension**

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Scanning Web Services]** in the directory tree.
4. In the **Setup (Required)** area, the following services will display the status of configuration:
   - **HTTP (SSL)** - displays the status of the HTTP (SSL) server. Click on the **[Settings]** button to review or change the HTTP Protocol Settings. For information on HTTP protocol settings, refer to the Enable Secure HTTP (SSL) on page 181.
   - **Scan Template Management** - displays the status of the Scan Template Management service. Click on the **[Settings]** button to enable or disable this HTTP Web Services.
   - **Scan Extension** - displays the status of the Scan Extension service (enabled or disabled). Click on the **[Settings]** button to enable or disable this HTTP Web Services.
5. For **Scan Template Management** and **Scan Extension** click on the **[Settings]** button to display the **HTTP - Web Services** page.

   c. Check or uncheck the **[Enable]** checkboxes for the individual services you want to enable or disable.

   d. Click on the **[Save]** button to accept the changes and return to the Scanning Web Services page.

Configuring the Default Template

The default template is created for the device, using Internet Services or SMARTsend software on the remote template pool server, and appears as DEFAULT in the list of templates on the device. The default template consists of configured scan settings and at least one network filing location. When the default template has been configured, all subsequent templates, created with Internet Services or SMARTsend software, inherit the settings. Users can modify these settings with any new templates they create. The default template settings, however, can only be changed by the System Administrator. The default template also cannot be deleted from either the local or remote template pool.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Default Template]** in the directory tree. The **Default Template** page displays.

4. In the **Destination Services** area, select the desired service by checking either the **[Fax]** or **[File]** (selected by default) checkbox.
   When selected, the service section will display on the page.

   Note: The **Fax** service requires the Server Fax feature to be enabled on the device.

File

In the **Default Template** page, in the **File** area, a list of file repository destinations for your scan distribution templates is displayed. The available file destinations is determined by the File Repository Setup:

- To specify an additional file destination (if one is available), click on the **[Add]** button. The File Destinations page will appear.
- To change an existing file destination, highlight the file and click on the **[Edit]** button. The File Destinations page will appear.
- To delete an existing file destination, highlight the file and click on the **[Delete]** button.

Add

1. To add an additional file destination, in the **File** area, click on the **[Add]** button.
2. In the **Add Destination to Template** area, select one of the following:
   - **Select from a Predefined List**.
   - **Enter a Scan Destination**.

- **Enter a Server Fax Number**.

If you select [Select from a Predefined List]:	If you select [Enter a Scan Destination]:
1. From the **File Destination** drop-down menu, select the destination file repository by its descriptive name. 2. **Protocol** will display the protocol (**FTP, SMB, HTTP, HTTPS**) used to communicate with the file repository. 3. **Host Name and Port** or **IP Address and Port** will display the host or the IP address of the repository. 4. Enter details in the **[Document Path]** field. 5. Select from the **[Filing Policy]** drop-down menu one of the following: • **Rename New File** - this adds an incrementing numeric value to the file name. • **Overwrite Existing File** - this deletes the previous file. • **Do Not Save** - the new file is not saved. • **Add Date to Name** - the current date and time are appended to the file name. 6. **Login Name** displays the account name used to access the repository.	1. Enter details in the **[Friendly Name]** field. 2. Select the protocol type used to communicate with the file repository from the **[Protocol]** drop-down menu. 3. Select either **[IPv4]**, **[IPv6]** or **[Host Name]**. 4. Enter details for either **[IP Address: Port]** or **[Host Name: Port]**. 5. Enter details in the following fields, depending on the Protocol selected: • If you selected **SMB**, enter details in the **[Share]** field. • If you selected **HTTP** or **HTTPS**, enter details in the **[Script path and filename (from HTTP root)]** field. 6. Enter the file path to the repository in the **[Document Path]** field. 7. Select from the **[Filing Policy]** drop-down menu one of the following: • **Rename New File** - this adds an incrementing numeric value to the file name. • **Overwrite Existing File** - this deletes the previous file. • **Do Not Save** - the new file is not saved. • **Add Date to Name** - the current date and time are appended to the file name. 8. Select the type of login and access required for **[Login Credentials to Access the Destination]**. 9. Enter details in the **[Login Name]**, **[Password]** and **[Retype password]** field.

3. Click on the **[Save]** button to return to the **Default Template** page.

Edit

1. In the **File** area, select a file destination, and click on the **[Edit]** button.
2. In the **Filing Destination** area the following information displays:
   - **File Destination** - this displays the descriptive name for the file repository.
   - **Protocol** - displays the protocol (**FTP, SMB, HTTP, HTTPS**) used to communicate with the file repository.
   - **IP Address and Port** or **Host Name and Port** - will display the host or the IP address of the repository.
   - **Login Name** - displays the account name used to access the repository.

- **Document Path** identifies the file path to the repository.

a. In the **[Add (Optional)]** field, specify a subdirectory for all scanning through this template.

b. Select from the **[Filing Policy]** drop-down menu one of the following:
   - **Rename New File** - this adds an incrementing numeric value to the file name.
   - **Overwrite Existing File** - this deletes the previous file.
   - **Do Not Save** - the new file is not saved.
   - **Add Date to Name** - the current date and time are appended to the file name.

c. Click on the **[Save]** button to return to the **Default Template** page.

Fax

From the **Default Template** page, in the **Fax** area, a list of file repository destinations for your scan distribution templates is displayed. The available fax destinations are determined by the File Repository Setup.

> Note: This option will only be available if the Server Fax option is installed on the device and Fax was selected as a Destination Service.

- To specify an additional fax destination (if one is available), click on the **[Add]** button. The Fax Recipients page will appear.
- To change an existing fax destination, highlight the fax destination from the list and click on the **[Edit]** button. The Fax Recipients page will appear.
- To delete an existing fax destination, highlight the fax destination and click on the **[Delete]** button.

1. In the **Fax** area, To add an additional file destination click on the **[Add]** button or to edit an existing file destination highlight the fax destination from the list and click on the **[Edit]** button. The **Fax Recipients** page will display.
2. In the **Fax Recipients** area:

   a. In the **[Add Fax Number]** field, enter a fax number and click on the **[Add]** button. The new number will appear in the **Fax Distribution List**.

   b. The **Fax Distribution List** field will display the list of fax numbers in the distribution list. To delete a fax number, highlight the number and click on the **[Delete]** button.

   c. To edit a fax number, highlight the number in the **Fax Distribution List** field. The number will appear in the **[Edit Fax Number]** field. Make the necessary changes and click on the **[Replace]** button.
3. In the **Delivery** area, select one of the following:
   - **Immediate** - this option will start the fax delivery process as soon as it is ready for delivery.
   - **Delayed Send** - this option will queue the fax delivery at the specified time of day.

   a. If you select **[Delayed Send],** in the **[Time]** field, enter the specific delayed time to start the fax delivery process.
4. Click on the **[Apply]** button to return to the **Default Template** page.

Document Management Fields (Optional)

This area allows you to add data fields to the Default Template. These data fields can either provide information or collect data from the user for each workflow scan job. This information is filed with your scanned documents in the Job Log. The Job Log can then be accessed by third party software for various purposes.

The following fields are available:

- To add a new field, click on the **[Add]** button. This brings up the **Add Document Management Field** page.
- To make changes to a field, highlight a Document Management from the list and click on the **[Edit]** button. This brings up the **Add Document Management Field** page.
- To delete a field, highlight a Document Management from the list and click on the **[Delete]** button.

At your Workstation:

1. From the **Default Template** page, in the **Document Management Fields (Optional)** area, to add an additional Document Management file, click on the **[Add]** button or to edit an existing file highlight the file from the list and click on the **[Edit]** button. The **Add Document Management Field** page will display.
2. In the **Field Attributes** area:
   a. Enter information in the **[Field Name]** field. This information entered assigns a name for the Document Management data that is to be associated with the scanned job. This value is not shown at the device user interface screen and is used by third party software to access the Document Management information. It can be up to 128 characters in length. This field cannot be left blank.

   b. For **User Editable** select one of the following method:
      - **Editable** - if you would like the user to be able to modify the value of this field. Enter a value in the **[Field Label]** field. The label should identify the purpose of this field to the user.
      - **Not Editable** - if the user can not change the Document Management Field's value. The user will not be presented with this Document Management Field at the device and the Default Value will be used.

   c. For **[Default Value]** field, enter details for this Document Management Field. The Default Value is optional if the user wants to edit the Document Management Field’s value. The Default Value is required if the user does not want to edit the Document Management Field’s value.

   d. If you selected **Editable,** you can check the following checkboxes:
      - **Require User Input** - to prompt the user to enter data for this Document Management field before scanning. This is done at the device.
      - **Mask User Input (****)** - selecting this will mask the user’s typing to protect privacy. This also enables the **Record User Input to Job Log**.
        Check the **[Record User Input to Job Log]** checkbox, to record all values entered by the user for this data field.

   Note: **Validate Data Before Scanning** options may also be available if there are validation servers configured for this device.
3. Click on the **[Apply]** button to return to the **Default Template** page.

Workflow Scanning

The **Workflow Scanning** section displays the image type settings.

To change the Workflow Scanning settings, click on the **[Edit]** button. This will display the **Workflow Scanning** page.

1. From the **Default Template** page, in the **Workflow Scanning** area:
   a. For **2-Sided Scanning**, select one of the following:
      - **1-Sided** - the scan service will only scan one side of each page of the input document.
      - **2- Sided -** the scan service will scan both sides of each page of the input document.
      - **2-Sided**, **Rotate Side 2 -** the scan service will scan both sides of each page of the input document and shall apply a 180 degrees rotation to the second side image such that the orientation of all input images are the same.

   b. The **Content Type** feature provides a convenient way to optimize the quality of your scanned output images based on the content in your original documents. Each selection adjusts the printer settings to compensate for the predominant attributes of the content that is being scanned. Select one of the following:
      - **Photo & Text** - this is best for documents that contain a mix of photographic images and text.
      - **Photo -** this is best for documents that contain photographic images and little or no text.
      - **Text** - this is best for documents that contain mostly text.

   c. The **Scan Presets** feature provides a convenient way to optimize scan settings to match the intended purpose of the scanned document. Select one of the following options:
      - **For Sharing & Printing** - this setting is best for sharing files to be viewed on-screen and for printing most standard business documents. Using this setting will result in small file sizes and normal image quality.
      - **For OCR** - this creates scanned images with clear, crisp lines and edges that provide the best OCR interpretation.
      - **For Archival Record** - this setting is best for standard business documents that will be stored electronically for record keeping purposes. Using this setting will result in the smallest file sizes and normal image quality.
      - **For High Quality Printing -** this setting is best for business documents containing detailed graphics and photos. Using this setting will result in large file sizes and the highest image quality.
      - **Simple Scan** - this provides faster scan processing by decreasing the overall quality of the scanned images.
2. Click on the **[Apply]** button to return to the **Default Template** page.

Advanced Settings

The Advanced Settings feature allows the user to select the enhancement feature for the scanned document.

1. From the **Default Template** page, to change the Advanced Settings, click on the **[Edit]** button in the **Advanced Settings** area. The **Advanced Settings** page displays.
2. In the **Advanced Settings** area:
   a. For the **Image Options**, adjust the following options:

- **Lighten/Darken -** use the controls (left and right arrow buttons) to adjust the overall brightness compared to the original.
- **Soften/Sharpen** - use the controls (left and right arrow buttons) to adjust how much edge sharpening is used.

b. For **Image Enhancement**, select the following options:

- **Contrast** - select either **[Auto Contrast]** or **[Manual Contrast]**. If Manual Contrast is selected, use the controls (left and right arrow buttons) to adjust the contrast.
- **Background Suppression** - this option prevents the reproduction of an unwanted background image, shading or bleed-through from the reverse side of the original. This will produce an output image with a mostly white background. Select either **[No Suppression]** or **[Auto Suppression]**.

c. Use the **[Resolution]** drop-down menu to set the scan resolution. Changing the resolution affects the amount of detail reproduced on graphic images. The range is from 72 DPI to 600 DPI.

d. For **Build Job**, check the **[Enabled]** checkbox to enable Build Job.

e. For **Quality/File Size**, use the controls (left and right arrow buttons) to select the level of compression to use for scanned images. When compression is increased, the file size drops, but at the expense of image quality. The middle setting is ideal for most scanning purposes.

3. Click on the **[Apply]** button to return to the **Default Template** page.

Layout Adjustment

The Layout Adjustment feature allows the user to select the page layout characteristics of the scanned images.

1. To change the Layout Adjustment settings, From the Default Template page, in the **Layout Adjustment** area, click on the **[Edit]** button. This will display the **Layout Adjustment** page.
2. In the **Layout Adjustment** area:

a. **Original Orientation** allows you to specify the format and placement of the originals when they are loaded on the document glass or document handler. This information is used to accurately display how the job will look when using page features such as Image Shift, Edge Erase, and Multiple Images. For **[Original Orientation]**, select one of the following options:

- **Portrait Originals** - this instructs the printer to orient all images in portrait mode.
- **Landscape Originals** - this instructs the printer to orient all images in landscape mode.

Note: If you are using the Document Glass, the orientation is as seen before turning it over on the Glass.

b. For **[Original Size]**, select one of the following options to specify the dimensions of the original scanned document:

- **Auto-Detect** - the scan service will automatically detect the size of the input document.
- **Manual Size Input** - allows you to identify the size of the input document from a pull-down menu. If the size you require is not listed, use the “Custom” option.
- **Mixed Size Originals** - select if the originals are different sizes.

c. The Edge Erase feature allows you to erase the spots, punch holes, noise, fold, crest, and staple marks that appear along any or all of the four edges of an input document. For **[Edge Erase]** select one of the following options:

- **Border Erase > All Edges** - this erases all four edges of an input document. Specify the width of the erased edges, in inches.
- **Edge Erase** - this erases some edges of an input document. Specify the width of each erased edge (Top, Bottom, Left, Right), in inches.
- **Scan to Edge** - this scans the entire document without losing any edge space.

3. Click on the **[Apply]** button to return to the **Default Template** page.

Filing Options

The **Filing Options** area displays the document name and the format type settings.

1. To change the Filing Options settings, from the Default Template, in the **Filing Options** area, click on the **[Edit]** button. This will display the **Filing Options** page.
2. In the **Filing Options** area:
   a. For **[Document Name]**, enter name for the document. The default name is **"DOC"**.
   b. For **File Format**, select one of the following document format options:
      - **TIFF (.TIF) -** select this for Full Color, Grayscale or Black/White documents. This option saves each page of a multiple page document as an individual TIFF file.
      - **Multi-Page TIFF (.TIF**) - select this for Full Color, Grayscale or Black/White documents. This option saves the entire multi-page document as a single TIFF file.
      - **PDF images (.PDF)** - select this for Full Color, Grayscale or Black/White documents. This option is often used when increased document portability is desired.
      - **PDF/A** - this setting provides a mechanism for representing electronic documents in a manner that pre serves their visual appearance over time, independent of the tools and systems used for creating, storing or rending the files.
      - **XPS images** - select this for Full Color, Grayscale or Black/White documents. This option is often used when increased document portability is desired.

   Note: Some document formats result in multiple files that represent components such as the content, layout and attributes of an image. The file extensions for these documents may include .XSM, .DAT and .XST files.

   c. If you selected either **PDF images**, **PDF/A** or **XPS images**, then select the following option for **Searchable Options**:
      - **Image Only** - if the documents scanned are images.
      - **Searchable** - selected if the original document is composed of multiple languages then select the main language used within the document from the drop-down menu.
3. Click on the **[Apply]** button to accept the changes, and return to the **Default Template** page.

Report Options

The **Report Options** area displays the reporting options.

1. To change the reporting options setting, from the Default Template page, in the **Report Options** area, click on the **[Edit]** button. This will display the **Report Options** page.
2. In the **Report Options** area:
   a. For **Confirmation Sheet**, check the **[Enabled]** checkbox to allow a confirmation sheet to print at the end of each workflow job.
   The Confirmation Sheet specifies the success or failure of the Workflow Scanning job.

   b. For **Job Log**, check the **[Enabled]** checkbox to produce a job log for reporting purposes. The job log contains information about the scanned document. The Job Log can be accessed by third party software, and the Document Management Fields information retrieved and associated with the scanned files.

3. Click on the **[Apply]** button to accept the changes, and return to the **Default Template** page.

Workflow Scanning Image Settings

The Workflow Scanning Image Settings page allows you to create compressed image files for faster web viewing, and also to select Searchable options.

> Note: Searchable options are only available when the Searchable File Formats service is enabled.

1. To change settings for Workflow Scanning Image Settings, from the **Default Template** page, in the **Workflow Scanning Image Settings** area, click on the **[Edit]** button.
2. In the **Fast Web Viewing Options** area, select one of the following:
   - **None**
   - **Linearized PDF** - if you want single pages of a PDF to be displayed in a web browser before the entire file is downloaded.
3. In the **Searchable XPS PDF and PDF/A Defaults** area:
   a. For **Searchable Options**, select either **[Image Only]** if you do not want the device to perform a search on text in the file, or select **[Searchable]** to enable XPS, PDF, and PDF/A documents to be text searched.
   b. If **Searchable** is selected, then select one of the following:
      - **Use Language Displayed on the Device User Interface** - select this setting to search in the language selected on the printer's control panel.
      - **Use this Language** - select this option and select a language from the drop-down menu.
   c. For **Text Compression Settings (PDF & PDF/A only)**, select either **[Disabled]** to disable text compression, or select **[Enabled]** to compress the resulting searchable files.
4. Click on the **[Apply]** button to accept the changes, and return to the **Default Template** page.

Compression Capability

The Compression Capability feature enables you to set the compression type you want to be enabled by default on the device.

1. To change settings for Compression Capability, from the **Default Template** page, in the **Compression Capability** area, click on the **[Edit]** button.
2. In the **Compression Capability** area, check the checkboxes to select the required compression:
   a. **CCITT Group 4 (G4 MMR)** - this provides lossless compression. This format is widely supported, but some document types may not compress significantly.
   b. **JBIG2** - JBIG2 compression is usually used for text and halftone documents. It yields a very small black and white file size with fast viewing performance, but the initial scan performance is typically slower. This compression format requires Acrobat 5 with PDF version 1.4 or greater.

c. **Flate Compression** - Flate compression works well on bi-level or color images, or with general data. It is a lossless compression format that combines LZ77 and adaptive Huffman encoding (RFC 1951). When used for PDF documents, Flate compression is applied after JPEG compression. It is also used in place of G3 compression for monochrome PDF images in Photo and Magazine mode.

d. **MRC Compression -** Mixed Raster Content (MRC) encoding extracts image components into layers and compresses each layer according to its content characteristics. MRC encoding can modify images causing image quality artifacts by the extraction and compression process. The MRC Compression settings allows you to customize the compression that will be applied to images that contain both text and images. Text and image parts are compressed separately using the best type of compression for each part.

e. **Text Compression > JBIG2** option will also display when you enable **MRC Compression**. JBIG2 compression is usually used for text and halftone documents. It yields a very small black and white file size with fast viewing performance, but the initial scan performance is typically slower. This compression format requires Acrobat 5 with PDF version 1.4 or greater. The following options can be selected:

- **Enable Arithmetic Encoding**
- **Enable Huffman Encoding**

f. **Image Compression > Flate Compression** option will also display when you enable **MRC Compression**.
Flate compression works well on bi-level or color images, or with general data. It is a lossless compression format that combines LZ77 and adaptive Huffman encoding (RFC 1951). When used for PDF documents, Flate compression is applied after JPEG compression. It is also used in place of G3 compression for monochrome PDF images in Photo and Magazine mode.
Check the **[Enabled]** checkbox to enable Image Compression.

3. Click on the **[Apply]** button to accept the changes and return to the **Default Template** page.

Apply Factory Defaults Settings

To restore the Default Template to its original settings click on the **[Apply Factory Default Settings]** button.

Note: This will delete any custom settings applied to the Default Template.

Update List of Templates

This feature allows you to update the list of templates that displays at the device's screen. This feature can be used when new templates have been created or existing templates have been changed.

At the Device:

1. Touch the **<Services Home>** button.
2. Touch **[Workflow Scanning]** icon on the touch screen.
3. Touch the **[Advanced Settings]** tab.
4. Select **[Update Templates]** to display the Update Template screen.
5. Select **[Update Template List]**.

6. On the **Confirmation Required** screen, touch **[Update List]**.

   Note: If you are not using a template pool repository, selecting **[Update List]**, will display only a partial list of templates.

7. Touch **[Close]**.

Custom File Naming

Use the Custom File Naming feature to set up an automatic naming of the generated files for Workflow Scanning.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Custom File Naming]** in the directory tree.
4. In the **File Naming** area, from the drop-down menu, select one of the following:
   - **Auto** - this option will type text that will automatically be a prefix of the file name. The system will add numbers to the end of the text you type to complete the file name.
   - **Custom Naming** - this option will allow you to select elements you want to use to build the file name, for example, Date, Time, Job ID, User ID and/or Custom Text.
     You can position the elements you choose to display first. For example, you can position the element chosen to be Time first, then Date, followed by User ID.
   - **Advanced** - this option allows you to type a string of variables to create an automatically generated file name.
5. If **Auto** is selected:
   a. In the **Name** area, enter text that will prefix the automatic file name. The device will add numbers to the end of the text you enter to complete the file name.
6. If **Custom Naming** is selected:
   a. Check to select **Standard** display option checkboxes. You can select **Date**, **Time**, **Job ID** and/or **User ID**.
   b. You can also add **Custom Text**, if you select Custom Text and check the checkbox to select the custom text. Enter details in the field.
      For example, select the first Custom Text box and type the custom text. The text appears in the **Position Box**.
      You can include up to four Custom Text strings in the file name. If you select Custom Text, enter details in the field.
   c. You can position the option you have selected in your own prioritized order, by using the **up** and **down** arrows in the **Position** area.

7. If **[Advanced]** is selected:
    a. In the **[Name]** field, type a string using the following variables to create an automatically generated file name.
    The following codes can be used to add dynamic information to the file name:

    % D (date)

    % T (time)

    % Y (year)

    % H (hour)

    % M (minute)

    % S (second

    % m (month)

    % d (day of month)

    % sn (device serial number)

    % ui (user id)

    % ji (job id)

    These variables can be in any order.
8. When complete, click on the **[Apply]** button.
9. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Display Settings

This feature enables you to set a user's template to be displayed in the top position in the list of templates, allows you to hide or show the default template in the template list, and also enables you to set the feature to select the top position template automatically.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[Display Settings]** in the directory tree.
4. In the **Template Order** area:
    a. In the **Templates** list, select the template you want in the top position.
    b. Click on the **[Update]** button.

    Your selected template will be in the top position and the remainder of the templates will display alphabetically.
5. In the **Default Template Display** area, select one of the following:
    - **Hide Default Template in the Templates list**
    - **Show Default Template in the Templates list**

    Note: If **Hide Default Template** is selected and no other Templates exist, the Default Template will automatically be shown until at least one template is added.
6. In the **Template Selection** area, select one of the following:

- **User must select template before pressing the Start button** - with this option, no template will be highlighted, the user must select a template before pressing the Start button.
- **Automatically select the top position template** - with this option, the top positioned template will be highlighted automatically.

7. Click on the **[Apply]** button.

Set up Remote Template Pool Repository

The Template Pool Setup can be used to view and modify information about the remote pool.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Click on the **[Advanced]** link.
4. Select **[Template Pool Setup]** in the directory tree. The **Template Pool Setup** page displays.

FTP Server

1. From the **Template Pool Setup** page, in the **Settings** area, select **[FTP]** from the **Protocol** drop-down menu.
2. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
3. Enter FTP server details in the **[IP Address: Port]** or **[Host Name: Port]** field.
4. Type in the path to the location of the scan folder in **[Document Path]**. Enter the full path to the directory, starting at the root of FTP services, for example: **\(directory name)\(directory name)**.
5. For **Login Credentials to Access the Destination**, select **[System]** to have the system directly log in to the file server.
6. Enter details in the **[Login Name]**, **[Password]** and **[Retype Password]** field.

   Note: A Login (account) Name and (server) Password is required for the system to access the remote server. This is mandatory for use with a SMARTsend server. For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide. Note that these accounts directly support the Login Source settings, accessed by clicking General under Workflow Scanning in Internet Services.

7. Check the **[Select to save new password]** checkbox if you need to change the password for an existing Login Name.
8. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
9. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

NetWare

Note: This feature is only available if the **NetWare** protocol is enabled. This requires a NetWare server.

1. From the **Template Pool Setup** page, in the **Settings** area, select **[NetWare]** from the **Protocol** drop-down menu.
2. Enter details in the following fields:
   - **Server Name** - enter the host name of the NetWare server.
   - **Server Volume** - enter the path of the Repository on the Netware server.
   - **NDS Tree** - allows you to set the name of the NDS tree. If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank. The default tree name is 'Xerox _DS_Tree'.
   - **NDS Context** - allows you to set the name of the NDS tree. If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank. The default tree name is 'Xerox _DS_Context'.
   - **Document Path** - enter the full path to the directory.
3. For **Login Credentials to Access the Destination**, select **[System]** to have the system directly log in to the file server.
4. Enter details in the **[Login Name]**, **[Password]** and **[Retype Password]** field.

   Note: A Login (account) Name and (server) Password is required for the system to access the remote server. This is mandatory for use with a SMARTsend server. For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide. Note that these accounts directly support the Login Source settings, accessed by clicking General under Workflow Scanning in Internet Services.

5. Check the **[Select to save new password]** checkbox if you need to change the password for an existing Login Name.
6. Click on the **[Apply]** button to accept the changes.
7. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

SMB

1. From the **Template Pool Setup** page, in the **Settings** area, select **[SMB]** from the **Protocol** drop-down menu.
2. Select either the **[IPv4 Address]** or **[Host Name]**.
3. Enter the details of the SMB server in the **[IP Address: Port]** or **[Host Name: Port]** field.
4. Enter the SMB share name in the **[Share]** field.
5. Type in the path to the location of the scan folder in **[Document Path]**. Enter the full path to the directory, starting at the root of FTP services, for example: **\(directory name)\(directory name)**.
6. For **Login Credentials to Access the Destination**, select **[System]** to have the system directly log in to the file server.

7. Enter details in the **[Login Name]**, **[Password]** and **[Retype Password]** field.

   Note: A Login (account) Name and (server) Password is required for the system to access the remote server. This is mandatory for use with a SMARTsend server. For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide. Note that these accounts directly support the Login Source settings, accessed by clicking General under Workflow Scanning in Internet Services.

8. Check the **[Select to save new password]** checkbox if you need to change the password for an existing Login Name.
9. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
10. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

HTTP or HTTPS

1. From the **Template Pool Setup** page, in the **Settings** area, select **[HTTP]** or **[HTTPS]** from the **Protocol** drop-down menu.
2. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
3. Enter the details in the **[IP Address: Port]** or **[Host Name: Port]** field of the server.
4. In the **[Script path and filename (from HTTP root)]** field enter the path and file name of the POST handling script or application used for filing. The script allows file transfers with the server. For example: **/directory name/folder name)**.
   Click on the **[Get Example Scripts]** link to download a working example script.
5. Type in the path to the location of the scan folder in **[Document Path]**. Enter the full path to the directory, starting at the root. For example, \\directory name\folder name.
6. If **HTTPS** is selected as a protocol, check the **[Validate Repository SSL Certificate (trusted, not expired, correct FQDN)]** checkbox to have the server's SSL certificate validated for the correct host name and checked for a signature of a trusted certificate authority.
7. For **Login Credentials to Access the Destination**, select **[System]** to have the system directly log in to the file server.
8. Enter details in the **[Login Name]**, **[Password]** and **[Retype Password]** field.

   Note: A Login (account) Name and (server) Password is required for the system to access the remote server. This is mandatory for use with a SMARTsend server. For information on creating accounts on the SMARTsend server, refer to the FreeFlow SMARTsend Installation and Administration Guide. Note that these accounts directly support the Login Source settings, accessed by clicking General under Workflow Scanning in Internet Services.

9. Check the **[Select to save new password]** checkbox if you need to change the password for an existing Login Name.
10. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
11. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Scan to Mailbox 10

The Scan to Mailbox feature is supported through the Workflow Scanning option. This feature provides the ability to scan to mailboxes in the device and then retrieve documents from the device using a web browser. This provides a convenient Workflow scanning feature for customers who do not wish to purchase and configure a separate networked server.

