Version 2.0
09 2009

Xerox ColorQube™ 9201/9202/9203
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 (09/09).

Table of Contents

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 ColorQube™ Series

These models have copying, printing, scanning and faxing capabilities. The devices supports scanning too and has the capability of storing print, copy and scan files on the device. It copies and prints at 38/45/50 pages per minute depending on the model.

A Document Feeder, Bypass Tray and Paper Trays 1, 2 and 3 are supplied as standard.

	ColorQube™ 9201	ColorQube™ 9202	ColorQube™ 9203
Digital Copying	Standard	Standard	Standard
Network Printing	Standard	Standard	Standard
Scanning	Standard	Standard	Standard
E-mail	Standard	Standard	Standard
Fax	Option	Option	Option
Paper Tray 1, 2 & 3	Standard	Standard	Standard
High Capacity Feeder	Option	Option	Option
Offset Catch Tray	Option	Option	Option
80 GB Hard Drive	-	Standard	Standard
USB Thumb Drive *	Standard	Standard	Standard
Low Capacity Stapler Stacker (LCSS)	Option	Option	Option
High Volume Finisher (HVF)	Option	Option	Option
HVF with Booklet Maker / Post Processor & Trifolder	Option	Option	Option
Foreign Device Interface	Option	Option	Option

* USB Thumb Drive is standard on the ColorQube series, and is only used for service engineering.

Related Information Sources

Information available for this product series consists of:

- The *System Administrator Guide* (this guide)
- The *Quick Use Guide*
- The *Interactive User Guide*
- The *Advanced User Guide*
- The Xerox website *www.xerox.com*

Customer Support

If you need assistance during or after product installation, please visit the Xerox website for online solutions and support:

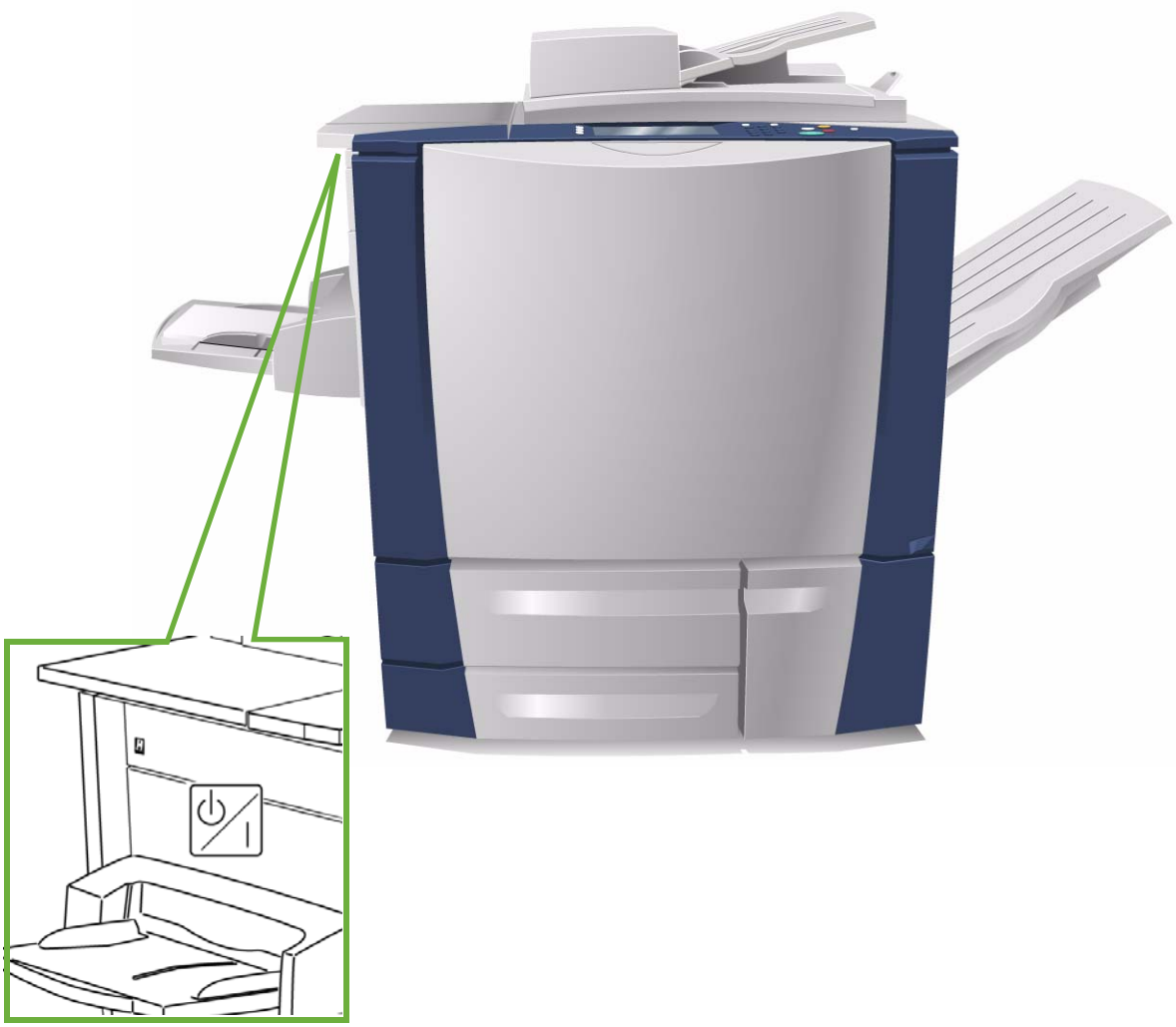
http://www.xerox.com

2

Device Connection and Quick Setup

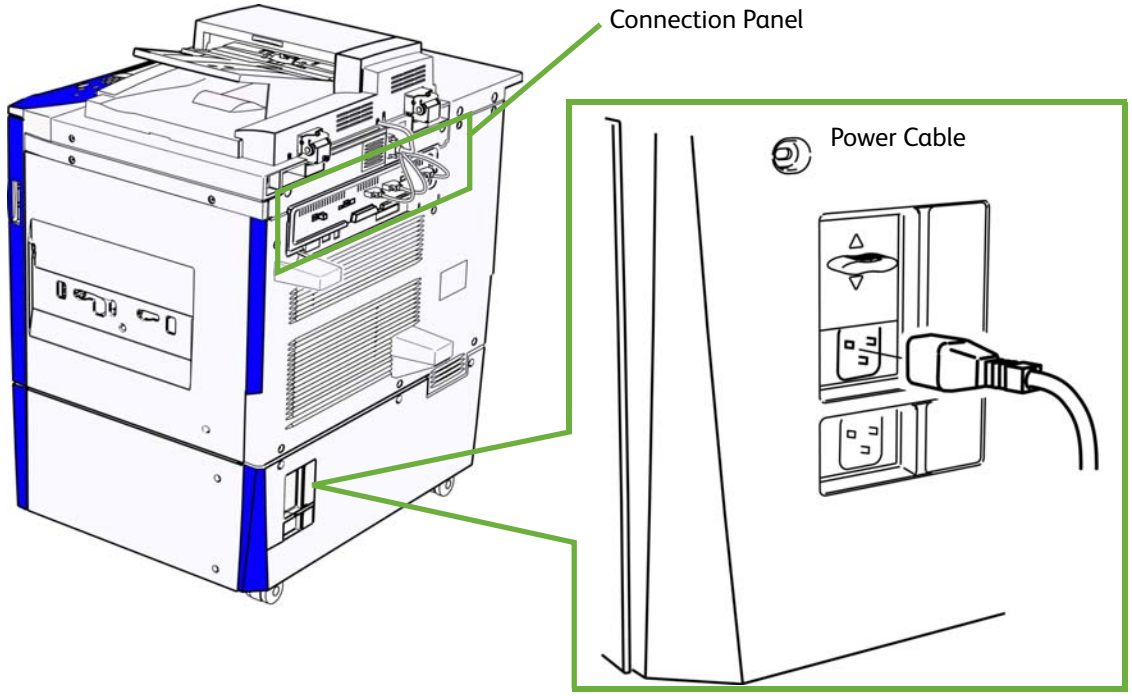
This chapter describes how to connect your device to a network and configure Ethernet settings.

Front View

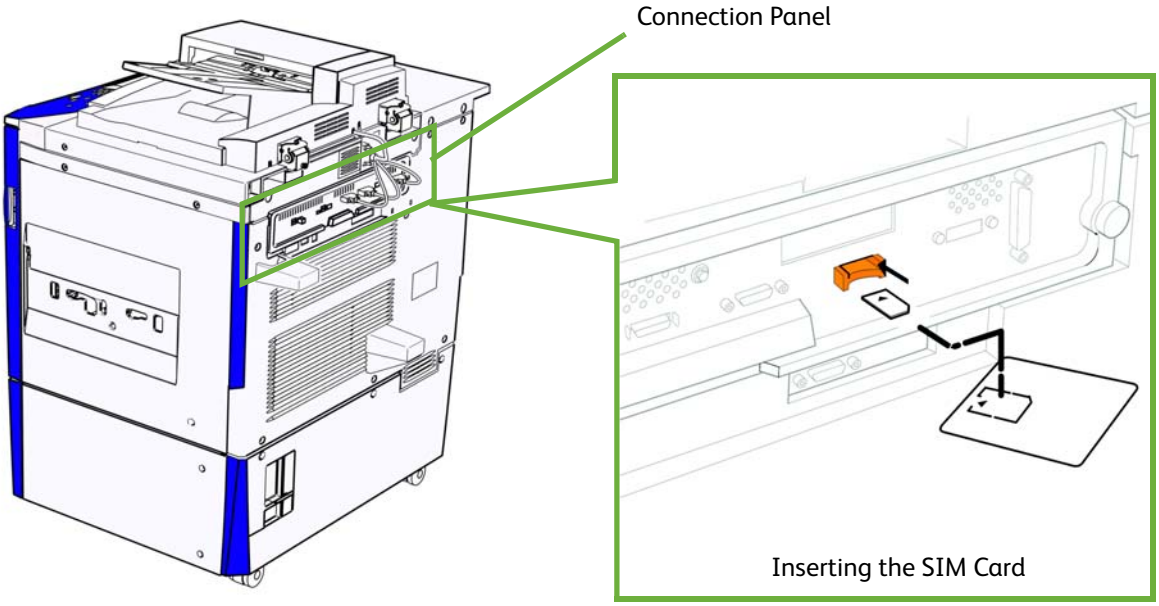


Power On/Off Switch

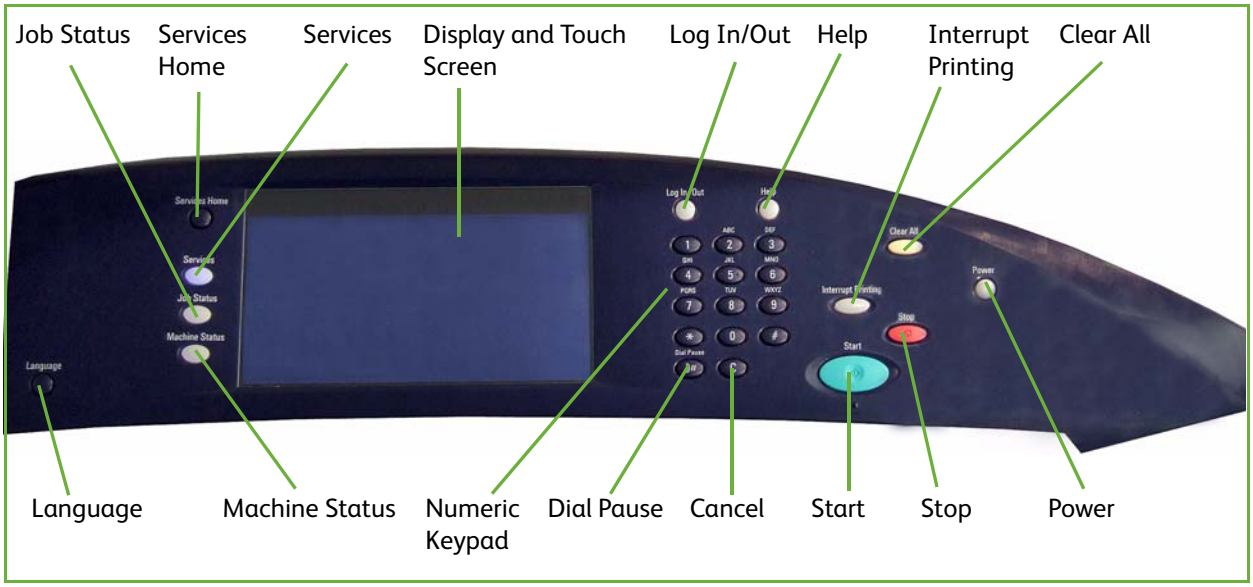
Rear View



Inserting the SIM Card



Device Control Panel Overview



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. Insert the SIM Card
   Insert the SIM Card before powering On the device, the SIM slot is located at the rear of the device.
4. Power On the Device
   The Power On button is located at the left-side of the device.

Install Wizard

If this is the first time the device has been powered on, the **Install Wizard** will run. If this screen does not appear, proceed to **Network Connectivity** in this chapter.
The install wizard will prompt you with questions to help with the configuring of your device.

Before the Install Wizard

1. At the device, before the Install Wizard begin, the **Installed Optional Hardware** screen displays, touch the **[Next]** button.
2. The **Machine Location** screen displays, select one of the following location and to allow the ink sticks to heat before the machine can be used:

- **Distribution Centre** - this option leaves the ink sticks cold. The device will power down when the **[Next]** button is touched.
- **Ready to Ship** - this option allows the device to power down when the **[Next]** button is touched, and when next powered on the ink sticks will be heated and the Installation Wizard will begin again.
- **Customer Site** - this option begins heating the ink sticks and continues with the Install Wizard when the **[Next]** button is touched.

Note: To prevent internal ink spillage, once the ink is heated, do not move the machine for 30 minutes from power down.

3. Touch the **[Next]** button, the device will power up and launch.
4. The **Languages** screen displays, select the required language, and touch the **[OK]** button.
5. A profile selection screen displays, select one of the following:
   - **Trained Xerox Installer**
   - **Customer**

   If the network cable is not connected, the **Network Connection Not Detected** screen displays
6. In the **Passcode Required** screen, enter the 4 digit Passcode you received with the device in the **[Enter PagePack Passcode]** field using the numerical keypad.
7. A Billing Plan is currently set to default plan for you device, to keep this plan, in the **Billing Plan** screen touch the **[Next]** button.
   If you have been provided with an alternative Billing Plan Passcode, touch the **[I Have a Passcode]**.
8. The **Install Wizard Welcome** screen displays.

Install Wizard

1. At the **Welcome** screen, touch the **[Next]** button.
2. The **Tools Access** screen displays, to proceed:
   a. Select one of the following access rights for the device configuration tools:
      - **Locked Restricted Access** - this option requires a login to access configuration tools.
      - **Unlocked Open Access** - this option allows all users to access the device configuration tools.

   Note: Access rights can be modified using the Internet Services, for more information, refer to Password Settings on page 151.

   b. Touch the **[Next]** button.
3. The **Paper Size Preference** screen will display, to proceed:
   a. Select one of the following paper size format that most frequently will be used on this device:
      - **Inches**
      - **Metric**
   b. Touch the **[Next]** button.
4. The **GMT Offset** screen displays, using the left and right arrow button set the Greenwich Meantime Offset according to the country you are in. Touch the **[Next]** button.
5. The **Date** screen displays:
   a. For **Format** select one of the following date format:

- **MM/DD/YYYY**
- **DD/MM/YYYY**
- **YYYY/MM/DD**

b. Set the date by touching the left and right arrow buttons. Touch the **[Next]** button.