You can save the scanned documents either to the default folder, other public folders or to a private mailbox folder.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Ensure Workflow Scanning is enabled on the device.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.
- Print a Configuration Report to verify that Workflow scanning (Scan to File) is enabled on the device:
  a. Press the **<Machine Status>** button.
  b. Touch the **[Machine Information]** tab.
  c. Touch **[Print Reports]**.
  d. Touch **[Print Report]**.
  e. Touch **[Close]**.

  The Configuration Report will print. Check under the **Network Scanning Setup** heading to verify **Workflow Scanning Enabled** is enabled.

Enable Scan to Mailbox

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Scan to Mailbox]** link.
3. Select **[Enablement]** from the directory tree.
4. In the **Feature Enablement** area, check the following checkboxes:
   - **Enable Scan to Mailbox** - to activate this feature on the device. When you enable Scan to Mailbox, the created mailboxes will appear in the Workflow Scanning.
   - **On Scan tab, view Mailboxes by default** - to view mailboxes as the default when entering the Scan tab.
5. Click on the **[Apply]** button.

6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

   Note: All Saved Jobs are stored as encrypted files if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan and e-mail these files. You can enable or disable encryption of user data on the **User Data Encryption** page. Refer to User Data Encryption on page 173.

Create a New Mailbox

If a user creates a public folder the contents of that folder can be viewed by all. If a private folder is created, the folder password must be known to access, edit or delete the folder contents.

When you create a Scan to Mailbox folder, it inherits the attributes of the **Default Public Folder**. These attributes can be changed by clicking on the **Personalize Settings** button. For further information on Personalize Settings, refer to Personalize Settings or Modify Settings on page 228.

1. At your workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Click on the **[Scan]** tab.
3. In the **Display** area, select **[Mailboxes]**.
4. Scan to Mailbox consists of a Default Public Folder which can be used by all users to store scanned images. New folders can be created for individual users. When a password is allocated to a new folder, it becomes a Private Folder. If a password is not allocated to a new folder it is called a Public Local Folder.
   The administrator can specify if passwords are required when new folders are created, within the Scan Policies screen. Scan Policies are discussed later in this section. In the **Scan to Mailbox** area, click on the **[Create Folder]** link to display the **Create Folder** page to create a new folder.
5. In the **New Folder** area:
   a. Enter a name for your folder in the **[Folder Name]** field (upto 20 characters). Folder names must be unique. The folder name will show in the Network Scanning Template Destination List on the device.

   Note: Folder names cannot contain forward slash and backward slash characters and spaces.

   b. If required enter a password for your folder in the **[Folder Password (Required)]** field. The user will be prompted to enter the password when they scan their documents at the machine.
   c. Enter the password again to confirm in the **[Confirm Folder Password]** field.
6. Click on the **[Apply]** button.
7. Enter the password in the **[Folder Password]** field.
8. Click on the **[OK]** button.

Personalize Settings or Modify Settings

This option allows you to change the attributes settings for your folder.

1. Click on the **[Scan]** tab.

2. In the **Scan to Mailbox** area, select either the **[Default Public Folder]** or your personal folder.
    a. If you select the **Default Public Folder**, click on the **[Modify Settings]** button. If you select a personal folder, enter the password for the folder in the **[Folder Password]** field.
    b. Click on the **[OK]** button.
    c. Click on the **[Personalize Settings]** button.

Workflow Scanning

To change the Workflow Scanning settings, in the **Workflow Scanning** area, click on the **[Edit]** button, this will display the **Workflow Scanning** page.

1. In the **Workflow Scanning** area:
    a. For **[2-Sided Scanning]**, select one of the following:
        - **1-Sided** - the scan service will only scan one side of each page of the input document.
        - **2- Sided -** the scan service will scan both sides of each page of the input document.
        - **2-Sided**, **Rotate Side 2 -** the scan service will scan both sides of each page of the input document and shall apply a 180 degrees rotation to the second side image such that the orientation of all input images are the same.

    b. The **Content Type** feature provides a convenient way to optimize the quality of your scanned output images based on the content in your original documents. Each selection adjusts the printer settings to compensate for the predominant attributes of the content that is being scanned. Select one of the following:
        - **Photo & Text** - this is best for documents that contain a mix of photographic images and text.
        - **Photo -** this is best for documents that contain photographic images and little or no text.
        - **Text** - this is best for documents that contain mostly text.

    c. **Scan Presets** feature provides a convenient way to optimize scan settings to match the intended purpose of the scanned document. Select one of the following options:
        - **For Sharing & Printing** - this setting is best for sharing files to be viewed on-screen and for printing most standard business documents. Using this setting will result in small file sizes and normal image quality.
        - **For OCR -** this creates scanned images with clear, crisp lines and edges that provide the best OCR interpretation.
        - **For Archival Record** - this setting is best for standard business documents that will be stored electronically for record keeping purposes. Using this setting will result in the smallest file sizes and normal image quality.
        - **For High Quality Printing -** this setting is best for business documents containing detailed graphics and photos. Using this setting will result in large file sizes and the highest image quality.
        - **Simple Scan** - this provides faster scan processing by decreasing the overall quality of the scanned images.
2. Click on the **[Apply]** button to return to the **Settings** screen.

Advanced Settings

The Advanced Settings feature allows the user to select the enhancement feature for the scanned document.

1. In the **Advanced Settings** area, click on the **[Edit]** button to display the **Advanced Settings** screen.
2. In the **Advanced Settings** area:
   a. For the **Image Options**, adjust the following options:
      - **Lighten/Darken -** use the controls (left and right arrow buttons) to adjust the overall brightness reproduction compared to the original.
      - **Soften/Sharpen** - use the controls (left and right arrow buttons) to adjust how much edge sharpening is used.

   b. For **Image Enhancement**, select the following options:
      - **Contrast** - select either **[Auto Contrast]** or **[Manual Contrast]**. If Manual Contrast is selected, use the controls (left and right arrow buttons) to adjust the contrast.
      - **Background Suppression** - this option prevents the reproduction of an unwanted background image, shading or bleed-through from the reverse side of the original. This will produce an output image with a mostly white background. Select either **[No Suppression]** or **[Auto Suppression]**.

   c. Use the **[Resolution]** option to set the scan resolution. Changing the resolution affects the amount of detail reproduced on graphic images. The range is from 72 DPI to 600 DPI.

   d. For **Build Job**, check the **[Enabled]** checkbox to enable Build Job.

   e. For **Quality/File Size**, use the controls (left and right arrow buttons) to select the level of compression to use for scanned images. When compression is increased, the file size drops, but at the expense of image quality. The middle setting is ideal for most scanning purposes.
3. Click on the **[Apply]** button to return to the **Settings** screen.

Layout Adjustment

The Layout Adjustment feature allows the user to select the page layout characteristics of the scanned images.

1. In the **Layout Adjustment** area, click on the **[Edit]** button. This will display the **Layout Adjustment** screen.
2. In the **Layout Adjustment** area:
   a. **Original Orientation** - allows you to specify the format and placement of the originals when they are loaded on the document glass or document handler. This information is used to accurately display how the job will look when using page features such as Image Shift, Edge Erase, and Multiple Images. For **Original Orientation**, select one of the following options:
      - **Portrait Originals** - this instructs the printer to orient all images in portrait mode.
      - **Landscape Originals** - this instructs the printer to orient all images in landscape mode.

   Note: If you are using the Document Glass, the orientation is as seen before turning it over on the Glass.

   b. For **[Original Size]**, select one of the following options to specify the dimensions of the original scanned document:

    - **Auto-Detect** - the scan service will automatically detect the size of the input document.
    - **Manual Size Input** - allows you to identify the size of the input document from a drop-down menu. If the size you require is not listed, select **[Custom]**.
    - **Mixed Size Originals** - select this if the originals are different sizes.

   c. The Edge Erase feature allows you to erase the spots, punch holes, noise, fold, crest, and staple marks that appear along any or all of the four edges of an input document. For **[Edge Erase]** select one of the following options:
    - **Border Erase - All Edges** - this erases all four edges of an input document. Specify the width of the erased edges, in inches.
    - **Edge Erase** - this erases some edges of an input document. Specify the width of each erased edge (Top, Bottom, Left, Right), in inches.
    - **Scan to Edge** - this scans the entire document without losing any edge space.

3. Click on the **[Apply]** button to return to the **Settings** screen.

Filing Options

The **Filing Options** area displays the document name and the format type settings.

1. In the **Filing Options** area, click on the **[Edit]** button, this will display the **Filing Options** page.
2. In the **Filing Options** area:
   a. For **[Document Name]**, enter name for the document, the default name is **"DOC"**.
   b. For **File Format**, select one of the following document format options:
    - **TIFF (.TIF) -** select this for Full Color, Grayscale or Black/White documents. This option saves each page of a multiple page document as an individual TIFF file.
    - **Multi-Page TIFF (.TIF**) - select this for Full Color, Grayscale or Black/White documents. This option saves the entire multi-page document as a single TIFF file.
    - **PDF images (.PDF)** - select this for Full Color, Grayscale or Black/White documents. This option is often used when increased document portability is desired.
    - **PDF/A** - this setting provides a mechanism for representing electronic documents in a manner that pre-serves their visual appearance over time, independent of the tools and systems used for creating, storing or rending the files.
    - **XPS images** - select this for Full Color, Grayscale or Black/White documents. This option is often used when increased document portability is desired.

   Note: Some document formats result in multiple files that represent components such as the content, layout and attributes of an image. The file extensions for these documents may include .XSM, .DAT and .XST files.

   c. If you selected either **PDF images**, **PDF/A** or **XPS images**, then select the following option for **[Searchable Options]**:
    - **Image Only** - if the documents scanned are images.
    - **Searchable** - if the original document is composed of multiple languages then select the main language used within the document from the drop-down menu.

3. Click on the **[Apply]** button to return to the **Settings** screen.

Report Options

The **Report Options** area displays the reporting options.

1. In the **Report Options** area, click on the **[Edit]** button. This will display the **Report Options** page.
2. In the **Report Options** area:
   a. For **Confirmation Sheet**, check the **[Enabled]** checkbox to allow a confirmation sheet to print at the end of each workflow job.
   The Confirmation Sheet specifies the success or failure of the Workflow Scanning job.
   b. For **Job Log**, check the **[Enabled]** checkbox to produce a job log for reporting purposes.
   The job log contains information about the scanned document. The Job Log can be accessed by third party software and the Document Management Fields information retrieved and associated with the scanned files.
3. Click on the **[Apply]** button to return to the **Settings** screen.

Workflow Scanning Image Settings

The Workflow Scanning Image Settings page allows you to create compressed image files for faster web viewing, and also to select Searchable options.

Note: Searchable options are only available when the Searchable File Formats service is enabled.

1. In the **Workflow Scanning Image Settings** area, click on the **[Edit]** button to display the **Workflow Scanning Image Settings** screen.
2. In the **Fast Web Viewing Options** area, select one of the following:
   - **None**
   - **Linearized PDF** - if you want single pages of a PDF to be displayed in a web browser before the entire file is downloaded.
3. In the **Searchable XPS PDF and PDF/A Defaults** area:
   a. For **[Searchable Options]**, select either **[Image Only]** if you do not want the device to perform a search on text in the file, or select **[Searchable]** to enable XPS, PDF, and PDF/A documents to be text searched.
   b. If **Searchable** is selected, then select one of the following:
      - **Use Language Displayed on the Device User Interface** - select this setting to search in the language selected on the printer's control panel.
      - **Use this Language** - select this option and select a language from the drop-down menu.
   c. For **Text Compression Settings (PDF & PDF/A only)**, select either **[Disabled]** to disable text compression, or select **[Enabled (Flate Compression]** to compress the resulting searchable files.
4. Click on the **[Apply]** button to return to the **Settings** screen.

Compression Capability

The Compression Capability feature allows you to set compression type you want to be enabled by default on the device.

1. In the **Compression Capability** area, click on the **[Edit]** button to display the **Compression Capability** screen.

2. In the **Compression Capability** area, check the checkboxes to select the required compression:
    a. **CCITT Group 4 (G4 MMR)** - this provides loss less compression, this format is widely supported, but some document types may not compress significantly.
    b. **JBIG2** - JBIG2 compression is usually used for text and halftone documents. It yields a very small black and white file size with fast viewing performance, but the initial scan performance is typically slower. This compression format requires Acrobat 5 with PDF version 1.4 or greater
    c. **Flate Compression** - Flate compression works well on bi-level or color images, or with general data. It is a loss less compression format that combines LZ77 and adaptive Huffman encoding (RFC 1951). When used for PDF documents, Flate compression is applied after JPEG compression. It is also used in place of G3 compression for monochrome PDF images in Photo and Magazine mode.
    d. **MRC Compression -** Mixed Raster Content (MRC) encoding extracts image components into layers and compresses each layer according to its content characteristics. MRC encoding can modify images causing image quality artifacts by the extraction and compression process. The MRC Compression settings allows you to customize the compression that will be applied to images that contain both text and images. Text and image parts are compressed separately using the best type of compression for each part.
    e. If you enable **MRC Compression**. The **MRC Compression Format** options will display. Select either **[Multi-Mask Compression]** or **[3-Layer Compression]**.
    f. **Text Compression > JBIG2** option will also display when you enable **MRC Compression**. JBIG2 compression is usually used for text and halftone documents. It yields a very small black and white file size with fast viewing performance, but the initial scan performance is typically slower. This compression format requires Acrobat 5 with PDF version 1.4 or greater. The following options can be selected:
        - **Enable Arithmetic Encoding**
        - **Enable Huffman Encoding**
    g. **Image Compression > Flate Compression** option will also display when you enable **MRC Compression**.
    Flate compression works well on bi-level or color images, or with general data. It is a loss less compression format that combines LZ77 and adaptive Huffman encoding (RFC 1951). When used for PDF documents, Flate compression is applied after JPEG compression. It is also used in place of G3 compression for monochrome PDF images in Photo and Magazine mode.
    Check the **[Enable]** checkbox to enable Image Compression.
3. Click on the **[Apply]** button to return to the **Settings** screen.

Configure Scan to Mailbox

Storage Capacity

To view the information on the amount of hard drive space being consumed by files in Mailboxes:

At your Workstation:

Note: To view this information access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.

2. Click on the **[Scan to Mailbox]** link.
3. Select **[Capacity]** in the directory tree to display the **Capacity** page.
4. In the **Capacity** area, the following information displays:
    - **Capacity -** the total amount of space available on the device for document storage.
    - **Used** - the amount of storage capacity currently used.
    - **Available** - the amount of storage available for document storage.
    - **Percentage Used** - the amount of storage, in percentage, currently used.

Files

This feature allows the System Administrator to perform maintenance on the Scan to Mailbox files that reside on the device.

There are two maintenance options on the Files page:

- **Immediate Cleanup of All Folder Files**
- **Schedule Cleanup of Folder Files**

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Scan to Mailbox]** link.
3. Select **[Files]** in the directory tree.

    The **Files** page allows administrators to delete files stored in Scan to Mailbox folders.
4. If you want to delete files immediately:
    a. In the **Immediate Cleanup of All folder Files** area, there are two options. Select one of the following option:
        - **Delete all files now** - select this option to indicate that you want to delete all Scan to Mailbox files in all folders immediately.
        - **Delete all files older than** - select this option to have files older than a certain time or date deleted.

    b. If you select **[Delete all files older than]**, enter a number in the field and select either **[Day]** or **[hours]** from the drop-down menu to indicate the time period desired.

    c. Click on the **[Delete Files]** button to perform the deletion.
5. To schedule files to be deleted regularly:
    a. In the **Schedule Cleanup of Folder Files** area, check the following option checkboxes:
        - **Delete all Default Public Folder files older than** - select this option to have all files in the Default Public Folder older than a certain time or date scheduled for deletion.
        - **Delete all Created Folder files older than** - select this option to have all Created Folder files older than a certain time or date scheduled for deletion.

    b. Enter a number in the field and select either **[Day]** or **[hours]** from the drop-down menu to indicate the time period desired.

    c. For **Cleanup Time**, select one of the following option:

- **Daily** - select this option to have cleanup occur daily. Type the hour and minute to indicate when the cleanup will begin.
- **Hourly (top of hour)** - select this option to trigger scheduled hourly maintenance. Note that this cleanup will occur every hour at the top of the hour.

d. Click on the **[Apply]** button.

e. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Folders

This feature allows the System Administrator to perform maintenance on the created Scan to Mailbox folders that resides in the device. The System Administrator can change folder passwords, delete folders or delete scanned images within folders.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Scan to Mailbox]** link.
3. Select **[Folders]** in the directory tree.
4. In the **Created Folder Operations** area:
   a. From the **[Select a Created Folder]** drop-down menu, select the required folder.
   b. To change the Folder password, enter new password in the **[Change Folder Password]** field and into the **[Confirm Folder Password]** field.
   c. Click on the **[Saved Password]** button.
   d. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.
5. To permanently remove all files within the selected folder:
   a. Click on the **[Delete Files]** button.
   b. Click on the **[OK]** button when you see the message **“Are you sure you want to delete all the files in the folder?”**.
6. To permanently remove the folder and all the files contained in the folder:
   a. Click on the **[Delete Folder]** button.
   b. Click on the **[OK]** button when you see the message **“Are you sure you want to delete this folder?”**.

Scan Policies

This feature allows the System Administrator to set the scanning policies for the Scan to Mailbox feature on the device.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Scan to Mailbox]** link.
3. Select **[Scan Policies]** in the directory tree.
4. In the **Scan Policies** area, check the required checkboxes:
   - **Allow scanning to Default Public Folder** - allows users to scan to the default Scan to Mailbox folder.

   Note: If this option is not selected, then users can only scan to their own personally created folders.

   - **Require per job password for public folders** - ensure users are required to enter a password at the device each time they scan to a public folder.
   - **Allow additional folders to be created** - allow users to create new folders.
   - **Require password when creating additional folders** - to create Private Folders, which require users to enter a password when they create a new folder.
   - **Prompt for password when scanning to private folder** - ensure users enter a password at the device each time they scan to a Private Folder.
     This is useful if you wish to create a private folder where users can save scans to a folder but you do not want them to see any files that have been saved there.
   - **Allow access to job log data file** - to be able to print the job log for specific scanned documents. The job log contains information about the scanned document. Third party applications can be used to search, file and distribute jobs based on their job log information. The job log can only be accessed for PDF or Multi-Page Tiff images.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

   Note: To see individual Mailboxes, click on the **[Scan]** tab on Internet Services. To scan to these mailboxes, refer to the **User Guides**.

Use Scan to Mailbox

At the Device:

1. Press the **<Services Home>** button.
1. Touch the **[Workflow Scanning]** icon.
2. Touch your mailbox folder template in the **Template Destinations** list.
3. In the **Document Management** screen:
   a. Touch the **[Enter Password for Folder]** from the list.
   b. Enter your mailbox folder password.
   c. Touch **[Done]** and touch **[Save]**.
4. Touch the **[Filing Options]** tab.
5. Touch **[File Format]**.

6. Select the required file format. PDF, PDF/A, XPS, Multi-Page TIFF, TIFF, or JPEG are supported.
7. Touch **[Save]**.
8. Place a document on the device and press the green start button.

At your Workstation:

1. Open the web browser and enter the IP Address of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Scan]** tab
3. In the **Display** area, select **[Mailboxes]**.
4. In the **Scan to Mailboxes** area, select your mailbox folder.
5. If prompted, enter your mailbox folder password in the **[Folder Password]** field and click on the **[OK]** button.
6. The scanned image will appear in the **Folder Contents** area. If it does not, click on the **[Update View]** button.
7. If you selected to create a PDF or Multi-Page TIFF image, select the required option from the **[Action]** drop-down menu:
   a. To save a copy of the image to your workstation, select **[Download]** and click on the **[Go]** button.
      - To view the file, click on the **[Open]** button.
      - To save the file, click on the **[Save]** button, select a location on your workstation and click on the **[Save]** button.

   b. To print the image at the device, select **[Reprint]** from the drop-down menu and click on **[Go]**.

   c. To delete the image select **[Delete]** from the drop-down menu and click on **[Go]**.

   d. If you selected **job log** on the Scan Policies screen you will see a **[Job Log]** option in the drop-down menu. Select option and click on the **[Go]** button.
      - To view the job log, click on the **[Open]** button.
      - To save the job log, click on the **[Save]** button, select a location on your workstation and click on the **[Save]** button.

   e. If you selected to create a Single-Page TIFF image, select **[Open]** from the **[Action]** menu and click on **[Go]**.
8. To remove all files from your mailbox, click on the **[Delete All]** button.
9. To change your mailbox folder password or to remove your mailbox folder, click on the **[Modify Folder]** button.
   a. In the **Folder Operations** area, enter your new password in the **[Change Folder Password]** and **[Confirm Folder Password]** areas.

   b. Click on the **[Save Password]** button.

   c. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   d. To remove your mailbox folder, click on the **[Delete Folder]** button.

   e. Click on the **[OK]** button when you see the message **"Are you sure you want to delete this folder?"**.

Scan to Home

11

Scan to Home lets users scan documents that are saved to a “home directory” on an external server. The home directory is distinct for each logged-in user. This is established either through LDAP or by setting a network path to the external server.

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

Users access the Scan to Home template by pressing the **[Workflow Scanning]** icon on the Services Home 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.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

  This is required to access Internet Services to configure Workflow Scanning. The Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure scan settings using an Internet browser.
- Workflow Scanning must be enabled on the Xerox device.
- Network Authentication must be configured on the Xerox device. The Authentication server and the server used to file scanned images must belong to same domain.

Additional Requirements for Scan to Home via LDAP Query

- A Windows 2000/2003 server with Active Directory Services (ADS) must be configured with LDAP Services and available on the network.
- The LDAP server information must be configured on the Xerox device.
- The user's Home Folder Location must be set on the ADS server. To verify the Home Folder Location, at the ADS server, go to **[Administrator Tools]** and then **[Active Directory Users and Computers]**. Select a user and select **[Properties]** and then **[Profile]**. Ensure the user's Home Folder Location is set. This will need to be set for each user who wants to use Scan to Home via LDAP Query.

Additional Requirements for Scan to Home with no LDAP Query

- Create a folder on your network where scans are to be filed. Share the folder and ensure users have Read and Write access.

Enable and Configure Scan to Home

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Scan to Home]** link.
3. Select **[General]** in the directory tree to display the Scan to Home page.
4. In the **Setup** area:
   a. for **Status**, check the **[Enabled]** checkbox.
   b. If a friendly (descriptive) name has been assigned for the external server, enter the name in the **[Friendly Name]** field. Type in a name of up to 127 characters for the template that will appear in **Destination Details** field on the device's user interface.
   c. If you want to change the default name of the Scan to Home template, enter the required name in the **[Template Name]** field. The default Scan to Home template is @S2HOME.

   Note: If you change the default template name it is recommended that you enter a name that is easy to identify as the Scan to Home template, and enter a Friendly Name as mentioned in step 8b. This will ensure users can identify the Scan to Home template. Templates with the same name can be created on the device by the Workflow Scanning, Scan to Mailbox and Scan to Home features.
5. For **Determine Home Directory**, select either **[LDAP Query]** or **[No LDAP Query]** to define the method that the device will use to find the user's home directory.
6. If you select **LDAP Query**:
   a. The device will use the login supplied by the user to determine the home directory on the external server.
   Also when LDAP Query is selected, the **LDAP Mapping for Home Directory** will display the default or retrieved (via LDAP query) home directory on the external server. By default, this is **"homeDirectory"**.
   b. Verify the LDAP mapping for Home Directory is correct. To test it, click the **[LDAP Mapping for Home Directory]** link. This will display the **LDAP - User Mappings** page.
   c. In the **LDAP - User Mappings** page, in the **[Server Information]** area, check that the **LDAP Server** is set correctly for your environment.
7. If you select **No LDAP Query**, you will need a method to distinguish individual ownership of job scans. To do this, select either **Append "User Name" to Path**, or **Automatically Create "User Name" directory if one does not exist**.
   a. Enter the path to a location on your network where scans are to be stored in the **[Network Home Path]** area. The format should be: *\\servername\foldername.*
8. Check the **[Automatically Create Subdirectory]** checkbox to have the output of scan jobs placed in separate subdirectories in the Network Home Path.
   a. In the **[Subdirectory]** field, enter the name of a subdirectory that will be automatically created on the external server when the Scan to Home feature is used. This allows all scanned pages to be stored in this specified directory, making it easier for users to locate them.
9. Check the **[Append "User Name" to Path]** checkbox to have the name or ID that was used to log into the printer added to the end of the external server directory path where the scanned pages

are saved. If the external server directory is used by many users, appending the user name makes it easier for users to locate their files.

a. Check the **[Automatically Create “User Name” directory if one does not exist]** checkbox to create a new directory if it does not exist. If this option is not selected and the ‘User Name’ directory does not exist, an error message appears, and the scan is not saved.

10. Click on the **[Apply]** button to accept changes.

Use Scan to Home

1. At the device, touch the **[Workflow Scanning]** tab.
2. Enter your network authentication username and password.
3. At the Workflow Scanning Template List, touch the Scan to Home template. The default name is **[@S2HOME]**.
4. Put your documents in the device to scan and press the green start button.
5. Retrieve your documents from the home directory.

E-mail 12

The E-mail feature allows a user to scan paper documents into an electronic format and have those documents delivered to a set of e-mail recipients.

E-mail Addressing

Recipient addresses can be added by entering the SMTP (Simple Mail Transport Protocol) address, for example name@company.com, at the E-mail screen.

In addition, both an internal and a public address book can be configured for the device and accessed from the E-mail screen. Lightweight Directory Access Protocol (LDAP) provides access to the internal, or corporate, address book.

A public address book can be created from a list of names and addresses saved in a .CSV (Comma Separated Values) file.

E-mail Authentication

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, before they can access the E-mail feature. For a full description of the Authentication feature refer to Authentication on page 155 of this guide. Authentication can be configured after E-mail has been installed.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to enabling E-mail.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional, so that the device web browser can be accessed. Ensure that DNS settings are configured on the device.

  This is required to access the device's Internet Services web pages, which can be used to configure E-mail settings from a network connected workstation's web browser.
- Ensure you have the Scanning Kit.
- Obtain the IP Address or Host Name of a functional SMTP mail server that accepts inbound mail traffic.
- If you require color or grayscale scanning, or scan to JPEG you will need the Color Scanning Enablement Kit.
  The Kit can be purchased from your Xerox Sales Representative. Follow the instructions with the Color Scanning Enablement Kit to ensure the Kit is installed before you continue with the E-mail instructions.

- Create an e-mail account on the mail server which the device will use as the default “From” address (optional).
- Test the e-mail account by sending an e-mail from an SMTP mail client on a networked workstation. Use the new account name and password, if any to access the account and verify that e-mail was received.

To Enable E-mail

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Scroll down, by touching the **down arrow**. Touch **[Optional Services]**.
3. Touch **[E-mail]**. The **Email Service** displays.
4. Touch **[Enable]**.
5. Touch **[Save]**.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools Pathway.

Configure SMTP Server

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SMTP Server]** in the directory tree.
4. In the **Required Information** area, select one of the following:
   - **Use DNS (to identify SMTP Server)** - use this to allow the DNS to look up the IP Address of the mail server.
   - **Specify SMTP Server Manually**.

   a. If you select **Specify SMTP Server Manually**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**. Enter details of the SMTP Server in the **[IP Address: Port]**, or the **[Host Name: Port]** field.

   b. Enter a valid E-mail address in the **[WorkCentre E-mail Address]** field (matching the account set up on the SMTP Server) which the device will use as a default E-mail From and Reply To address.
5. In the **Optional Information** area:

   a. Enter the maximum allowable size for an e-mail with an attachment in the **[Maximum Message Size (Message and Attachment]** field. The range is from 512Kb to 20480 Kb.

   b. Enter the allowable number of fragments in the **[Number of Fragments]** field. The range is from 1 to 500; the default is 1.

   c. Enter allowable size to control the size of E-mail jobs sent to the SMTP server in the **[Total Job Size]** field. The range is from 512Kb to 2,000,000Kb (2Gb); the default is 512Kb.

d. Select the required setting for the **[E-mail Job Splitting Boundary]**. This option sets the job splitting options, the option is only available when Scan to E-mail is enabled and when the number is greater than 1 for **Number of Fragments**.

e. For **[Login Credentials for the multifunction device to Access the SMTP Server to send automated emails]**, select one of the following authentication method that the printer will use to access the SMTP server for any automated e-mail messages that it sends for notification or confirmation:

- **None** - if no authentication is required.
- **System** - select this option to have the printer authenticate itself using the credentials you provide for the Login Name and Password.
  Enter details for the SMTP server account in the **[Login Name]**, **[Password]** and **[Retype Password]** fields.
  Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

f. For **Login Credentials for the Walkup User to send Scanned E-mails**, select how walkup users can be authenticated by the SMTP server. Users can be prompted to log in or users can be authenticated using the system credentials specified on the SMTP Server configuration screen. Select one of the following:

- **Authenticated User** - when selected the device will prompt to log in using their own network credentials.
- **Same as Automated E-mails: System** or **None** - when selected, each user will need to enter the system credentials specified on the SMTP Server configuration screen.