6. The **Time** screen displays:
   a. Set the time by touching the left and right arrow buttons.
   b. Touch the **[Display 24-Hour Clock]** box to display 24-Hour format.
   c. Touch the **[Next]** button.
7. The **Quick Setup Home** screen displays, this will display the Features and its Status, touch the **[Next]** button
8. The **Device Setup Complete** screen will display with the message **'Your Xerox machine is now: Ready to Copy'**. Touch the **[Finished]** button. The device will save the settings and reboot. If enabled a configuration report will print.

The Welcome Page

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

A **[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.

Administrator Access for the Tools Menu

The **<Log In/Out>** button provides access to the Administrator Tools area. Administrator access is required to change settings such as network information on the device.

1. Press the **<Log In/Out>** button on the Control Panel.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.

Print a Configuration Report to Verify Current Device Settings

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

1. Press the **<Machine Status>** button on the device.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.

4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then 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 28.

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
- 1 Gbps Half-Duplex.
- 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

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch **[Tools]**.
5. Touch **[Network Settings]**.
6. Touch **[Advanced]**, if a warning message appears, touch **[Continue]**.
7. Touch **[Ethernet Physical Media]**.
8. Select the required **Ethernet Physical Media** speed to match the speed set on your hub or switch.
9. Touch **[Save]**, touch **[Close]**.
10. Press the **<Log In/Out>** button.
11. 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 use of the device's web user interface for network and options configuration. If necessary, reset TCP/IP addressing (including DHCP and DNS settings) and enable HTTP as follows:

1. At the device and press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
   Tip: This password can be changed by following the steps provided in the Administrator Tools topic in the General Setup section of this guide.
3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Wait for the screen to refresh, touch **[Network Settings]**, touch **[Advanced]**, if a warning message appears, touch **[Continue]**.
5. Touch the **[HTTP Settings]** button, touch **[Enable]**, touch **[Save]**, then touch **[Close]** to return to the Network Setting screen.
6. Touch **[TCP/IP Settings]**.
7. 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 24.

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.

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, go to the device:

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

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

At the Device:

1. Press the **<Log In/Out>** button.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, then touch **[Enter]**.
3. Touch the **<Machine Status>** button.
4. Touch **[Tools]**.
5. Touch **[Network Settings]**.
6. Touch **[TCP/IP Settings]**.
7. Touch **[Dynamic Addressing]**.
   a. Touch **[Disable]** to disable DHCP, and touch **[Save]**.
8. Touch **[IP Address/Host Name]**.
   a. Touch **[IP Address]** and enter a valid IP Address and touch **[Save]**.
   b. Touch **[Host Name]** and enter host name and touch **[Save]**.

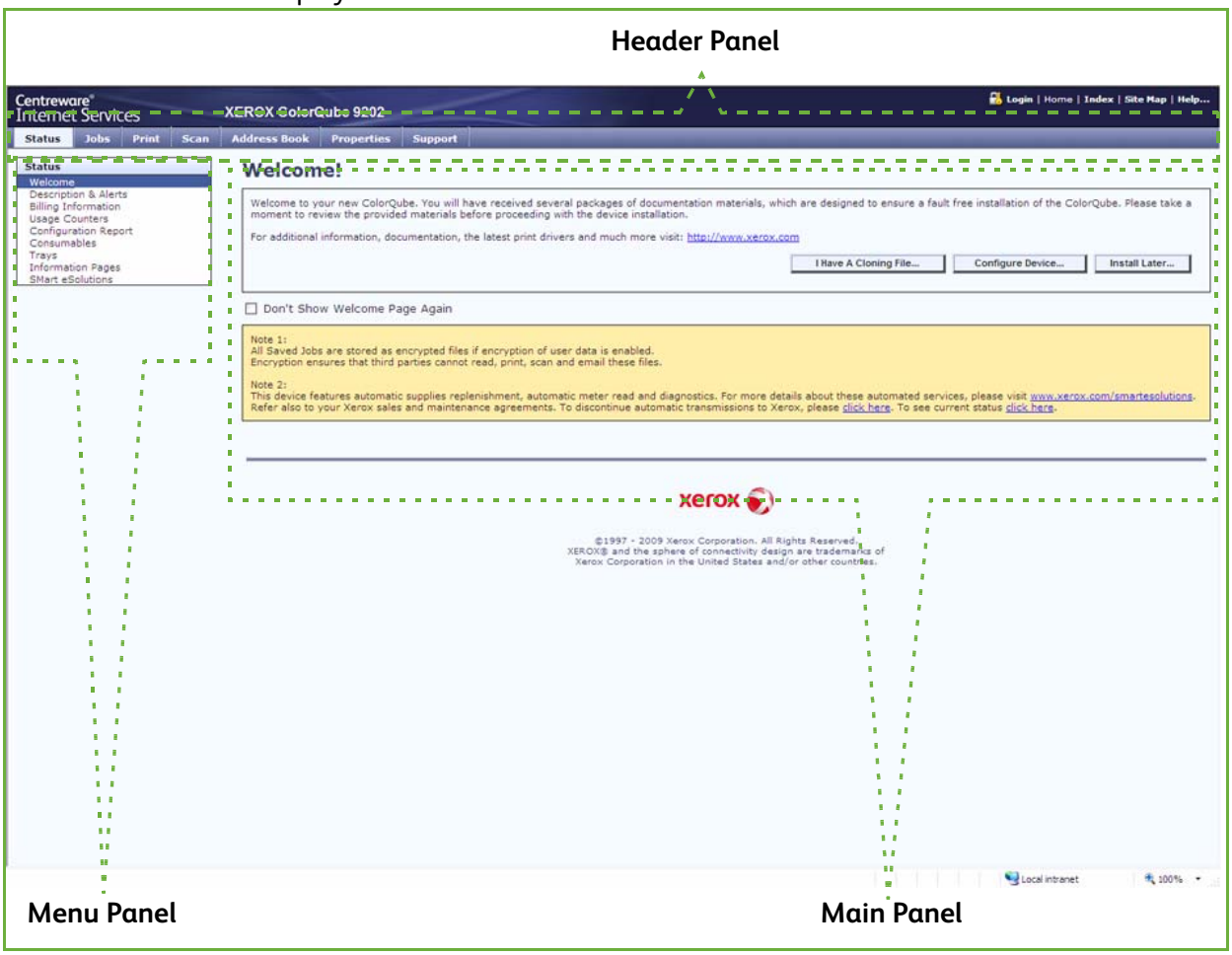
   c. Touch **[Close]**.
9. Touch **[Subnet and Gateway]**.
   a. Touch **[IP Gateway]** and enter a valid gateway address and touch **[Save]**.
   b. Touch **[Subnet Mask]** and enter a valid subnet mask address and touch **[Save]**.
   c. Touch **[Close]**.
10. Touch **[TCP/IP Enablement]**, ensure it is enabled and 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's *IP Address* in the web browser.
2. Press **[Enter]** or click on the **[Go]** button. For example:

The **Welcome** screen displays.



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 ColorQube 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 page buttons. These are **[Status]**, **[Jobs]**, **[Print]**, **[Scan]**, **[Address Book]**, **[Properties]**, and **[Support]**. You can navigate through the pages when you click 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 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 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.

To Setup HTTP

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

1. At your Workstation, open the web browser, 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[HTTP]** in the directory tree.
8. In the **Configuration** area:
   a. 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.

   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, see *Machine Digital Certificate Management* on page 157.

   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. 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 the Protocols section of this guide and follow the instructions to configure protocols.

To configure individual protocols only, using your web browser, perform the following steps:

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 **[Connectivity]** link, then 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 IP (v6).

6. 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.

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. Select **[Description]** in the directory tree.
6. In the **Identification** area:
   a. Type a name of your choice for the device in **[Device Name]**.
   b. Type the site location for the device in **[Location]**.
   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 using the **Service Registration** screen in on Internet Service.

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 **[Services]** link.
6. Select **[Service Registration]** in the directory tree.
7. In the **Service Registration** area:
   a. Either click on the **[Enable All]** button to ensure all the listed services are enabled, or check the required services checkbox you want to be displayed on the device's touch screen.
   b. Click on the **[Apply]** button.

To View the Service Status at the Device

To view the service status at the device.

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch the **[Installed Options]** button.
4. All the services selected on the Internet Services page are displayed and the Status will display either **Enabled** or **Disabled**.

To Install Print Drivers

Refer to Print Drivers on page 113 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 179
- E-mail on page 223
- Internet Fax on page 237
- Server Fax on page 259
- Embedded Fax on page 245
- LAN Fax on page 269
- Network Accounting on page 297

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. Select **[Configuration Overview]** in the directory tree.
6. Click on the **[Settings]** button next to the service that you want to configure, for example E-mail.

   Note: If you cannot see any services, then they have not been installed on your device.

7. Click the **[Configure]** button next to each step and enter the information to configure your service. Click on the **[Save]** button when you have finished with each screen.
8. If you have more than one service to configure, click on the **[Configure Next Service]** button. Otherwise, click **[Close]**.

Test your service at the device to verify that it is configured correctly.

3

General Setup

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: Note that the web user interface (Internet Services) is now protected by the Administrator password, so that you will need 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 9 characters in length should be sufficient for a year. Once changed, ensure the password is kept in a secure place for future use.

New Administrator Password

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 **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **New Password** tab is highlighted on the top of the screen.
8. Enter detail in the **[New Password]** and **[Retype New Password]** fields.
9. Click on the **[Apply]** button.

Note: The user name **"admin"** is reserved for the Device System Administrator Account. Do NOT use the username **"admin"** for any local or network accounts on the device.

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 Report]** 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 powered 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

To Prevent the Configuration Report to Print at Power On

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Device Settings]**.
5. Scroll down by touching the scroll down arrow, touch **[Configuration/Information Pages]**.
   a. Touch the **[No]** button under **Print Configuration at Power On**.
   b. Touch **[Save]**.
6. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

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 **[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.
7. Select **[General]** in the directory tree.
8. In the **General** area:
   a. for **Configuration Report** uncheck the **[Print at power on]** checkbox.
   b. Click on the **[Apply]** button to save your settings.
   c. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

To Restrict Configuration Report to System Administrator

You can restrict any printing of the Configuration Report to a logged-in System Administrator.

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 **[Services]** link.
6. Click on the **[Printing]** link.
7. Select **[General]** in the directory tree.
8. In the **General** area:
   a. For **Configuration / Information Pages Report**, check the **[Restrict to SA]** checkbox.
   b. Click on the **[Apply]** button to save you settings.
   c. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

   Note: If Configuration Report is restricted to System Administrator only, the Configuration button in the **Machine Information** screen will be greyed out and will require you to log into the device to access the Configuration Report.

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 **Configuration Report**, check the **[Print at Power on]** checkbox to enable a configuration report to print at power on.
   b. For **Configuration/Information Pages Report**, check the **[Restrict to SA]** checkbox to restrict Configuration Report and Information Pages to the System Administrator.
   c. 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 **Print Banner Sheets**, select **[Yes]** to allow a banner sheet to print with every print job.
   b. For **Allow the Print Driver to Override**, select **[Yes]** to allow the print driver to override the banner sheet option.
   c. For **Banner Sheet Identification**, select one of the following:
      - **Job Owner User ID and Job Name**
      - **Xerox Network Accounting User ID and Job Name**
      - **Generic User ID and Job Number**
10. In the **Secure Print** area:

    The Secure Print requires a user to be authenticated as the owner of a print job using a passcode, printing will only begin when the secure passcode is entered at the device,
    a. For **Secure Print Passcode Length**, enter the minimum required length of the Secure Print Passcode.
    b. For **Release Behavior**, select one of the following:
       - **Release all owner's jobs with passcode** - this will release all jobs associated with the user, with the supplied passcode.
       - **Release only the selected job** - this will release only a selected job with a supplied passcode.
11. 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.
    - **Paper Feed Edge Default** - allows you to select either long or short edge feed.
    - **2 Sided Printing** - allows you to select either 1-Sided Print, 2-Sided Print or 2-Sided Print Flip on short edge.
    - **Output Color** - allows you to select whether the output is color.
    - **Collate** - allows you to enable or disable the collation.
    - **Staple** - allows you to set the default staple position.
12. Click on the **[Save]** button to return to the **Print Protocols** screen.
13. Click on the **[Configure]** button next to the **IP (Internet Protocol),** to enable on the device to support your network environment.
14. 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.

15. Click on the **[Save]** button. 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 113.

Cloning

Cloning enables 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. In other words, it is not possible to install an optional feature (for example, Workflow Scanning or E-mail) through the process of cloning.
> 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

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 **[General Setup]** link.
6. Select **[Configuration Report]** in the directory tree.
7. Scroll down to the **Software Versions** area and view the System Software version.

To Clone a 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 **[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 **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. In the **Create Clone File** area:

c. 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
- Administration
- Audit Log
- Authentication & Authorization Configuration
- Connectivity Settings
- E-mail
- Fax
- Internet Fax
- Internationalization
- Job Management
- Security
- SMart eSolution
- System Disk
- Power Saver
- Print Settings
- Workflow Scanning
- Templates
- Device Upgrade
- Web Services
- Public Address Book

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

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

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

8. 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. Once rebooted a Configuration Report will print, if enabled.

Date and Time

This feature enables the System Administrator to set the Date and Time (including Time Zone for Daylight Saving Time) for the system. It can automatically be set up via NTP, if enabled on the internet services, or it can be manually set on the device interface.

Automatic Setup Using NTP

Note: If Setup is set to **Automatic 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.

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 **[General Setup]** link.
6. Click on the **[Date and Time]** link from the directory tree.
7. In the **Setup** area select **[Automatic using NTP]** from the **Date and Time Setup** drop-down menu to use an NTP server.
8. In the **NTP Server Settings** area, select one of the following:
   - **IPv4 Address** and enter the **IP Address** and **Port** and the **Alternate 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.
9. In the **Date & Time** area:
   a. For **Format**, select one of the following:
      - **MM/DD/YYYY**
      - **DD/MM/YYYY**
      - **YYYY/MM/DD**

   b. Using the **Up** and **Down** arrow select the required value for the following:
      - **Day** - the range will be dependant on the selected month.
      - **Month** - the range is from 1 to 12.
      - **Year** - the range is from 2007 to 2033.

   c. Check the **[Display 24 hour clock]** checkbox if you require a 24 hour format, if unchecked, a 12 hour format is displayed.

   d. Using the **Up** and **Down** 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 to23.
      - **Minutes** - the range is 00 to 59.
      - If 12 hour format is selected, select either **AM** or **PM** from the drop-down menu.

   e. In the **Time Zone** area, select a time zone from the drop-down menu.

10. Click on the **[Apply]** button, the system will reboot.

Manual Setup

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 **[General Setup]** link.
6. Click on the **[Date and Time]** link from the directory tree.
7. In the **Setup** area select **[Manual (NTP Disabled)]** from the **Date and Time Setup** drop-down menu to use an NTP server.
8. In the **Date & Time** area:
   a. For **Format**, select one of the following:
      - **MM/DD/YYYY**
      - **DD/MM/YYYY**
      - **YYYY/MM/DD**
   b. Using the **Up** and **Down** arrow select the required value for the following:
      - **Day** - the range will be dependant on the selected month.
      - **Month** - the range is from 1 to 12.
      - **Year** - the range is from 2007 to 2033.
   c. Check the **[Display 24 hour clock]** checkbox if you require a 24 hour format, if unchecked, a 12 hour format is displayed.
   d. Using the **Up** and **Down** 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 to23.
      - **Minutes** - the range is 00 to 59.
      - If 12 hour format is selected, select either **AM** or **PM** from the drop-down menu.