6. Click on the **[Apply]** button to implement any changes.
7. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Configure E-mail Settings

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[E-mail]** link, select **[Defaults]** in the directory tree. The **E-mail: Defaults** screen displays.

General

1. From the **E-mail: Defaults** screen, in the **General** area, click on the **[Edit]** button.

a. To change the **E-mail From** address, enter a valid e-mail address in the **[From Address]** field.

b. Optional Step: Enter a name of the sender in the **[From Name]** field.

c. If LDAP is configured, check to select the required option next to the **[Allow Authenticated Users to Edit “From:” Field when]**:

- **Address Book (LDAP) Search Successful** - users can edit the 'From' field when the LDAP server finds the user's address.
- **Address Book (LDAP) Search Failure** - users can edit the 'From' field when the LDAP server did not find the user's address.

- **Address Book (LDAP) Search Not Performed** - users can edit the 'From' field when Personalization has not been enabled.

d. Select **[Yes]** next to **[Edit "From:" Field when Authentication is not Required]** if users can edit the 'From' field when authentication is not enabled on the device.

e. In the **[Message Body]** section, enter text that you want to appear as default in the body of e-mails sent from the device. You can also check the following details checkboxes to add in the message:

   - **User Name**
   - **E-mail Address**
   - **Number of Images attached to the e-mail**
   - **Attachment File Type (TIFF, JPEG)**
   - **Device Name (WorkCentre)**
   - **Device Location**
   - **Serial Number**
   - **IP Address**
   - **MAC Address**

f. In the **[Signature]** entry fields, enter text that you want to appear as the default signature in every e-mail.

g. Select one of the following options from the **[Confirmation Sheet]** drop-down menu:

   - **Off** - This setting will not produce a Confirmation Sheet.
   - **On** - This setting will produce a Confirmation Sheet that will provide the job status and any error information.
   - **Errors Only** - This setting will produce a Confirmation Sheet only when error detected.

h. For **Auto Add Me**, check the **[Enable]** checkbox if you want to have the sender's e-mail address included in the destination (To:) field.

Note: Only works if the 'From' field is auto populated from LDAP server or manually configured. For example, the default 'From' will not be put in the 'To:' list.

i. For **Only Send to Self**, click the checkbox to ensure that the only the user's email address is added to the email.

Note: When **Only Send to Self** is enabled, the **[New Recipient]** and **[Address Book]** buttons will be disabled.

j. For **Enable E-mail Security**, check the **[Enabled]** checkbox to provide enhanced security when sending e-mail messages and attachments. This feature utilizes the authentication options of the device, along with an optional secure e-mail server, to protect data that is transmitted as an e-mail.

k. Click on the **[Save]** button to implement changes and return to the **Default** page.

l. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Scan to E-mail

Scan to E-Mail settings will set the defaults for the following: E-mail Subject, Output Color, 2-Sided Scanning and Original type.

1. From the **E-mail: Default** screen, in the **Scan to E-mail** area, click on the **[Edit]** button.
2. In the **Scan to E-mail** area:
   a. For **Subject**, enter details in the field to identify or describe the e-mail document to be sent.
   b. For **2-Sided Scanning**, select the required document scanning option.
   c. For **Content Type**, select the required method used to optimize the quality of your scanned output images based on the content in your original documents.
   d. For **Scan Presets**, select the required option used to optimize scan settings to match the intended purpose of the scanned document.
3. Click on the **[Apply]** button to accept the changes.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Advanced Settings

Advanced settings allows you to select options as follows:

- **Image Options** - allows you to lighten - darken and soften - sharpen the image to be scanned.
- **Image Enhancement** - prevents reproduction of unwanted shading from the originals (Background Suppression), and select the level of contrast (Manual Contrast).
- **Resolution** - allows you to choose the resolution setting to be applied to the scan.
- Changing the resolution affects the amount of detail reproduced on graphic images.
- **Quality/File Size** - allows you to select the level of compression to use for scanned images or document.

Note: By increasing the compression, the files size will decrease depending on the image quality being scanned and mailed.

1. From the **E-mail: Default** screen, in the **Advanced Settings** area, click on the **[Edit]** button.
2. Select the required options in the **[Advanced Settings]** area.
3. Click on the **[Apply]** button to implement changes and return to the **E-mail: Default** page.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Layout Adjustment

Layout Adjustment settings includes:

- **Original Orientation** - allows you to choose the format and direction your images are loaded in the Document feeder or on the Document glass.
- **Original Size** - allows you to choose either **[Auto Detect]** which allows the device to automatically detect the original size of the document, or **[Manual Size Input]** which requires user to select the size of the document, or **[Mixed Size Originals]** if the original documents are of mixed sizes.

- **Edge Erase** - when selected allows you to erase the spots, punch holes, noise, fold, crest, and staple marks that appear along any or all edges of an input document.

1. From the **E-mail: Default** screen, click on the **[Edit]** button in the **Layout Adjustment** area.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **E-mail: Default** page.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Filing Options

Filing options allow you to specify the default e-mail file format. There are two options:

- **File Format** - allows user to select the format of the document from either TIFF, mTIFF, PDF, PDF/A or XPS.
- **Searchable Options** - allows user to select searchable option of searching either Image Only or Searchable Languages.

1. From the **E-mail: Default** screen, click on the **[Edit]** button in the **Filing Options** area.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **E-mail: Default** page.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

E-mail Image Settings

Image Settings allow you to select linearized PDF and interleaved XPS images for faster web viewing.

> Note: Searchable options are only available when the Searchable File Formats service is enabled.

Email Image Settings enables you to specify the e-mail Image Settings. There are two options:

- **PDF & PDF/A Settings** - allows you to select Optimized for Fast Web Viewing, select this option if you want to create linearized PDF or PDF/A images.
- **Searchable XPS PDF & PDF/A Defaults** - allows you to select the Searchable Options and Text Compression Setting (XPS PDF & PDF/A only).

1. From the **E-mail: Default** screen, click on the **[Edit]** button in the **E-mail Image Settings** area.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **E-mail: Default** page.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Configuring Public and Internal Address Books (LDAP)

A Public Address Book is created from a list of names and addresses saved in a CSV file (Comma Separated Values) format. If a site does not have an LDAP server to provide access to a corporate address list, the device will accept a Public Address Book file that contains a list of user names and associated e-mail addresses. This file must be in a CSV (Comma Separated Values) format for the device to be able to read the file contents. The device can have access to both an LDAP server and a public address book. If both are configured the user will be presented with the choice to use either address book to select e-mail recipients.

The majority of word processing or spreadsheet packages will allow you to create a CSV file. A selection of e-mail applications will also allow you to export a list of users in the CSV file format. There are also several conversion packages available on the web.

LDAP Addressing - Internal Address Book

> Note: Configuration of the LDAP directory settings requires the network to support LDAP services.

For Public Address book, see To Create a Public Address Book on page 256.

LDAP (Lightweight Directory Access Protocol) is a popular protocol used by large accounts to access large quantities of data including corporate address books. The local system will need to know where the LDAP server is located on the network and may need a login name and password if the LDAP server is not configured to allow NULL names and passwords.

The Internet Services **LDAP** page allows you to configure Lightweight Directory Access Protocol information.

LDAP is used for the following activities:

- To access the corporate address book to locate e-mail addresses for use with the E-mail and Internet Fax services.
- To authenticate users when configured as the method of Authentication.
- To authorize users to gain access to device features, when configured as the method of Authorization.

For instructions on how to configure Authentication and Authorization, refer to Authentication on page 155.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the E-mail feature is functional on the device and your network supports LDAP services.
- Obtain the IP Address (or Host Name) of your LDAP Server. The device may also need a login name and password if the LDAP server is not configured to allow NULL names and passwords.
- Use an LDAP client to validate your settings before inputting them into the Internet Services menus. LDAP clients include Microsoft Outlook Express, Microsoft Outlook and Netscape Communicator.
- To use host names, DNS must be configured on the device.

To Configure LDAP Server

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[LDAP]** in the directory tree.
4. To add a new LDAP directory, click on the **[Add New]** button.
5. In **Server Information** area:
   a. Select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   b. Enter details in the **[Friendly Name]** field.
   c. Enter details of the LDAP server in the **IP Address: Port** or the **Host Name: Port** field.
   d. Select the server type from the **[LDAP Server]** drop-down menu.
6. In the **Optional Information** area:
   a. Enter the search directory location of the server where the LDAP information is stored in the **[Search Directory Root]** field.
   b. For **Login Credentials to Access LDAP Server**, select one of the following:
      - **None** - if no login is required.
      - **Authenticated User** - the device will use the login details entered by the user to access the LDAP server. This option requires Authentication to be configured on the device.
      - **System** - if selected the device will specify the LDAP server login details and enter the required information in the **[Login Name]** and **[Password]** fields. Format for the login name may be login name or domain/login name.

   c. Enter a **Login Name** and **Password**, if required, for the device to access the LDAP server. Format for the login name may be login name or domain/login name.
   d. For **SSL**, check the following checkbox:
      - **Enable SSL** - To enable SSL (Secure Socket Layer).

   Note: SSL requires a server certificate to be available to the device.

      - **Validate Repository SSL Certificate** - If you want the device to verify that the server certificate is trusted, valid and has a fully qualified domain name (FQDN).

   e. Click on the **[View Trusted SSL Certificates]** link to view secure certificates that have been uploaded to the device. (Click the browser **[Back]** button to return to the LDAP Settings screen.)
   f. For **Maximum Number of Search Results** select either **[Use LDAP Server Maximum]** or **[Maximum Number of Search Results]**. If you select the latter, enter the maximum number of addresses that will appear which match the search criteria selected by the user. Set the search results to one less than the server will allow. For example, if the LDAP server limit is 75, set the search results to 74 or less. The range is between 5 and 100.
   g. For **LDAP Referrals**, check the **[Enabled]** checkbox if the primary LDAP server is connected to additional servers, the search will continue on those servers as well.

h. The **Perform Query on** option will help control the returns by allowing the LDAP query to be either on **[Mapped Name Field]** or **[Surname and Given Name Fields]**. Netscape and Lotus Domino will typically require a setting of Surname to allow returns of “lastname, firstname”.

i. **Search Timeout:** There are two options. You can let the server use its timeout limit by selecting the **[Use LDAP Server Timeout]**, or select **[Wait]** and specify how many seconds the search should last (between 5 and 100). If the search takes longer than the time specified in the **[Wait... seconds]** box the user will be notified that the search failed.

7. Click on the **[Save]** button to implement the changes.

To Figure Contexts for LDAP

1. From the **LDAP** screen, click on the **[Contexts]** tab under the LDAP title at the top of the screen.

   Contexts are used with the Authentication feature. Contexts speeds up searching through the LDAP tree by specifying where to look in the tree. The administrator can configure the device to automatically add an authentication context to the Login Name provided by a user.
2. Enter the default login information in the **[Default Login Context]** field. This is the first context that will be searched.

   Note: The word LDAP should appear in the login context, for example, cn=LDAP, o=xerox, c=us.
3. Click on the **[Save]** button.

To Define User Mappings

Fields contained within LDAP structures are not standardized. This section allows you to find out what results you will get when searching for a name using one of the LDAP servers. Editing the mapping will give some control over your LDAP server results, therefore improving name searches for the user.

To map the LDAP fields:

1. From the **LDAP** screen, click on the **[User Mappings]** tab under the LDAP title at the top of the screen.

   a. The **Server Information** area will display a summary of the LDAP server settings assigned in the **LDAP Server** screen.

   b. In the **Search** area, enter details in the **[Enter Name]** field and click on the **[Search]** button this lets you test the LDAP name search and field matching capability.

   c. The information about this user is then displayed against the fields shown on the device. By using the drop-down menu under **Imported Heading** boxes re-map any fields you require against the device’s properties.

   Note: Internet Fax users should ensure that the **Internet Fax** field is NOT set to **“No Mappings Available”** in the drop-down menu. This setting will prevent the LDAP Address Book appearing on the Internet Fax screen at the device. Select the field that contains the Internet Fax addresses. In many cases, there is no unique Internet Fax address, therefore, regular e-mail address is used.
2. When you have finished making your selections click on the **[Save]** button.

Authorization Access

For 'From' address configuration refer to the E-mail Settings screen within Internet Services. For instructions refer to the Configure E-mail Settings on page 245.

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. (LDAP server will find members nested up to five levels down a group. For example, if LDAP searches for a user within the Admin Group, it may not find that user, but may find another group. It will also look for the user in that group as well and so on). If the LDAP server confirms that the user is a member of the ’Admin’ group, the user will have administrator access to the device.

There are three ways to control access to various group accounts:

- **User Roles**
- **Device Access**
- **Service Access**

Define User Role Access At Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.
2. Select the **[User Roles]** tab. Use this tab to define the access groups that are authorized for the following roles:
   - For the **System Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with System Administrator access to the device.
   - In the **Accounting Administrator Access [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with accounting administrator access to the device.

   a. Click on the **[Apply]** button.
3. To verify either group, in the **User Name Test** field, enter a name of one of the members of the LDAP server group in the **[Enter User Name]** field, then click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist.

   Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When no access group is listed, all members will have access.
4. When done, click on the **[Close]** button.

Setup Device Access at Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.

2. Select the **[Device Access]** tab.
   a. For **Services Pathway [Access Group]** field, enter the name of a group, defined at the LDAP server, that you want to provide with Service access to the device.
   b. Repeat the process for **Job Status Pathway** and **Machine Status Pathway**.
   c. Click on the **[Apply]** button.
3. To verify any of these groups, in the **User Name Test** area, enter a name of one of the members of the LDAP server groups in the **[Enter User Name]** field, then click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

   Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When two or more groups are entered, they must be separated by commas. When no access group is listed, all members will have access
4. When done, click on the **[Close]** button.

Setup Service Access at Your Workstation:

1. From the **LDAP** screen, click on the **[Authorization Access]** tab under the LDAP title at the top of the screen.
2. Select the **[Service Access]** tab. Use this tab to define the groups that are authorized to access various device functions and services.
   a. Enter the names of LDAP groups, as required in the **Access Group** field, to allow access to individual device services.

   Note: By default everybody has access to all of the services on the device. By entering a group name in any of the services, access is then restricted to those users belonging to that group.

   b. Verify each group by entering a group user in the **Enter User Name** field, and click on the **[Test]** button.
   Under the **Test Results** column, it will display **Access**. If the test result displays **No Access**, this will mean that the user name is not a member of the Access Group, or the Access Group name was misspelled, or that the Access Group does not exist

   Note: When an access group is entered in one of the Access Group fields, only the members from that group will have access to those features. When no access group is listed, all members will have access

   c. Click on the **[Close]** button.

Custom Filters

This feature allows System Administrator to specify custom filter information for LDAP servers. These filters, for example, allow you to filter out non-users such as machines.

1. From the **LDAP** screen, click on the **[Custom Filters]** tab under the LDAP title at the top of the screen.
2. In the **LDAP Authentication** area, check the **[Append base DN]** checkbox to enable. This will specify the distinguished name(s) that will lead to the entry in the LDAP directory under which all users and groups will be retrieved. Distinguished name is a unique name for an entry in your LDAP directory. For example: cn=USERID, o=xerox, c=us.

Note: Many UNIX/Linux LDAP servers require this attribute to be set and is used frequently when **Login Credentials to Access LDAP Server** is set to **[Authenticated User]**.

3. In the **Email Address Book Filter** area:
   a. Check the **[Enable Custom Filter]** checkbox.
   b. In the field 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 parentheses. 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.
4. In the **User ID Query Filter** area:
   a. Check the **[Enable Custom Filter]** checkbox.
   b. In the field 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 attributes placed inside parentheses. For example, to find the user with a sAMAccountName of Bob, type (objectClass=user) (sAMAccountName=Bob). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.
5. Click on the **[Apply]** button to implement any changes.
6. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

You have completed the steps to configure a company address book via LDAP.

Verify LDAP Settings at the Device

At the Device:

1. Select the **[E-mail]** icon. It may be necessary to press the **<Services Home>** button.
2. Touch the **[New Recipient]** button.
3. Enter a name which corresponds with an entry in your company’s e-mail address list, using the on-screen keyboard, for example: *lastname, firstname*.
4. Touch **[Search]**. The search result screen displays. Select the required name from the list.
5. Touch the **[Add]** button to select the name as a recipient for your e-mail.
6. Touch **[Close]**. The e-mail address will appear in the Address List.
7. Place a document to e-mail in the document handler and press the green start button.
8. Verify that the recipient received the scanned document in his/her e-mail inbox.

Public Address Book

If you do not have an LDAP server to provide access to a set of external addresses commonly used with corporate addresses or a corporate address list, the device will accept a Public Address Book file that contains a list of user names and associated e-mail addresses. This file must be in a CSV (Comma Separated Values) format for the device to be able to read the file contents. The device can have access to both an LDAP server and a public address book. If both are configured the user will be presented with the choice to use either address book to select e-mail recipients.

The Internet Services Public Address Book screen allows you to upload a list of names and e-mail addresses which can be accessed via the Public Address Book at the device.

The Public Address Book consists of a text file a CSV (Comma Separated Values) format. The majority of word processing or spreadsheet packages will allow you to create a CSV file. A selection of E-mail applications will also allow you to export a list of users in the CSV file format. There are also several conversion packages available on the web.

The E-mail or Internet Fax services must be enabled at the device to access the Public Address Book.

To Add New Names

At your Workstation:

Note: To configure this feature or these settings you will have to access the **Address Book** tab, this will require you to log in as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. Click on the **Address Book** tab.
2. In the **[Common Tasks]** area, click on the **[Add New Name]** link.
3. In the Enter Name Address Area, enter details in the following fields:
   - **Friendly Name**
   - **E-mail Address**
   - **Internet Fax Address**
4. Click on one of the following:
   - **Close** button to save details and to return to the **Public Address Book** list page.
   - **Save & New** button to save the details and clear the fields to enter additional names.
   - **Save & Close** button to save the details and return to the **Public Address Book** list page.

To Edit a Name

1. From the **Address Book** tab, in the **Public Address Book** area, ensure **[View All Names]** link is highlighted.
2. Click on the **[Edit]** link for the name you want to edit.
3. Edit the required fields, click on the **[Save & Close]** button when finished.

To Delete a Name

1. From the **Address Book** tab, in the **Public Address Book** area, ensure **[View All Names]** link is highlighted.
2. Click on the **[Delete]** link for the name you want to delete.
3. Click on the **[OK]** button when the **‘Are you sure you want to delete this record?’** message displays.

To Download a Sample Address Book

You can download a sample address book which allows you to create a list of addresses and then import to the device.

1. From the **Address Book** tab, in the **Management** area, click on the **[Download Sample]** link.
2. Click on the **[Save]** button.
3. Select a location on your workstation and click on the **[Save]** button.

To Create a Public Address Book

1. Open either an application that supports CSV files (for example, Microsoft Excel) or open the downloaded sample file.
2. Create a list of names and addresses in the following format. For example:

Friendly Name	E-Mail Address	Internet Fax Address
lastName, firstName	firstName.lastName@company.com	machine@company.com
lastName, firstName	firstName.lastName@company.com	machine@company.com
lastName, firstName	firstName.lastName@company.com	machine@company.com

   The order in which entries are displayed in the Public Address Book at the device will depend on how the entries are sorted in the CSV file.

3. Save the file as a CSV (Comma Separated Values) file with the extension .csv.

   We recommended that you keep a copy of the CSV file when created.

To Import an Address Book

1. From the **Address Book** tab, in the **Management** area, click on the **[Import]** link.
2. In the **Import Your Address Book File** area, click on the **[Browse]** button.
3. Browse to the location of the Address Book File **(*.CSV)** and highlight the **CSV** file and click on **[Open]** in the **Choose File** window.

   Note: The first row of the CSV file will be ignored.
   The device assumes the first row contains column headings.
   If your file contains a name in the first row, insert a new first row with labeled column headings.

4. Click on the **[Next]** button.
5. In the **Import Options** area, for **When importing your Address Book File (*.CSV)**, select one of the following:
   - **Add your new content to the existing Public Address Book** - this allows you to add the content in your CSV file to the existing Public Address Book.
   - **Replace the existing Public Address Book with your new content** - this allows you to replace the Public Address Book content with the CSV file content.
6. In the **Map Your File to the Public Address Book Fields** area, the following information is displayed:
   - **Label** - will display the set heading label.

- **Imported Heading** - you can use the drop-down menu to select the option **No Mappings Available** for E-mail Address and Internet Fax Address. When this is selected, nothing will show in the **Imported Sample** fields.
- **Imported Sample** - displays sample information of the selection made from the **Imported Heading** drop-down menu.

Note: **No Mappings Available** is not available for **Friendly Name**. Friendly Name is a required field.

7. Click on the **[Import]** button to import the CSV file.
8. When the confirmation screen is displayed, click on the **[Close]** button. The Public Address Book will display the list of addresses.

To Export the Public Address Book

1. From the **Address Book** tab, in the **Management** area, click on the **[Export]** link.
2. Click on the **[Save]** button.
3. Select a location on your workstation and click on either the **[Save]** button to save the file as CSV format or click on the **[Open]** button to open the CSV file.

To Delete All Names in the Public Address Book

You can delete all the names in the address book.

1. From the **Address Book** tab, in the **Management** area, click on the **[Delete All Names]** link.
2. When the pop-up window displays **"Are you sure you want to remove all names from the Public Address Book?"**, click on either the **[Delete All Names]** button to confirm deleting all the names in the address book or click on the **[Cancel]** button to return to the Public Address Book screen.

To Select Access Rights to the Public Address Book

You can select access rights to view and manage the public address book.

1. From the **Address Book** tab, in the **Security** area, click on the **[Access Rights]** link.
2. In the **Access Rights** area, for **Access rights to view and manage the Public Address Book**, select one of the following options:
   - **System Administrators Only** - only users assigned a SA role will be granted access to view and mange the Public Address Book.
   - **Open to All Users** - if selected, does not require any security access.
3. Click on the **[Save]** button.

Domain Filter

The Domain Filter feature for e-mail will allow administrators to define a list of domains that are either set as restricted, or allowed for e-mail destinations. If a set of restricted domains is defined, then all e-mails to other domains are allowed. If a set of allowed domains is defined, then all e-mails to other domains are not allowed.

The domain is defined to be the string in the e-mail address which follows the @ symbol. Exact matches are checked. Sub-strings are not checked.

- Up to 50 domains can be defined in the list of domains (allowed or restricted).
- The settings will be able to be entered on the Internet Services by an administrator.
- The settings will be able to be cloned.

The e-mail filtering will apply to e-mail destinations for the device's e-mail and iFax services. It will not apply to device generated e-mails whose destination address is programmed by the administrator (such as e-mail alerts). It will not apply to Fax Forwarding addresses which are programmed by the administrator.

E-mail addresses will be checked before being added to the local (public) address book (Internet Services entry only). Only valid addresses will be added.

E-mail addresses added as an e-mail or iFax destination will be checked regardless of the source of the address (address book, user entered, secure access, LDAP, auto send to self, only send to self and so on).

The user will be able to edit the e-mail address if they get an error for trying to enter a restricted e-mail address at the local UI (and the Internet Services for the address book) when submitting a job.

When domains are added to the list, they will be checked against the current list to prevent duplicate values from being entered from SNMP or the Internet Services.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[E-mail]** link, select **[Domain Filters]** in the directory tree, The **E-mail: Domain Filter** screen displays.
3. In the **Domain Filter Settings** area:
   a. Select one of the following:
      - **Off** - (default)
      - **Allow Domain** - this setting will cause the device to check the domain of a destination e-mail address against the domain list and only allows the destinations when there is an exact match to a specified domain in the list of domains.
      - **Block Domain** - this setting will cause the device to check the domain of a destination e-mail address against the domain list and only blocks the destinations when there is an exact match to a specified domain in the list of domains.

   b. If you select either **Allow Domains** or **Block Domains**, enter the domain details in the **[Add Domain]** field.

Note: The **Allow Domains** setting is preferred for the highest security.

Note: Duplicate domain details entered in the **Add Domain** field are not allowed and will not be added.
If a duplicate entry is entered, a pop-up screen displays with the message; **'Unable to add the new E-mail Domain - An e-mail Domain with the same name already exists'**.

c. Click on the **[Add]** button to add the entered domain in the **Domains** list. The new added domain will be highlighted in the **Domains** list.
   A maximum of 50 domains can be added to the Domain list.

d. You can remove a domain from the **Domains** list by selecting the required domain from the Domain list and clicking on the **Remove** button.
   You can remove all the domains from the **Domains** list by clicking on the **[Remove All]** button.

e. Click on the **[Sort]** button to sort the domains alphabetically.

4. Click on the **[Apply]** button to implement any changes.
5. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Note: Settings configured within this page are applied to E-mail and Internet Fax services.

Note: Changes within this page will not be saved until the Apply button is clicked.

Note: If Allow Domain is enabled with no entries in the Domains list, the behavior will be to block all domains.

Note: If Block Domain is enabled with no entries in the Domains list, the behavior will be to allow all domains.

Internet Fax 13

Internet Fax allows you to send documents to one or more Internet Fax destinations, and receive an Internet Fax at the device without requiring a telephone connection.

The Internet Fax service provides confirmation of delivery in much the same way as for the standard Fax service, by returning the Delivery Status Notifications (DSN's) and Message Disposition Notifications (MDN's) for the job via the Internet.

Using Mixed Size Originals

It is recommended that the originals used with the Internet Fax feature are of the same size. If mixed sized originals are to be used ensure that the Mixed Sized Originals option is selected when performing an Internet Fax at the device. When the Internet Fax feature has been configured, select the **Internet Fax** tab at the device, followed by **Image Adjustment** and then **Original Input**. **Mixed Sized Originals** can be selected as an option.

Internet Fax Addressing

Recipient addresses can be added by entering the SMTP (Simple Mail Transport Protocol) address, for example, **name@company.com**, at the Internet Fax screen.

In addition, both an internal and a public address book can be configured for the device and accessed from the Internet Fax screen. Lightweight Directory Access Protocol (LDAP) provides access to the internal, or corporate, address book.

A public address book can be created from a list of names and addresses saved in a .CSV (Comma Separated Values) file.

Internet Fax Authentication and Authorization

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, before they can access the Internet Fax feature. For a full description of the Authentication feature refer to Authentication on page 155 of this guide. Authentication can be configured after Internet Fax has been installed.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to enabling Internet Fax.
- Ensure TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 19.

This is required to access the device's Internet Services web pages, which can be used to configure Internet Fax settings from a network connected workstation's web browser.

For instructions on how to configure TCP/IP and HTTP refer to Configure Network Connectivity Protocols with Internet Services on page 25.

- Ensure you have the Internet Fax Kit.
- Obtain the IP Address (or Host Name) of a functional SMTP (Simple Mail Transport Protocol) mail server that accepts inbound mail traffic.
- If you require color scanning you will need the Color Scanning Enablement Kit, this is available on the 5765, 5775 and 5790.
  It is available on the 5735, 5740 and 5745, but without the Scanning Enablement Kit.
  The Kit can be purchased from your Xerox Sales Representative. Follow the instructions with the Color Scanning Enablement Kit to ensure the Kit is installed before you continue with the Internet Fax instructions.
- Ensure that DNS settings are configured on the device.
- Obtain the IP Address, account and password details of a POP3 (Post Office Protocol 3) Mail Server.
- Create an e-mail account which the device will use as the Internet Fax “From” address.
- Test the e-mail account by sending an e-mail from a networked workstation running SMTP and POP3 clients. After sending the e-mail, log in to the POP3 server to verify receipt of same.

Enable Internet Fax

Print a Configuration Report to verify that Internet Fax is an Installed Option.

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report check under **Installed Options** heading to verify if **Internet Fax** is installed/enabled.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Scroll down, by touching the scroll **arrow**, touch **[Optional Services]**.
3. Touch **[Internet Fax]**.
4. Touch **[Enable]**.
5. Touch **[Save]**.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools Pathway.

Configure an SMTP Address

At Your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[SMTP Server]** in the directory tree.
   a. In the **Required Information** area, select one of the following:
      - **Use DNS (to identify SMTP Server)** - use this to allow the DNS to look up the IP Address of the mail server.
      - **Specify SMTP Server Manually**.

   b. If you select **Specify SMTP Server Manually**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**. Enter details in the **[IP Address: Port]**, or the **[Host Name: Port]** field of the SMTP Server.

   c. Enter a valid E-mail address in the **[WorkCentre E-mail Address]** field (matching the account set up on the SMTP Server) which the device will use as a default E-mail From and Reply To address.
4. In the **Optional Information** area:
   a. Enter the maximum allowable size for an e-mail with an attachment in the **[Maximum Message Size (Message and Attachment]** field (the range is 512Kb to 20480 Kb)

   b. Enter the allowable number of fragments in the **[Number of Fragments]** field (the range is from 1 to 500), the default is 1.

   c. Enter allowable size to control the size of E-mail jobs sent to the SMTP server in the **[Total Job Size]** field. The range is from 512Kb to 2,000,000Kb (2Gb). The default is 512Kb.

   d. Select the required setting for the **[E-mail Job Splitting Boundary]**. This option sets the job splitting options, and is only available when Scan to E-mail is enabled and when **Number of Fragments** is greater than 1.

   e.

   f. For **[Login Credentials for the multifunction device to Access the SMTP Server to send automated emails]**, select one of the following authentication method that the printer will use to access the SMTP server for any automated e-mail messages that it sends for notification or confirmation:
      - **None** - if no authentication is required.
      - **System** - select this option to have the printer authenticate itself using the credentials you provide for the Login Name and Password.

   g. Enter details for the SMTP server account in the **[Login Name]**, **[Password]** and **[Retype Password]** fields.

   h. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

   i. For **Login Credentials for the Walkup User to send Scanned E-mails**, select how walkup users can be authenticated by the SMTP server. Users can be prompted to log in or users can be authenticated using the system credentials specified on the SMTP Server configuration screen, select one of the following:

- **None** - when selected the device will prompt to log in using their own network credentials
- **System** - when selected, each user will need to enter the system credentials specified on the SMTP Server configuration screen.

5. Click on the **[Apply]** button to implement any changes.

Configure POP3 Settings

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[POP3 Setup]** in the directory tree.
4. In the **Server Information** area:
   a. Select either **[IPv4 Address]** or **[Host Name]**.
   b. Enter details in the **[IP Address: Port]** or **[Host Name: Port]** field of the POP3 server.
   c. Enter details in the **[Login Name]** and **[Password]** field.
   d. Retype details in the **[Retype password]** field.
   e. Check the **[Select to save new password]** checkbox to save the password.
5. In the **POP3 Settings** area:
   a. Check the **[Enable receipt of E-mail by POP3]** checkbox to allow the device to check the POP3 server and retrieve e-mail.
   b. Enter the required setting for the **[Polling interval]**. The range is from 1 to 60 minutes. The default is 15.
6. Click on the **[Apply]** button to implement any changes.

Configure Default Settings

Note: To configure this feature or settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Internet Fax]** link. Select **[Defaults]** in the directory tree to display the **Internet Fax: Defaults** screen.

General

1. From the **Internet Fax: Defaults** screen, in the **General** area, click on the **[Edit]** button.
2. In the **General** area:
   a. For **Activity Report**, check the **[Enable]** checkbox to automatically print an Internet Fax activity report after every 50 completed jobs. You can also print an Internet Fax activity report manually at any time by clicking on the **[Print Activity Report]** button.
   b. For **Delivery Confirmation Timeout**, enter the maximum number of hours that the printer will attempt to confirm an Internet Fax job. The range is from 0 to 72 hours. If the printer cannot confirm the job within the specified time, the confirmation will fail.

c. For **Message Body** section, enter text that you want to appear as default in the body of e-mails sent from the device. You can also select to add the following details in the message:
    - **User Name**
    - **E-mail Address**
    - **Number of Images**
    - **Attachment File Type (TIFF, JPEG)**
    - **Device Name (WorkCentre)**
    - **Device Location**
    - **Serial Number**
    - **IP Address**
    - **MAC Address**

d. For **Signature**, enter text that you want to appear as the default signature in every mail in the entry fields.

e. Select an option from the **Confirmation Sheet** drop-down menu:
    - **Off** - This setting will not produce a Confirmation Sheet.
    - **On** - This setting will produce a Confirmation Sheet that will provide the job status and any error information.
    - **Errors Only** - This setting will produce a Confirmation Sheet only when an error is detected.

3. Click on the **[Save]** button to implement changes and return to the **Internet Fax: Default** screen.

Internet Fax

1. From the **Internet Fax: Default** screen, in the **Internet Fax** area, click on the **[Edit]** button.
2. In the **Internet Fax** area:
    a. For **Subject**, enter text to define a default subject that will appear in the internet faxes sent from the device.
    b. For **2-Sided Scanning**, select the required document scanning option.
    c. For **Content Type**, select the required method used to optimize the quality of your scanned output images based on the content in your original documents.
3. Click on the **[Apply]** button to accept the changes and return to the **Internet Fax: Default** screen.

Advanced Settings

Advanced settings allows you to select options as follows:

- **Image Options** - allows you to Lighten or Darken and Soften or Sharpen the image to be scanned.
- **Image Enhancement** - allows you to select the suppression settings to prevent reproduction of unwanted shading from the originals and selecting the level of contrast.
- **Resolution** - allows you to choose the resolution setting to be applied to the scan.

    Note: Changing the resolution affects the amount of detailed reproduced on graphic images.

- **Quality/File Size** - allows you to select the level of compression to use for scanned images or document.

  Note: By increasing the compression, the files size will decrease depending on the image quality being scanned and mailed.

1. From the **Internet Fax: Default** screen, in the **Advanced Settings** area, click on the **[Edit]** button.
2. Select the required options in the **[Advanced Settings]** area.
3. Click on the **[Apply]** button to implement changes and return to the **Internet Fax: Default** screen.
4. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Layout Adjustment

Layout Adjustment settings includes **Original Size**. This allows you to choose either **[Auto Detect]** which allows the device to automatically detect the original size of the document, or **[Manual Size Input]** which requires user to select the size of the document from the drop-down menu.

1. From the **Internet Fax: Default** screen, in the **Layout Adjustment** area, click on the **[Edit]** button.
2. Select the required options.
3. Click on the **[Apply]** button to accept changes and return to the **Internet Fax: Default** screen.
4. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Filing Options

Filing options allow you to specify the default e-mail file format. There are two options:

- **File Format** - allows user to select the format of the document from either mTIFF, PDF, PDF/A or XPS.
- **Acknowledgment Report** - allows user to select the device to print an acknowledgment report containing the delivery status of the Internet Fax job.

  Note: Reports may be delayed due to the recipient’s response time.

1. From the **Internet Fax: Default** screen, in the **Filing Options** area, click on the **[Edit]** button.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **Internet Fax: Default** screen.
4. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.

Internet Fax Image Settings

Image Settings allow you to select linearized PDF and PDF/A files for faster web viewing.

  Note: Searchable options are only available when the Searchable File Formats service is enabled.

Internet Fax Image Settings allow you to specify the Internet Fax Image Settings. There are two options:

- **PDF & PDF/A Settings** - allows you to select Optimized for Fast Web Viewing.

- **Searchable XPS PDF & PDF/A Defaults** - allows you to select the Searchable Options and Text Compression Setting (PDF & PDF/A only).

1. From the **Internet Fax: Default** screen, in the **Internet Fax Image Settings** area, click on the **[Edit]** button.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **Internet Fax: Default** screen.
4. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Internet Receive Settings

This feature allows you to define the settings for receiving Internet faxes, for example, setting the Filter Options, Finishing Options and Receipt Options. The device is able to receive Internet Fax jobs which consist of an e-mail message and MIME encoded e-mail attachment with the following file formats: single-page TIFF/TIF, PDF, PS, TXT, PCL, PRN, or JPEG/JPG.

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Internet Fax]** link, click on the **[Internet Receive Settings]** link in the directory tree.
3. In the **Filter Options** area, check the **[Accept E-mail with no attachment]** checkbox, to filter out attachments, or for **Accept the following attachments:** check the individual checkboxes to select the file types that will be allowable as e-mail attachments.
4. In the **Finishing Options** area, select the required options from the drop-down menu for **[Stapling]** and **[2 Sided Printing]** to determine how the printed fax jobs are handled by the device's finisher, if applicable.

   Note: Values will only be applied if the file does not define these print variables.
5. In the **Receipt Options** area, check the following checkboxes:
   - **Send confirmation reply when requested (allow device to send MDN)**: When selected, the device will send a Mail Delivery Notification (MDN) e-mail to the requestor or originator when the fax job is completed.
   - **Print cover sheet with incoming E-mail messages**: When selected, the device will print a cover sheet containing the requestor or originator's e-mail message prior to printing the fax job.
6. Click on the **[Apply]** button to save the changes.
7. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Address Books

The device supports two types of address book:

- Internal: A global address book provided by LDAP services.
- Public: A public address book created from a list of addresses saved in a .CSV file (comma separated values) format.

Both address book types can be configured for use on the device at the same time.

To configure **LDAP Services**, refer to LDAP Addressing - Internal Address Book on page 249.

To configure **Public Address Book**, refer to Public Address Book on page 254.

Use the Internet Fax Feature

At the Device:

1. Touch the **[Internet Fax]** icon. It may be necessary to press the **<Services Home>** button.
2. Touch **[New Recipient]** button.
3. Enter an internet fax recipient address using the on-screen keyboard.
4. Touch the **[Add]** button, then touch **[Save]**. The e-mail address will appear in the Address List.

   Note: The Internet Fax **'From:'** address is the e-mail address entered within the Internet Services SMTP Server screen and cannot be edited at the device.
5. Place a document to e-mail in the document handler and press the **[Start]** button.
6. Verify the recipient receives the document at the internet fax address.

Domain Filter

The Domain Filter feature for e-mail will allow administrators to define a list of domains that are either set as restricted, or allowed for e-mail destinations. If a set of restricted domains is defined, then all e-mails to other domains are allowed. If a set of allowed domains is defined, then all e-mails to other domains are not allowed.

The domain is defined to be the string in the e-mail address which follows the @ symbol. Exact matches are checked. Sub-strings are not checked.

- Up to 50 domains can be defined in the list of domains (allowed or restricted).
- The settings will be able to be entered on the Internet Services by an administrator.
- The settings will be able to be cloned.

The e-mail filtering will apply to e-mail destinations for the LUI e-mail and iFax services. It will not apply to device generated e-mails whose destination address is programmed by the administrator (such as e-mail alerts). It will not apply to Fax Forwarding addresses which are programmed by the administrator.

E-mail addresses will be checked before being added to the local (public) address book (Internet Services entry only). Only valid addresses will be added.

E-mail addresses added as an e-mail or iFax destination will be checked regardless of the source of the address (address book, user entered, secure access, LDAP, auto send to self, only send to self and so on).

The user will be able to edit the e-mail address if they get an error for trying to enter a restricted e-mail address at the local UI (and the Internet Services for the address book) when submitting a job.

When domains are added to the list, they will be checked against the current list to prevent duplicate values from being entered from SNMP or the Internet Services.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Internet Fax]** link and select **[Domain Filters]** in the directory tree. The **Domain Filter** screen displays.
3. In the **Domain Filter Settings** area:
   a. Select one of the following:
      - **Off** - (default)
      - **Allow Domain** - this setting will cause the device to check the domain of a destination e-mail address against the domain list and only allows the destinations when there is an exact match to a specified domain in the list of domains.
      - **Block Domain** - this setting will cause the device to check the domain of a destination e-mail address against the domain list and only blocks the destinations when there is an exact match to a specified domain in the list of domains.

   b. If you select either **Allow Domains** or **Block Domains**, enter the domain details in the **Add Domain** field.

   Note: The **Allow Domains** setting is preferred for the highest security.

   Note: Duplicate domain details entered in the **Add Domain** field are not allowed and will not be added.
   If a duplicate entry is entered, a pop-up screen displays with the message; **'Unable to add the new E-mail Domain - An e-mail Domain with the same name already exists'**.

   c. Click on the **[Add]** button to add the entered domain in the **Domains** list. The new added domain will be highlighted in the **Domains** list.
   A maximum of 50 domains can be added to the Domain list.

   d. You can remove a domain from the **Domains** list by selecting the required domain from the Domain list and clicking on the **Remove** button.
   You can remove all the domains from the **Domains** list by clicking on the **[Remove All]** button.

   e. Click on the **[Sort]** button to sort the domains alphabetically.
4. Click on the **[Apply]** button to implement any changes.
5. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   Note: Settings configured within this page are applied to E-mail and Internet Fax services.

   Note: Changes within this page will not be saved until the **Apply** button is clicked.

   Note: If Allow Domain is enabled with no entries in the Domains list, the behavior will be to block all domains.

   Note: If Block Domain is enabled with no entries in the Domains list, the behavior will be to allow all domains.

Embedded Fax 14

Embedded Fax allows users to send hard copy documents to another fax device (or multiple fax devices) via a telephone connection. The Embedded Fax option requires a fax card to be fitted to the device and connected to a telephone line. When you install the fax card and power on the device, the Fax Setup window appears on the screen with step-by-step instructions to lead you through the configuration. The Fax Setup procedure can be undertaken immediately following installation of the fax card, or at a later date.

Embedded Fax is an optional feature for the device.

> Note: Embedded Fax and Server Fax services are mutually exclusive. Only one of them can be enabled at any time.
> If Server Fax is currently enabled and Embedded Fax is then enabled, Server Fax will be disabled automatically. If Embedded Fax is currently enabled and Server Fax is then enabled, Embedded Fax will be disabled automatically.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning in its existing configuration prior to installation.
- Ensure the device has access to a telephone connection.
- Obtain the telephone number that you want to assign to the fax device.

Hardware:

- Locate the Fax Hardware Kit. Contact your Xerox Sales Representative if you do not have the Fax Hardware Kit.

Install the Fax Hardware Kit

> Note: If Server Fax is installed on the device when the Embedded Fax Install Wizard is running, the Server Fax feature will be disabled and users will only have access to the Embedded Fax feature.

1. Switch the power off by pressing the **<Power Off>** button.
2. Wait for the Network Controller to fully power off. The blinking green network activity light will be extinguished when this occurs.
3. Install the Fax Hardware Kit following instructions contained with the kit.
4. Connect the telephone cable to the port on the device.
5. If you have purchased the 2 Line Fax Kit, connect the second telephone cable to the second port on the back of device.
6. Switch the device on by pressing the **<Power On>** button.

Complete the Fax Setup Screens

1. The **Fax Setup** screen should display. If it does, touch **[Next]** if it does not, see Deferred Fax Settings on page 273.

   Note: If you do not wish to run through the fax configuration, touch the **[Cancel Setup]** button. Embedded Fax will be unavailable until the fax configuration screens are completed from within the administrator tools screens. See Deferred Fax Settings on page 273, for instructions.

2. The **Fax Country Setup** screen displays. Select the required country location by touching an entry in the **[Country Selection]** list. Touch **[Next]**.
3. The **Line Configuration** screen displays:
   a. Touch either **[Line 1]** or **[Line 2]** if applicable.
   b. For **Dial Type**, select the required dialing method. For a tone line select **[Tone]**. For a 10 pulse per second line select **[Pulse]**. If in doubt, touch **[Tone]**.

   Note: The Pulse/Tone feature is not available in some countries.

   c. For **Line ID**, touch the type-in region. Enter the Line 1 Local name using the on-screen keyboard. Touch **[Save]** to return to the **Line Configuration** screen.

   Note: Line ID is used to identify your device, for example, Finance Fax Machine.

   d. For **Fax Number**, touch the type-in region. Enter the Fax Number using the on-screen keypad. Touch **[Save]** to return to the **Line Configuration** screen.

   Note: Fax Number should match the phone number of the selected line.

   e. For **Options**, select the required option for the line by touching one of the following:
      - **Send and Receive -** the device is capable of sending and receiving fax transmissions.
      - **Send Only** - the device is only capable of sending faxes.
      - **Receive Only** - the device is only capable of receiving faxes.

   f. Touch **[Next]**.
4. The **Fax Setup Complete** screen displays, touch **[Save]** to save the Fax Setup settings.

   The device will reboot with the new settings.

   Note: The settings may be changed at any time. Refer to Deferred Fax Settings on page 273, for instructions.

Test the Fax Connection

1. Test the fax connection by sending a fax document. Press the **<Services Home>** button.
2. Touch the **[Fax]** icon button.
3. Enter the number of a nearby fax device using the keypad and touch the **[Add]** button.
4. Place your documents in the document handler and press the **<Start>** button.
5. Verify that your documents are received at the other fax device.

You have completed the embedded fax setup.

Deferred Fax Settings

This procedure is only necessary if you have not yet configured the fax settings, or if you have already fitted the fax card and wish to change any settings for the fax option.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Fax Settings]**.
3. The **Fax Country Setting** screen displays. Select the required country from the **Country Selection** list. Touch **[Save]**.
4. Select the **[Line Configuration]**.
5. The **Fax Line Setup** screen displays.
   a. Touch either **[Line 1 Setup]** or **[Line 2 Setup]**.
   b. For **Fax Number**, touch the type-in region. Enter the Fax Number using the on-screen keypad. Touch **[Save]** to return to the **Line Configuration** screen.

   Note: Fax Number should match the phone number of the selected line.

   c. For **Fax Line ID**, touch the type-in region. Enter the Line 1 Local name using the on-screen keyboard. Touch **[Save]** to return to the **Line Configuration** screen.

   Note: Fax Line ID is used to identify your device, for example, Finance Fax Machine.

   d. For **Options**, select the required option for the line by touching one of the following:
      - **Send and Receive -** the device is capable of sending and receiving fax transmissions.
      - **Send Only** - the device is only capable of sending faxes.
      - **Receive Only** - the device is only capable of receiving faxes.

   e. For **Dial Type**, select the required dialing method. For a tone line select **[Tone]**. For a 10 pulse per second line select **[Pulse]**. If in doubt, touch **[Tone]**.

   Note: The Pulse/Tone feature is not available in some countries.

   f. To remove the selected fax line, touch **[Uninstall Line]**.

   Note: This will remove the selected line when **[Save]** is selected. It must be re-installed before it can be used again.

6. Touch **[Save]** to exit the **Fax Line Setup** screen.
7. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools pathway.
   The device will reboot with the new settings.

Test the Fax connection

1. Test the fax connection by sending a fax document. Press the **<Services Home>** button.
2. Touch the **[Fax]** icon.
3. Enter the number of a nearby fax device using the keypad.
4. Place your documents in the document handler and press the **<Start>** button.
5. Verify that your documents are received at the other fax device.

You have completed the embedded fax setup.

Setting Fax Defaults

Setting Feature Defaults

Use this option to define the fax feature settings.

Fax

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Feature Defaults]**.
3. Touch **[Set Fax Defaults]**.
4. From the **Fax Service** screen, select the **Fax** tab.
5. Touch the **[Cover Letter]** icon.
6. The **Cover Letter** screen displays:
   a. To assign a Cover Sheet to the fax job, touch **[Enable]**.

   Note: To use the Cover Sheet assigned to the recipients selected from the Address Book, touch **[Off]**.

   b. Touch the **[To...]** type-in region, enter description for the “To Field” using the on-screen keyboard and touch **[Save]**.
   c. Repeat for the **[From...]** field.
   d. For **Comment...**, upto six different comments can be added. Select a comment field and touch **[Edit]**.
   e. Enter comment using the on-screen keyboard, and touch **[Save]**.
   f. To delete a comment, select comment and touch **[Clear]**.
   g. Touch **[Save]** to return to the **Fax** tab.
7. Touch the **[2-Sided Scanning]** drop-down menu and select one of the following scanning method:
   - **1-Sided** - this method will only scan one side of each page of the input document.
   - **2-Sided** - this method will scan both sides of the page of the input document.
   - **2-Sided, Rotate Side 2** - this method will scan both sides of each page of the input document and shall apply a 180 degrees rotation to the second side image such that the orientation of all input images are the same.
8. Touch the **[Original Type]** drop-down menu and select one of the following method to optimize the quality of your fax images based on the content in your original fax job:
   - **Text** - this method is best for documents that contains mostly text
   - **Photo** - this method is best for documents that contains photographic images and little or no text.

- **Photo & Text** - this method is best for documents that contain a mix of photographic images and text.

9. Touch the **[Resolution]** drop-down menu and select one of the following resolution setting:
   - **Standard (200x100 dpi)** - this method is best for standard office documents and photographic images.
   - **Fine (200 dpi)** - this method produces a better image quality for documents and photographic images.
   - **Super Fine (600 dpi)** - this method is best for high quality photographic images.

Image Quality

1. From the **Fax Service - Setting** screen, select the **Image Quality** tab.
2. Touch the **[Image Options]** icon.
   a. The **Lighten/Darken** screen displays. Move the slider **up** to lighten and **down** to darken the output of the original fax job. Touch **[Save]** to return to the **Image Quality** tab.
3. Touch the **[Image Enhancement]** icon.
   a. The **Image Enhancement** screen displays. For **Background Suppression** option, select either **[Off]** or **[Auto Suppression]**.
   b. Touch **[Save]** to return to the **Image Quality** tab.

Layout Adjustment

1. From the **Fax Service - Setting** screen, select the **Layout Adjustment** tab.
2. Touch the **[Original Size]** icon.
   a. The **Original Size** screen displays. Select one of the following method for the device to determine the size of the original fax documents:
      - **Auto Detect** - this method allows the device to identify the size of the original automatically.
      - **Preset Scan Areas** - this method allows you to quickly define the scan area using the standard paper size dimensions. If selected, from the **Scan Area Presets** list touch to select the required dimension.
      - **Custom Scan Area** - this method allows you to manually enter the dimension specifying the scan area. If selected, for the **Scan Area**, touch the Up or Down arrows for **[Height - Y]** and **[Width - X]** to specify the dimension.
      - **Mixed Size Originals** - this method allows you to scan originals of different sizes at one time without any additional changes.

   b. Touch **[Save]** to return to the **Layout Adjustment** tab.
3. Touch the **[Reduce/Split]** icon.
   a. The **Reduce/Split** screen displays, select one of the following methods to determine how the receiving device will handle images that are too large:
      - **Reduce to Fit** - this method will shrink the large document to fit on a smaller size paper.
      - **Split Across Pages** - this method will continue a single image across several pages.

   b. Touch **[Save]** to return to the **Layout Adjustment** tab.

4. Touch the **[Book Faxing]** icon.
   a. The **Book Faxing** screen displays. Select one of the following options:
      - **Off**
      - **Both Pages** - this option will fax both right and left pages.
      - **Left Page Only** - this option will fax the left side of the document.
      - **Right Page Only** - this option will fax the right side of the document.

   Note: These positions are based upon the orientation of the pages as you read the bound document.

   b. If you select either **Both Pages**, **Left Page Only** or **Right Page Only**, for **Binding Edge Erase** you can select a required edge erase value from **0.0** to **2.0"** using the left and right scroll button.
   c. Touch **[Save]** to return to the **Layout Adjustment** tab.

Fax Options

1. From the **Fax Service - Setting** screen, select the **Fax Options** tab.
2. Touch the **[Confirmation Report]** icon.
   a. The **Confirmation Report** screen displays. Select **[On]** to enable a confirmation report to print every time fax has been sent.
   b. Touch **[Save]** to return to the **Fax Options** tab.
3. Touch the **[Starting Rate]** icon.
   a. The **Starting Rate** screen displays. Select one of the following starting speed for the transmission of the embedded fax job:
      - **Super G3 (33.6 Kbps)**
      - **G3 (14.4 Kbps)**
      - **Forced (4800 bps)**
   b. Touch **[Save]** to return to the **Fax Options** tab.
4. Touch the **[Delay Send]** icon.
   a. The **Delay Send** screen displays. Select one of the following:
      - **Off**
      - **Specific Time** - allows you to select the time you wish the job to be sent.
   b. If you select **Specific Time**, select the time you want the job to be sent using the up and down scroll buttons for **Hour** and **Minute**. Select either **AM** or **PM**.
   c. Touch **[Save]** to return to the **Fax Options** tab.
5. Touch the **[Send Header Text]** icon.
   a. The **Send Header Text** screen displays, select **[On]** to allow the header text set by the System Administrator.
   b. Touch **[Save]** to return to the **Fax Options** tab.
6. Touch the **[Mailboxes]** icon.
   a. The **Mailboxes** screen displays. Select one of the following options:
      - **Off**

    - **Send to a Remote Mailbox** - this option allows you to send a fax transmission direct to a private mailbox on a remote machine. The number of the remote mailbox is required.
    - **Store to Mailbox** - this option allows you to scan documents into your mailbox, where they can be held and retrieved by remote machines which have your mailbox number and mailbox passcode.
    - **Print Mailbox Documents** - this option allows you to print all faxes within the Fax Mailbox using your mailbox number and mailbox passcode.
    - **Delete Mailbox Document** - this option allows you to delete all faxes within the Fax Mailbox.

   b. Touch the **[Mailbox Number]** type-in region and enter the preferred mailbox number.

   c. Touch **[Save]** to return to the **Fax Options** tab.

7. Touch the **[Polling]** icon.
8. The **Polling** screen displays. Select one of the following icons to setup incoming and outgoing fax polls, and to store documents for polling:
   - **Local Polling** - this option allows you to scan documents into the machine's memory, where they can be held and retrieved by remote machines.
   - **Poll Remote Fax** - this option allows you to retrieve a document stored on a remote machine. You may poll a single machine or several machines as one job.
   - **Poll Remote Mailbox** - this option allows you to retrieve a document stored within a private Mailbox on a remote machine. Only one mailbox may be polled at a time and its password must be known.

   a. If you select **Local Polling**, the Local Polling screen displays, select **[On]**. Select one of the following options:
    - **Secure Polling** - selecting this option allows you to enable or disable the feature.
    - **Print Polling Documents**.
    - **Delete Polling Documents**.

   b. Touch **[Save]** to return to the **Fax Options** tab.

9. Touch the **[Fax Reports]** icon.
10. The **Fax Reports** screen displays. To print a report, select one of the following reports from the **Fax Reports list** area:
    - **Activity Report** - this option prints details of the last 50 fax transmissions.
    - **Address Book Individuals Report** - this option prints details of all entries in the Individual directory.
    - **Address Book Groups Report** - this option prints details of all groups in the Group directory.
    - **Options Report** - this option prints of the fax card configuration.
    - **Pending Jobs Report** - this option prints information about jobs currently queued in the machine memory and details of available memory.

    a. Touch **[Print Report]**.

    b. Touch **[Close]** to return to the **Fax Options** tab.

Select the Fax Country Setting

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch the **[Fax Settings]** to display the **Embedded Fax Settings** screen.
3. Touch the **[Fax Country Setting],** to display the **Fax Country Setting** screen.
4. Select the relevant country from the **Country Selection** list.
5. Touch **[Save]** to return to the **Fax Settings** screen.

Configuring Embedded Fax Settings

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch the **[Fax Settings]** to display the **Embedded Fax Settings** screen.
3. Select **[Line Configuration]** to display the **Fax Line Setup** screen.
   a. Touch either **[Line 1]** or **[Line 2]** for **Line Setup.**

   Note: Line 2 will be available if a Line 2 Fax Kit has been purchased and installed on the device.

   b. Touch **[Fax Number]** type-in region and enter the fax number using the on-screen keypad.
   c. Touch **[Save].**
   d. Touch **[Fax Line ID]** type-in region and enter the Line Name using the on-screen keyboard. A maximum of 30 characters can be entered.
   e. For **[Options]**, select one of the following options for sending and receiving fax:
      - **Send and Receive** - the device is capable of sending and receiving fax transmissions.
      - **Send Only** - the device is only capable of sending faxes.
      - **Receive Only** - the device is only capable of receiving faxes.

   f. For **Dial Type**, select either **[Tone]** or **[Pulse]**.
   g. Touch **[Save]** to return to **Fax Settings** screen.