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

   e. In the **Time Zone** area, select a time zone from the drop-down menu.
9. Click on the **[Apply]** button.
10. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

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 for Email & Internet Fax Only

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 **[General Setup]** link.
6. Select **[Image Settings]** in the directory tree, the **Image Setting (Email & Internet Fax Only** screen will display.
7. In the **TIFF Settings** area, for **TIFF Color Compression**, select one of the following options to specify the file compression method used for color TIFF images when the device saves them for Email attachment or Internet fax:
   - **TIFF 6.0 (old JPEG)** - this version utilizes the most universally compatible version of the JPEG compression format.
   - **TIFF Specification Supplement 2 (New JPEG)** - this is an update to the TIFF 6.0 specification and provides a more fault-free JPEG compression algorithm, but may not be compatible with older graphics software.
   - **LZW** - This is a lossless compression method yielding very high compression efficiency, LZW works best for files containing repetitive data, such as is the case with text and monochrome images. LZW has long been associated with TIFF and GIF images. This compression algorithm was widely used in Adobe Photoshop, until version 6, and Adobe Acrobat, until version 5.
8. In the **PDF & PDF/A Settings** area, select the following compression types for PDF and PDF/A documents:
   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. **JBIG** 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, select both of the following options for optimal compression:

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

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** option:

- **Multi-Mask Compression** - tends to produce cleaner and sharper pages. On a multi-mask MRC compressed page, contents with similar colors are extracted, combined and encoded as masks. However, occasional mistakes can be made causing image artifacts such as lines and text shifting colors.
- **3-layer Compression** - segments the image into a layer with the image's sharp edges (generally known as the text or mask layer), a graphic (background) layer, and a foreground layer that defines the colors of the text in the mask layer. The mask layer is compressed using JBIG2 (PDF) or Flate (XPS) compression as configured by the SA. The background layer is compressed using either JPEG or Flate compressed-JPEG. The foreground layer is compressed using a lower quality JPEG compression than the background layer since the only data that is to be retained are the colors of the text in the Mask layer. The layers are re-assembled as a PDF, PDF/A or XPS page for export.

9. XPS is Microsoft's new electronic paper format, an alternative to PDF. XPS is currently supported as a saved file format in Microsoft Office 2007, with an XPS viewer built into Windows Vista. Microsoft states that Windows vista uses the XPS format as a document format, a windows spool file format, and a page description language for printers.
In the **XPS Setting (Email Only)** area, for **MRC Compression**:

a. Check the **[Enabled]** checkbox.

b. If enabled, select one of the following **MRC Compression Format** option:

- **Multi-Mask Compression**
- **3-layer Compression**

Note: Regarding Searchable XPS: 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 XPS file format. 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.

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

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

Accessing Image Settings for Workflow Scanning

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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Default Template]** in the directory tree.
8. Scroll to the **Workflow Scanning** area, click on the **[Edit]** button.
9. In the Workflow Scanning area:
   a. For **Original Type**, select either the **[Photo & Text]**, **[Photo]**, **[Text]**, **[Map]** or **[Newspaper/Magazine]**.
   b. Select **[for OCR]** option for **Scan Presets**.
   c. Click on the **[Apply]** button.
10. Scroll to **Filing Options** area, click on the **[Edit]** button.
11. Within Filing Options area:
    a. For **File Format**, select either **[TIFF], [mTIFF], [JPEG], [PDF], [PDF/A]** or **[XPS]**.
    b. For **Searchable Options**, select **[Searchable]**.
    c. Click on the **[Apply]** button.
12. Scroll to the **Workflow Scanning Image Settings** area, click on the **[Edit]** button.
13. 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.

At the Device:

1. Press the **<Services>** button.
2. Touch the **[Workflow Scanning]** icon.
3. Input documents to scan and touch the **[Start]** button.

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

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 **[Services]** link.
6. Click on either **[Workflow Scanning]**, **[E-mail]**, or **[Internet Fax]** link.
7. 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**.
8. 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.
9. When done, click on the **[Apply]** button to save changes or **[Undo]** to remove changes and refresh the page.

Job Deletion

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

Note: System Administrators can always delete any job, regardless of the setting selected on the Job Deletion page.

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.
5. Touch **[Security Settings]**.
6. Touch **[Authentication]**.
7. Touch **[Job Deletion]**.
8. Touch either:
   - **[All Users]** to allow any user to delete any job in the job list. There is no authentication needed when the user clicks on a job in the job list and selects **Delete**.
   - **[System Administrators Only]** to allow only users with administrative access (password) to delete jobs. The System Administrator must provide a username and password when deleting a job.
9. Touch **[Save]** button.
10. Press the **<Log In/Out>** button, then 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 coding used by the device to interpret data, such as print 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. 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 **[General Setup]** link.
6. Click on the **[Internationalization]** in the directory tree.
7. If you want to specify the locale, select the required setting from the **[Select Locale]** drop-down menu. The device will make an assumption on the encoding that are most likely used.
8. If you want to enter the specific encoding of user strings provided for the device, select **[Custom]** from the **[Select Locale]** drop-down menu, and select the required encoding priority order.
9. Click on the **[Apply]** button to save your changes.
10. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Extensible Services Setup

This feature allows the System Administrator to set up and enable extensible services on the device. Extensible Services enables independent software vendors and partners to develop customized programs to access directly from the device's 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, please ensure the following items are available or 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.
- Ensure Extensible Service Registration must be configured.

To Enable Extensible 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. 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 **[General Setup]** link.
6. Select **[Extensible Service Setup]** in the directory tree.
7. In the **Setup (Required)** area, ensure HTTP (SSL) and Extensible Service Registration have been configured to enable Extensible Services. If they have not been enabled, click on the **[Settings]** button and configure the settings and click on the **[Apply]** button.
8. In the **Enable Extensible Services** area check the **[Export password to Extensible Services]** checkbox to send passwords to Extensible Services.
9. In the **Browser Settings** area, check the following required checkboxes to enable options for Extensible Services:
   - **Enable the Extensible Services Browser**

- **Verify Server Certificates** - if this option is enabled, Extensible Services will check and require valid server certificates.

10. Click on the **[Apply]** button to save your changes.
11. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

SMart eSolutions

SMart eSolutions provides a setup page to guide you through the steps required to configure the device for automatic meter readings. SMart eSolutions enables the device to automatically send data to Xerox to be used for billing (Meter Assistant) and solid ink (Supplies Assistant).

SMart eSolutions provides the following features:

- **MeterAssistant™ -** submits meter reads to Xerox from network devices. This ends the need to collect and report meter read information manually.
- **SuppliesAssistant™** - allows to manages ink supplies for network equipment, and also monitor actual usage.
- **MaintenanceAssistant™ -** allows you to troubleshoot your device. You can send detailed diagnostic information to Xerox, start online troubleshooting sessions with Xerox, and download usage information to your computer in .csv format.

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

- **Client Direct registration** - this is available as a standard feature on the device.
- **SMart eSolutions Windows Client** - this is an optional feature and the Windows Client can be downloaded, visit www.xerox.com/smartesolutions.
- **Internet Services** - this is a web based software that manages, configure, installs and reports for network installed devices, for further information, see www.xerox.com/centrewareweb.

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

Information Checklist

Before registering the device for Meter Assistant, please ensure the following items are available or have been performed.

- Create an account on Xerox.com. Add all devices in inventory that you wish to register for Automatic Meter Readings to your account, visit www.xerox.com/meterreads.
- 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.
- Enable SNMP (Smart eSolutions Client and Internet Services). If you want to use Smart eSolutions Windows Client or Internet Services. Visit www.xerox.com/smartesolutions for further instructions and to download the software.

SMart eSolutions Information

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 **[General Setup]** link.
6. Select **[SMart eSolutions]** in the directory tree.
7. In the **Enrollment** area, for **SMart eSolution Enrollment** ensure **[Enrolled]** is selected.
8. 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]** button to configure or update the internet proxy settings.
9. In the **HTTP Proxy Server** area:
   a. Check the **[Enabled]** checkbox.
   b. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]**.
   c. Enter the Proxy Server address and port number in the **[Proxy Server Address]** field.
   d. Click on the **[Save]** button to return to the **SMart eSolution Setup** page.
   e. Click on the **[Apply]** button.

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

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

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 email 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.
   f. In the **[Recipient Group Addresses]** area, check the required Group.
   g. Click the field under **E-mail Addresses**, and enter e-mail address or addresses.
   h. Continue to add e-mail addresses to create your Alert Notification group, as required.
   i. 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.

   j. 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 that you want the Group to be notified of.
   k. 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 email status is sent. If the jam is cleared before the timer completes, no jam message will be sent.
   l. Click on **[Apply]** to save the changes.
8. If prompted, enter the *User ID* and *Password* of the Administrator's account and click on **[Login]**.
9. 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 once the device is registered with Xerox. When you call to order supplies, let the representative know the on-hand balance and that you would like to use Supplies Assistant.

Maintenance Assistant

Maintenance Assistant is a useful feature in troubleshooting device related problems. It is a monitoring and reporting program that runs on your device and communicates with Xerox through you network.

When calling for assistance you can send up-to- the minute performance related data to Xerox to help diagnose problems. You can also open an online diagnostic session with Xerox directly with Maintenance Assistant. This feature sends your device's diagnostic information to Xerox to be immediately analyzed and matched with solutions to resolve detected issues.

You can also download usage information to your workstation. The downloaded file is in CSV format which can be opened in a spreadsheet program.

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 **[Maintenance Assistant]** tab.
5. Click on the **[Send Diagnostic Information to Xerox]** bar. A **"Sending Diagnostic Information"** message will display. When the transmission is complete a success message will be displayed.

   Note: The **Send Diagnostic Information to Xerox** button is not available if the device is not enrolled in SMart eSolutions.

6. Click on the **[Close]** button.

To Open an Online Troubleshooting Session with Xerox:

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 **[Maintenance Assistant]** tab.
5. Click on the **[Start an Online Troubleshooting Session at www.xerox.com]** bar. A **"Starting Online Troubleshooting Session"** message will display. When transmission is complete your browser will automatically be redirected to Xerox.com for online assistant.

   Note: If there are any communication problems, a message window will display. Check your configuration and communication settings by clicking the **[Settings]** button. This will take you to the **SMart eSolution Setup** page.

To Download File to Your Workstation:

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 **[Maintenance Assistant]** tab.
5. Click on the **[Download File to Your Computer]** bar. The **Generating Diagnostic Information** screen will display, showing "This may take a few minutes".
6. Once the file is ready, **File Ready** screen will display, indicating **"File Successfully generated"**. Right-click on the link **[UsageLog.csv]** to download the file.
7. Select **[Save Target As....]**.
8. Select the folder you want to save the file in and click on **[Save]**.
9. Click on the **[Close]** button.

   Note: If there are any communication problems, a message window will display. Check your configuration and communication settings by clicking the **[Settings]** button. This will take you to the **SMart eSolution Setup** page.

Energy Saver

This feature allows you to set the device to save energy when not in use. This feature can be set at the device as well as at the web browser.

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 **[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 **[General Setup]** link.
6. Click on **[Energy Saver]** in the directory tree.
7. In the **Energy Saver Mode** area, select one of the following mode for **[Energy Saver Mode]**:
   - **Intelligent Ready** - the device wakes up and sleeps automatically based on previous usage.
   - **Job Activated** - the device wakes up when an activity is detected.
   - **Scheduled** - the device wakes up and sleeps at set time on a daily basis.
8. If you select either **Intelligent Ready** or **Job Activated**, you can select **[On]** or **[Off]** for **Fast Resume**. This option reduces the time taken for the device to wake up. This option will change the default sleep or low time-outs and increase energy usage.
9. If you select **Scheduled**, then select the specific day you want the device to wake up by selecting **[Time]** form the **Scheduled Based on** drop-down menu. Select the time you want it to warm (wake) up from the **[Warm Up]** drop-down menu and select the time you want the device to sleep to save energy form the **[Energy Saver]** drop-down menu.
10. Click on the **[Apply]** button to accept the changes.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then touch the **[Tools]** tab.
4. Touch **[Device Settings]**.
5. Touch **[General]**.
6. Touch **[Energy Saver]**.
7. Select one of the following type of mode under **[Energy Saver Mode]**:
   - **Intelligent Ready**
   - **Job Activated**
   - **Scheduled**
8. If you select either **Intelligent Ready** or **Job Activated**, you can select **[On]** or **[Off]** for **Fast Resume**. This option reduces the time taken for the device to wake up. This option will change the default sleep or low time-outs and increase energy usage.
9. If you select **Scheduled**, touch **[Scheduled Settings]**.

10. In the **Scheduled Settings** page, select the day you want the schedule to start.
    a. Select either **[Activity]** or **[Time]** for **Schedule Based On**.
    b. If you select **[Time]**, select time from the **[Warm Up Time]** drop-down menu.
    c. Select time from the **[Energy Saver Time]** drop-down menu.
    d. Repeat step **a** to **c** for the rest of the week.
11. Touch **[Save]**.
12. Touch **[Save]**.
13. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools Pathway.

Network Log

The Network Logs feature allows customer the following ability:

- Control the amount information gathered within the log files.
- Download the log files to a USB drive.

  Note: Customers will only use this feature if requested by Xerox Customer Support. The Log files are only meaningful to a trained Xerox personnel. The level of information gathered will be specific to Xerox Customer Representative.

You can download Network Log from the device which will only provide the current network logs. Or from the device web browser, where the customer has the option to download the current network log as well as downloading the following information:

- Configuration Report
- Fault Logs
- Archive Logs (the last 10 Logs that have been saved).

  Note: Network Logs are saved to the archive collection every time the device is restarted and when the **[Download]** button is selected within the Network Log feature.

  Note: When Network Log is downloaded form the device the downloaded file is not encrypted, but is encrypted if downloaded from the device web browser.

Procedure to Download Network Logs

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 **[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 **[General Setup]** link.
6. Click on **[Network Logs]** in the directory tree.
7. In the **Information Level** area, select one of the following options:
   - **Basic** - records a minimum list of network actions that have occurred on the machine.

- **Enhanced** - records a detailed list of network actions that have occurred on the machine.

Note: Job processing times will increase as long as this option is selected.

8. Click on the **[Save]** button to save changes.
9. In the **Download Files** area, for **Log Content**, Basic Network Logs is automatically selected. You can select additional reports, from the **Additional Content** as follows:
   - **Configuration Report**
   - **Fault Logs**
   - **Archive Logs**
10. When you selected the required reports you want to download, click on the **[Start Download]** button.
11. The Download Status screen will display, after a brief moment, the information requested will be organized into one file, click on the **[Download File Now]** button, in the **File Download** window click on the **[Save]** button**,** select the place on the workstation you want to save the file to and click on the **[Save]** button to save the file.
12. Click on the **[Close]** button.

At the Device:

Note: Ensure you have an USB memory device to save the network log.

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then touch the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Network Logs]**.
6. In the **Network Logs** screen, under **[Information Level]** select either **[Basic]** or **[Enhanced]**.
   a. If you select **[Basic]**, follow the steps below:
      - Click on the **[Download Basic Log File]** button.
      - A note will display, if USB drive is not detected, insert your USB drive and touch the **[OK]** button. The file will download onto the USB drive.

   b. If you select **[Enhanced]**, follow the steps below:
      - Touch the **[Save]** button, a pop-up dialog will appear, displaying **"A system restart is required for your changes to take effect."** If USB drive is inserted, remove the USB drive before touching the **[Restart]** button.
      - A pop-up dialog will appear displaying **System Restart**.
      - Once the system has restarted, insert your USB drive, and click on the **[OK]** button. The file will download onto the USB drive.
7. A pop-up dialog will appear, displaying download is complete. Remove your USB drive and touch the **[Close]** button.
8. Press the **<Log In/Out>** button, touch **[Logout]** to exit the Tools Pathway.

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

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 **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Click on the **[E-mail Alerts]** in the directory tree.
8. In the **[Recipient Group Addresses]** area:
   a. Check the required Group.
   b. Click the field under **E-mail Addresses**, and enter 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 and click on **[Login]**.
   g. 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.
   h. If you want to create more than one Alert Notification group, select the group number and add e-mail addresses to the group.
9. 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 or some services are not available:** 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:** Enter how many minutes (0 - 60) in the field to wait after a jam has been detected before an email 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:** device has stopped all functions or has been turned off.
   - **Potential persistent problems exist:** If area specified does not receive attention problems may re-occur.
   - **Machine requires administrator assistance:** Authorized System Administrator must address problem.
   - **Machine is operational, but degraded:** 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/Solid Ink Sticks or other usable item needs attention (see LUI).
   - **Paper jam is detected:** Paper jam is in need of attention in specified area if you have been notified.

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

e. Select **[Apply]** to save your settings or **[Undo]** to cancel.

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

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 **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Select **[Local UI Alerts]** in the directory tree.
8. In the **Scan Disk Memory Warning** area, select one of the following option 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.
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"**.

Low Supply Warning

System Administrators can set the device to display a low warning message about a supplies level, for example, ColorQube Ink, Cleaning Unit and Document Feeder Feed Roller.

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 **[General Setup]** link.
6. Click on the **[Alert Notification]** link.
7. Select **[Low Supply Warning]** in the directory tree.
8. In the **Days Remaining** area, select a value from either **ColorQube Ink**, **Cleaning Unit** or/and **Document Feeder Feed Roller** drop-down menu.

   Note: If you set the value to '**0**', then the user will get a '**NO WARNING MESSAGE**' that the Supply is getting low.
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"**.

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. and click on the **[Refresh]** button to refresh 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.

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. These instructions describe how to disable the banner sheet from the device.

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Job Sheets]**.
6. Touch **[Banner Sheets]**.
7. Touch the **[Disabled]** button.
8. Touch **[Save]**.
9. Press the **<Log In/Out>** button, then press **[Logout]** to exit the Tools pathway.

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 **[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.
7. Select **[General]** in the directory tree.
8. In the **Banner Sheet** area:
   a. For **Print Banner Sheet**, select **[Yes]** to enable the feature.

b. For **Allow the Print Driver to Override**, select **[Yes]** to allow your print driver to override this option.
c. From the **Banner Sheet Identification** drop-down menu, select one of the following:
d. For **Use Generic User Name and Job Name**, check the **[Enabled]** checkbox to enable Banner Sheet or uncheck to disable.

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"**.

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 page 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

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]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Reprint Saved Jobs]** link.
6. Select **[Enablement]** in the directory tree.
7. Click the **[Enabled]** radio button 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. Under Settings, from the **[Protocol]** drop-down menu, note that only FTP is available.
3. Select either the **[IPv4 Address]**, **[IPv4 Address]** or **[Host Name]** radio button for your FTP server.
4. Specify the *IP address* or *host name* of the repository.
5. For **[Document Path]**, specify the path to the file repository.
6. For **[File Name]**, type the file name for the backup. This name will be appended onto the end of the document path.
7. 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.
8. 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.

9. Check **[Select to Save New Password]** for an existing Login Name. You must then click 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 considerable 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. Note that only FTP is available in the **[Protocol]** drop-down menu under Settings.
3. Select either the **[IP Address]**, **[IPv4 Address]** or **[Host Name]** radio button for your FTP server.
4. Specify the *IP address* or *host name* of the repository.
5. For **[Document Path]**, specify the path to the file repository.
6. For **[File Name]**, type the file name for the backup to restore. This name will be appended to the document path.
7. 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.
8. 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.
9. Click **[Select to Save New Password]** for an existing Login Name. You must then 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:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.
5. Touch **[Network Settings]**.
6. Touch **[Online/Offline]**.
7. To stop the device receiving or sending jobs over the network touch the **[Offline]** button. 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.
8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Auxiliary (Foreign Device) Interface Kit

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 administrator must enable Auxiliary Access as the Accounting Mode from the Tools menu of the device, as follows:

1. Press the **<Log In/Out>** button.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button.
4. Touch the **[Tools]** tab.
5. Touch **[Accounting Settings]**.
6. Touch **[Accounting Mode]**.
7. Select **[Auxiliary Access]**.
8. Select the required **[Auxiliary Device Configuration]** and configure your device and touch **[Save]**.
9. Touch **[Save]**.
10. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

For further instructions on Auxiliary (Foreign Device) Interface Setup options refer to the **Interactive User Guide** delivered with your device.

SNMP (Simple Network Management Protocol)

It is possible to remotely define and modify GET, SET, and TRAP SNMP (Simple Network Management Protocol) community names for the device. You can also configure SNMP trap destinations for TCP/IP and NetWare (IPX) that will receive traps from any device on the network.

SNMP Community Name properties that can be configured are:

- GET Returns the password for SNMP GET requests to the device. Applications obtaining information from the device via SNMP, such as Xerox PrinterMap or Internet Services, use this password.
- SET Returns the password for SNMP SET requests to the device. Applications that set information on the device via SNMP, such as Xerox PrinterMap or Internet Services, use this password.
- TRAP Returns the password for SNMP TRAPS from the device. This is the default password for SNMP TRAPS sent from the device via SNMP.

Configure SNMP Community Names

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 **[Connectivity]** button.
6. Click on the **[Protocols]** link.

7. Select **[SNMP]** in the directory tree.
8. Check the **[Enable SNMP v1/v2c Protocol]** and/or **[Enable SNMP v3 Protocol]** checkbox to enable the protocol.
9. To edit SNMP properties click either **[Edit SNMP v1/v2c Properties]** or **[Edit SNMP v3 Properties]**.

   Note: Configure **HTTPS** before editing SNMP v3 Properties. Configuring this feature requires secure web page communication.

   Note: Turning off the SNMP protocols will cause an interruption in the communication between the device and remote client applications.

   For Edit SNMP v1/v2c Properties:

   a. Enter a name (up to 256 characters) for the **[GET Community Name]**. The default is **public**.
   b. Enter a name (up to 256 characters) for the **[SET Community Name]**. 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).

   CAUTION: If you change the GET and/or SET Community Names, you must change all network applications that are communicating via SNMP with this device to use the new GET/SET names.

   c. Enter a name (up to 256 characters) for the default **[TRAP Community Name]**. 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.

   d. Click **[Save]**, to apply the changes or **[Undo]** to return to the previous settings.

   For Edit SNMP v1/v2c Properties:

   e. Use this page to configure Authentication Password and Privacy Password for the Administrator Account.
   f. In the **Administrator Account** area, check the **[Account Enabled]** checkbox to create an administrator account that can be used to provide more extensive access to the objects on the printer.
   g. Enter details for **Authentication Password** and **Privacy Password** as desired.
   h. Check the **[Select to save new password]** checkbox.
   i. In the **Print Drivers / Remote Clients Account** area, check on the **[Account Enabled]** checkbox, to create an account for bi-directional Print Drivers and Xerox Remote Clients.

   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.

   j. Click **[Save]**, to apply the changes or **[Undo]** to return to the previous settings.
10. In the **Authentication Failure Generic Traps** area, check the **[Enabled]** checkbox if you want the machine to generate a trap for every SNMP request that is received by the machine which contains an invalid community name.
11. Click on the **[Apply]** button to accept the changes or **[Undo]** return to the previous settings.

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

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.

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 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 **[General Setup]** link.
6. Select **[Configuration Report]** in the directory tree, scroll down to the **Common User Data** 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. At your Workstation, open the web browser and enter the *IP address* 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 **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Upgrades]** in the directory tree.
8. In the **Upgrades** area, check the **[Enabled]** checkbox to enable Machine Software upgrade.
9. Click on the **[Apply]** button.

Manual Upgrade

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 **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Manual Upgrade]** in the directory tree.

   Note: Note the current software level in the Last Successful Upgrade box.
8. In the Manual Upgrade area, click on **[Browse]** to locate the software upgrade file obtained earlier.
9. Select the file and click **[Open]**.
10. 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.
11. Once 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 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 the Software Upgrade link to the left of the page and select Auto.

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. 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 **[General Setup]** link.

6. Select **[Configuration Report]** in the directory tree, scroll down to the **Common User Data** section to see your System Software Version.
7. Contact your Xerox Customer Support Representative to make certain that Auto Upgrading is appropriate for your device. If it is not, refer to the Software Upgrade via Network Connection topic for manual upgrade instructions.
8. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

Set the Auto Upgrade Time

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 **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Select **[Auto Upgrade]** in the directory tree.
8. Check the **[Enabled]** checkbox to enable the Auto Upgrade feature.
9. Select either **[Hourly]** or **[Daily]** to activate the feature accordingly, in the **Refresh Start Time** section.
10. If **[Daily]** has been selected, enter the required time for the upgrade to be performed.
11. Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** for **Protocol**.
12. If IP Address is selected, enter details in the IP address and Port of the server where the software upgrade file (obtained earlier) is located, in the **[IP Address]** and **[Port]** field (the default port number is 21) and if Host Name is selected, enter details in the **[Host Name]** and **[Port]** field (the default port number is 21).
13. Enter the path to the upgrade file on the server in the **[Directory Path]** field.
14. Enter the **[Login Name]** and **[Password]** for the server, retype the password.
15. Click on the **[Apply]** button to accept the changes.

The upgrade will now be performed automatically on the device at the time specified. Once 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.

4

Internet Services

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 as in 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 59.

Enable HTTP on the device

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

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then touch the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**.
6. Touch **[Continue]**.
7. Touch **[HTTP Settings]**.
   a. Touch **[Enable]**.
   b. Touch **[Save]**.
8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, 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 Login 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

The Description and Alerts page allows you to view the Device Model, Name, location, IP Address and Status of 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. Click on the **[Description and Alerts]** link.

Alerts

The Alerts page allows you to view 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. Click on the **[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 47.

To Reboot the Device

It is possible to reboot the device from Internet Services.

1. Click on the **[Status]** tab.
2. Click on the **[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 and previous 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. Click on the **[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. Click on the **[Consumables]** in the directory tree.
4. The **[Consumables]** screen will show consumable information for:
   - **ColorQube Stick**

- **Cleaning Unit**
- **Document Feeder Feed Roller**

One of the following **Status** message is displayed:

- **OK**
- **Reorder** (Supply is getting low)
- **Replace** (Unit Supply is used up and requires immediate replacement).

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. Click on the **[Trays]** in the directory tree.
4. The **[Trays]** page displays the current paper supply.

Instructions for changing the paper stock are contained in the **Interactive User Guide** delivered with your device.

Information Pages

The Information Pages feature allows users to print out a sheet that summarizes useful information about the device.

The following information is available to print:

- Configuration Report
- Paper Tips Page
- Billing Summary
- Copying Guide
- Scanning Guide
- Faxing Guide
- Office Demo Page
- Graphics Demo Page
- 2-Sided Demo Page
- CMYK Sampler Pages
- RGB Sampler Pages
- Spot Color Sampler Pages
- PCL Font List
- PostScript Font List

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 **[Status]** tab.
3. Click on the **[Information Pages]** in the directory tree.
4. In the **Page Name** area select the required information page and click on the **[Print]** button.

At the Device:

5. Press the **<Machine Status>** button.
6. Touch the **[Machine Information]** tab.
7. Touch **[Information Pages]**.
8. Select the required information and touch the **[Print]** button.
9. Touch **[Close]**.

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 memory used on the device, you can also create new saved job folders and manage saved job folders.

Create a New Folder

1. Click on **[Create New Folder]** link in the **Folder Operation** area.
2. In the **New Folder** area, enter details in the **[Name]** field.

3. 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.
4. Click on the **[Apply]** button to create the folder. The folder will appear in the **Folders** list

Manage Folders

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

1. Click on the **[Manage Folder]** link in the **Folders Operation** area.
2. **To Delete**:
   a. Check the checkbox for the folder you want to delete.
   b. Click on the **[Delete]** 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 new name on the folder 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 print you require 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]** 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 printer driver.

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

- PCL® 5e
- PCL® XL

- PostScript® Level 2 and 3
- TIFF
- ASCII Text
- PDF
- JPEG

  Note: ASCII text files, from systems other than PCs, may not print correctly if hard carriage returns (ASCII Control-M) are not used as line delimiters in the text.

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. Click on **[Enter]**.
2. Click on the **[Print]** tab.
3. In the **[File Name]** area at the bottom of the screen, enter the name of the document that you want to print, or click the **[Browse]** to locate the document on your workstation.
4. In the **[Printing]** area, enter the number of **[Copies]** required (between 1 - 9999).
5. 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's user interface to release the document for printing
   - **Sample Set**- if several copies of the document have been selected, one copy only will print to allow the reader to check for errors. Once validated, the remaining copies can be released from the device's user interface
   - **Save Job for Reprint** - the document will be saved for reprinting.
   - **Delayed Print** - specify a time for your document to print
6. Select the required Printing options from the drop-down menu for 2 Sided Printing, Output Color, Collate, Orientation, Staple 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.
7. 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.
8. Retrieve the printed document(s) from the device.

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.

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**

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 **[Description]** link.
6. 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:

- Report Profile
- Common User Data
- Machine Profile
- Machine Hardware
- General Setup
- Software Versions
- Connectivity Physical Connections
- Connectivity Protocols
- Services

- Accounting
- Security
- Media Trays

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 **[General Setup]** link.
6. Click on the **[Configuration Report]** link from the directory tree.
7. To print a configuration report from this screen, press 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.

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 **[Connectivity]** link.
6. Click on the **[Physical Connections]** link.
7. Click on **[Ethernet]** in the directory tree.
8. In the **General** area, select the speed from the **[Rated Speed]** drop-down menu.
9. Click on the **[Apply]** button, then 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 or Administrator Support 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. Enter the contact details in the entry fields.

5. 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
   c. **[Cancel]** button to cancel the changes.

Other features and Services

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

5

Network Installation

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

TCP/IP Settings

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

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 TCP/IP Settings using Internet Services on page 73.

Configure Static Addressing using the Device

Information Checklist

Before starting the procedure, please ensure the following items are available or 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.

Enter a Static IP Address

1. At the device and press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[TCP/IP Settings]**.

6. Touch **[TCP/IP Enablement]**.
   a. Touch **[Enable]** for **IPv4** and **IPv6**.
   b. Touch **[Save]**.
7. Touch **[Dynamic Addressing]**.
   a. Touch **[Disabled]** to disable DHCP.
   b. Touch **[Save]**.
8. Touch **[IP Address/Host Name]**.
   a. Touch button under the **[IPv4 Address]** heading
   b. Enter the IP Address using the on-screen keypad and touch **[Save]**.
   c. Touch button under the **[Host Name]**.
   d. Type the host name EXACTLY as you want it to appear. To access more characters, touch **[123]** on the user interface.
   e. Touch **[Save]**, then touch **[Close]**.
9. Touch **[Subnet and Gateway]**.
   a. Touch **[Subnet Mask]**, enter the Subnet Mask address using the on-screen keypad.
   b. Touch **[Save]**.
   c. Repeat this process for the **IP Gateway**. When you are finished, touch **[Save]** to accept the changes and return to the TCP/IP Settings screen.
   d. Touch **[Close]** twice to return to the feature menu.
10. Touch **[Advanced Settings]**.
11. Touch **[Continue]**.
12. Touch **[HTTP Settings]**.
    a. Ensure **Enable** is selected. If not, touch **[Enable]**.
    b. Touch **[Save]**, then touch **[Close]** twice to return to the **Tools** menu.

DNS/DDNS Configuration

1. From the **Tools** menu,
2. Touch **[Network Settings]**.
3. Touch **[TCP/IP Settings]**.
4. Touch **[DNS Configuration]**. This feature will be inaccessible (grayed out) if TCP/IP protocol is not enabled.
   a. Touch the **[Domain Name]** button.
   b. Touch the button 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 **[Close]**.
5. Touch **[Preferred DNS Server]**.
   a. Touch the button under **Preferred DNS Server #1**, enter the *DNS Server IP Address* using the on-screen keypad.
   b. Touch **[Save]**, then touch **[Close]**.