Incoming Fax Defaults

Use this feature to configure settings for incoming faxes.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch the **[Fax Settings]**.

3. Touch **[Incoming Fax Defaults]** to display the **Incoming Fax Defaults** screen.

Auto Answer Delay

This feature allows you to set an answer delay time before the fax systems answers the line.

1. From the **Incoming Fax Defaults** screen, touch **[Auto Answer Delay]** icon.
2. The **Auto Answer Delay** screen displays. Enter a delay time from 0 to 15 seconds using the left and right arrows.
3. Touch **[Save]** to return to the **Incoming Default Settings** screen.

Junk Fax Prevention

This feature prevents the receipt of unwanted 'junk' fax documents. When enabled, the device allows the receipt of faxes from numbers held in the Dial Directory.

1. From the **Incoming Default Settings** screen, touch **[Junk Fax Prevention]** icon.
2. The **Junk Fax Prevention** screen displays. Select **[Enable]**.
3. Touch **[Save]**, to return to the **Incoming Default Settings** screen.

Receive Printing Mode

This feature allows you to select whether a received fax is printed onto media selected automatically by the device, or media specified manually by the system administrator.

1. From the **Incoming Default Settings** screen, touch **[Receive Printing Mode]** icon.
2. The **Receive Printing Mode** screen displays. Select one of the following option:
   - **Automatic** - when selected, incoming faxes will be printed on the paper size which most closely matches the attributes of the incoming fax.
   - **Manual** - when selected, allows you to specify the exact paper attributes.
3. When required settings have been configured, touch **[Save]** to return to the **Incoming Fax Defaults** screen.

Ring Volume

This feature allows the user to hear an audible ringing sound when an Embedded Fax is received.

1. From the **Incoming Default Settings** screen, touch **[Ring Volume]** icon.
2. The **Ring Volume** screen displays. Select **[Enable]**.
3. Select the required audible volume level.
4. Touch **[Save]** to return to the **Incoming Default Settings** screen.

Secure Receive

This feature allows the device to hold received Embedded Faxes in the job queue as 'Secure Receive' fax jobs. The held faxes shall remain in the queue and will only be released from the queue when the user enters a valid passcode.

1. From the **Incoming Default Settings** screen, touch **[Secure Receive]** icon.
2. The **Secure Receive** screen displays. Select **[Enable]**.
3. Touch the **[Print on Passcode]** type-in region and enter a four digit passcode using the keypad.

4. Touch **[Save]** to return to the **Incoming Default Settings** screen.

Default Output Options

This option allows you to select the finishing options which will be applied to the incoming fax documents.

1. From the **Incoming Default Settings** screen, touch **[Default Output Options]** icon.
2. The **Default Output Options** screen displays. Select one of the following options:
   - **Staple** - this option allows staples on the incoming fax document to be positioned according to the paper orientation specified in Tools pathway. If the incoming document does not match this orientation, the position of the staples may not be as expected.
   - **Punched** - this option allows punch holes on the incoming fax documents will be positioned according to the paper orientation specified in the Tools pathway. If the incoming document does not match this orientation, the position of the punch holes may not be as expected.
   - **Duplex** - this option allows the incoming faxes to be printed on both sides of the pages in Head to Head orientation. If the incoming document does not match this, the orientation may not be as expected.
3. Touch **[Save]** to return to the **Incoming Default Settings** screen.

Advanced Capabilities

This option when enabled allows the full use of the capabilities of the fax card, it improves document transmission speed and resolution. This feature may prevent successful fax reception from older devices.

When disabled, it improves the compatibility with older devices for fax reception.

1. From the **Incoming Default Settings** screen, touch **[Advanced Capabilities]** icon.
2. The **Advanced Capabilities** screen displays. Select either **[Enable]** or **[Disable]**.
3. Touch **[Save]** to return to the **Incoming Default Settings** screen.

Fax Transmission Defaults

This feature allows you to set the outgoing fax settings.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch the **[Fax Settings]** to display the **Fax Settings** screen.
3. Select **[Fax Transmission Defaults]** to display the **Fax Transmission Defaults** screen.

Automatic Redial Setup

Automatic Radial Setup allows you to specify the time interval before the devices redials after a failed transmission. It also allows you to specify the number of attempts the device shall make to transmit a fax, before rejecting the job.

1. From the **Fax Transmission Defaults** screen, touch the **[Automatic Redial Setup]** icon.
2. The **Automatic Redial Setup** screen displays. There are two options:
   - **Redial Time Interval** (in minutes, the range is from 1 to 25).
   - **Automatic Redial Attempts** (the range is from 0 to 14).
3. Use the **left** and **right** arrow buttons to select the required amount.
4. Touch **[Save]** to return to the **Fax Transmission Defaults** screen.

Automatic Resend

The Automatic Resend automatically resends part or all of a failed fax transmission. You can set the number of automatic resend attempts.

1. From the **Fax Transmission Defaults** screen, touch the **[Automatic Resend]** icon.
2. The **Automatic Resend** screen displays. For **[Number of Resends]**, use the **left** and **right** arrow buttons to select the required amount. The range is 0 to 5.
3. Select one of the following options for what part of the Fax job to re-send if transmission fails:
   - **Failed page(s) without a cover page**
   - **Failed page(s) with a cover page**
   - **Whole job without a cover page**
   - **Whole job with a cover page**
4. Touch **[Save]** to return to the **Transmission Defaults** screen.

Audio Line Monitor

Audio Line Monitor allows you to hear the Fax transmission taking place across the telephone line.

1. From the **Fax Transmission Defaults** screen, touch the **[Audio Line Manager]** icon.
2. The **Audio Line Manager** screen displays. Select **[Enable]**.
3. For **Line Monitor Volume**, select one of the following:
   - **High**
   - **Medium**
   - **Low**
4. For **Line Monitor Duration**, use the left and right arrow buttons to select the required time, from 1 to 25 seconds.
5. Touch **[Save]** to return to the **Transmission Defaults** screen.

Transmission Header Text

Transmission Header Text feature allows you to specify a text string to be transmitted as part of the transmission header.

1. From the **Fax Transmission Defaults** screen, touch the **[Transmission Header Text]** icon.

2. The **Transmission Header Text** screen displays. Touch the type-in region for **Transmission Header Text**. Use the on-screen keyboard to type the text strings. Up to 30 characters can be entered.
3. Touch **[Save]**, then **[Save]** to return to the **Fax Transmission Defaults** screen.

Batch Send

The Batch Send feature allows multiple fax jobs to be sent to the same destination during the same transmission session. This reduces the connection time for the customer and provides an economy rate for call connection charges.

Batch Send jobs are supported when the Batch Send feature is enabled and two or more separate jobs to the same telephone number destination are submitted; each job is concatenated as a single transmission to the destination telephone number.

1. From the **Fax Transmission Defaults** screen, touch the **[Batch Send]** icon.
2. The **Batch Send** screen displays. Select **[Enable]**.
3. Touch **[Save]** to return to the **Fax Transmission Defaults** screen.

File Management - Retained Document Policy

This feature allows you to configure how you will like to keep the document received or stored.

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch the **[Fax Settings]** to display the **Fax Settings** screen.
3. Select **[File Management]**.
4. The **File Management** screen displays. Select **[Mailbox & Polling Policies]** icon.
5. The **Mailbox & Polling Policies** screen displays. To set option for received documents within a mailbox, select **[Documents Received in Mailbox]** icon.
   a. Select one of the following:
      - **Delete On Print** - select this option to delete received document as soon as it prints.
      - **Keep 1-72 Hours** - select this option to save the received document for a set period of time. If selected, use the **left** or **right** arrow buttons to set time scale from 1 - 72 hours.
      - **Keep Forever** - select this option to save the document forever.

   b. Touch **[Save]** to return to the **Documents Received in Mailbox** screen.
   c. To set option for Stored Documents, select **[Document Stored for Polling]** icon.
   d. Select one of the following for **General and Mailbox**:
      - **Delete On Poll** - select this option to delete document as soon as it is polled.
      - **Keep 1-72 Hours** - select this option to save the document for a set period of time. If selected, use the **left** or **right** arrow to set time scale from 1 - 72 hours.
      - **Keep Forever** - select this option to save the document forever.

   e. Touch **Save]** to return to the **Mailbox & Polling Policies** screen.
   f. Touch **[Close]** to return to the **File Management** screen.

File Management - Mailbox Setup

A fax received can be stored on the device or on a remote fax machine. A stored fax can be accessed by remote polling and then printed. There are 200 fax mailboxes available.

To Edit a Mailbox

1. From the **File Management** screen, touch the **[Mailbox Setup]** icon.
2. Select a mailbox from the **Mailbox List** and touch the **[Edit]** icon.
3. The **Edit Mailbox** screen displays. To assign a name for the mailbox, touch the **[Mailbox Name]** icon.
   a. Touch **[Delete Text]** to clear the text. Type a name for the mailbox using the on-screen keyboard.
   b. Touch **[Save]** to return to the **Edit Mailbox** screen.
4. To assign a passcode for the mailbox:
   a. Touch **[Mailbox Passcode]** icon.
   b. Touch the **[C]** button to delete the default passcode. Enter a 4-digit passcode for the mailbox using the numeric keypad.

   Note: If no passcode is entered, the mailbox will use the default passcode of '0000'.

   c. Touch **[Save]** to return to the **Edit Mailbox** screen.
5. To receive fax notification, ensure the **Mailbox Notification** option is set to **[Enable]**.
6. Touch **[Save]** to return to the **Mailbox Setup** screen.

To Delete a Mailbox

1. From the **Mailbox Setup** screen, touch an assigned mailbox from the **Mailbox List**.
2. Touch **[Delete Mailbox]**.

   Note: Deleting a mailbox deletes the mailbox and all documents it contains.

3. On the Delete Mailbox confirmation screen, touch **[Confirm]** to delete this mailbox and all documents it contains, or **[Close]** to exit.

To Print Mailbox List

1. To print the list of mailboxes, from the **Mailbox Setup** screen, touch **[Print Mailbox List]**.
2. Touch **[Close]** to exit and return to the **Embedded Fax Settings** screen.

Fax Reports

This features allows you to configure the following reports:

- Activity Report
- Broadcast and Multipoll Report
- Transmission/Broadcast Report Appearance
- Transmission Report

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Fax Settings]** to display the **Fax Settings** screen.
3. Touch **[Fax Reports]** to display the **Fax Reports Option** screen. Select one of the following:
    - **Activity Report** - this option displays the result of the incoming and outgoing fax jobs.
      If selected, select one of the following options:
        - **Auto Print** - to automatically print a confirmation report informing you whether the fax transmission was transmitted successfully or not.
        - **Disable** - to disable the option.
    - **Broadcast and Multipoll Report** - this option when configured, shows the result of transmissions and polling requests to multiple machines.
      If selected, select one of the following:
        - **Always Print** - to automatically print a confirmation report informing you whether the fax transmission was transmitted successfully or not.
        - **Print On Error** - to print a report if the fax transmission failed.
        - **Disable** - to disable the option.
    - **Transmission/Broadcast Report Appearance** - this option allows you to choose if the report should include a reduced image of the fax or not.
      If selected, select one of the following:
        - **Reduce Image** - to print a thumbnail image of the fax on the confirmation report.
        - **No Image** - to remove the thumbnail image of the fax from the confirmation report.
    - **Transmission Report** - this option allows you to choose whether or not a transmission report is printed following a fax transmission.
      If selected, select one of the following:
        - **Always Print** - to automatically print a confirmation report informing you whether the fax transmission was transmitted successfully or not.
        - **Print On Error** - to print a report if the fax transmission failed.
        - **Disable** - to disable the option.
4. Touch **[Save]** to return to the **Fax Settings** screen.

Fax Forward

This feature allows you to specify that the incoming faxes are automatically forwarded to one or more e-mail addresses, or a file share repository or a combination of both.

> Note: In order to enable the Fax Forwarding feature the system must have either Scan-to-File or Scan-to-E-mail enabled and Embedded Fax installed and enabled.

There are two uses of the feature:

- **Fax Forwarding setup** - allows you to set up the Fax Forwarding functionality and the fax forwarding rules.
- **Customer Receives Forwarded Fax** - the system performs the Fax Forwarding function and the user receives the document either as an e-mail attachment or file in an SMB file share repository.

At Your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Embedded Fax]** link, select **[Fax Forward]** in the directory tree. The **Fax Forward on Receive** page displays.

   Note: Fax Forwarding is disabled for the fax line specified.
   Upto five rules can be defined.

3. In the **Fax Forward Rules** area, if you do not require fax forward, select **No Fax Forward**.
4. If you require fax forwarding, and you want to create a rule or change the setting of a rule, click on the corresponding **[Edit]** button.

   Note: If you apply a Rule to a fax line, you must ensure that the line is set to either **Send and Receive** or **Receive Only**. For further information, refer to Configuring Embedded Fax Settings on page 278.

5. For **Based On Rules**, the drop-down menu lets you select the settings from another rule, if set previously, in order to modify them for the current rule. The drop-down menu will always have a “Default Settings” selection, with additional selections for rules which have been defined.
6. In the **General** area:
   a. Enter a name in the **Rule Name** field.
   b. From the **File Format Type** drop-down menu, select one of the following:
      - **PDF - Image Only** - this is the default setting. Select this for Full Color, Grayscale or Black/White documents.
      - **PDF - Searchable** - select this for Full Color, Grayscale or Black/White documents and with searchable text.
      - **XPS - Image Only** - select this for Full Color, Grayscale or Black/White documents.
      - **XPS - Searchable** - select this for Full Color, Grayscale or Black/White documents and with searchable text.
      - **Multi-Page TIFF** - select this for Full Color, Grayscale or Black/White documents. This option saves each page of a multiple page document as an individual TIFF file.

   c. From the **Print Local Copy** drop-down menu, select one of the following:
      - **On Error Only** - this option allows the incoming fax to print only when there is an error in forwarding the fax.
      - **Always** - this option allows the incoming fax to print always.

   Note: The rule must specify either a **Forward to E-mail** section and/or a **Forward to File Destination** section.

7. In the **Forward to E-mail** area:
   a. Check the **[Email]** checkbox to enable Forward to E-mail.
   b. Enter details of the destination e-mail address in the **[Address 1]** field. A further four e-mail addresses can be added.

   Note: **Address 1** is a required field. One e-mail address is allowed per address field.

c. Enter the e-mail address the e-mail server will use to identify the sender of the forwarded e-mail in the **[From Address]** field. This is a required field.

d. Enter a descriptive details referred to as the friendly name for the sender of the forwarded fax document in the **[From Name]** field.

e. Enter a descriptive detail to describe the content in the **[Subject]** field.

f. The **[Attachment Name]** field will display the filename that will be applied to the forwarded fax document. Click on the **[Customize]** button to define how the Attachment Name is generated. For further information, refer to Custom Attachment Name on page 286.

g. In the **[Message]** field enter a descriptive statement of the purpose of the e-mail message.

h. Enter details in the **[Signature]** field.

8. In the **Forward to File Destination** area:

a. Check the **[SMB Protocol]** checkbox, to allow the fax to be forwarded to a specified file location using the Server Message Block (SMB) protocol.

b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** for the SMB server. Enter details in either the **[IP Address: Port]** or **[Host Name: Port]** fields.

c. Enter the SMB share name in the **[Share]** field.

d. Enter the path to the filing destination in the **[Document Path]** field.

e. Enter a login name the device will use to login into the server in the **[Login Name]** field.

f. Enter a password the device will use to login into the server in the **[Password]** and **[Retype Password]** fields.

g. Check the **[Select to save the new password]** checkbox to save the new password on this device.

h. The **[File Name]** field will display the filename that will be applied to the forwarded fax document.
Click on the **[Customize]** button to define how the File Name is generated. For further information, refer to Custom Attachment Name on page 286.

i. Check the **[Email Notification (without Attachment)]** checkbox to enable for a notification e-mail to be sent to the specified address when a fax is received and forwarded.

j. Enter an e-mail address in the **[Notification Address]** field.

9. Click on the **[Save]** button to return to the **Fax Forward On Receive** screen.
10. Repeat above steps if necessary for a further four rules.

Custom Attachment Name

When a fax is forwarded to an e-mail address, the fax is attached as a file. This page is used to build up a unique file name for the fax attachment based on individual text elements which can be enabled and rearranged.

The Custom Attachment Name is accessed by clicking the **[Customize]** button in the **Fax Forward On Receive** screen for **Forward to Email** and **Forward to File Destination**.

At Your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.

2. Click on the **[Embedded Fax]** link and select **[Fax Forward]** in the directory tree. The **Fax Forward on Receive** page displays.
3. Click on the **[Customize]** button: the **Custom Attachment Name** screen displays.
    a. In the **Display** area, the following are programmed as **Standard** options, which can be selected by checking the relevant checkbox:
        - **Date** - selecting this allows the date “**<Received_Date>**” to display. When the fax is forwarded, this is replaced by the current date.
        - **Time** - selecting this allows the date “**<Received_Time>**” to display. When the fax is forwarded, this is replaced by the current time.

    b. For **Custom Text**, further four text fields are available. Check the required checkbox to allow text entry into the corresponding field. Up to 20 characters or numbers are allowed per field.

    c. The **Position** area will display the order of the fields which comprise the attachment file name. You can re-arrange the order of the fields appear by selecting a field and using the **up** and **down** arrows.

    d. Click on the **[Save]** button.

Server Fax 15

Server Fax is a standard feature that can be enabled on your device. If enabled, it can be accessed by pressing the **<Services Home>** button then selecting the **Server Fax** icon. Server Fax scans your documents and sends them to any type of fax machine that is connected to a telephone network.

Your images are sent from your device to a Third Party fax server, which relays them over the telephone network to the fax number of your choice. This means that your fax transmissions are controlled by the server, which may limit your faxing options. For example, the server may be set-up to collect and send all faxes at off peak times.

This section contains instructions to configure a fax filing location (repository) on your server. The fax server retrieves the documents from the filing location and transmits them via the telephone network. The fax server manages the fax transfer and has the ability to send confirmation reports which are printed at the device.

> Note: Server Fax and Embedded Fax services are mutually exclusive. Only one of them can be enabled at any time.
> If Server Fax is currently enabled and Embedded Fax is then enabled, Server Fax will be disabled automatically. If Embedded Fax is currently enabled and Server Fax is then enabled, Embedded Fax will be disabled automatically.

Server Fax Authentication and Authorization

Authentication (Service Access Control) can be enabled on the device to prevent unauthorized access to the network options. If Authentication is enabled a user will be prompted to enter a user name and password, before they can access the Fax feature. For a full description of the Authentication feature refer to Authentication on page 155. Authentication can be configured after Server Fax has been installed.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to enabling Server Fax.
- Ensure that the TCP/IP and HTTP are configured on the device as per Enable TCP/IP and HTTP at the Device on page 19.

  This is required to access the device's Internet Services web pages, which can be used to configure E-mail settings from a network connected workstation's web browser.

  For instructions on how to configure TCP/IP and HTTP, refer to Configure Network Connectivity Protocols with Internet Services on page 25.
- Install and configure the Xerox certified fax server solution on your network. Refer to the manufacturer's documentation contained with the server fax solution for instructions to complete this task.

- If the server fax solution uses the TCP/IP protocol to communicate, it is recommended that the server be assigned a static IP Address. However, dynamic IP Addressing may be used provided DNS settings are fully configured and the DHCP server has been configured with sufficient lease time so that the normal maintenance and service down times of the fax server does not result in a change in IP Address.

Print a Configuration Report to verify that Server Fax is an Installed Option:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report check under **Installed Options** heading if **Network Server Fax** is installed and enabled.

Enable Server Fax

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Optional Services]**.
3. Scroll down, by touching the scroll **arrow**, touch **[Server Fax]**.
4. Touch **[Enable]**.
5. Touch **[Save]**.
6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools Pathway.

Configure a Server Fax Repository

The device can be configured to transfer the fax images to a directory on the fax server. The directory is known as the fax repository. The fax server monitors the fax repository for documents to be faxed.

Select your required transfer method from the list below.

- **FTP (File Transfer Protocol)** - requires an FTP server running on a server or a workstation.
- **NetWare** - this available only if the Network Protocol is enabled. This requires a NetWare server.
- **SMB (Server Message Block)** - available for filing to an environment that supports the SMB protocol.
- **HTTP/HTTPS** - supports scans to a web server using a CGI script.
- **SMTP (**Simple Mail Transfer Protocol) - available to file to a mail server.

Configure a Fax Repository using FTP Server

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that File Transfer Protocol (FTP) services is running on the server or workstation where images to be faxed by the device will be stored. Note the IP Address or host name.
- Create a user account and password for the device. When the Server Fax feature is used, the device logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory within the FTP root to be used as a fax repository. Note the directory path.
- Test the FTP connection by logging in to the fax repository 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.

Enter the Fax Repository Details Using Internet Services

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Fax Repository Setup]** in the directory tree.
4. In the **Settings** area:
   a. Select **FTP** from the **[Protocol]** drop-down menu.
   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter details of the **Repository Server** in the **IP Address: Port** or **Host Name: Port** field.
   d. Type in the path to the location of the repository server in **[Document Path]**. For example: **/(directory name)/(directory name)**.
   e. In the **[Login Credentials to Access the Destination]** area, select one of the following:
      - **Authenticated User and Domain** - select this method to be used in conjunction with the network accounting or another authentication method, such as Secure Access, to validate the user.
      - **Authenticated User** - when selected, the device will prompt to log in using your own network credentials.
      - **System** - selecting this method allows the device to authenticate to the server with the credentials entered in the **[Login Name]**, **[Password]** and **[Retype Password]** entry fields.

   f. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
5. Click on the **[Apply]** button to accept the changes.
6. Configure the Defaults settings, refer to Configure Default Settings on page 296.

Configure a Fax Repository using NetWare

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Create a new directory on the NetWare server to be used as the fax repository. Note down the server name, server volume, directory path, NDS Context and Tree, if applicable.
- Create a user account and password with access to the fax repository. When a document is faxed, the machine logs in using the account, transfers the file to the server and then logs out.
- Ensure the NetWare protocol is enabled on your machine.

Print a Configuration Report to verify that the NetWare protocol is enabled on your machine.

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report check under **Network Setup** heading if **Netware** protocol is enabled.

Enter the Fax Repository Details via Internet Services

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Fax Repository Setup]** in the directory tree.
4. In the **Settings** area:
   a. Select **NetWare** from the **[Protocol]** drop-down menu.
   b. Enter the host name or the NetWare server in the **[Server Name]** field.
   c. Enter the path to the Repository on the NetWare server in the **[Server Volume]** field.
   d. Enter NDS tree details in the **[NDS Tree]** field. The default tree name is “Xerox_DS_Tree”.

   Note: If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank.

   e. Enter the name for the NDS context in the **[NDS Context]** field. The default context name is “Xerox_DS_Context”.

   Note: If you are using Bindery or Bindery emulation, leave this field blank. If you are using NDS, this field cannot be left blank.

   f. Type in the path to the location of the repository server in **[Document Path]**. For example: **/(directory name)/(directory name)**.
   g. In the **[Login Credentials to Access the Destination]** area, select one of the following:

- **Authenticated User and Domain** - select this method to be used in conjunction with the network accounting or another authentication method, such as Secure Access, to validate the user.
- **Authenticated User** - when selected, the device will prompt to log in using your own network credentials.
- **System** - selecting this method allows the device to authenticate to the server with the credentials entered in the **[Login Name]**, **[Password]** and **[Retype Password]** entry fields.

h. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

5. Click on the **[Apply]** button to accept the changes.
6. Configure the Default settings. Refer to Configure Default Settings on page 296.

Configure a Fax Repository using SMB

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Create a shared folder to be used as a fax repository. Note the Share Name of the folder and the Computer Name or Server Name.
- Create a user account and password for the device with full access rights to the fax repository. Note the user account and password.
- 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 Fax Repository Details Using Internet Services

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Fax Repository Setup]** in the directory tree.
4. In the **Settings** area:
   a. Select **SMB** from the **[Protocol]** drop-down menu.
   b. Select either **[IPv4 Address]** or **[Host Name]**.
   c. Enter details of the **Repository Server** in the **IP Address: Port** or **Host Name: Port** field.
   d. Enter details of the Share name in the **[Share]** field.
   e. Type in the path to the location of the repository server in **[Document Path]**. For example: **/(directory name)/(directory name)**.
   f. In the **[Login Credentials to Access the Destination]** area, select one of the following:

- **Authenticated User and Domain** - select this method to be used in conjunction with the network accounting or another authentication method, such as Secure Access, to validate the user.
- **Authenticated User** - when selected, the device will prompt to log in using your own network credentials.
- **System** - selecting this method allows the device to authenticate to the server with the credentials entered in the **[Login Name]**, **[Password]** and **[Retype Password]** entry fields.

g. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

5. Click on the **[Apply]** button to accept the changes.
6. Configure the Default settings. Refer to Configure Default Settings on page 296.

Configure a Fax Repository using HTTP/HTTPS

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that web services are installed on the server where you want to store scanned images. Examples of web servers include: Microsoft Internet Information Services (IIS) and Apache. Note the IP Address or host name of the server.
- For HTTPS, ensure that your web server is installed with a secure certificate.
- Create a user account and password for the device. When a document is scanned, the device logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory on the HTTP/HTTPS server to be used as a scan filing location (repository). Note the directory path.
- Note any script that is required to be run.

Enter the Fax Repository Details via Internet Services

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Fax Repository Setup]** in the directory tree.
4. In the **Settings** area:
   a. Select **HTTP** or **HTTPS** from the **[Protocol]** drop-down menu.
   b. Select either **[IPv4 Address], [IPv6 Address]** or **[Host Name]**.
   c. Enter details of the **Repository Server** in the **IP Address: Port** or **Host Name: Port** field.
   d. To view the proxy server settings, click on the **[View HTTP Proxy Server Settings]** link.

e. **HTTPS only**: Check the **[Validate Repository SSL Certificate]** checkbox to have the repository's SSL certificate validated for the correct hostname and checked for signature of a trusted certificate authority.

f. Enter details of the Script path and filename in the **[Script path and filename (from HTTP root)]** field, or follow the instruction below to get example script:

   - Click on the **[Get Example Scripts]** link to download an example script in either **PHP**, **ASP** or **Perl** language.

Note: HTTP and HTTPS both require server-side scripts to allow files to be transferred to your HTTP server from the multifunction device.
The scripts are written in common scripting languages and documented with comments. You can use them as written, modify them to suit your needs, or use them as examples to create a custom solution. Choose a file that corresponds with the scripting language supported on your server.
PHP example: **.zip .gz**
ASP example: **.zip .gz**
ASP .NET: **.zip .gz**
Perl example: **.zip .gz**
The first line of the Perl script needs to point to Perl on your server. For example, **/usr/bin/perl**.
The script must reside on the HTTP Scan Repository server to work properly. You must indicate the path and filename of this script (relative to the HTTP root) in the Filing Destination setup. If authentication is required to access the script on the server, specify login information on the setup page.
The Document Path directory permissions must allow write operations

   - Right-click on the required script language file **[.zip]** or **[.gz]**, which is supported by your HTTP Scan Repository server and select **[Save Target As...]** to save the file to a location on the desktop.
   - Write down the path and filename to enter in the **[Script path and filename (from HTTP root]** field.

g. Type in the path to the location of the repository server in **[Document Path]**. For example: **/(directory name)/(directory name)**.

h. In the **[Login Credentials to Access the Destination]** area, select one of the following:

   - **Authenticated User and Domain** - select this method to be used in conjunction with the network accounting or another authentication method, such as Secure Access, to validate the user.
   - **Authenticated User** - when selected, the device will prompt to log in using your own network credentials.
   - **System** - selecting this method allows the device to authenticate to the server with the credentials entered in the **[Login Name]**, **[Password]** and **[Retype Password]** entry fields.

i. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

5. Click on the **[Apply]** button to accept the changes.
6. Configure the Default settings. Refer to Configure Default Settings on page 296.

Configure a Fax Repository using SMTP

Information Checklist

Before starting the procedure, ensure the following task has been performed:

- Obtain the domain name of your SMTP mail server.