6. 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]**.

   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.

7. Touch **[Dynamic DNS Registration]**.
   a. Click on **[Enable]**, then **[Save]**.
8. Touch **[Close]** twice.
9. Press the **<Log In/Out>** button, touch **[Logout]** to exit **Tools** mode.

Configure Dynamic Addressing

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

The Configuration Report is printed, verify the TCP/IP information under **Connectivity Protocols**.

Installation via BOOTP or DHCP

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

1. Go to the device and press the **<Log In/Out>** button to enter the Tools pathway.

2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, and then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[TCP/IP Settings]**.
6. Touch **[Dynamic Addressing]**. By default, DHCP is selected.
7. Select the required Dynamic Addressing method:
   - **BOOTP**
   - **DHCP**
8. Touch **[Save]**.
9. Touch **[Close]**.
10. Press the **<Log In/Out>** button, touch **[Logout]** to exit **Tools** mode.

IPv4

Configure TCP/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.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Ensure that **[IPv4]** is selected.
9. In the **General** area:
   a. The **[Enabled]** checkbox for **Protocol** will 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's 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 method 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]**.

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 **[Primary 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. 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.

10. In the **DHCP/DDNS** area:
    a. Check the **[Enabled]** checkbox for **Release Registration** ONLY if you wish to release this device's IP address upon reboot. Default is unchecked.
11. In the **Zero-Configuration Networking** area:
    a. Check the **[Enabled]** checkbox for **Self Assigned Address**, 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. Check the **[Enabled]** checkbox for **Multicast DNS** to resolve host names to IPv4 addresses without using a conventional DNS server.
12. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
13. 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.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   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.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Ensure that **[IPv6]** is selected.
9. In the **General** area:
   a. Check the **[Enabled]** checkbox for **Protocol** 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.
10. 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.
11. 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**.

12. In the **DNS Configuration** area:
    a. Enter an IP address for the **[Primary DNS Server]**. Enter an IP address for **[Alternate DNS Server 1]** and **[Alternate DNS Server 2]**.
    b. Check to enable **[Prefer IPv6 Address over IPv4]**.
    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.
13. The **Default Gateway** will displays the link-local address of the router (known in IPv4 as the default gateway).
14. 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.
15. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
16. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Supporting LPR Printing

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.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LPR/LPD]** in the directory tree.
8. 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.
9. In the **Advanced Settings** area:
   a. 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. Check the **[Enabled]** checkbox to enable **PDL banner page attributes override LPR control file attributes for job name and owner**. 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:
      - **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.
      - **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.
      - **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.
10. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
11. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Configure 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.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. 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"**.
9. Upto 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 the **[Default All]** button to check 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 is using port 9100. this prevents each print job from generating a banner page.
10. 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).
11. 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.
12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
13. Scroll down and click 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.

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 to a User Agents (UA) via SLP.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SLP]** in the directory tree.
8. 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.
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"**.

    Note: The settings are not applied until you restart the device.

11. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
12. Scroll down and click 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.

SNMP

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/v2c

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. 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.

8. In the **SNMP Properties** area:
   a. Check to ensure the **[Enable SNMP v1/v2c Protocols]** checkbox is selected.
   b. 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.
   c. In the **Community Names** area, enter a name in the **[GET Community Name]** field. The default is **public**.
   d. 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).

   e. In the **Default Trap Community Name**, 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.

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

9. 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.

10. 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 82.

To configure SNMP v3

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 **[Connectivity]** link.
6. 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. Once 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, see *Machine Digital Certificate Management* on page 157.

7. 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.
8. Select **[SNMP]** in the directory tree.
9. 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 v1/v2c Properties]** button.
      System Administrator uses the **Edit SNMP v3 Properties** page to configure Authentication Password and Privacy Password for the Administrator Account.
10. 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.
11. 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.

12. 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.

13. 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 82.

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.

1. From the **SNMP** page, click on the **[Advanced Settings]** button.
2. 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.
3. 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.
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"**.

To Add or Edit an IP 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 IP 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 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 with.
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

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.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SSDP]** in the directory tree.
8. 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.
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"**.

Microsoft Networking

Configure Microsoft Networking

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Microsoft Networking]** in the directory tree.
8. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable Microsoft Networking.
   b. Enter the device's workgroup in the **[Workgroup]** field.

c. Enter the device's 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's 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.

9. 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.
10. 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"**.

   Note: The settings are not applied until you reboot the device.
5. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
6. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

AppleTalk

To Enable AppleTalk on the Device

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar. 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[AppleTalk]** in the directory tree.
8. 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's 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.

   - **Physical Connection** displays physical network connection. This will display **"Ethernet"**.
   - **Printer Type** displays the current assigned printer type. This will display **"LaserWriter"**.
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"**.

    Note: The settings are not applied until you reboot the device.
11. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
12. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Create an IPP Printer (Internet Printing Protocol)

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. 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"**.
9. Upto 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 **[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.
10. 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).
11. 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.
12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
13. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Create an IPP Printer at Your Workstation

Verify the correct software is loaded

1. At the Desktop, right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click the **[Local Area Connection]** icon.
4. Click **[Properties]**.
5. Verify that the **[Internet Protocol (TCP/IP)]** protocol has been loaded.

Install the Print Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]** (Windows 2000) or **[Printers and Faxes]** (Windows XP). The Vista path is *Start\Control Panel\Printer(s)*.
2. Double-click the **[Add Printer]** icon and click **[Next]**.
3. Verify that **[Network Printer]** is selected and click **[Next]**.

   The **[Locate Your Printer]** (Windows 2000) or **[Specify a Printer]** (Windows XP) screen will appear.
4. To create an IPP printer select **[Connect to a printer on the Internet or on your intranet]**.
5. Type *HTTP://...* followed by the printer's fully qualified Domain name or IP address in the URL field. The Printer Name can be either the Host Name or the SMB Host Name as shown on the device configuration report, depending on the name resolution used by your network (WINS or DNS).
6. Click **[Next]**.
7. Select **[Have Disk]** and browse to the location of the print driver (.INF).
8. Click **[OK]** to install the print driver.
9. Select the Printer Model and click **[Next]**.
10. Select **[Yes]** if you wish to make this the default printer.
11. Select **[Yes]** to print a Test Page. Verify that it prints at the device.
12. Click **[Finish]**.

Internet Services

Once installed an IPP printer should provide a link directly to the Internet Services web pages.

To Access Internet Services

1. From the **[Start]** menu select **[Settings]** and then **[Printers]**.
2. Click on the device printer icon and a '**Get More Info'** link will appear in the left hand pane of the window.
3. Click the **[Get More Info]** link to go to straight to the device home page.

You have completed the installation of an IPP port and print drivers.

At the Windows 2000 Desktop:

1. Right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the network connection you want to configure AppleTalk on, and then click **[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. Click **[Start]**, **[Settings]**, then **[Printers]**.
6. Double-click the **[Add Printer]** icon to start the Add Printer Wizard.
7. Click **[Next]**.
8. Click **[Local Printer]**. Deselect the **Automatically detect and install my Plug and Play printer** option.

9. Click **[Next]**.
10. Click **[Create a New Port]**.
11. Select **[AppleTalk Printing Devices]** and click **[Next]**.
12. In the Available AppleTalk Printing Devices box, click the printer you want to connect to. It may be necessary to double-click the required Zone to locate the printer. Click **[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 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 **[Have Disk]**. Load the Internet Services Print and Fax Drivers CD into your CD drive.
14. Click **[Browse]** and locate the CD drive.
15. Locate the folder containing print drivers on the CD and select the required Windows 2000 print driver.
16. Select **[Open]**.
17. Select **[Open]** again, if necessary.
18. Select **[OK]**.
19. Select your printer model from the list and click **[Next]**.
20. Type a name for the printer (or accept the default name), and then click **[Next]**.
21. If you want this to be your default printer click **[Yes]**.
22. Click **[Next]**.
23. If you want to share this printer from your computer, click **[Share As:]**. Enter a share name (or accept the default name), then click **[Next]**.
24. If you want to print a test page, click **[Yes]**, then click **[Finish]**.

Windows XP

Configure TCP/IP and SLP Settings

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

   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.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. In the **General** area:

   CAUTION: Disabling TCP/IP or changing the IP address will affect NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP printing. If TCP/IP is disabled, Internet Services will not be available until TCP/IP is enabled from the device's control panel. If you change the IP address, you must reference the new address within you web browser to locate the device.

   a. Check the **[Enabled]** checkbox to enable the TCP/IP protocol.
   b. **Physical Connection** will display the physical network connection. This will display **"Ethernet"**.
   c. Select the on of the following method for obtaining a Dynamic IP address from the **[IP Address Resolution]** drop-down list:
      - **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]**.

   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 in which the device is connected in the **[Domain Name]** field.
   g. If DNS configuration is required, enter IP address for the **[Primary 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. 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.

9. In the **DHCP/DDNS** area, check the **[Enabled]** checkbox for **Release Registration** ONLY if you wish to release this device's IP address upon reboot. Default is unchecked.
10. In the **Zero-Configuration Networking** area:
    a. Check the **[Enabled]** checkbox for **Self Assigned Address**, 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. Check the **[Enabled]** checkbox for **Multicast DNS** to resolve host names to IPv4 addresses without using a conventional DNS server.
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"**.

    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.

Supporting LPR Printing

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LPR/LPD]** in the directory tree.
8. 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.
9. In the **Advanced Settings** area:
    a. 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. Check the **[Enabled]** checkbox to enable **PDL banner page attributes override LPR control file attributes for job name and owner**. 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:
   - **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.
   - **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.
   - **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.

10. Click on the **[Apply]** button to accept changes or **[Undo]** to return the settings to their previous value.
11. 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 to User Agents (UA) via SLP.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[SLP]** in the directory tree.
8. 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. Select the Message type from the drop-down menu for **[Multicast or Broadcast]**. 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.

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"**.

    Note: The settings are not applied until you restart the device.

11. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
12. Scroll down and click 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

Configure 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.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. 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"**.

9. 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 **[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.
10. 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).
11. 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.
12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
13. Scroll down and click 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

Create an IPP Printer (Internet Printing Protocol)

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[Raw TCP/IP Printing]** in the directory tree.
8. In the **General** area, ensure the **[Enabled]** checkbox for **Protocol** is checked to enable Raw TCP/IP Printing.

9. In the **Port Information** area:
   a. Leave the **[TCP Port Number]** set to 9100 for Port 1. If two additional ports are available, click **[Default All]** to see if they set to 9101 and 9102 respectively (emulating HP JetDirect EX Plus 3).
   b. Leave the **[Bidirectional]** and **[Maximum Connections]** 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.
   d. Leave the **[PDL Switching]** Enabled box at its default value.
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"**.

    Note: The settings are not applied until you restart the device.
12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
13. Click 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
14. A Configuration Report should have printed (by default) when the device rebooted. If the Configuration Report did not print, go to the device:
    a. Press the **<Machine Status>** button.
    b. Touch the **[Machine Information]** tab.
    c. Touch **[Information Pages]**.
    d. Touch **[Configuration Report]**.
    e. Touch **[Print]**, then touch **[Close]**.
15. Review the settings for Raw TCP/IP Printing under the heading TCP/IP Settings. These settings should read as follows:
    a. Raw TCP/IP Printing Enabled: Enabled
    b. Raw TCP/IP Port Number: 9100

Create an IPP Printer at your Workstation

Verify the correct software is loaded

1. At your Workstation, right-click the **[My Network Places]** icon.
2. Select **[Properties]**.
3. Right-click on the **[Local Area Connection]** icon.
4. Click **[Properties]**.
5. Verify that the **[Internet Protocol (TCP/IP)]** protocol has been loaded.

Install the Print Driver

1. From the **[Start]** menu, select **[Settings]** and then **[Printers]** (Windows 2000) or **[Printers and Faxes]** (Windows XP). The Vista path is Start\Control Panel\Printer(s).
2. Double-click the **[Add Printer]** icon and click **[Next]**.
3. Verify that **[Network Printer]** is selected and click **[Next]**.

4. The **[Locate Your Printer]** (Windows 2000) or **[Specify a Printer]** (Windows XP) screen will appear.
5. To create an IPP printer select **[Connect to a printer on the Internet or on your intranet]**.
6. Type **HTTP:// followed by the printer's fully qualified Domain name or IP address** in the URL field. The Printer Name can be either the Host Name or the SMB Host Name as shown on the device Configuration Report, depending on the name resolution used by your network (WINS or DNS).
7. Click **[Next]**.
8. Select **[Have Disk]** and browse to the location of the print driver (.INF).
9. Click **[OK]** to install the print driver.
10. Select the Printer Model and Click **[Next]**.
11. Select **[Yes]** if you wish to make this the default printer.
12. Select **[Yes]** to print a Test Page. Verify that it prints at the device.
13. Click **[Finish]**.

Internet Services

Once installed, an IPP printer will provide a link directly to the Internet Services web pages.

To Access Internet Services

1. From the **[Start]** menu select **[Printers and Faxes]**.
2. Click on the device printer icon and a Get More Info link will appear in the left hand pane of the window.
3. Click the **[Get More Info]** link to go to straight to the device home page.

You have completed the installation of an IPP port and print drivers.

Apple Talk

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address bar. 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[AppleTalk]** in the directory tree.
8. 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's 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"**.
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"**.

    Note: The settings are not applied until you reboot the device.

11. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
12. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Install the Print Driver

Refer to the Print and Fax Drivers Guide for Macintosh on the Internet Services Print and Fax Drivers CD for detailed instructions.

1. View the Configuration Report and note the *Name* given to the device under AppleTalk Settings.

At the Macintosh Workstation

2. Load the Internet Services Print and Fax Drivers CD-ROM into your CD drive.
3. Open the CD and locate the **[Drivers]** folder.
4. Locate and open the **[Mac]** folder.

Instructions for Version 10.x (OS X)

1. Double-click to open the folder containing the drivers for version 10.x.
2. Double-click to open the **[machine model.dmg]**.
3. Double-click to open the **[machine model.pkg]** file.
4. When the Welcome screen displays, click **[Continue]**.
5. Click **[Continue]**, then **[Agree]** to accept the License Agreement.

6. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
7. Click **[Install]**.
8. Click **[Close]**, and restart the workstation.
9. When the workstation has restarted, double click the hard drive icon.
10. Double-click the **[Applications]** icon.
11. Double-click the **[Utilities]** folder.
12. Double-click **[Print Center]** icon.
13. Double-click **[Add]** to add a new printer.
14. Select AppleTalk as your network protocol.
15. Select the required AppleTalk zone.
16. Select the printer that you wish to set up.
17. Select the Printer Model (that is, choose the PPD for your printer).
18. Click **[Add]**.
19. Print a document from an application to verify that the printer is installed correctly.

View the Macintosh Printer Utility on the Internet Services Print and Fax Drivers CD.

The device Internet Services is a suite of applications used for installing, maintaining and using the Xerox devices. The device Internet Services Macintosh Printer Utility is a Internet Services application that enables network administrators to rename and rezone Xerox systems that are configured for AppleTalk connectivity. Locate the Internet Services Print and Fax Drivers CD-ROM delivered in the Internet Services Network Services Pack with your device follow the instructions contained in the Internet Services Print and Fax Drivers Guide for Macintosh.

Apple Macintosh (TCP/IP)

Information Checklist

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

- An existing operational TCP/IP network with Macintosh workstation computers equipped with Ethernet network interface cards.
- Macintosh Operating System of 10.x or higher.
- A live network drop and Ethernet Cable for the Macintosh workstation.
- The printing device should already be configured with a static IP address (preferred), Subnet Mask, and Gateway Address, as well as with a Host Name.
- The Internet Services Print and Fax Drivers CD (delivered with your device). Review any README file contained with the print drivers.

Enabling TCP/IP 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 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 **[TCP/IP]** in the directory tree.
8. Verify that the printing device has been configured with a static IP address (preferred), Subnet Mask, Gateway Address, and Host Name.
9. Verify that the Domain Name for your network has been supplied, and that DNS is enabled and configured to resolve Host Names to IP Addresses.

   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 reenabled from the local user interface.

10. If any of the above items are incorrectly set, reset them and click on the **[Apply]** button.
11. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
12. Select **[LPR/LPD]** in the directory tree and verify that the **Protocol** is Enabled, and the **Port Number** is set to 515.

    Note: The settings are not applied until you restart the device.

13. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
14. Click 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.
15. A Configuration Report should have printed by default when the device rebooted. Look at the report to verify TCP/IP settings. If the Configuration Report did not print, go to the device:
    a. Press the **<Machine Status>** button.
    b. Touch the **[Machine Information]** tab.
    c. Touch **[Information Pages]**.
    d. Touch **[Configuration Report]**.
    e. Touch **[Print]**, then touch **[Close]**.

    The Configuration Report will print, check under the Connectivity Protocol heading for TCP/IP settings.

Select the PPD - PostScript® Printer Definition

1. Insert the Internet Services Print and Fax Drivers CD into your CD drive.
2. Double-click the printer icon on your desktop.
3. Select **[Printing]**.
4. Select **[Change Setup]**.
5. Select **[Change]**.
6. Locate the **[Drivers]** folder on the CD.
7. Select the appropriate PPD for OS 10.x.
8. Select the options according to those installed on your device.
9. Click **[OK]**.

10. Print a document from an application to verify that the printer is installed correctly.

Set up LPR (Line Printer Remote) Printing in Mac OSX

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

   Note: There may be more than one Print and Fax Drivers CD. If the Mac folder does not appear, check for another Print and Fax Drivers CD.

5. Double-click to open the folder containing the drivers for version 10.x.
6. Double-click to open the **[machine model.dmg]** file.
7. Double-click to open the **[machine model.pkg]** file.
8. The Welcome to the Installer dialog box appears. Click **[Continue]**
9. Click **[Continue]** and then **[Agree]** to accept the License Agreement.
10. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
11. Click **[Install]**.
12. Click **[Close]**.
13. Restart your computer.
14. When your computer has restarted, open Print Centre. To do this:
15. Double-click the hard drive icon on the desktop.
16. Double-click to open **[Applications]**
17. Double-click to open **[Utilities]**.
18. Double-click to open **[Print Center]**.
19. Double-click **[Add]** to add a new printer.
20. Select **[IP Printing]** from the menu.
21. Enter the IP address of the printer.
22. Select **[Xerox]** from the printer model list.
23. Select Xerox ColorQube 9201/9202/9203 (according to your model) from the model name list.
24. Click **[Add]**.
25. Print a document from an application to verify that the printer is installed correctly.

View the Macintosh Printer Utility on the Internet Services Print and Fax Drivers CD

The device Internet Services is a suite of applications used for installing, maintaining and using the Xerox devices. the device Internet Services Macintosh Printer Utility is a Internet Services application that enables network administrators to rename and rezone Xerox systems that are configured for AppleTalk connectivity. Locate the Internet Services Print and Fax Drivers CD-ROM delivered in the Internet Services Network Services Pack with your device and follow the instructions contained in the Internet Services Print and Fax Drivers Guide for Macintosh.

NetWare

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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]**, and click on the **[Login]** button.
4. Click on the **[Connectivity]** link.
5. Click on the **[Protocols]** link.
6. Select **[NetWare]** in the directory tree.
7. In the **General** area:
   a. For **Protocol**, check the **[Enabled]** checkbox to enable NetWare protocol.
   b. Select the required **[Filing Transport]** from the drop-down menu.
   c. Select the required **[Frame Type]** from the drop-down menu, selection for the frame type are dependant upon the Physical Connection.
   d. For **[Queue Poll Interval]**, enter the queue poll interval in seconds. The range is from 1 - 240 seconds, and the default is 5.
   e. **Physical Connection** displays physical network connection. This will display **"Ethernet"**.
   f. **External IPX Number** displays the current IPX number.
   g. 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.
   h. Enter the print server password in the **[New Print Server Password]** field, then re-enter it in the **[Retype New Print Server Password]** field.
   i. Check the **[Select to save new password]** checkbox.
8. 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.

9. 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.
10. 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”.
11. Click on the **[Apply]** button to accept the changes or **[Undo]** to return the settings to their previous values.
12. 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.
13. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
14. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

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 enables 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 have the ease of automatically creating a printer object in the NDS tree and automatic driver download capability, eliminating 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

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 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 **[Raw TCP/IP Printing]** in the directory tree.
8. 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"**.
9. 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 **[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.
10. 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).
11. 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.
12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.

13. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

Create a Device Description

Create a device description from your AS400 terminal's command line.

1. Select the F-4 key to prompt the CRTDEVPRT command. Enter the following parameters:

   Device Description: Xeroxprinter

   Device Class: *lan

   Device Type: 3812

   Device Model: 1
2. Press **[Enter]** to continue, and enter the following parameters:

   Lan Attachment: *IP

   Port Number: 9100

   Online at IPL: *yes

   Font Identifier: 11

   Form Feed *autocut

   Note: For some versions of AS400, the default may match some of these parameters.
3. Leave all other parameters at 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 will indicates that you have created the device Xerox printer.
7. Power on the device and start a print writer. Then 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 ColorQube 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 104 step 2.

3. At this point, a spool file (document) should be able to be sent to the ColorQube 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. Use the correct case when entering commands; UNIX commands are case-sensitive.

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

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

- 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

1. Add the machine hostname to the etc/hosts file on the HP-UX workstation or DNS server.
2. Ensure that you can ping the machine from the HP-UX workstation, using the hostname found in the
   /etc/hosts file.
3. 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 **[OK]** to complete form.

9. Click **[Yes]** at the Configure HP UX Printers Subpanel screen. This screen may be obscured by 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

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 **[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, please ensure the following items are available or 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 **[Information Pages]**.
d. Touch **[Configuration Report]**.
e. Touch **[Print]**, then touch **[Close]**.

The Configuration Report will print. Verify the addresses detailed under TCP/IP Settings.

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 into 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 **[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 **[Enter]** to accept default of a non-SCO remote printer.
4. Click **[Enter]** to accept default of non-default printer.

5. Click **[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, please ensure the following items are available or 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

1. At your Workstation, open the web browser and enter the *IP address* of the machine 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 **[Raw TCP/IP Printing]** in the directory tree.
8. 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"**.
9. Upto 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 **[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.
10. 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).

11. 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.

12. Click on the **[Status]** tab, select **[Description & Alerts]** in the directory tree.
13. Click the **[Reboot Machine]** button and click **[OK]** to reboot the machine. The network controller takes approximately 5 minutes to reboot and network connectivity will be unavailable during this time.

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 **[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.

6

Print Drivers

This chapter summarizes the print driver features and functions. You can use Internet Services to configure the Print Drivers.

Windows 2000/2003 Server

Xerox Printer Installer

This section provides instructions on how to install 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then 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.

Windows Add Printer Wizard

1. At the Desktop, right-click the **[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.
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]**.
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 **[Details]**.

7. Check the checkbox to select **[Print Services for UNIX]**.
8. Click **[OK]**.
9. Click **[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 deselect **[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 **[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 **[Open]** and then **[OK]**.
13. Select the model of your machine from the list. Click **[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 a details in the **[Location]** and **[Comment]** if required. Click **[Next]**.
17. Select **[Yes]** to print a test page. 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 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then 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 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 **[Add Printer]** and click **[Next]**.
4. Verify that **[Network Printer]** is selected and click **[Next]**.
5. The **Locate Your Printer** screen will appear. Select the **[Type the Printer Name]** option or click **[Next]** to browse for a printer.
6. Enter the path to the printer or click **[Next]** to browse for the print queue created on your server.
7. Select the printer and click **[Next]**. Select **[Yes]** if you wish to make it the default printer. Click **[Next]**.
8. Click **[Finish]**. The print driver will download to the Windows 2000 Professional workstation.
9. Once 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 **[Details]**.
7. Check the checkbox to select **[Print Services for UNIX]**.
8. Click **[OK]**.
9. Click **[Next]**.
10. Close the **[Add/Remove Programs]** window.

Add the Printer

1. From the **[Start]** menu, select **[Settings]** then **[Printers]**.
2. Double-click **[Add Printer]** and click **[Next]**.
3. Select **[Local Printer]** and deselect **[Automatically detect and install my Plug and Play printer]**.
4. Click **[Next]**.
5. Select **[Create a new port]** and choose **[LPR Port]** from the Type pull-down menu.
6. Click **[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 **[Open]**.
11. The wizard will return you to the previous dialog. Verify the path and file name are correct and click **[OK]**.
12. Select the model that corresponds to your device and click **[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 **[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 **[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 **[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 **[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 the Internet Services to configure the Print Driver in this environment.

Xerox Printer Installer

This section provides instructions on how to install 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then 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 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 Welcome Page will display, 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 on 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 **[Next]**.
10. Decide whether or not you want to make this printer your default printer, then click **[Next]**.
11. Click **[Finish]**. The printer will download to the Windows XP workstation.
12. Once the print driver has installed, open an application on the workstation and print a test page to verify operation.

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 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 the **[Details]** button.
7. Check the checkbox to add **[Print Services for UNIX]** if not already installed and click **[OK]**.
8. Click **[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 **[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 the location of your print driver.
11. Select the required driver then click **[Open]**.

12. When the Install from Disk screen appears, verify that the path and file name are correct, then click **[OK]**.
13. Select the model of your device from the list. Click **[Next]**.
14. The Name your Printer screen appears. Enter a printer name.
15. Decide whether or not you want to make this printer your default printer, then click **[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 **[Next]**.
17. Enter a location and comment in the **[Location and Comment screen]** (optional).
18. Select **[Yes]** to print a test page. Click **[Next]**
19. Click **[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 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 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then 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 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]**. Open the **[Printers]** folder.
2. Click on **[Add a Printer]**.
3. Select **[Add a network, wireless or Bluetooth printer]**.
4. Click on **[Next]**.
5. The **Select a printer** screen will display, select **[The printer that i want isn't listed]**, and click on **[Next]**.
6. 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]**.

7. 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.
8. Select your printer from the list and click on **[OK]**.
9. The **status bar** will display. In the **[Type a printer name],** check the **[Set as the default Printer]** checkbox.
10. Click **[Next]**.
11. The **You've successfully added.....** pop-up window will display, you can print a test page by clicking on the **[Print a test page]**.
12. Click **[Finish]**.

Create a New Print Queue

- Ensure you have the Internet Services Print and Fax Drivers CD (delivered with your device).
- The device must be configured with a valid IP address or host name, subnet mask and gateway address.
- LPD (Line Printer Daemon) must be enabled on the device.

Verify that LPR Port Monitor is Loaded

1. Click **[Start]**, **[Control Panel]** and double-click **[Programs and Features]**.
2. Double-click **[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]**. Open the **[Printers]** folder.
2. Click on **[Add a Printer]**.
3. Select **[Add a network, wireless or Bluetooth printer]**.
4. Click on **[Next]**.
5. The **Select a printer** screen will display, select **[The printer that i want isn't listed]**, and click on **[Next]**.
6. 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]**.
7. 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.
8. Select your printer from the list and click on **[OK]**.
9. The **status bar** will display. In the **[Type a printer name],** check the **[Set as the default Printer]** checkbox.
10. Click **[Next]**.

11. The **You've successfully added.....** pop-up window will display, you can print a test page by clicking on the **[Print a test page]**.
12. Click **[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]**. Open the **[Printers]** folder.
2. Right click the appropriate printer icon and select **[Properties]**.
3. Click the **[Configuration]** tab.
4. Click **[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.
5. Click **[Automatic]** to have the driver automatically configure the IP address of the device or click **[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.
6. Click on **[OK]**.
7. Click on the **[Installable Options]**.
8. If Bi-directional setup has not been enabled select the options that are installed on the device.
9. Click on **[OK]**.
10. Click on **[OK]** to close the Properties box.
11. Right click the printer within the Printers folder and select **[Printing Preferences]**.
12. 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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

  The Configuration Report will print. Verify the AppleTalk settings has been configured under AppleTalk.
- Locate the Internet Services Print and Fax Drivers CD. 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.
8. When the Welcome screen displays, click **[Continue]**.
9. Click **[Continue]**, then **[Agree]** to accept the Licence Agreement.
10. Select the required disk (if necessary) where you want to install the printer. Click **[Continue]**.
11. Click **[Install]**.
12. Click **[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 **[Add]**. The device will appear in the Printer List.
25. Select the printer and click the **[Show Info]** button.
26. Click **[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 **[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.

7

Authentication

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 email.

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:

- **Remotely on the Network** - The System Administrator can select one of these environments to provide network authentication:
  - Kerberos (Solaris)
  - Kerberos (Windows 2000/2003)
  - NDS (Novell)
  - SMB (Windows 2000/2003).
  - LDAP (Lightweight Directory Access Protocol).
- **Locally on the Device** - 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 301.
- **CAC (Common Access Card) / PIV (Personal Identification Verification)** - For information on this type of authentication, please refer to the CAC guide supplied with your device.

Administrators who choose to enable authentication locally are required to configure user accounts in the **User Information Database** (**Properties > Security > User Information Database > Setup**), refer to User Information Database on page 149

Authorization Overview

This feature works in conjunction with the Authentication feature to determine what an authenticated user is allowed to do.

Once 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 Administrators** Access - Users who has all access to the device and change the device settings.
- **Account Administrator** Access - these users have access to the accounting settings.
- **User**

There are two options for Authorization:

- **Locally on the Device (Internal Database)** - refers to the database included on your device.
- **Remotely on a 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 require 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 authenticated 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, please ensure the following items are available or 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)

Initially when **Setup** is selected (at your workstation web browser: **Properties > Security > Access Rights > Setup**), Step 1 of 3 for **Authentication Configuration** will display.

- **Authentication Configuration - Step 1 of 3**

  This screen explains the concepts of Authentication, Authorization, and Personalization.
  - **Authentication** - Determines that the person who logs in has given the proper credentials and is known to the system.
  - **Authorization** - Determines what an authenticated user can do, for example, the authenticated user has permission to use the Copy Service.
  - **Personalization** - Adds personal settings for the authenticated user optimizing productivity, for example, automatically enter my email address to the From field.
- **Authentication Configuration - Step 2 of 3**

  This page allows you to select methods for:
  - **Device User Interface Authentication**.
  - **Web User Interface Authentication**.
  - **Authorization**.
  - **Personalization**.

  Note: **Web User Interface Authentication** only needs to be defined if you have specified Xerox Secure Access as the method of authentication.
- **Authentication Configuration - Step 3 of 3**

  This page displays the current status and configuration of Authentication, Authorization and Personalization. This page is used for confirming or editing the authentication options that were established on Step 2 of 3.
- Once the **Authentication Configuration Steps** have been completed, click on the **[Finish]** button.

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)

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 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.