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Fax Repository Setup]** in the directory tree.
4. Select **[SMTP]** from the **Protocol** drop-down menu.
5. Enter details in the **[Domain Name]** field.
6. For **Enable Email Security**, check the **[Enable]** checkbox to automatically include the Authenticated User's e-mail address in the **CC:** field.
   Additionally, the Authenticated User's e-mail address will be used as the **Reply To:** address.

   Note: This feature requires Network Authentication to be enabled. The **Perform LDAP Query** to populate the **From:** field option must be enabled.
7. Click on the **[Apply]** button to accept the changes.

Configure Default Settings

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Server Fax]** link.
3. Select **[Defaults]** in the directory tree. The **Fax - Defaults** page displays.
   The following options can be configured:
   - **General**
   - **Fax**
   - **Image Quality**
   - **Layout Adjustment**
   - **Filing Options**

General

1. From the **Fax - Defaults** page, in the **General** area, click on the **[Edit]** button. The **General** page displays.
   a. In the **General** area, for **Job Log**, check the **[User Name]** and/or **[Domain]** checkbox if you want these attributes to appear in the Job Log when users log in to the device.

b. For **Confirmation Sheet**, select the type of information that you want to be included with the Confirmation Sheet from the drop-down menu:
    - **Errors Only** - this setting will produce a Confirmation Sheet only when error information is detected.
    - **On** - this setting will always produce a Confirmation Sheet that will provide error information and job status.
    - **Off** - this setting will not produce a Confirmation Sheet.

c. Click on the **[Save]** button to return to the **Fax** - **Default** page.

Fax

1. From the **Fax - Defaults** page, in the **Fax** area, click on the **[Edit]** button. The **Fax** page displays.
    a. In the **Server Fax** area, for **[2 Sided Scanning]** select the required document scanning option, either **[1 Sided]**, **[2 Sided]** or **[2 Sided, Rotate Side 2]**.
    b. Select the required method used to optimize the quality of your scanned output images based on the content in your original documents for **[Content Type]**.
    c. Specify the resolution from the **[Resolution]** drop-down menu. The resolution affects the amount of detail reproduced on graphic images, and transmit time. Select **[Standard (200 x 100 DPI)]** or **[Fine (200 DPI)]**.
    d. Click on the **[Apply]** button to return to the **Fax** - **Default** page.

Image Quality

1. From the **Fax - Defaults** page, in the **Image Quality** area, click on the **[Edit]** button. The **Image Quality** page displays.
    a. In the **Image Quality** area, for **Lighten / Darken**, use the **[Lighten]** or **[Darken]** arrow buttons to adjust the overall brightness of the original output.
    b. For **Background Suppression**, select either **[No Suppression]** or **[Auto Suppression]**. Use this feature to prevent the reproduction of an unwanted background image, shading or bleed-through from the reverse side of the original. This will produce an output image with a mostly white background.
    c. For **Soften/Sharpen**, use the left **[Soften]** or right **[Sharpen]** arrow buttons to adjust the overall softness or sharpness of the original output.
    d. For **Manual Contrast**, use the left **[Least Contrast]** or right **[Most Contrast]** arrow buttons to adjust the overall contrast of the original output
    e. Click on the **[Apply]** button to return to the **Fax** - **Default** page.

Layout Adjustment

Layout Adjustment setting includes **Original Size**. This allows you to choose either **[Auto Detect]** which allows the device to automatically detect the original size of the document, or **[Manual Size Input]** which requires the user to select the size of the document, or **[Mixed Size Originals]** if the original documents are of mixed sizes.

1. From the **Fax - Defaults** page, in the **Layout Adjustment** area, click on the **[Edit]** button. The **Layout Adjustment** page displays.
2. Select the required options.
3. Click on the **[Apply]** button to accept changes and return to the **Fax** - **Default** page.

Filing Options

Filing options allow you to specify the Delay Start. When **[Specific Time]** is selected, this allows you to specify the time of day (each day) when the fax jobs will start. This feature is convenient for international calls and for sending documents at night when the telephone rates are at their lowest. If set to **[Off]**, any fax jobs are begun (or queued) immediately.

1. From the **Fax - Defaults** page, in the **Filing Options** area, click on the **[Edit]** button. The **Filing Options** page displays..
2. For **Delay Start**, select the required option. If **[Specific Time]** is selected, enter required time.
3. Click on the **[Apply]** button to implement changes and return to the **Fax** - **Default** page.

LAN Fax 16

LAN (Local Area Network) Fax allows users to send documents to fax devices directly from their computers. When enabled, users select the Fax option from their Print Driver. The LAN fax option requires the Embedded Fax Kit to be fitted to the device.

Information Checklist

Make sure that you have configured the Embedded Fax. For further information, refer to Embedded Fax on page 271 before continuing with this procedure.

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that the device is fully functioning in its existing configuration.
- The Embedded Fax option must be installed on the device.
- The WorkCentre Print Driver must be installed on your Workstation.

Enable LAN Fax (Windows Print Driver)

LAN Fax must be enabled in your Print Driver to support the LAN fax feature. LAN fax can be enabled automatically, with either Bi-directional communication or manually. Both instructions are detailed below.

Configure the Print Driver - Automatically

1. At your Workstation, from the **[Start]** menu click on:
    - **[Printers and Faxes]** - Windows XP. If you cannot see this option in the **[Start]** menu, then click on **[Start]**, followed by **[Control Panel]** first.
    - **[Settings]** then **[Printers]** - Windows 2000.
    - **[Settings]** then **[Printers and Faxes]** - Windows 2003
2. Right-click on your Print Driver and click on **[Properties]**.
3. Click on the **[Configuration]** tab.
4. Click on **[Bi-Directional Setup]**.
5. Ensure **Bi-directional Communication** is set to **[Automatic]**, or click on **[Manual]** and enter the Device Name or IP Address. Click on **[OK]**.
6. Click on the **[Installable Options]** button.
7. Ensure that **LAN Fax** displays **[Installed]**.
8. Click on **[OK]**.
9. Click on **[Apply]**.

Configure the Print Driver - Manually

To configure the Print Driver without using bi-directional communication return to the **Configuration** tab within the **Properties** of the Print Driver.

1. Click on **[Installable Options]**.
2. Click on the **[LAN Fax]** drop-down menu and select **[Installed]**.
3. Click on **[OK]**.
4. Click on **[Apply]** to close the Print Driver **Properties** menu.

Using LAN Fax

Windows	MAC
1. Open a document that you want to fax. 2. Click on **[File]** then **[Print]**. 3. In the **Printer** area, from the **Name** drop-down menu, select your printer. 4. Click on the **[Properties]** (or **[Preferences]**) button. a. Ensure you are on the **[Paper/Output]** tab. b. Select **[Fax]** from the **[Job Type]** drop-down menu to display the **Fax** screen.	1. Open a document to fax and click on **[File]** and then **[Print]**. 2. Click on the *Xerox* printer. 3. Click on **[Xerox Features]** from the **[Copies and Pages]** menu. a. Ensure you are on the **[Paper/Output]** area. b. Select **[Fax]** from the **[Job Type]** drop-down menu to display the **Fax** screen. 4. Click on **[Fax]**.

Add Fax Recipient

1. On the **Fax** screen, click on the **[Add Recipient]** icon.
2. In the **Add Fax Recipient** area:
   a. Enter the name of the fax recipient in the **[Name]** field.
   b. Enter the fax number of the recipient in the **[Fax Number]** area.
   c. Enter details such as **Organization**, **Telephone Number**, **E-mail Address** and **Mailbox** number if required.
   d. If you want to add this recipient to your personal phonebook, check the **[Save to Personal Phonebook]** checkbox.
   e. Click on **[OK]**.

   The recipient will show in the **[Recipients]** list.
3. If you have a Personal Phonebook created you can add a recipient name from it. On the Fax screen, click on the **[Add from Phonebook]** icon.
4. In the **[Add from Phonebook]** area:
   a. If you have more than one phonebook available, select the required phonebook from the **[Phone book]** drop-down menu.
   b. Click on the recipient that you want to fax to and click on the add (green arrow) button. To view the details for the recipient, double-click on the recipient.
   c. If you want to add more than one recipient, hold down the **[Ctrl]** key on your keyboard and click on each name, and click on the add (green arrow) button.

   d. The names will appear in the **[Fax Recipients]** list. Click on the **[OK]** button.
5. If you want to save this list of names as a group, click on the **[Save As Group]** icon.
6. In the **Save To Personal Phonebook** area:
   a. Enter a name for your group in the **[Group Name]** field.
   b. Click on the **[OK]** button to return to the **Fax** screen.
7. Click on the **[OK]** button to return to the **Properties** screen.

Setting up a Cover Sheet

1. On the Fax screen, click on the **[Cover Sheet]** tab.
2. If you want to add a cover sheet to your document, select **[Print a Cover Sheet]** from the **Cover Sheet Options** drop-down menu.
3. A new screen displays. Select required options from the following drop-down menu:
   - **Recipient Information**
   - **Sender's Information**
   - **Cover Sheet Paper Size**
4. Enter the information that you want to show on the cover sheet in the following fields:
   - **Name**
   - **Fax Number**
   - **Organization**
   - **Telephone Number**
   - **E-mail Address**
5. If you want to add a graphic or logo to the cover sheet (a .bmp, .gif or .jpeg), select **[New]** from the **Cover Sheet Image** drop-down menu.
   c. The **Cover Sheet Image Editor** screen displays. To add a graphic or logo, select **[Picture]** from the **[Options]** drop-down menu.
   d. Click on the **[Choose File]** button, select the required graphic or logo from your Workstation, and click on the **[Open]** button.
   e. Adjust the required settings for the following options:
      - **Scale**
      - **Density**
      - **Position**
      - **Preview Options**
   f. Click on the **[OK]** button to return to the **Cover Sheet** screen.
6. Select **[Options]** from the **Cover Sheet Image** drop-down menu.
   g. Select one of the following options:
      - **Print in Background -** to print the graphic behind any text on the cover sheet.
      - **Print in Foreground -** to print the graphic at the front of your cover sheet.
      - **Blend -** to print a faint image of the graphic.
7. Click on the **[OK]** button to return to the **Fax** screen.

Additional Fax Options

1. On the **Fax** screen, click on the **[Options]** tab.
2. Select the required option from the **[Confirmation Sheet]** drop-down menu.
3. Select from the **[Send Speed]** drop-down menu, one of the following required speeds.
    - **Forced 4800 bps** - used in areas of low quality communication, when experiencing telephone noise, or when fax connections are susceptible to errors. 4800 bps is a slower transmission rate but is less susceptible to errors. In some regional areas, the use of 4800 bps is restricted.
    - **G3 (14.4 Kbps)** - selects the transmission rate based on the maximum capabilities of the receiving fax device. Initial transmission speed will be 14,400 Bits Per Second (bps). This rate minimizes transmission errors by using Error Correction Mode (ECM).
    - **Super G3 (33.6 Kbps)** - this is the fastest transmission rate and is the default setting. This rate minimizes transmission errors by using Error Correction Mode (ECM). Initial transmission speed will be 33,600 Bits Per Second (bps).
4. Select the required resolution from the **[Fax Resolution]** drop-down menu.
5. For **Send Time**, select either **[Send Now]** or **[Send At]**. If you want to send your fax at a specific time, enter the time in the next 24 hours that you want the device to send your fax.
6. For **Fax Dialing Options**, check the following checkbox:
    - **Dialing Prefix** - if your telephone system requires Fax users to enter a prefix in front of fax numbers. If selected, enter the prefix in the entry field.
    - **Credit Card** - if your call requires a Charge Code number for billing purposes. If selected, enter the details for the charge code in the entry field.

Setup Phone book Preferences

1. On the Fax screen, click on the **[Options]** tab and click on the **[Preferences]** button.

    If you have more than one phonebook configured, you can specify which phonebook to use as the default from the **[Default Phonebook]** drop-down menu.
2. The Personal Phonebook is created when you add fax numbers on the **[Fax Recipients]** tab. The Personal Phonebook is automatically saved on your PC in a file called **default.xpb**. To view the Personal Phonebook:
    a. Click on the **[Select File...]** icon for **Personal Phonebook** and select the **[default.xpb]** file.
    b. Click on the **[Open]** button.
    c. Click on the **[Open]** icon for **Personal Phonebook**.
3. The Shared Phonebook is a list of fax numbers and recipient details that has been saved to a network drive for more than one person to use. To access a shared phonebook:
    a. Click on the **[Select File...]** icon for **Shared Phonebook** and locate the **[default.pb]** shared phonebook file on your network.
    b. Click on the **[Open]** button.
    c. Click on the **[Open]** icon for **Shared Phonebook** to view the phonebook.
4. For **User Preferences**, check the following required checkboxes:
    - **Prompt When Adding Duplicate Recipients** - if you want to be notified when you add duplicate recipients to the phonebook.
    - **Prompt When Removing a Recipient** - if you want to be notified when you delete a recipient from the phonebook.

- **Always Use Current Recipient List** - if you want to always use the Current Recipient List.
- **Always Use Current Cover Sheet Notes** - if you want to use the current Cover Sheet notes.

5. Click on the **[OK]** button to return to the **Fax** screen.
6. Click on the **[OK]** button to close the **Fax** screen.
7. Click on the **[OK]** button on the **Properties** screen.
8. Click on the **[OK]** button on the **Print** screen to send a LAN fax. The document will fax with the specified settings.

Reprint Saved Jobs 17

Reprint Saved Job is a feature that allows users to store documents into folders located on the device.

Using the Print Driver settings or the Internet Services, the job type can be set to Save Job For Reprint. When this job type is selected, an option is provided to Save Only or Save and Print. Some of the job settings are stored with the job and they can be modified at the time of printing.

Reprint Saved Job allows you to reprint jobs which have been stored on the device while standing at the device using the local UI or remotely using Internet Services Print Submission. Jobs are placed into a folder located on the device and can be accessed and retrieved for printing at later date. Jobs can be recalled and printed as many times as you need.

All Saved Jobs are stored as encrypted files, if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan or e-mail these files.

You can enable/disable encryption of user data. Refer to User Data Encryption on page 173.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network.
- To backup jobs and folders an FTP server must be available on the network (recommended). Create an account with rights to the FTP root which the device can use to access the FTP server.

Enable Reprint Saved Jobs

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Reprint Saved Jobs]** link.
3. Select **[Enablement]** in the directory.
4. In the **Enablement** area:
    a. Select **[Enabled]** to enable Saved Jobs for Reprint or **[Disable]** to disable Saved Jobs for Reprint.
    If **Disable** is selected, two further options are available. Select one of the following:
        - **Retain All Jobs** - all saved jobs currently on the system will be retained.
        - **Delete All Jobs** - all saved jobs currently on the system are deleted.

5. Click on the **[Apply]** button.

   Note: All Saved Jobs are stored as encrypted files if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, scan and e-mail these files. You can enable or disable encryption of user data on the **User Data Encryption** page. Refer to User Data Encryption on page 173.

Enable Reprint Saved Jobs in your Print Driver

Windows Operating Systems	MAC Operating Systems
1. At your Workstation, open the **Printers Folder**. • For **Windows 2000/2003** - From the **[Start]** menu, select **[Settings]** then **[Printers]**. • For **Windows XP** - From the **[Start]** menu, select **[Printers and Faxes]**. • For **Windows Vista** - From the **[Start]** menu, (select **[Control Panel]**) then select **[Printers and Faxes]**. 2. Right-click on the Xerox WorkCentre Print Driver. 3. Select **[Properties]**. 4. Click on the **[Configuration]** tab. 5. Click on the **[Installable Options]** button. 6. Ensure **[Installed]** is selected from the **[Job Storage]** drop-down menu. 7. Click on the **[OK]** button to close the Installable Options screen. 8. Click on the **[OK]** button to close the Properties screen.	1. At your Mac Workstation, open the **[Printer Setup Utility]**. 2. Select the Xerox printer and click on the **[Show Info]** button. 3. Click on **[Installable Options]**. 4. Select **[Installed]** from the **[Job Storage]** drop-down menu. 5. Click on the **[Apply Changes]** button. 6. Close the Printer Info box.

Enable Save Job for Reprint

At Your Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Select **[Optional Services]**.
3. Scroll down using the down arrow button and select **[Save Job For Reprint]**.
4. The **Save Job for Reprint** screen displays, select one of the following:
   - **Disable and Delete Jobs** - this option will disable the feature and delete the user folders and it contents.
   - **Disable and Keep Jobs** - this option will disable the feature, but will not delete the user folder or its content.
   - **Enable** - this option enables the feature, and does not require a system restart to activate the feature.
5. Touch **[Save]** to return to the Optional Services screen.

6. Press the **<Log In/Out>** button.
7. Touch **[Logout]** to exit the Tools pathway.

Back-up Jobs

The Back-up Jobs feature allows you to configure a server to save jobs stored on the device.

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Reprint Saved Jobs]** link.
3. Select **[Backup Jobs]** in the directory tree.
4. In the **Settings** area:
   a. Select **FTP** from the **[Protocol]** drop-down menu.

   Note: Only FTP is available for the Protocol.

   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter details in the **[IP Address: Port]** or **[Host Name: Port]** field of the Repository Server.
   d. Type in the path to the location of the repository server in the **[Document Path]** field. For example: **/(directory name)/(directory name)**.
   e. Enter the file name for the backup in the **[File Name]** field. This name will be appended to the document path
   f. Enter the system login name in the **[Login Name]** and the password in the **[Password]** field.
   g. Re-enter the password in the **[Retype Password]** field.
   h. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
5. Click on the **[Start]** button to begin the backup.

Restore Jobs

Use the Restore Jobs feature to restore the saved jobs stored on a repository.

> Note: When Saved Jobs are restored, all current Saved Jobs data will be deleted. The restore process may take considerable time to complete depending on how many files were backed up. If the restore is aborted, the Default Public Folder will be empty.

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Reprint Saved Jobs]** link.
3. Select **[Restore Jobs]** in the directory tree.

4. In the **Settings** area:
    a. Select **FTP** from the **[Protocol]** drop-down menu.

    Note: Only FTP is available for the Protocol.

    b. Select the method by which the repository server is identified. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
    c. Enter details of the Repository Server in the **[IP Address: Port]** or **[Host Name: Port]** field.
    d. Type in the path to the location of the repository server in the **[Document Path]** field. For example: **/(directory name)/(directory name)**.
    e. Enter the file name for the backup to restore in the **[File Name]** field. This name will be appended to the document path.
    f. Enter the system login name in the **[Login Name]** and the password in the **[Password]** field.
    g. Re-enter the password in the **[Retype Password]** field.
    h. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
5. Click on the **[Start]** button to begin the restore process.

Manage Folders

Create New Folder

Folders and the files saved within them can be managed using Internet Services.

1. At your workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Select the **[Jobs]** options.
3. Select the **[Saved Jobs]** tab to access the folder options.
4. In the **Folder Operations** area, select **[Create New Folder]**.
5. Input the name for the folder in the **[Name]** field.
   As a normal user you are only able to create **Public folders**. There are the other kind of folders you may see in the **[Folder Permissions]** drop-down menu.
    - **Public folder** - it can be used by any user and has no access authority limitations. Any user can access and modify the documents in this folder.
    - **Read Only** - any user can print from the folder but documents cannot be deleted or modified by non System Administrator users.
    - **Private** - the user marks the folder as **Private** and the folder is only visible to the Owner and the System Administrator.
6. When you have selected the appropriate Permissions, click on the **[Apply]** button.

The Folder is displayed in the **Folders List**.

Modify or Delete Folder

You can modify or delete existing folders that contain **Saved Jobs** using Internet Services.

1. At your workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Select the **[Jobs]** tab.
3. Select **[Saved Jobs]** tab to access the folder options.
4. In the **Folder Operations**, select **[Manage Folders]**.
   The window displays all the **Public** folders and any **Private** folders belonging to you.
5. Check the checkbox next to the folder you want to modify.
6. Select options required for the folder.
   The folder can be deleted by selecting the **[Delete Folders]** button.
   The folder and the contents of the folder are deleted from the list on this screen and the list of available folders at the device.

Saving a Job

Prior to using the Reprint Saved Jobs option, a job must be saved to a folder on the device. The folders are setup by the System Administrator using Internet Services and can be managed by the users. Refer to Manage Folders on page 308 for more information.

Jobs can be saved in the folders by selecting the Save Job for Reprint Job Type when submitting a print job from your PC, or when submitting a print job using Internet Services.

Using the Print Driver

Select or create a document on your PC.

1. Select **[Print]** from the application's **[File]** menu.
   The application Print window is displayed.
2. Select the WorkCentre printer from the **[Printer Name]** drop-down menu.
3. Select **[Properties]** to access the print settings for the job.
4. Select the **[Job Type]** drop-down menu and select **[Saved Job...]**.
   The **Saved Job** options are displayed.
5. Configure the Saved Job options as required:
   - Select **[Save]** to store the job only or **[Save and Print]** to store and print the job.
   - **Job Name** is used to enter a name for the job or select **Use Document Name** to use the filename of the document being submitted.
   - **Folder** is used to select a location to store the job. The **Default Public Folder** is available to all users, other folders may have restricted access.
     Names entered are for Public Folders only. If the entered name is not an existing public folder, a public folder will be created with the submitted name.
   - **Secure Saved Job** is used to add a passcode to the job. The job can only be accessed and printed using the **Passcode** entered here.
   - Select **[OK]** to save the settings and exit the Saved Job options.

   Note: The **Help** option provides an explanation of all the options.

6. Select **[OK]** to save the print settings.
7. Select **[OK]** on the Print dialogue window to send the job.
   The job is processed and sent to the device for saving or saving and printing, depending on the selection.

Using Internet Services

The Print option within Internet Services can also be used to create a Saved Job. The job file submitted must be a print ready file, such as a PDF or PostScript file.

1. At your workstation, open the web browser and enter the IP Address of the device in the Address bar, and press **<Enter>**.
2. Select **[Print]** to access the **Job Submission** options.
3. Enter the file name of the job requiring saving, or use the **[Browse]** option to locate the file.
4. From the **[Job Type]** drop-down menu and select **[Save Job for Reprint]**.
   The Saved Job options are displayed.
   - Select **[Save]** to store the job only or **[Save and Print]** to store and print the job.
   - Enter a name for the job in the **[Job Name]** field.
   - From the **[Save in Folder]** drop-down menu, select a location to store the job. The **Default Public Folder** is available to all users, other folders may have restricted access.
   - Check the **[Secure Saved Job]** checkbox to add a passcode to the job. The job can only be accessed and printed using the passcode entered here.
   - Select the required settings from the **Paper**, **2 Sided Printing**, **Collate**, **Orientation, Staple, Folding** and **Output Destination** drop-down menus.
5. Click on **[Submit Job]** at the top of the page to send the job to the device over the internet.

The job is processed and sent to the device for saving or saving and printing, depending on the selection.

Custom Services 18

Validation Options

The Validation Options feature is used with the Workflow Scanning Validation Server and the Network Authentication features.

When a user enters their metadata information at the user interface, the metadata is passed to the validation server to be verified. When Validation Options is enabled, the user's ID is also passed with the validation request to the Validation Server. The user ID is recorded when the user enters their network authentication account details at the user interface.

Enable Validation Options

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Custom Services]** link.
3. Select **[Validation Options]** in the directory tree.
4. To have the user name sent with the validation request if the user is authenticated at the device user interface, check the **[Include User Name with validation request]** checkbox.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

19 Extensible Services Setup

Xerox Extensible Interface Platform (EIP) is a software platform inside many Xerox MFPs that allows independent software vendors and developers to create personalized and customized document management solutions that you can access directly from the MFP touch screen.

For example, an organization could customize the device to help manage client forms. By touching an icon on the display, a office worker could access the organization's web based document management system and browse a list of client forms.

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

The following Xerox Partner solutions use the Xerox Extensible Interface Platform:

- **Xerox Secure Access Unified ID System**: Secure Access integrates with your personalized ID badge. This convenient security solution allows people to simply swipe their ID badge at the device to unlock access to features that can be tracked for accounting and regulatory requirements. Secure Access is also the key to the personalized experience at the device.
- **Xerox Scan to PC**: This solution bridges the gap between documents, PDFs and paper, helping you to personalize your Xerox workflow scanning and PDF workflow. It also gives you the ability to customize, directly from your desktop, the scanning menus available to you on your Xerox EIP enabled device. This makes it easy to securely scan from the device to specific folders on your workstation.

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

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network.
- Ensure SSL is enabled on the device. For further information refer to Security Certificate Management on page 179.

At your Workstation

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Custom Service Setup]** in the directory tree.

3. In the **Setup (Required)** area, for **Custom Service Registration**, click on the **[Configure]** button to display the **HTTP**: **Web Services** screen.
   a. In the **Remote System Management** area, check the following checkboxes to enable EIP:
      - **Custom Service Registration** - this feature enables the Xerox EIP.
      - **Device Configuration** - this feature allows the EIP application or other remote application to retrieve printer configuration information such as the control panel display dimensions and software version numbers.

   b. In the **Scan Services** area, check the following required checkboxes:
      - **Scan Template Management** - this feature enables web services needed for Scanning Web Services, a feature under Workflow Scanning. this feature lets you manage scan templates residing in the device through third party applications.
      - **Scan Extension** - this feature allows a scan to be initiated from an EIP application.

   c. In the **Security** area, check the following required checkboxes:
      - **Xerox Secure Access** - this feature is one of the authentication options available to restrict access to printer services and features.
      - **Session Data** - this feature allows an EIP application to access user session information.

   d. Click on the **[Save]** button to return to the **Custom Service Setup** screen.
   e. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
4. In the **Enable Custom Services** area:
   a. Check the **[Export password to Custom Services]** checkbox to send passwords to Extensible services.
   b. In the **Browser Settings** area, check the following checkboxes:
      - **Enable the Custom Services Browser** - check to enable the Extensible Services browser.
      - **Verify Server Certificates** - this feature is optional. Leave unchecked unless Extensible Services require a Valid Server Certificate signed by a Trusted Certificate Authority.

   c. Click on the **[Apply]** button.
   d. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

At the Device:

1. Press the **<Services Home>** button.
2. Touch the **[EIP Application]** icon that you registered. Your XEIP workflow is accessible from the new icon.

WSD (Web Services for Devices) 20

WSD (Web Services for Devices) provides a way for clients to discover the device and the services the device offers. It is based on Devices Profile for Web Services (DPWS).

When a device is discovered, a client can retrieve a description of services hosted on that device and use those services. WSD allows a client to:

- Send messages to and from a web service.
- Dynamically discover a web service.
- Obtain a description of a web service.
- Subscribe to, and receive events from a web service.

Vista (only) operating system provides a WSD client to connect with printing and scanning peripherals that offer the WSD interface.

Enable WSD (Web Services for Devices)

Note: WSD Services are not related to the HTTP Web Services (accessed by selecting **Properties > Connectivity > Protocols > HTTP > Web Services** tab).

At your Workstation:

Note: To configure this feature or setting access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Protocol]** link.
3. Click on the **[WSD (Web Services for Devices]** in the directory tree.
4. In the **WSD Services** area, check the **[Enabled]** checkbox to enable the services.
5. Click on the **[Apply]** button.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Xerox Standard Accounting

21

When enabled, XSA (Xerox Standard Accounting) tracks the numbers of Copy, Print, Fax, and Network Scan jobs (when these features are enabled on the device), for each user. Usage limits can also be applied to users to restrict the total numbers of Copy, Print, Fax, and Network Scan jobs that a user can perform. Administrators can print a report which contains all XSA data.

XSA is set up through Internet Services, the device's HTTP pages displayed on your web browser. Administrators must create accounts and specify limits before users are authorized to access the device.

When XSA is set up, users must enter their account details at the device 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 Print Driver to print documents from their workstations.

The XSA feature and any other accounting features are mutually exclusive. If XSA is enabled at the device, you cannot enable Foreign Device Interface or Network Accounting.

Each device supports a maximum of:

- 2500 unique XSA user IDs
- 500 General Accounts
- 500 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 device. It is strongly recommended that you back-up the settings and data regularly using the Cloning procedure available through the Internet Services screens. Should the device lose your XSA data and settings you can restore them from the backup file that you produced by the Cloning process.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure that your device is configured on the network.
- Ensure that the TCP/IP and HTTP protocols are configured on the device and fully functional.

Enable Xerox Standard Accounting

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Accounting]** link.
2. Click on the **[Xerox Standard Accounting]** link.
3. Select **[Enablement]** from the directory tree**.**
4. In the **Enablement** area, select **[Enable - Xerox Standard Accounting]**.

   Note: Selecting **[Disabled]** will allow any users to access the services on the device.
5. Click on the **[Apply]** button.
6. A sub-menu will display. Select either **[Enabled]** or **[Disabled]** for the services for Xerox Standard Accounting to track and prompt.
7. Click on the **[Apply]** button.
8. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Accounting Settings]**.
2. Touch **[Authentication]**.
3. In the **Authentication Mode** screen, for **Xerox Standard Accounting**, select **[On]**.
4. Touch **[Save]** to return to the **Tools** pathway.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

To Add New User

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Accounting]** link.
2. Click on the **[Xerox Standard Accounting]** link.
3. Select **[Users]** from the directory tree.
4. The **Users** screen displays. In the **Users** area click on **[Add New User]**.
5. The **Add New User** screen displays. In the **User** area enter details in the **[User ID]** and **[User Name]** field.
6. In the **Usage Limits** area, specify the usage limit in the **[User Limits]** fields.
7. Click on the **[Apply]** button.
   Information on the user's access is available in the **Access Rights** area.

8. In the **Access Rights** area, select the necessary account group you want the new user to be a part of by clicking the **[Edit]** button.
   a. Check the **[Access]** checkbox.
   b. Click on **[Save]**.

To Create a General Account

The XSA feature allows administrators to create both Group and General Accounts. Users must be a member of at least one Group Account. However, the creation of General Accounts is optional. General Accounts can be created to identify a subset of a group or project that a user is involved in. The XSA Report specifies the numbers of documents produced per group.

Account example

In the example below, the administrator creates a Group Account called Finance Department and two General Accounts called Company A Project and Company B Project. The administrator adds the user Jane Smith to each account.

Jane can now record any impressions that she makes at the device to a particular account.

At the device, Jane enters her user ID and selects Company A Project. The number of impressions is recorded specifically to the Company A Project.

The administrator can print an XSA Report which lists the numbers of impressions recorded for each user, Group and General Account.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Accounting]** link.
2. Click on the **[Xerox Standard Accounting]** link.
3. Select **[Accounts]** in the directory tree.
4. Select **[General Accounts]** tab to create a new General Account.
5. In the **Add New General Accounts** area:
   a. Enter an ID in the **[Account ID]** field for the new group account (for example 001). The Group Account can be numeric values up to a maximum of 12 digits. Group Account ID's must be unique.
   b. Enter a name for the group account in the **[Account Name]** field (for example Xerox). The group name can be alphanumeric characters to a maximum of 32 characters. The Group Account name must be unique.
   c. Click on the **[Add Account]** button, and click on the **[OK]** button to confirm the account has been added to the list.
      The account will appear in the **General Accounts** list. Continue on to the next steps to create a new user.
   d. To add a user to an account group, click on the **[Manage]** link in the **General Accounts** area.
   e. In the **Account** area, make any relevant changes.

f. In the **User Access** area, check the checkboxes for the users to have access to.

g. Click on the **[Save Changes]** button. The user appears as a member of the Group and General accounts.

h. Click on the **[View Usage]** link in the **General Accounts** area.

i. In the **Usage** area, the System Administrator can view the user usage limits and access rights for this account. Usage limits can be specified for:

- **Black Printed Impressions** - displays the number of documents that has been printed by a user, from their workstation via the Print Driver.
- **Black Copied Impressions** - displays the number of copies that has been produced by the user via the Copy feature on the device.
- **Scanned Images** - displays the maximum number of scanned images that has been accounted for by the user.
- **Faxed Images** - displays the maximum number of sent and Black Faxed Impressions that has been accounted for by the user.

Click on the **[Reset]** button to reset the corresponding usage counter. Or click on the **[Reset All]** button reset all corresponding usage counter.

Note: Usage information will only be displayed for those options that are enabled and supported on the device.

6. Click on the **[Close]** button.

To Create a Group Account

All Login IDs must be assigned to one or more Group Accounts. If a user is a member of more than one Group Account or General Account, they will be asked to select an account associated with their Login ID.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Accounting]** link.
2. Click on the **[Xerox Standard Accounting]** link.
3. Select **[Accounts]** from the directory tree to display the **Group Accounts** page.
4. In the **Group Accounts** area:

a. Enter an ID in the **[Account ID]** field for the new group account (for example 001). The Group Account can be numeric values up to a maximum of 12 digits. Group Account ID's must be unique.

b. Enter a name for the group account in the **[Account Name]** field (for example Xerox). The group name can be alphanumeric characters to a maximum of 32 characters. The Group Account name must be unique.

c. Click on the **[Add Account]** button, and click on the **[OK]** button to confirm the account has been added to the list.
The account will appear in the **Group Accounts** list. Continue on to the next steps to create a new user.

Note: This page is also accessed from the **Limits & Access** page.

5. To add a user to this account group, click on the **[Manage]** link for the account group.
    a. In the **[Account]** area, make any relevant changes.
    b. In the **[User Access]** area, check the checkboxes for the users you want to add to the Account.
    c. Click on the **[Save Changes]** button to return to the **Group Accounts** screen.
6. To view usage of the group account, click on the **[View Usage]** link for that group.
    a. In the **Usage** area, the System Administrator can view the user usage limits and access rights for this account. Usage limits can be specified for:
        - **Black Printed Impressions** - displays the number of documents that has been printed by a user, from their workstation via the Print Driver.
        - **Black Copied Impressions** - displays the number of copies that has been produced by the user via the Copy feature on the device.
        - **Scanned Images** - displays the maximum number of scanned images that has been accounted for by the user.
        - **Faxed Images** - displays the maximum number of sent and Black Faxed Impressions that has been accounted for by the user.

    Click on the **[Reset]** button to reset the corresponding usage counter. Or click on the **[Reset All]** button reset all corresponding usage counter.

    Note: Usage information will only be displayed for those options that are enabled and supported on the device.

    b. you can reset the usage total, click on the **[Reset]** button.
    c. Click on the **[Close]** button.

Generate Report and Reset User Limits

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Accounting]** link.
2. Click on the **[Xerox Standard Accounting]** link.
3. Select **[Report and Reset]** from the directory tree. The **Report and Rest** page displays.
4. To generate a Report, in the **Generate Report** area:
    a. Click on the **[Generate Report]** button. This will generate a report in .CSV format.
    b. When the page refreshes, to save the report, right-click on the **[Right-click to download]** link and select **[Save Target As...]**.
    c. Select where on the workstation you want to save the file, and click on **[Save]**.
5. To reset the usage data to zero, in the **Reset Usage Data** area:
    a. Click on the **[Reset Usage Data]** button.
    b. When the message **"All current usage data will be reset to zero and lost?"** displays, click on the **[OK]** button.

⚠ WARNING: **The following step will delete all the XSA accounts set up for your device!**

6. To delete all user, group and general accounts, in the **Reset to Default** area:
   a. Click on the **[Reset to Default]** button,
   b. When the message **"All users, accounts and usage data will be lost?"** appears, click on the **[OK]** button.

Enable XSA in Windows Print Driver

1. From the **[Start]** menu select **[Printers and Faxes]** (Windows XP), or select **[Settings]** and then **[Printers]** (Windows 2000/20003).
2. Right-click on the Print Driver.
3. Select **[Properties]**.
4. Select **[Configuration]**.
5. Select **[Accounting]**.
6. From the **Accounting System** drop-down menu, select **[Xerox Standard Accounting]**.
7. Select **[Prompt for Every Job]** if you want users to enter their User and Account ID each time they print.
   a. Select the **[Save Accounting Codes]** to save selection.
   b. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to show asterisks (******) when ID's are entered.
8. Otherwise select **[Use Default Accounting Codes]**.
   a. Enter details of the default user in the **[Default User ID]**.
   b. Select from the drop-down menu the **[Default Account Type]**.
   c. Enter the details in the **[Default Account ID]**.
9. Click on **[OK]**.
10. Click on **[Apply]**, then click on **[OK]** to exit.

When you use the Print Driver to print a document you will be asked to enter your user ID.

Enable XSA in Apple Macintosh Print Driver

Mac OS X

1. Open a document to print and select **[File]** and then **[Print]**.
2. From the Print Options Menu select **[Printer Features]**.
3. Select the **[Feature Sets]** menu.
4. Select **[JCL]**.
5. Select **[Accounting]** to enable it.
6. Print the document.

To Back-up XSA Data, Settings and Clone to Another Xerox Device

The Cloning feature allows you to copy settings, including 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 device or to clone other devices. You can only clone XSA settings to another Xerox device that supports the XSA feature.

Check that the device you want to clone settings to supports XSA

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Select **[Cloning]** in the directory tree.
3. From the display of available check boxes, verify that **Accounting** is among them.
4. Then select **[Configuration]** in the directory tree, and verify that both devices have the same System Software Version.
   The System Software Version is located in the **Printer Setup** area.

To make a Back-up file

1. From the **Properties** tab, select **[Cloning]** in the directory tree.
2. From the display of available groups, select the settings that you wish to clone. To clone all features, click on the **[Clone]** button, or to customize the configuration file disable any of the features by clicking the checkboxes next to the feature(s) and then click on the **[Clone]** button.
3. Right-click on the **[Cloning.dlm]** link that appears and select **[Save Target As]**.
4. A dialog box will prompt you to specify the name and location for the cloned file. Ensure the extension reads **.dlm**.
5. Click on the **[Save]** button. The .dlm file can now be used to restore the information to the same device or to clone other devices.

To Restore Settings or Clone Settings to Another Device

Note: This procedure will cause the device to reboot and be unavailable over the network for several minutes.

1. From the **Properties** tab, select **[Cloning]** in the directory tree.
2. In the **[Install Clone File]** area, click on the **[Browse]** button.
3. Locate the **[Cloning.dlm]** clone file and click on **[Open]**.
4. Click on the **[Install]** button.

   The device will be unavailable over the network for several minutes. When rebooted a Configuration Report will print, if enabled.
5. The XSA settings and data will be restored as they were when the back-up file was created. If you are cloning another device you may want to change, delete or reset the XSA accounts as appropriate for the new device.

Network Accounting 22

Network Accounting provides the ability to manage usage of the device with detailed cost analysis capabilities. Print, Scan, Fax, and Copy jobs are tracked at the device and stored in a job log. Jobs require an authentication of User ID and Account ID and this information is logged with the job details in the job log.

The device requires the Network Accounting Solution package to be installed and network access to a Xerox certified Network Accounting third party software solution. Refer to your Xerox Sales Representative for further information.

Internet Services Print and Fax Drivers are required to be installed on workstations. The user is prompted for accounting information when submitting jobs to the device.

The job log information can be compiled at the accounting server and formatted into reports.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the device is fully functioning on the network prior to installation.
- Ensure that the TCP/IP and HTTP protocols are configured on the device as per Enable TCP/IP and HTTP at the Device on page 19.

  This is required to access Internet Services to configure Network Accounting.
- Locate the Network Accounting Kit.
  Contact your Xerox Sales Representative if you do not have the Network Accounting Kit. This kit contains the License Agreement and Kit Code Number to enable the feature.
- Install and configure the Xerox certified network accounting solution package on your network. Refer to the manufacturer's instructions with the network accounting package to complete this task.
- Test communication between the accounting server and the device. To do this:

  Go to your network accounting server and open a web browser. Enter the IP Address of the device in the address bar, and press **<Enter>**. The device's Internet Services web page will appear.

  If you do not have a web browser, test connectivity by pinging the IP Address of the device from your network accounting server.

Enable and Configure Network Accounting

The Network Accounting option is an optional feature for the machine. When you purchase the Kit, you will receive the Network Accounting Kit Instructions containing the License Agreement and Kit Code Number. Keep this number in a safe place for the set up.

To Enable the Network Accounting Feature at the Device

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Accounting Settings]**.
2. Touch **[Authentication]**. The **Authentication Mode** screen displays.
3. For **Network Accounting**, select **[On]** and touch **[Save]** to return to the **Tools** pathway.

To Configure Network Accounting

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Accounting Settings]**.
2. Touch **[Network Accounting Setup]** and select **[Network Accounting Authentication]**.
   a. In the **Network Accounting Authentication** screen, for **Authentication**, select **[Enable]**.

   Note: If you enable Authentication, users who enter incorrect User or Account ID’s will not be permitted to use the machine.

   b. Touch **[Save]** to return to the **Network Accounting** screen.
3. Select **[Network Accounting Login]**.
   a. If you want user details to display on the device screen, touch **[Display User ID Details]** and **[Display Account ID Details]** as required. If you want user details to be replaced by asterisks on the device screen, touch **[Mask User ID Details]** and **[Mask Account ID Details]** as required.
   b. Touch the **[Save]** button to retain the settings and return to the **Network Accounting Setup** screen.
4. Select **[Network Accounting Validation]**.
   a. In the **Network Accounting Validation** screen, touch the **[User ID]** text box.
   b. Enter the details for the User ID using the on-screen keyboard, when finished, touch **[Save]** to return to the **Network Accounting Validation** screen.
   a. Touch the **[Account ID]** text box.
   b. Enter the details for the User ID using the on-screen keyboard, when finished, touch **[Save]** to return to the **Network Accounting Validation** screen.
   c. Touch **[Save]**.
5. Press the **<Log In/Out>** button, and touch **[Logout]** to exit the Tools pathway.
6. To verify Accounting is enabled, press the **<Services Home>** button on the front panel. Select one of the services. For example, touch **[Copy]** icon.
7. The Touch Panel should display a screen with two buttons. One is the **[User ID]** button and the other is the **[Account ID]** button. This indicates the system has enabled accounting successfully.
8. Go to the Network Accounting Server to Activate the Device
   Open the Network Accounting application and configure it so that the IP Address (or fully qualified domain name) of device is entered as the destination for retrieval of data. Refer to the manufacturer's documentation with your Network Accounting server to complete this task.

Enable Network Accounting in Windows Print Driver

Note: If Accounting is enabled on the device but not in the Print Driver, any print jobs sent to the device will be deleted.

Windows 2000

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Right-click on the device printer icon and select **[Properties]**.
3. Select **[Configuration]**.
4. Select **[Accounting]**.
5. Select **[Xerox Network Accounting]** from the **Accounting System** drop-down menu.
   a. Select **[Prompt for Every Job]**. If you want users to enter their User ID and Account ID each time they print, check the following checkboxes:
      - **Mask User ID (***)**
      - **Mask Account ID (***)**

   When you select these options, the information entered will display asterisks (***) for extra security.

   b. If you do not require the security option, select **[Use Default Accounting Codes]** and enter the required information for the following field:
      - **Default User ID**
      - **Default Account ID**

   c. Click on **[OK]**.
   d. Click on **[Apply]**, then click on **[OK]** to exit.

Windows XP, Vista

1. From the **[Start]** menu select **[Settings]** and then **[Printers]**.
2. Right-click on the device printer icon.
3. Select **[Properties]**.
4. Select the **[Configuration]** tab.
5. Check the **[Enable Accounting]** box.
   a. Select **[Prompt for Every Job]**. If you want users to enter their User ID and Account ID each time they print, check the following checkboxes:
      - **Mask User ID (***)**
      - **Mask Account ID (***)**

   When you select these options, the information entered will display asterisks (***) for extra security.

   b. If you do not require the security option, select **[Use Default Accounting Codes]** and enter the required information for the following field:
      - **Default User ID**
      - **Default Account ID**

   c. Click on **[OK]**.
   d. Click on **[OK]** to exit.

Enable Network Accounting in Mac Print Driver

Mac OS X

1. Open a document to print and select **[File]** and then **[Print]**.
2. Select the Xerox printer.
3. From the **Copies and Pages** menu select **[Accounting]**.
4. Select **[Xerox Network Accounting]** from the **Accounting System** menu.
   a. Select **[Prompt for Every Job]**. If you want users to enter their User ID and Account ID each time they print, check the following checkboxes:
      - **Mask User ID (***)**
      - **Mask Account ID (***)**

   When you select these options, the information entered will display asterisks (***) for extra security.

   b. If you do not require the security option, select **[Use Default Accounting Codes]** and enter the required information for the following field:
      - **Default User ID**
      - **Default Account ID**

   c. To save your settings select the **[Presets]** menu and click **[Save As]**.
   d. Enter a name to define the preset, for example, **Accounting**.
   e. Click on **[OK]**. Ensure the **Accounting** preset is selected in the **Presets** menu each time you print.
   f. Click on **[Print]**.
   g. Enter your Network Accounting information.
   h. Click on **[OK]** to print the document.

Test Network Accounting

1. Open an application and print a job. Verify that you are presented with the User ID and Accounting ID screen.
2. Enter a valid User ID and Accounting ID and click on **[OK]**. If you selected **[Save Accounting Codes]** it will only be necessary to enter this information the first time the driver is used.
3. If your print job does not print, try to copy a job at the device using the same Account and User ID. If the copy job completes then the Account and User ID are valid.
4. It may be necessary to check the network accounting solution software or server configuration to verify the User ID and Account ID.
5. Distribute the Print Driver with the Network Accounting option already selected (if possible). If the Print Drivers are distributed without the option enabled, workstation users will need to configure the drivers. If the drivers are not properly configured, jobs sent to the device will be deleted.

Auditron

The Auditron is an accounting feature of the device which automatically tracks copy usage for each user. The Auditron will prevent unauthorized access to the Copy or ID Card Copy features of the device. It is enabled, or disabled by the System or Auditron Administrator. The Auditron comes as standard on all devices. The Auditron cannot be enabled if the Save Job for Reprint feature is installed and enabled.

If the Auditron is enabled, and the user selects Copy or ID Card Copy, a passcode must be entered before the features become available. On completion of the session the user must log out of the Auditron. This enables logs to be kept of all Copy jobs so that costs can be charged to different departments or customers. Limits can be set on the number of impressions allowed by each account holder.

To setup and manage the Auditron, the System Administrator uses the Tools login User Name and Password.

Enabling and Initializing the Auditron

To setup the Auditron you must first select the mode of authentication you require, then the Auditron must be initialized.

1. Press the Machine Status button.
2. Select the Tools tab.

   To have access to all the Tools options you must be logged in as an Administrator.

   To log in select the Log In/Out button on the control panel.
3. Use the keyboard to enter your User Name, then select the Next button.

   Use the keyboard to enter your Password, then select the Enter button.

   Note: The default user name and password are: admin and 1111.

   The Tools options are displayed.
4. Select **Accounting Settings** and **Accounting Mode**.
5. Select Auditron and On. The Auditron is enabled and ready to initialize.

   Note: The Auditron cannot be enabled if the Save Job for Reprint feature is installed and enabled.
6. Select Account Settings and Internal Auditron Setup.
7. Select Auditron Initialization. The Auditron Initialization screen gives access to two types of activities performed within Auditron Initialization:
   - Partitioning means dividing the machine memory between User and General Accounts. After entering the number of User Accounts required, the number of General Accounts is automatically calculated. If more User Accounts are created, fewer General Accounts will be created. The number of Group Accounts is fixed and is not affected by the partitioning.
   - Initialize Auditron once the Auditron has been partitioned, it needs to be initialized. This completes the Auditron Initialization module.
8. To change the number of User Accounts, select the User Accounts numeric entry region and enter the new number on the numeric keypad. Alternatively, use the arrow buttons to increase or decrease the number of User Accounts. The number of General Accounts changes in proportion.
9. Once you have finished partitioning, select Initialize Auditron. You are asked to confirm the initialization twice. A message at the top of the screen displays Please wait...Initialising accounts. Once initialization is complete the message changes to Initialization Complete.

Xerox Secure Access 23

Administrators can configure the device so that users must be authenticated and authorized before they can access specific services or areas. Xerox Secure Access provides a means of authenticating users via an authentication server and optional card reader.

This convenient security solution allows people to simply swipe the ID card at the device to unlock access to features that can be tracked for accounting and regulatory requirements.

Secure Access and Accounting

Secure Access can be enabled with **Network Accounting and Xerox Standard Accounting** features to provide accounting functionality.

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

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Ensure the Xerox device is fully functional on the network. TCP/IP and HTTP protocols must be configured so that Internet Services can be accessed.
- Ensure the Xerox Secure Access authentication server is installed and configured with user accounts. Refer to the documentation with the authentication server to complete this task.

  Contact your Xerox Sales Representative if you do not have the Xerox Secure Access authentication server.

  Note: If you want authorization, there must be a mapping between the accounts created on the authentication server and accounts created in the Local User Information Database or remote Authorization server.
- Connect and configure your card reader, if required. Attach the card reader to the left hand shelf on the device. Place the controller box on the floor at the back of the device.
- Ensure that SSL (Secure Sockets Layer) is configured on the Xerox device via Internet Services.
- To configure Authorization locally, the **User Information Database** must be configured. For instructions, refer to User Information Database on page 173. There must be a mapping between the accounts created on the Authentication Server and the User Information Database (the user names must match so that the device can cross reference each user as they log in at the device).
- To configure Remote Authorization, the LDAP server must be configured on the device and Authorization Access configured. For instructions, refer to LDAP on page 115 and Authentication Configuration for LDAP/LDAPS on page 160. There must be a mapping between the accounts created on the Authentication Server and the LDAP server (the user names must match so that the device can cross reference each user as they log in at the device).

Access Authentication Configuration

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page displays. In the **Authentication, Authorization, and Personalization** area click on the **[Edit..]** button.
4. In the **Enablement** area:
   a. Select the required option from the **[Alternate Authentication method on the machine's touch interface (Touch UI)]** drop-down menu. The alternate login method provides an alternative method of accessing the device's services if the smart card is unavailable. The option selected from the menu defines how the device will validate the user's access rights.
      - Select **[Username / Password Validated Locally on the Xerox Machine]** to validate users listed in the Local User Information Database. This option requires you to configure accounts in the Local User Information Database.
      - Select **[Username / Password Validated Remotely on the Network]** to validate users via an Authentication Server. This option requires you to have a server that will provide authentication of user login details. Authentication via Kerberos (Solaris, Windows 2000), NDS (Novell), SMB (Windows NT4/2000) or LDAP is supported.

   b. Select the required option from the **[Authentication method on the machine's web user interface (Web UI)]** drop-down menu. When a user attempts to access Internet Services they are prompted to enter their login information. The option selected from the web user interface Authentication menu defines how the device will validate the user's rights to access Internet Services. This is required because if the user normally authenticates at the device with a card reader, there would be no method for the device to authenticate users who access Internet Services from their workstations.
      - Select **[Username / Password Validated Locally on the Xerox Machine]** to validate users listed in the Local User Information Database. This option requires you to configure accounts in the Local User Information Database.
      - Select **[Username / Password Validated Remotely on the Network]** to validate users via an Authentication Server. This option requires you to have a server that will provide authentication of user login details. Authentication via Kerberos (Solaris, Windows 2000), NDS (Novell), SMB (Windows NT4/2000) or LDAP is supported.

   c. Select required method from the **[Authorization is stored]** drop-down menu. The card reader and Authentication Solution authenticates (validates) the user. The Authorization method determines which areas of the device a user is allowed to access. There are two options:
      - Select **[Locally on the Machine]** if you want the device to check the Local User Information Database for levels of authorization.
      - Select **[Remotely on the Network]** if you want to use an LDAP server to determine levels of authorization.

   If you selected **Remotely on the Network** (from the Location of Access Rights box), configure LDAP communications as stated in the Configure Authentication for LDAP/LDAPS in the Authentication section of this guide. For details refer to Authentication Configuration for LDAP/LDAPS on page 160.

d. In the **Personalize the machine's touch interface** area, check the checkbox to allow the **From:** address to be automatically set to the logged in user's e-mail address, when they log in via Secure Access and for the Scan-to Home home directory to be automatically set to that of the logged in user.

e. Click on the **[Save]** button to return to the **Xerox Access Setup** page.

To Configure Xerox Secure Access on the Device

Note: Before you complete these steps ensure that the Xerox Secure Access authentication server has been configured to point to the device.

1. From the **Authentication Configuration** screen, in the **Current Configuration** area:

   a. Click on the **[Configure]** button for **Device User Interface Authentication - Xerox Secure Access**.

   b. The device will automatically configure itself to work with the XSA remote server. Click on the **[Manually Configure]** button if the XSA remote server does not configure automatically.

   c. In the **Server Communication** area, select either **[IPv4 Address]** or **[Hostname]**.

   d. Enter details in the **[IP Address: Port]** or **[Host Name: Port]** fields.

   e. Enter the details in the **[Path]** field.

   Note: Enter the HTTP path of **[public/dce/xeroxvalidation/convauth]** and port number of **[1824]** to facilitate communication.

   f. Under the **Device Log In Methods** heading, select one of the following:

   - **Xerox Secure Access Device Only (e.g., Swipe Cards** - if you want to allow the user to swipe their swipe cards at the UI.
   - **Xerox Secure Access Device + alternate on-screen authentication method** - if you want users to authenticate using the device’s control panel as well as the XSA feature. When the second option is enabled, a button labelled “Alternate Login” is displayed on the “Instructional Blocking Window” providing users with an alternate method to log in. For example, this feature can be enabled for users who are unable to use their swipe card. When the alternate button is selected, the remote server presents a series of log in screens on the local user interface. The remote server is still responsible for authenticating the user. All other Xerox Secure Access options are supported with this setting.

   g. Under the **Accounting Information** heading, note that this item will be grayed out if Network Accounting is not enabled. If accounting is enabled, select **[Automatically apply Accounting Codes from the server]**, if the Secure Access Server has been configured to return the accounting User ID and Account ID login. If you want the user to enter these values at the local user interface during login, select **[User must manually enter accounting codes at the device]**.

   h. Under the **Device Instructional Blocking Window** heading, enter text in the **[Window Title]** and **[Instructional Text]** fields to create the prompt that will be displayed on the device’s user interface informing users how to authenticate themselves at the device.

   Note: If the Title and Prompt have been configured on the Secure Access Server, then this information will override the Title and Prompt text entered here.

   i. Click on the **[Save]** button when done.

2. Click on the **[Close]** button to return to the **Authentication Configuration** page.

Enable Web User Interface Authentication

A second, networked Authentication Server will be necessary for web user interface Authentication, if **Remotely on the Network** was selected. Full instructions for configuring network authentication, using Kerberos, NDS, SMB, and LDAP/LDAPS are contained in the Network Authentication section of this guide.

The path to the Authentication Server configuration screen is:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Security]** link.
2. Click on the **[Authentication]** link and select **[Setup]** in the directory tree.
3. The **Xerox Access Setup** page displays. In the **Authentication, Authorization, and Personalization** area click on the **[Edit..]** button.
4. Select the **[Username / Password Validated Remotely on the Network]** option from the **[Authentication method on the machine's web user interface (Web UI)]** drop-down menu.
5. Follow the instructions to select the required Authentication Type from the drop-down menu.
   - See Authentication Configuration for Kerberos (Solaris) on page 157.
   - See Authentication Configuration for Kerberos (Windows 2000/2003) on page 158.
   - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003/2008) on page 159.
   - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003/2008) on page 159.
   - See Authentication Configuration for LDAP/LDAPS on page 160.
6. When you have configured the required Authentication Type, click on the **[Save]** button to return to the **Xerox Access Setup** page.

Configure your LDAP Server

Configure LDAP communications on the device as stated in the LDAP/LDAPS topic. Refer to Authentication Configuration for LDAP/LDAPS on page 160.

7. To set Authentication to control access to individual Services, in the **Current Configuration** area, click on the **[Edit]** button for **Access Setup Wizard**.
   a. On the **Device Access** page, in the **Pathway Access** area, select either **[Unlocked]** or **[Locked]** for the following options:
      - **Service Pathway**
      - **Job Status Pathway**
      - **Machine Status Pathway**

   b. Click on the **[Next]** button. The **Service Access** page displays. To set Authentication to control access to individual Features, select individual feature radio button for the following authentication access:
      - **Unlocked**
      - **Locked**
      - **Hidden**
8. Click on the **[Next]** button to return to the **Authentication Configuration** screen.

9. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

Use Secure Access

At the Device:

1. Touch/press an area of the device that you have locked.
2. Read the user interface prompt to determine what you need to do to be authenticated at the device. Authentication methods include:
   - Swipe a card
   - Place a proximity card near to the reader
   - Enter a user ID or PIN number.

If you need to enter information, touch the **[Keyboard Access]** button and enter your login information.

3. The screen may request further information, such as a primary PIN or password, or account information. The primary PIN may have been set on the Xerox Secure Access authentication server. The account information may be requested because an accounting option is configured on the device.
4. The Xerox device will confirm successful authentication and you will now have access to the features.
5. When you have finished using the features, press the **<Clear All>** button on the keypad to close your account.