8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]/[Configure]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Remotely on the Network]** form the drop-down menu for **Device User Interface Authentication** and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page:
    a. Select **[Kerberos (Solaris)]** from the **Authentication Type** drop-down menu.
    b. In the **Default Key Distribution Center (Required)** area:
        - Enter details in the **[Realm]** field.
        - Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
        - If IPv4 or IPv6 Address is selected, enter the **[IP Address]** and **[Port]** and **[Backup IP Address]** and **[Port]** details of the default **Default Key Distribution Centre (Required)**.
        - If Host Name is selected, enter the **[Host Name]** and **[Port]** and **[Backup Host Name]** and **[Port]** details of the **Default Key Distribution Centre (Required)**.
    c. Enter details for up to 8 **[Alternate Key Distribution Centres (Optional)]** and backups, if required.
    d. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.
12. To set Authentication to control access to individual Services:
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
13. To set Authentication to control access to individual Features:
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.
14. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
15. 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)

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 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop-down menu for **Device User Interface Authentication**, and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page:
    a. select **[Kerberos (Windows 2000/2003)]** from the **Authentication Type** drop-down menu.
    b. In the **Default Domain Controller (Required)** area:
        - Enter details in the **[Domain]** field.
        - Select either **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button.
        - If IPv4 or IPv6 Address is selected, enter the **[IP Address]** and **[Port]** and **[Backup IP Address]** and **[Port]** details of the default **Default Domain Controller**.
        - If Host Name is selected, enter the **[Host Name]** and **[Port]** and **[Backup Host Name]** and **[Port]** details of the **Default Domain Controller**.
    c. Enter details for up to 8 **[Alternate Domain Controllers (Optional)]** and backups, if required.
    d. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.
12. To **set Authentication to control access to individual Services:**
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration** page.
13. To **Set Authentication to control access to individual Features**:
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.
14. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
15. 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 NDS (Novell)

Information Checklist

Before starting the procedure, please ensure the following item has been performed.

- Ensure the NetWare protocol is enabled on your device by printing a Configuration Report.

  At the Device:

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

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

  c. Touch **[Information Pages]**.

  d. Touch **[Configuration Report]**.

  e. Touch **[Print]**, then touch **[Close]**.

  The Configuration Report will print. Verify the NetWare settings configured under Network Setup. NetWare should read Enabled.

  For instructions on how to enable NetWare, refer to NetWare on page 101 of this guide.

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 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop-down menu for **Device User Interface Authentication**, and click on the **[Save]** button to return to the **Authentication Configuration** page.

   Note: Make sure that the NetWare protocol has been enabled per the instructions contained in this guide in the Network Installation section. For NDS you will need to supply the NDS tree and context.

10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page:

    a. Select **[NDS (Novell)]** from the **Authentication Type** drop-down menu.

    b. In the **Default Tree/Context (Required)** area, enter details in the **[NDS Tree]** and **[NDS Context]** fields.

    c. In the **Alternate Tree/Context (Optional)**, enter details for up to 2 **[NDS Tree]** and **[NDS Context]** field, if required.

    d. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

12. To **Set Authentication to control access to individual Services:**
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
13. To **Set Authentication to control access to individual Features:**
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.
14. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
15. 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)

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 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop-down menu for **Device User Interface Authentication**, and click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.
11. In the **Authentication Server** page:
    a. Select **[SMB (Windows 2000/2003)]** or **[SMB (Windows NT4)** from the **Authentication Type** drop-down menu.
    b. In the **Configuration (Required)** area, enter details in the **[Default Domain]** field.
    c. Check the **Optional Information** checkbox.
    d. Select either **[IPv4 Address]** or **[Host Name]** radio button.
    e. If IPv4 Address is selected, enter the **[IP Address]** and **[Port]** details in the required fields.

f. If Host Name is selected, enter the **[Host Name]** and **[Port]** details in the required fields.
g. In the Alternate Domains (Optional) area, enter details for up to 8 **[Alternate Domains (Optional)]**, if required.
h. Click on the **[Save]** button to save the settings and return to the **Authentication Configuration** page.

12. To **Set Authentication to control access to individual Services:**
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
13. To **Set Authentication to control access to individual Features:**
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.
14. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
15. 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

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 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Remotely on the Network]** from the drop-down menu for **Device User Interface Authentication**, and click on the **[Save]** button to return to the **Authentication Configuration** page.

   Note: LDAP can also simply be used as an Information (Personalization) server, supplying information to other Authentication servers being used on the network.
10. In the **Current Configuration** area, click on the **[Configure]** button for **Authentication Server**.

11. In the **Authentication Server** page:
    a. Select **[LDAP]** from the **Authentication Type** drop-down menu.
    b. In the **Configuration** area, click on the **[LDAP Settings]** link.
    c. In the **[Server Information]** area, select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button, and enter the **IP Address** and **Port** or the **Host Name** and **Port** of the Primary and Alternate LDAP Server.
    d. Specify the LDAP Server environment from the **[LDAP Server]** drop-down menu, this sets the default user mappings.
    e. Enter any further information, as required, in the **Optional Information** area.
        - **Search Directory Root** allows you to limit the LDAP search by entering the location on the server where the LDAP information is stored.
        - **Login Credentials to Access LDAP Server**: Select the **[None]** radio button if no login is required.
          If you select **[Authenticated User]** the device will use the login details entered by the user to access the device and the LDAP server. This option requires Authentication to be configured on the device.
          If **[System]** is 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.
        - **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.
        - **SSL**: If SSL is required, check the **[Enable]** checkbox.

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

        - If you want the device to verify that the server certificate is trusted, valid and has a fully qualified domain name (FQDN), check the **[Validate Repository SSL Certificate]** checkbox.

          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).
        - **Maximum Number of Search Results** (between 5 and 100). This is 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.
        - **Search Timeout:** There are two options. You can let the server use its timeout limit by selecting the [Wait LDAP Server Limit], or 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.
        - **[LDAP Referrals]:** if the primary LDAP server is connected to additional servers, the search will continue on those servers as well.
        - The **Perform Query on option** will help control the returns by allowing the LDAP query to be 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'.
    f. Click on the **[Apply]** button when done.

12. To configure Filters for LDAP (if required)
    a. Click on **[Custom Filters]** heading tab under the LDAP title.
    b. On the **Custom Filters** screen, under **LDAP Authentication** area, check the **[Append Base DN]** checkbox to select it.
    When enabled, 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]**.

    c. Select one or both of the **[Enable Custom Filter]** boxes, for the type of filter that you wish to apply.
    d. For the **[E-mail Address Book filter]**, 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 parenthesis. For example, to find all users that have an E-Mail attribute (mail enabled), type (objectClass=user) (mail=*). If you are not familiar with LDAP search strings, use an Internet browser search to find examples.
    e. For the **[User ID Query Filter]**, 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 parenthesis. 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.
    f. Click on the **[Apply]** button when done.
13. To **set Authentication to control access to individual Services:**
    a. Click on **[Setup]** in the directory link under **Access Rights** to display **Authentication Configuration** page, in the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
14. To **set Authentication to control access to individual Features:**
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.

    c. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
15. 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 Contexts for LDAP (Used when LDAP is enable via NetWare)

Contexts are used with the Authentication feature. The administrator can configure the device to automatically add an authentication context to the Login Name provided by the user.

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* of the device in the Address or Location field. 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 **[Protocol]** link.
7. Select **[LDAP]** in the directory tree.
   a. Click on **[Contexts]** heading tab under the LDAP title.
   b. Enter details in the **[Default Login Context]** field provided.
   c. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
8. 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 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.

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 **[Protocol]** link.
7. Select **[LDAP]** in the directory tree.
8. Click on **[Authorization Access]** heading tab under the LDAP title.
   d. 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.

e. 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 no access group is listed, all members will have access.

f. When done, click on the **[Apply]** button.

9. 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 **[Apply]** button.
10. 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 **[Apply]**.

11. Select the **[Feature Access]** tab.
    a. For the **Color Copying [Access Group]** field, enter the name of a access group, defined at the LDAP server, that you want to provide with Color Copying access to the device.
    b. To verify the groups, 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

    c. When done, click on the **[Apply]** button.
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.

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 an 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.

1. At your 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page is displayed, in the **Current Configuration** area click on the **[Edit Methods]** button for **Authentication**.
9. In the **Where is the Information Located?** area select **[Locally on the Device (Internal Database)]** from the drop-down menu for **Device User Interface Authentication** and **Authorization**, click on the **[Save]** button to return to the **Authentication Configuration** page.
10. In the **Current Configuration** area:
    a. Click on the **[View]** button for **Local User Information Database**.
    b. Click on the **[Add New User]** button, in the **User Identification** area, enter details of the new user in the **[User Name]**, **[Friendly Name]**, **[Password]** and **[Retype Password]** fields.

c. In the **[User Role]** area, select either one of the three radio button.

d. Click on the **[Add New User]** button to add the user, then press the **[Close]** button to return to the **Authentication Configuration** page.

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.

11. To **set Authentication to control access to individual Services:**
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkbox to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
12. To **set Authentication to control access to individual Features:**
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
    - **Standard Access - Only Lock Tools**
    - **Open Access - Unlock All Tools and Features**
    - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.

    c. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
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.

802.1X Authentication

The device supports 802.1X authentication based on the Extensible Application Protocol (EAP). 802.1X can be enabled for devices connected through both wired and wireless Ethernet networks. As described here, the 802.1X configuration is used to authenticate the device, rather than individual users. After the device has been authenticated, it will be accessible to users on the network.

The administrator can configure the device to use one EAP type. EAP types currently supported on the device are:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2

Information Checklist

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

- Create a user name and password on your authentication server which will be used to authenticate the Xerox device.
- Ensure your 802.1X authentication server and authentication switch are available on the network.

Enable 802.1X

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**.
6. At the Warning screen, touch **[Continue]**.
7. Touch **[802.1X]**.
8. Touch **[Enable]**.
9. Select the Authentication Method (EAP type) used on your network by touching the **[Authentication Method]**.
10. Touch **[Username]**.
11. Enter the user name required by your authentication switch and server.
12. Touch **[Save]**.
13. Touch **[Close]**. The network controller will now reset taking the device offline for several minutes.
14. 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, then touch **[Logout]** to exit the Tools pathway.

Configure 802.1X with Internet Services

In addition to enabling 802.1X at the device, 802.1X can be configured with Internet Services (the embedded HTTP server running on the device). Make sure that the HTTP and TCP/IP protocols are properly configured for your network before attempting to use your web browser to communicate with the device's HTTP server.

Note: Some ports in an 802.1X environment may not be open, preventing Internet Services screens from being displayed. If this is the case, enable and configure 802.1X first at the device as previously stated in this section, then use Internet Services to modify settings as required and stated below.

Note: 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 multifunction device rather than an individual user. After the device has been authenticated, it will be accessible to users on the network.

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 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 **[Security]** link.
6. Select **[802.1X]** in the directory tree.
   a. Check the **[Enable 802.1X]** checkbox.

b. Select the required **[EAP]** type from the **[Authentication Method]** drop-down menu.
c. Enter the **[User Name (Device Name)]** and **[Password]** required by your authentication switch and server.
d. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

7. 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 Xerox Secure Access, refer to Xerox Secure Access on page 301

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 (running LDAP in an ADS environment, for example) to communicate with the Secure Access Server providing that server with user credentialing information. A second Authentication Server 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

1. At your 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 **[Security]** link.
6. Click on the **[Access Rights]** link.

7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page displays, in the **Current Configuration** area, click on the **[Edit Methods]** button for **Authentication**.
   a. In the **Where is the Information Located?** area select **[Xerox Secure Access]** form the drop-down menu for **Device User Interface Authentication**.
   b. Select your required option from the **[Web User Interface Authentication]** 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 **[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.
   c. 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.

   d. Check the checkbox next to **[Automatically retrieve the following information for the authenticated user from LDAP: Home directory for the 'Scan to Home' service. E-mail address for the 'E-mail' and 'Internet Fax' services]** under **Personalization** is checked if you want to set the From address to the logged in user's e-mail address, when they log in via Secure Access.
   e. Click on the **[Next]** button to return to the **Authentication Configuration** page.
9. In the **Authentication -(Required)** 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** and **Port** or **Host Name** and **Port** fields.
   e. Enter the details in the **[Path]** field.
   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 **[Save]** when done.

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:

1. At your 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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree.
8. The **Authentication Configuration** page displays, Click on the **[Edit Methods]** button for **Authentication** in the **Current Configuration** area.
   a. In the **Where is the information located?** area, select **[Xerox Secure Access]** from the drop-down menu for **Device User Interface Authentication**, and select **[Remotely on the Network]** from the drop-down menu for **Web User Interface Authentication**. Click on the **[Save]** button to return to the **Authentication Configuration** page.

9. In the **Current Configuration** area, click on the **[Configure]** or **[Edit]** button for **Web User Interface Authentication**.
10. Follow the instructions to select the required Authentication Type.
    - See Authentication Configuration for Kerberos (Solaris) on page 129.
    - See Authentication Configuration for Kerberos (Windows 2000/2003) on page 130.
    - See Authentication Configuration for NDS (Novell) on page 132.
    - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003) on page 133.
    - See Authentication Configuration for LDAP/LDAPS on page 134.

    When you have configured the required Authentication Type, click on the **[Save]** button to return to the **Authentication Configuration** 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 134.

11. To **set Authentication to control access to individual Services:**
    a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
    b. On the **Service Registration** screen, check the checkboxes to select the services you want to display on the machine touch interface.
    c. Click on the **[Save]** button and return to the **Authentication Configuration**.
12. To **set Authentication to control access to individual Features:**
    a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
    b. In the **Tools & Feature Access** page, under **Presets**, select either:
        - **Standard Access - Only Lock Tools**
        - **Open Access - Unlock All Tools and Features**
        - **Custom Access**

    If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.

    c. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
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.

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.

8

Security

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.

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 network controller then the encrypted data remains protected because the encryption key is not stored on the network controller hard drive.

To Disable User Data Encryption

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 **[Security]** link.
6. Select **[User Data Encryption]** in the directory tree.
7. In the **[User Data Encryption Enablement]** area, select **[Disabled]**.
8. 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 form 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 127.

To Add a New User to the Database

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 **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **User Information Database** page, click on the **[Add New User]** button.
9. 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.
10. 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"**.
11. Click on the **[Add New User]** button to save the new user settings.

To Edit a User on the Database

Note: Accounting Administrator cannot access this page.

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 **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **User Information Database** page, click on the **[Edit]** link next to the user you want to edit.

9. 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.
10. Click on the **[Edit User]** button to save the changes.

To Delete a User

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 **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Setup]** in the directory tree.
8. On the **User Information Database** page, under the **User Name** column, check the user box you want to delete and click on the **[Delete]** button to delete the user.
9. A pop-up window will to 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

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 **[Security]** link.
6. Click on the **[User Information Database]** link.
7. Select **[Password Settings]** in the directory tree.
8. On the **Password Settings** page, in the **Password Rules** area:
   a. Enter the minimum length 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"**.
9. Click on the **[Save]** button to save your changes and return to the **User Information Database** page.

Admin Password

There are two options on this page:

- **New Password** - this option allows you to change password
- **Reset Policy** - this option allows you to either enable or disable Password Reset.

New Password

This page is part of the **Authentication Configuration Wizard**. It is also accessible from the Authentication Configuration page.

Note: The first time that Authentication Configuration is selected the **Device System Administrator Password** page appears. Use this page to change the default password before proceeding to any authentication configuration settings.

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 **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **New Password** tab is highlighted on the top of the screen.
8. In the **New Admin Password** area, enter detail in the **[New Password]** and **[Retype New Password]** fields.

   Note: The **User Name**: "admin" is not editable and is reserved for the Device Administrator Account.
   Do NOT use the username **"admin"** for any local or network accounts on the device.

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

Reset Policy

This page allows you to enable or disable the Password Reset Policy.

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 **[Security]** link.
6. Select **[Admin Password]** in the directory tree.
7. Ensure **Reset Policy** tab is highlighted on the top of the screen.
8. In the **Password Reset Policy** select either:
   - **Enable Password Reset**
   - **Disable Password Reset**

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

   Note: This policy will be applied if the admin password is forgotten!
   If enabled, the password can be reset to the Factory Default using directions available from Xerox Support.
   If disabled, a **chargeable service call** would be required if the password is forgotten.