Software Upgrade

24

The Software Upgrade feature allows the customer to upgrade the device software as requested by a Xerox Customer Support Center Representative, without needing a Customer Service Representative to be present.

When Should I Upgrade the Software?

Xerox is continually seeking to improve its products and a software revision may become available to improve functionality on the device. Your Customer Support Center Representative will instruct you to upgrade your device when it is necessary.

How Do I Upgrade the Software?

IMPORTANT: Any jobs in the queue must be allowed to complete or be deleted before initiating a software upgrade.

There are three methods for upgrading the software on the device:

- Over a network connection using Internet Services via a web browser.
- Auto upgrade.
- USB Stick and DLM.

1. Software Upgrade Over a Network Connection

If your device is connected to the network, it is possible to upgrade the software through Internet Services. The device will need to be configured for TCP/IP and HTTP.

2. Auto Upgrade

If performing a software upgrade on the device via Internet Services it is possible to set the Auto Upgrade feature to schedule automatic device software upgrades from a central server at a specific time on a regular basis.

3. Software Upgrade via the USB Port

If your device does not have a network connection it is possible to upgrade the software by connecting a workstation or a laptop to the USB port.

To Upgrade Using the Internet Services

Note: This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software.
All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Information Checklist

Before starting the procedure, ensure the following item is available or task has been performed:

- Obtain the new software upgrade file for your device from the www.xerox.com website or from your Xerox Customer Support Representative.

  The upgrade file will have an extension of .dlm (dynamically loaded module). Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.

It is important to obtain the correct upgrade file for your particular model of device.

System Software Version

To determine which model of device you have, check the system software version.

Manual Upgrade

At the Device:

1. Press the **<Machine Status>** button.
2. Touch **[Machine Information]** tab.
3. In the **General Information** area, view the **System Software Version**.

   Note: TCP/IP and HTTP protocols must be enabled on the device so that the device can be accessed via the web browser.

At your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to, Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Machine Software]** link.
3. Select **[Upgrades]** in the directory tree.
4. In the **Upgrades** area:
   a. Check the **[Enabled]** checkbox.
   b. Click on the **[Apply]** button.
5. Select **[Manual Upgrade]** in the directory tree.
6. In the **Manual Upgrade** area:
   a. Click on the **[Browse]** button to locate the software upgrade file **[.dlm]** obtained earlier.

b. Click on the **[.dlm]** file obtained earlier.

c. Click on the **[Open]** button.

d. Click on the **[Install Software]** button to proceed with the upgrade.

- If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
- Click on the **[Login]** button.

The file will be sent to the printer and will disable the printing functionality. The web browser will become inactive and you will not be able to access the device via this method until the upgrade has completed and the device has rebooted. The upgrade should take no longer than 30 minutes.

7. When the device has completed the upgrade it will reboot automatically. The Configuration Report will print (if enabled). Check the Configuration Report to verify that the software level has changed.

Auto Upgrade

You can set the device to automatically schedule device software upgrades from a central server at a specific time on a regular basis.

> Note: This procedure will delete any current jobs in the device print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software.
> All configured network settings and installed options will be retained by the device after the Software Upgrade process.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- Obtain the new software for your device this will have an extension of .dlm (dynamically loaded module) from the www.xerox.com website or from your Xerox Customer Support Representative.
- Download the upgrade file to a local or network drive. You will be able to delete the file after the upgrade procedure.
- TCP/IP and HTTP protocols must be enabled on the device so that the device web browser can be accessed.

At your Workstation:

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to, Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[General Setup]** link.
2. Click on the **[Machine Software]** link.
3. Select **[Upgrades]** in the directory tree.
4. In the **Upgrades** area:

   a. Check the **[Enabled]** checkbox.

   b. Click on the **[Apply]** button.

5. Select **[Auto Upgrade]** in the directory tree to set the Auto Upgrade time.

6. In the **Auto Upgrade** area:
    a. Check the **[Enabled]** checkbox to enable the **Schedule Upgrade** feature.
    b. For **Refresh Start Time**, select either **[Hourly]** or **[Daily]**.
    c. If **[Daily]** has been selected, enter the required time of the day for the upgrade to be performed.
    d. For **[Protocol]**, select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
    e. Enter the details in the **[IP Address: Port]** or the **[Host Name: Port]** of the server where the software upgrade file (obtained earlier) is located.
    f. Enter the path to the upgrade file on the server in the **[Directory Path]** field.
    g. Enter the **[Login Name]** and **[Password]** for the server.
    h. Click on the **[Apply]** button to accept the changes.

    The upgrade will now be performed automatically on the device at the time specified. When the upgrade process starts network connectivity with the device will be unavailable, including access from Internet Services. The upgrade progress can be monitored from the device screen interface.

    Note: Software Installation will begin several minutes after the software file has been submitted to the device. When Installation has begun all Internet Services from this device will be lost, including this web user interface. The installation progress can be monitored from the local user interface.

Upgrade Through USB

This section provides instructions to upgrade machine software via the Utilities Software Upgrade Tool installed on a workstation or laptop and connected to the machine via a USB cable.

> Note: This procedure will delete any current jobs in the machine print queue and prevent further jobs from printing until the upgrade has completed. If you wish to preserve these jobs, allow them to complete before upgrading your software.

All configured network settings and installed options will be retained by the machine after the Software Upgrade process.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- A type A-B USB Cable.
- The Utilities CD3 delivered with your machine. The Utilities CD contains the tool used for performing machine software upgrades.
- A laptop or workstation (close to the machine) that supports USB connectivity.
- The software upgrade file obtained from your Customer Service Representative. The file will have an extension .UGD (upgrade). It is important to obtain the correct upgrade file for your particular model of machine.
- If you are performing the upgrade on a networked (connected printer) device, ensure the device is online before continuing.

System Software Version

To determine which model of machine you have, check the system software version.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch **[Machine Information]** tab.
3. In the **General Information** area, view the **System Software Version**.

Instructions to ensure the machine is online

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[Online/Offline]**. The **Online/Offline** screen displays.
3. View the **[Online/Offline]** button. Ensure the button **Online** is selected. If not, touch the **[Online]** button to enable.
4. Touch **[Save]**.
5. Press the **<Log In/Out>** button.
6. Touch **[Logout]** to exit the Tools pathway.

Prepare for the Upgrade

1. Obtain the upgrade file (.UGD) to be used for the upgrade. You will be able to delete the file after the upgrade procedure.
2. Verify that you have the upgrade tool installed onto the laptop or PC which will be attached to the machine to perform the upgrade.
   From the **Start** menu on the workstation, select **Programs**. The **Xerox *[machine model]* Utilities** link should appear in the list.
3. Connect the USB cable to the USB port located on the upper half of the rear of the machine next to the serial port. You may need to remove the black plastic stopper from the USB port. Replace the stopper after the upgrade procedure.
4. The first time the USB cable is connected to the PC, the Found New Hardware Wizard will appear. Follow the wizard to install the USB Print Drivers, if necessary. The USB Print Drivers are located on the Print and Fax Drivers CD, delivered with your machine. Refer to the documentation on the CD for assistance with this task.

At the Device

1. Press the **<Machine Status>** button.
2. Touch **[Machine Information]** tab.
3. In the **General Information** area, view the **System Software Version**.

At the Workstation

Note: It is recommended that you save any open data before running the Software Upgrade Tool.

1. From **Start** select **[Programs]**, followed by **Xerox [machine model] Utilities**.
2. Select **[Software Upgrade]**.
3. Select **[Software Upgrade]**.
4. Note the Current system software version. The **Preparing Xerox machine software for Upgrade** window appears. This should take no longer than 5 minutes. There are two Advanced Upgrade Options. Ensure **[Upgrade Only Software which has Changed]** is selected.

   Note: Force an Update of all Software. Only select this option if requested to by a Customer Support Representative. This option upgrades all machine software, even if the software is at the same level.

5. Click on **[OK]** to proceed with the upgrade.
6. The machine will prepare itself for the software upgrade. A progress bar will appear in the application window. This may take several minutes. When ready, the **[Upgrade Status]** (Software Upgrade in Progress) window will display. The Upgrade Screen window is used to inform the user of the installed version of software currently on the machine and to offer the option of upgrading the parts of the software set which are of an earlier version.
7. Click on the **[Select File]** button. Browse to locate the software upgrade file that you obtained earlier. (The .ugd file).
8. Select **[Open]**. The file will be extracted. This may take up to two minutes.
9. Click on **[Upgrade]**.

   Note: Any file matching the current software version will not be updated.

10. The Upgrade Progress window will appear. This window provides a bar-chart indication of the upgrade operation progress. The upgrade will take about 15 minutes to complete.

    Note: Do not remove any cables from the machine during the upgrade process.

11. The **Upgrade Successful** Status Report Window will appear informing you that the upgrade has been successful. The machine will automatically reboot.

    Note: In the event the upgrade fails, the tool will indicate a failure has occurred. The machine will reboot and go back into upgrade mode. Re-run the procedure to attempt the upgrade again. If the upgrade subsequently fails, additional assistance may be required from your Customer Support Representative.

12. Click on the **[Finish]** button to close the Upgrade Successful window and end the program.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch **[Machine Information]** tab.
3. Touch **[Machine Software Versions]** button. The **Machine Software Versions** screen displays. Verify the software has upgraded.

USB Printer Port 25

The optional USB Printer Port provides a USB connection on the device for Walk-up printing. The USB Printer Port can be used for printing directly from a workstation or laptop connected with a USB. The USB port is located at the back of the device.

Information Checklist

Before starting the procedure, ensure the following items are available or tasks have been performed:

- The USB cable.
- The Print and Fax Driver disk delivered with your device.

Enable the USB Port

At Your Workstation:

Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Connectivity]** link.
2. Click on the **[Physical Connections]** link.
3. Select **[USB Port]** in the directory tree, the **USB Port** page displays.
   a. In the **General** area, for **Connection Mode** select **[Direct Printing Via Driver]**.
   b. Enter time in seconds in the **[Timeout]** field. The default is 10 seconds, the range is 0 - 60.
   c. Click on the **[Apply]** button.
   d. Click on the **[OK]** button when you see the message **“Properties have been successfully modified”**.
4. Click on the **[Status]** tab.
5. Select **[Description and Alerts]** from the directory tree.
6. Click on the **[Reboot Machine]** button.
7. Print a Configuration Report At the Device:
   a. Press the **<Machine Status>** button.
   b. Touch the **[Machine Information]** tab.
   c. Touch **[Print Reports]**.
   d. Touch **[Print Report]**.
   e. Touch **[Close]**

   The Configuration Report will print. On the report, check under **USB Printer Port Settings** heading to verify that **USB Port Enabled** is enabled.
8. Connect your workstation or laptop to the device with a USB cable.
9. Install Print Driver. For Details, refer to Print Drivers on page 141.

At the Device:

Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Network Settings]**.
2. Touch **[USB Printer Port]**. The **USB Settings** screen displays.
   a. For **USB Connection Mode**, touch **[Direct Printing via Driver]**.
   b. For **Print Timeout (Seconds)**, set time in seconds using the **up** and **down** arrow buttons. The range is 0 - 60.
   c. To disable the Print Timeout set the value to **0**.
   d. Touch **[Save]**.
3. Press the **<Log In/Out>** button.
4. Touch **[Logout]** to exit the Tools pathway.
5. Connect your workstation or laptop to the device with a USB cable.
6. Install Print Driver. For Details, refer to Print Drivers on page 141.

Troubleshooting 26

Troubleshooting: Workflow Scanning

If you are experiencing problems with Workflow Scanning, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test print from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Is the Device Functioning on the Network as a Printer?

Configure your device on the network or resolve any networking issues before attempting to use the Workflow Scanning feature. For instructions to configure the device on the network see Enable TCP/IP and HTTP at the Device on page 19.

Ensure Workflow Scanning is installed properly on the device.

At the device, verify that you have a Workflow Scanning feature icon on the device screen interface and that this is not grayed out or unavailable.

To view the Workflow Scanning feature icon, you may need to press the **<Services Home>** button.

Is the Workflow Scanning Button Available on the Device?

If there is no Workflow Scanning feature icon available on the device, install the Scanning Kit and configure the Workflow Scanning feature. For instructions, refer to Workflow Scanning on page 201.

> Note: If you have enabled Workflow Scanning, but the icon is grayed out or unavailable.
> To enable this feature, access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18. From the **Tools** pathway:
>
> - Touch **[Service Settings]**, touch **[Optional Services]**.
> - Touch **[Workflow Scanning]**.
> - The **Workflow Scanning Service** screen displays. Select **[Enable]**, and touch **[Save]**.

When you perform a scan, a Scan Confirmation Report prints (if it has been enabled). The Scan Confirmation Report will report a job status of SUCCESS or FAILED.

Try to Scan a Document. Does the Scan Confirmation Report Print?

If the Scan Confirmation Report does not print, perform the following steps at your workstation and accessing the Internet Services.

> Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

1. From the **Properties** tab, click on the **[Services]** link.
2. Click on the **[Workflow Scanning]** link.
3. Select **[General]** in the directory tree.
4. Select **[On]** from the **Confirmation Sheet** drop-down menu and click on the **[Apply]** button.
5. Return to the device and scan another document using the DEFAULT template. View the error message as detailed on your confirmation report.

   View the Scan Confirmation Report. If the Report reads FAILED 'Failure transferring job to network server', the scan repository location may be incorrect. Check the following:

   > Note: To configure this feature or these settings access the **Properties** tab as a System Administrator. For details, refer to Access Internet Services as System Administrator on page 24.

6. From the **Properties** tab, click on the **[Services]** link.
7. Click on the **[Workflow Scanning]** link.
8. Select **[File Repository Setup]** in the directory tree.
9. Select the file from the **File Destination** list.
10. Click on the **[Edit]** box and check the details configured for your Scan Filing Repository.
11. Make any amendments as necessary and try scanning your documents again.

Scanning Using FTP

Check that your FTP service is configured properly.

1. Open a command prompt window and on one line type **FTP** then enter a space, then IP Address of your FTP Server. Press Return.
2. At the 'User' prompt enter the **[user name]** for the account you created for the device scanner.
3. At the 'Password' prompt enter the **[password]** for the account you created for the device scanner.
4. This user account should be able to log in. If you cannot log in as this user check that your FTP server setups have Read/Write access enabled. Ensure the password is correct. If the user can log in, try copying a file into the scan directory to check write access (using get and put commands). Ensure that the FTP server has the Read and Write boxes checked.

Ensure that the user account has full access rights to the scanning directory (repository). Type **quit** to exit FTP. Close the command prompt window.

Scanning Using NCP (NetWare Core Protocol)

From another workstation log in to the network with the scan user account and password created for the scanning function. Browse to the scan filing location and attempt to create and delete a folder. If you cannot perform this function, check the user account rights.

Scanning Using SMB (Server Message Block)

Test the configuration of the scan filing location by attempting to connect to the shared folder (the scan filing location) from another PC, with the user account and password created for the device. Create a new folder within this location and try to delete it. If you cannot perform this function check the user account rights. Verify that the information has been properly set in the Internet Services File Repository Setup page.

Scanning Using HTTP(S)

From a TCP/IP networked workstation, test the connection to the web server by Telnet. From a command prompt, start a Telnet session, log in to the device's directory on the web server, and send a POST request and file to the web server. Check to see if the file was received at the repository. If the file was not received, refer to HTTP/HTTPS on page 207.

The fault requires further investigation.

Refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: E-mail

If you are experiencing problems with sending an E-mail, first verify the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Configure your device on the network or resolve any networking issues before attempting to use the E-mail feature.

Ensure E-mail is Installed Correctly

At the device, verify that you have an E-mail feature icon on the device screen interface and that it is not grayed out or unavailable. For instructions to configure the device on the network, refer to Enable TCP/IP and HTTP at the Device on page 19.

To view the E-mail feature icon, you may need to press the **<Services Home>** button.

Enable E-mail before proceeding. For instructions refer to E-mail on page 243.

> Note: If you have enabled E-mail but the icon is grayed out or unavailable.
> To enable this feature, access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18. From the **Tools** pathway:
>
> - Touch **[Service Settings]**, touch **[Optional Services]**.
> - Touch **[E-mail]**.
> - The **E-mail Service** screen displays. Select **[Enable]**, and touch **[Save]**.

Verify that the E-mail settings have been correctly configured on the device by printing a configuration report.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report, check under heading. Verify that the SMTP IP Address is correct and that the TCP/IP Domain Name, Host Name and DNS settings are properly configured.

Was the E-mail Settings Correctly Configured?

For instructions, refer to E-mail on page 243.

From a desktop e-mail client, send a test e-mail to the new e-mail account created on the SMTP server for the device. Log in to the mail server with the new account name and password to verify that the e-mail was received at the server.

> Note: A webmail application makes a convenient tool to use to log in to the mail server to check for the receipt of e-mail.

Was E-mail Received at the SMTP Server?

While logged in to the device's e-mail account on the SMTP server, forward the e-mail to yourself.

If you receive the forwarded e-mail, you have verified that a valid path exists for receiving and forwarding e-mail, using the device's account.

If there is still a problem, check for restricted host addresses at the SMTP server that could cause mail to not be received from the device. Other possibilities are that an authentication server is interfering with the device's log in to the mail server, or that the mail client on the device is not working correctly. By successfully sending e-mail to a mail server not subject to authentication, the possibility of a malfunctioning client can be eliminated.

- Is the device's account name and password correct?
- Is the mail server down?
- Check that the mail server is configured to accept SMTP mail, as not all servers are configured to accept SMTP e-mail. The device requires access to a mail server that accepts inbound mail traffic.
- Check for restricted host addresses at the SMTP server. Verify that the device is not a restricted host.
- Try sending an e-mail from the device again. Ask the SMTP administrator to confirm that no errors were encountered and check for 'bounce' messages to the device's “Reply To” address.
- Check that the message size does not exceed the attachment or message size limit policy of your SMTP server.
- Troubleshoot the network path to the SMTP server. It may be necessary to perform a network trace analysis.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Internet Fax

If you are experiencing problems with sending an Internet Fax, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Configure your device on the network or resolve any networking issues before attempting to use the Internet Fax feature. For Instruction to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 19.

Ensure Internet Fax is installed properly on the device.

At the device, verify that you have an Internet Fax feature icon on the device screen interface and that this is not grayed out and unavailable.

To view the Internet Fax feature icon, you may need to press the **<Services Home>** button.

Install Internet Fax before proceeding. For instructions, refer to Internet Fax on page 261.

> Note: If you have enabled Internet Fax but the icon is grayed out or unavailable.
> To enable this feature, access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18. From the **Tools** pathway:
>
> - Touch **[Service Settings]**, touch **[Optional Services]**.
> - Touch **[Internet Fax]**.
> - The **Internet Fax Service** screen displays. Select **[Enable]**, and touch **[Save]**.

Verify that the Internet Fax settings have been correctly configured on the device by printing a Configuration Report.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report, view the **Network Setup** details. Verify that the SMTP Server Address is correct and that the TCP/IP Domain Name, Host Name and DNS settings are properly configured. Verify the POP3 Server Address is correct.

Are the Internet Fax Settings Correctly Configured?

For instructions, refer to Internet Fax on page 261.

From a desktop e-mail client, send a test e-mail to the new e-mail account created on the SMTP server for the device. Log in to the mail server with the new account name and password to verify that the e-mail was received at the server.

> Note: A webmail application makes a convenient tool to use to log in to the mail server to check for the receipt of e-mail.

Has the Internet Fax (e-mail) Been Received at the SMTP Server?

SMTP Items to Check

- Is the device's account name and password correct?
- Is the mail server down?
- Ask the SMTP administrator to confirm that no errors were encountered and check for 'bounce' messages to the device's “Reply To” address.
- Check that the message size does not exceed the attachment or message size limit policy of your SMTP server.
- Check that the mail server is configured to accept SMTP mail, as not all servers are configured to accept SMTP e-mail. The device requires access to a mail server that is configured for SMTP.
- Check for restricted host addresses at the SMTP server. Verify that the device is not a restricted host.
- Troubleshoot the network path to the SMTP server. It may be necessary to perform a network trace analysis.

POP3 Errors

If you are experiencing problems with receiving Internet Fax messages at the device, verify the POP3 address details have been properly configured.

At the Device:

1. Touch the **[Internet Fax]** feature icon.
2. Enter the Internet Fax address of the device (the E-mail address configured within Internet Services).
3. Touch the **[Add]** button, then touch **[Close]**. Place a document in the document handler and press the green start button. The document should be received as an Internet Fax job. If it is not - check the POP3 server address details to make sure they have been properly configured within Internet Services.

Check the operation of the device's SMTP and POP 3 account, as follows:

1. On a network connected workstation, set up e-mail using the same SMTP and POP 3 server and account (with passwords) as the device.
2. Send an e-mail to yourself.
3. If the e-mail arrives at your e-mail in box, you have proven that the device's account for both the SMTP and POP3 server(s) is valid.
4. If there is still a problem, check for restricted host addresses at the SMTP server that could cause mail to not be received from the device. Other possibilities are that an authentication server is interfering with the device's log in to the mail server, or that the mail client on the device is not

working correctly. By successfully sending e-mail to a mail server not subject to authentication, the possibility of a malfunctioning client can be eliminated.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Server Fax

If you are experiencing problems with sending a Server Fax, first verify the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Is the Device Functioning on the Network as a Printer?

Configure your device on the network or resolve any networking issues before attempting to use the Server Fax feature. For instructions to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 19.

Ensure Server Fax is Installed Correctly

At the device, verify that you have a Server Fax feature icon on the device screen interface and that this is not grayed out and unselectable.

To view the Server Fax feature icon, you may need to press the **<Services Home>** button.

Is the Fax Button Available on the Device?

Install Server Fax before proceeding. For instructions, refer to Server Fax on page 289.

Note: If you have enabled Server Fax, but the icon is grayed out or the service is unavailable. To enable this feature, access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18. From the **Tools** pathway:

- Touch **[Service Settings]**, touch **[Optional Services]**.
- Touch **[Server Fax]**.
- The **Server Fax Service** screen displays. Select **[Enable]**, and touch **[Save]**.

Verify that the Server Fax settings Have Been Properly Configured on the Device by Printing a Configuration Report.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report, view the Server Fax Setup details. Verify that the Protocol is correct and that the Server Name and Path to the Fax repository settings are properly configured.

Are the Server Fax Settings Correctly Configured?

Configure the Server Fax settings before continuing. For instructions, refer to Server Fax on page 289.

Check the Third Party Fax Server Configuration

1. At the fax server, disable the service so that it does not try to collect new faxes from the fax filing repository. This will depend on the particular product but often the relevant service can be stopped. Refer to the manufacturer's instructions contained with the fax server software to complete this task.
2. Send a test fax from the device.
3. View the location on the server where the fax filing repository was created. Verify that a directory with the extension .XSM has been created and contains the correct TIFF files (one per page of the fax sent).

Does the Fax Filing Repository Contain the TIFF Files?

If the fax filing repository contains the TIFF files then the device has successfully completed its task. The problem lies with the third party fax server. Ensure the server is configured properly and the path to the fax filing repository is set. Refer to the manufacturer's instructions contained with the fax server software to complete this task.

Check the User Account and Fax Filing Location

1. Verify that the user account and password created for the Server Fax feature are correct and have sufficient rights (permissions) to write files and create directories in the directory (the fax filing location).
2. Try logging into the fax filing location from another PC using the device’s account and password. Try to create a directory and delete the directory. If you cannot perform this function check the user account permissions.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Embedded Fax

If you are experiencing problems with Embedded Fax, first verify that the device is functioning in its existing configuration by making a photocopy at the device.

Is the Device Functioning?

Resolve any mechanical issues before attempting to use Embedded Fax. For assistance and support, refer to the www.xerox.com website.

Ensure Embedded Fax is Installed Correctly

At the Device:

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Optional Services]**.
3. Touch **[Embedded Fax]**. The **Embedded Fax Service** screen displays.
4. This should read **[Enable]**. If this is not Enabled or the Fax Install screen appears, refer to the instructions to configure Embedded Fax in Embedded Fax on page 271.

Ensure the Fax Settings are Correctly Configured

Ensure the device has been configured with the correct fax (telephone) number.

At the Device

> Note: To configure this feature or these settings access the **Tools** pathway as a System Administrator. For details, refer to Access Tools Pathway as a System Administrator on page 18.

1. From the **Tools** pathway, touch **[Service Settings]**.
2. Touch **[Fax Settings]**.

Verify that all Fax Setting configuration steps have been performed. Refer to Embedded Fax on page 271.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Troubleshooting: Network Accounting

If you are experiencing problems with Network Accounting, first verify that the device is connected on the network and functioning as a printer by performing the following activities:

- Check the network cable at the back of the device.
- Send a test page from your PC to the device.
- If connected via TCP/IP try a PING from your workstation to the device.

Is the Device Functioning on the Network as a Printer?

Configure your device on the network or resolve any networking issues before attempting to use the Network Accounting feature. For instructions to configure the device on the network, see Enable TCP/IP and HTTP at the Device on page 19.

Ensure Network Accounting is Installed Correctly

At the device, press the **<Services Home>** button and touch any feature icon on the screen interface.

Does the device ask you for a User Name and Account?

Verify that Network Accounting is Installed and Enabled Before Proceeding

To Print a Configuration Report

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

The Configuration Report will print. On the report check under **Installed Options** heading, to verify if **Network Accounting** is installed/enabled.

For instructions to both install and enable the Network Accounting feature, refer to Network Accounting on page 325. Note that Network Accounting can be installed, but not enabled.

Finally, try rebooting the device with the Power On/Off button. For instructions on use of the Power On/Off button, click the Previous Menu button at the top of this page, then click the button labelled Power On/Off Button.

Test Communication Between the Network Accounting Server and the Device

At your network accounting server:

1. Open the web browser and enter the IP Address of the device in the address bar, and press **[Enter]**.
2. The device's Internet Services web pages should appear. It they do not, verify the IP Address settings on the device. If you do not have a web browser, test connectivity by pinging the IP Address of the device from your Network Accounting server.
3. Verify that your network accounting server is configured properly. Consult the manufacturer's documentation with your network accounting server to perform this task.

Dynamic IP Addressing and Network Accounting

If Dynamic TCP/IP Addressing is used, be sure to set lease times long enough on the DHCP server to allow for normal maintenance shutdowns. If your device suddenly stops communicating with the network accounting solution, print a Configuration Report to check TCP/IP settings to be sure that they have not changed. Also, verify, by pinging, that the server's settings have not been changed.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Print Reports]**.
4. Touch **[Print Report]**.
5. Touch **[Close]**.

If the fault requires further investigation, refer to the Xerox website at www.xerox.com for further support.

Power On/Off Button

The Power On/Off button is located on the front left of the device. Press the button to power on the device. If the device does not show signs of powering on, (with lights flashing on the user interface, for example), check the circuit breaker and power cable located at the lower, right rear of the device. The power cable must be plugged in to the device, as well as to a live source of electric power.

When switching off the device, press the button to the Off (O) position. The printer will power off quickly, however for the system to be fully powered off you must observe the network activity light on the Controller at the rear of the device. When the network activity light stops blinking, the Controller has shut off and the entire system is powered off.

Font Management Utility and Unicode

A Unicode font kit is available for this 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.

The Font Management Utility is used to manage fonts on one or more printers.

The management process involves downloading soft fonts to your printer(s). For example, you may have a logo or graphic that uses a particular font. By downloading the font to a printer, you can print the logo or graphic with the appropriate typeface and other attributes, such as weight and colour. Downloading fonts to printers can also improve printing performance and reduce network traffic.

Downloaded fonts may then be added, deleted or exported to a file. The utility also allows you to add or delete printers or view printer lists.

The utility is available at no cost from the Support and Drivers section of www.xerox.com.

Unicode

Xerox Unicode 3.0 for SAP fonts will enable printing Japanese, Korean, and Chinese characters from SAP using the following fonts:

- ANMDJ.ttf Andale Mono WT J(Japanese version)
- ANMDK.ttf Andale Mono WT K(Korean version)
- ANMDS.ttf Andale Mono WT S(Simplified Chinese version)
- ANMDT.ttf Andale Mono WT T(Traditional Chinese version)

Unicode uses the Font Management Utility.

Refer to your Xerox Representative for further information.

Index