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 will allow access to the device, and/or a list of addresses that cannot allow access to the device.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. 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 **[Security]** link.
6. 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 packet
   - **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 meant 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 packet 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).

f. **[Source Port]**: This selection is only available when the Protocol has been set to TCP. Enter 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 will not be applied.

g. **[Destination Port]**: This selection is only available when the protocol is set to TCP or UDP. Enter the destination port that the rule has been created to handle. If the incoming packet was not sent to this port, the rule will not be applied.

h. **[ICMP Message]**: This selection is only available when the protocol is set to ICMP. Select which ICMP Message the rule is meant to handle.

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, see Machine Digital Certificate Management on page 157.

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 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 **[Security]** link.
6. Select **[Audit Log]** in the directory tree.

   Note: You must enable SSL before enabling Audit Log.

7. In the **Enabling Audit Log on machine** area, check the **[Enabled]** checkbox for the **Audit Log**.

8. Click on the **[Apply]** button, then click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
9. Click on the **[Save]** button to save the Audit Log as a text file.
10. 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, and click on the **[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 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: For a scan-to-mailbox job there may not be an entry made in the Audit Log for this 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

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

8	IFAX
9	E-mail job
10	Audit Log Disabled
11	Audit Log Enabled

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)

Machine Digital Certificate Management

Machine Digital Certificates provide keys for encryption/decryption of data. It ensures the data is not tampered with and to validate 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, 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, please ensure the following items are available or 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.

To Create a Digital Certificate

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 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 **[Security]** link.
6. Select **[Machine Digital Certificate Management]** in the directory tree.

   Note: SSL cannot be implemented until a digital certificate is installed on the system.

7. In the **Machine Digital Certificate** area, the **Current Status** displays the current status of the device's digital certificate. By default, no certificate will be installed.
   Other status messages you may see:
   - **A Self Signed Certificate is established on this machine**:
     This indicates that a new certificate has been installed on this printer. A self-signed certificate does not contain a path to a Trusted Certificate Authority, and may result in certificate error messages at the Web browser when Internet Services is accessed via SSL
   - **A Certificate Signing Request was downloaded for processing by a Trusted Certificate Authority**:
     This occurs during the Create New Certificate process, but indicates the process is incomplete.
   - **Upload the Signed Certificate when it is received**:
     When a signed certificate is received from a Trusted Certificate Authority, use the Upload Signed Certificate function to copy it to the printer.

   a. Click on the **[Create New Certificate]** button.

   b. In the **Create New Certificate** area, select one of the following:
      - **Self Signed Certificate -** select this type of certificate if you have your own PKI infrastructure or other means of internal certificate authority.

- **Certificate Signing Request** - this type of certificate can be processed by a Trusted Certificate Authority.

Note: A self-signed 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.

8. Click on the **[Continue]** button.
9. If you selected **Self Signed Certificate**:
   a. Complete the Self Signed Certificate form with details for:
      - 2 Letter Country Code
      - State/Province Name
      - Locality Name
      - Organization Name
      - Organization Unit
      - E-mail Address
      - Days of Validity.

   Note: **Common Name** on the form is generated by the device and cannot be changed.

   b. Click on the **[Apply]** button to continue. Values from the form will be used to establish a self-signed certificate, and you will be returned to the main page.
10. If you selected **Certificate Signing Request**:
    a. Complete the Certificate Signing Request (CSR) form with details for:
       - 2 Letter Country Code
       - State/Province Name
       - Locality Name
       - Organization Name
       - Organization Unit
       - E-mail Address

    Note: **Common Name** on the form is generated by the device and cannot be changed.

    b. Click on the **[Apply]** button to continue. Values from the form will be used to generate a Certificate Signing Request.
    c. When the process is complete, you will be prompted to save the Certificate Signing Request. Right click on the link and select **[Save Target As]**.
    d. Save the Certificate to your hard drive and send it to a **Trusted Certificate Authority**.
    e. 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.

1. Click the **[Properties]** tab.

2. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
3. Click on the **[Login]** button.
4. Click on the **[Security]** link.
5. Select **[Machine Digital Certificate Management]** in the directory tree.
6. In the **Machine Digital Certificate** area:
   a. Click on the **[Upload Signed Certificate]** button.
   b. In the **Upload Machine Digital Certificate**, click on the **[Browse]** button to locate the signed certificate from the Trusted Certificate Authority and click on the **[Open]** button.
   c. Click on the **[Upload Certificate]** button.
   d. If successful, the Current Status in the **Machine Digital Certificate** area will show '**A Self Signed Certificate is established on this device**'.

   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"**.
7. To view installed certificates click the **[Trusted Certificate Authorities]** in the directory tree for **[Security]**. The installed certificate will appear in the list.

Enable Secure HTTP (SSL)

Once the device has a device server certificate, you can enable secure HTTP.

1. In the **Properties** menu, click on the **[Connectivity]** link.
2. Click on the **[Protocols]** link.
3. Select **[HTTP]**.
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.
6. 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 the **[OK]** button to continue.

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 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 EMail
- 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, see Machine Digital Certificate Management on page 157.

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 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 **[Security]** link.
6. Select **[IP Sec]** in the directory tree.
7. Ensure **[Security Policies]** tab is highlighted under the **IPsec** heading.
8. In the **Settings** area, check the **[Enabled]** checkbox to enable the IP Sec.
9. 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 enable 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.

10. In the **Define Policy** area, there are three policy options:
    - **Hosts**
    - **Protocols**
    - **Action**

    This area allows you to select setting for allowing or discarding Hosts and Protocol and what action to be taken.
11. For each individual option select settings from each drop-down menu.
12. Click on the **[Add Policy]** button.

Saved Policies

13. In the **Saved Policies** area, there will be a list of all the policies saved.
14. To delete a policy, highlight the policy and click the **[Delete]** button.
15. Also you can make individual policy to be prioritized by clicking the **[Promote]** and **[Demote]** buttons.

Disable IP Sec at the device

1. At the device, press the **<Log In/Out>** button to access the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter the Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. In Tools menu, touch **[Security Settings]**.
5. Touch **[Image Overwrite Security]**.
6. Touch **[IP Sec]**.
7. Touch the **[Disable IP Sec]** button, then touch **[Close]**.
8. Press the **<Log In/Out>** button to exit Tools pathway.
9. Touch **[Logout]**.

Host Groups

Host Group page allows you to view and manage host group. 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 Group saved and the details of each Host Group.

1. Form the **IP Sec** page, click on the **[Host Groups]** tab under **IPsec** heading.
2. 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.
3. 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.

4. 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.
5. 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.
      - **Subnet** - to specify a range of IP Addresses.
      - **All** - if all addresses of the IP type are to be included.

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.

6. Click on the **[Save]** button, then 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 Group** 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 Group** 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 IP Sec 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. In the **IP Actions** area, 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. 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 Internet Key Exchange (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]**.

   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]** 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 or ESP 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 Secs 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 IP Sec - Action page.

Trusted Certificate Authorities

A Trusted Certificate Authority is a Certificate Authority (CA) that is trusted to authenticate digital certificates. This page enables 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 Trusted Certificated Authorities Screen

The device exports the signed certificate to the client to establish an SSL/HTTPS connection.

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 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 **[Security]** link.
6. Select **[Trusted Certificate Authorities]** in the directory tree.

   The Trusted Certificate Authorities page shows any currently installed trusted root certificate in the **Installed Certificate** area.

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 Machine Digital Certificate Management on page 157.

1. At the **Trusted Certificate Authorities** screen, click on the **[Add]** button.
2. Click on the **[Browse]** 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 **[Upload Certificate Authority]** button.
4. The digital certificate will appear in the list of **Installed Certificates** area.

To Delete a Certificate

1. At the **Trusted Certificate Authorities** 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 **Trusted Certificate Authorities** screen, right-click on the **[Download the Generic Xerox Device CA]** link which appears at the bottom of the screen, under the **Installed Certificates** box.
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.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 your Workstation:

1. Open the web browser and enter the *IP address* 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 **[Security]** link.
6. Select **[802.1X]** in the directory tree.
7. 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.
   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.
8. Click on the **[Apply]** button to save changes.

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

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**, touch **[Continue]**.
6. In the **Network Settings** screen, touch **[802.1X Settings]**.
7. In the **802.1X** screen:
   a. Touch **[Enable]** button.
   b. Touch **[Authentication Method]** to select the authentication method form the drop-down menu.
   c. Touch **[Username]** and enter the username, and touch the **[Save]** to return to the **802.1X** screen.
   d. Touch **[Password]** and enter the password, and touch the **[Save]** to return to the **802.1X** screen.
   e. Touch **[Save]**.
8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

To Disable 802.1X

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 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 **[Security]** link.
6. Select **[802.1X]** in the directory tree.
7. In the **Configure 802.1X** area:
   a. For **Protocol**, uncheck the **[Enable 802.1X]** checkbox to disable this feature.
8. Click on the **[Apply]** button to save changes.
9. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.

3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Network Settings]**.
5. Touch **[Advanced Settings]**, touch **[Continue]**.
6. In the **Network Settings** screen, touch **[802.1X Settings]**.
7. In the **802.1X** screen:
   a. Touch **[Disable]** button.
   b. Touch **[Save]**.
8. Touch **[Close]**.
9. Press the **<Log In/Out>** button, then touch **[Logout]** to exit the Tools pathway.

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 20 minutes to complete. The device is taken offline until the overwrite is complete and any existing jobs in the print queue are terminated. 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 60 minutes to complete. The device is taken offline until the overwrite is complete and any existing jobs in the print queue are terminated. The overwrite process cannot be cancelled.

Information Checklist

Before starting the procedure, please ensure the following item is available or has been performed:

- Ensure the device is fully functioning in its existing configuration prior to installation.

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 **[Information Pages]**.

4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close].**

On the Configuration Report, check under the **Security** heading if On Demand Image Overwrite is an installed 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. The device screen indicates a status of 'Diagnostics Mode'- this mode is used by a Customer Service Representative when servicing the device. The device should not be used to perform any jobs and the power should not be switched off while an Overwrite is being performed.

At the Device:

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. From Tools, touch **[Security Settings]**.
5. Touch **[Image Overwrite Security]**.
6. Touch **[On Demand Overwrite]**.
7. Select one of the following:
   - **Standard**
   - **Full**
8. Touch **[Overwrite Now]** to start the Image Overwrite process.
9. The Image Overwrite Confirmation screen will appear, touch **[Overwrite]** to begin.The device will be taken offline and will be unable to receive any incoming jobs.
10. 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.
11. Once rebooted, the Disk Overwrite confirmation report is printed. This details the status and time of the overwrite.
12. 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. The device screen indicates a status of the 'Diagnostics Mode'- this mode is used by a Customer Service Representative when servicing the device. The device should not be used to perform any jobs and the power should not be switched off while an Overwrite is being performed.

Information Checklist

Before starting ensure the following items are available or 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:

1. 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 **[Security]** link.
6. Click on the **[On Demand Overwrite]** link.
7. Click **[Manual]** in the directory tree.
8. Click on the **[Start]** button for either **Standard** or **Full**. image overwrite.
9. A confirmation pop-up screen appears, click on the **[OK]** button. 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.
10. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
11. Click on the **[Login]** button.
12. 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. Once rebooted, the Disk Overwrite confirmation report will print. 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**'.

    Note: If you wish to backup jobs and folders prior to Full Overwrite, on the **On Demand Overwrite** 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 275.

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.

1. At your Workstation, open the web browser and enter the *IP address* of the device in the Address or Location field. 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 **[Security]** link.
6. Click on the **[On Demand Overwrite]** link.
7. Select **[Scheduled]** in the directory tree.
8. 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 you require for **Type**.
   d. Click on the **[Apply]** button.
   e. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
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.

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.

Once 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 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

On the Configuration Report, check under the **Security** heading if Immediate Image Overwrite is an installed option.

To Disable or Enable Immediate Image Overwrite

At the Device

1. Press the **<Log In/Out>** button to access the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. If necessary, press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. From Tools, touch **[Security Settings]**.
5. Touch **[Image Overwrite Security]**, then **[Immediate Overwrite]**.
6. Touch **[Enable]** or **[Disable]**, then touch **[Save]**. The change in status will be immediately effective.
7. Press the **<Log In/Out>** button, touch **[Logout]** to log out of 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 **[Completed Jobs]** tab (if necessary).
3. Touch the drop-down menu and select **[All Jobs]** (if necessary).
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]**.

PostScript (R) Passwords

The PostScript language has some powerful utilities that could be used to compromise the security of a system. These utilities can be password protected so as to prevent abuse. This feature is concerned with the ability to set the various passwords. In addition, we have extended the PostScript language with custom operators; the same passwords could be used to secure the custom extensions.

Without a password in place, anyone with slight knowledge of Postscript can potentially abuse the system. They can use the **Startjob** and **Exitserver** operators, change the system parameters, and run jobs that can re-define PostScript operators and so on.

There are three passwords defined in the PostScript Password page, as follows:

- **Start Job Password** - A write-only string. Authorizes the use of startjob and exitserver
- **Run Start Job** - An integer. Controls the execution of the Sys/Start file, which runs as an unencapsulated job and loads definitions into VM. This parameter should only ever be set to zero or one in normal use.
- **System Parameters Password -** A write-only string. Controls use of the setsystemparams and setdevparams operators

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 **[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 **[Security]** link.
6. Click **[PostScript (R) Passwords]** in the directory tree.
7. On the **PostScript (R) Passwords** page, in the **Run Start Job** area select either **[Disabled]** or **[Enabled]** for **StartupMode**.
8. Enter details in the **[Password]** and **[Retype Password]** fields for **System Parameters Password** and/or **Start Job Password**.
9. You can also check the **Select to save new password** checkbox for **System Parameters Password** and/or **Start Job Password**.
10. When finished, click on the **[Apply]** button.

9

Workflow Scanning

Workflow Scanning allows a user to scan an original document, convert it to an electronic file, and distribute and archive that 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 enables 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, please ensure the following items are available or have been performed:

- Ensure the device is fully functioning 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 Workflow Scanning. The Internet Services function is accessed through the embedded HTTP server on the device and allows System Administrators to configure scan settings by using an Internet browser.

Configure General Settings

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 the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Click on the **[General]** link in the directory tree.

   Note: The Confirmation Sheet specifies the success or failure of the Workflow Scanning job.

7. In the **Settings** area, select one of the following options from the **[Confirmation Sheet]** drop-down menu:
   a. **Errors only** - select to prints a Confirmation Sheet only when the job is unsuccessful.
   b. **On** - select to print a Confirmation Sheet after every Workflow Scanning job
   c. **Off** - when selected, turns off the Confirmation Sheet printing function.
8. In the **Distribution Templates** area:
   a. Under **Maximum Number or Job Templates**, it will display the maximum number of job templates that can be viewed from the device's control panel.
   b. 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.
   c. 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.

9. 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** - to have a standalone server prompt device users for access. This works well for small offices without an Authentication server.
   - **Prompt if Authenticated User Does Not Match Template Owner** - to prompt authenticated system credentials do not match the template owner.
   - **None** - if no user authentication is required.

10. In the **Job Log** area, for **Optional Information** Check on **[Username]** 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.
11. Click on the **[Apply]** button.
12. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

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, please ensure the following items are available or 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

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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, 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.

9. 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]** button.
   d. Enter the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the FTP location for **[Alt1 Repository Server]**.
   e. Type in the path to the repository in **[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
   g. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
   h. 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.

Go to the Device

1. Touch the **[Workflow Scanning]** icon on the touch screen.
2. Touch **[All Templates]**.
3. Select **[All Templates]** from the **[All Templates]** drop-down menu.
4. Select **[Advance Setting]** tab.
5. Touch the **[Update Template]** icon.
6. Touch **[Update Now]**.
7. Touch **[Confirm]**, touch **[Use Partial List]**.

8. Touch **[Close]**.
9. Touch the **[Workflow Scanning]** tab.
10. Select the **[Default]** template and place a document in the document handler.
11. View template details on the monitor.
12. Press the **<Start>** button to scan the document.
13. Check the scan folder on your file server to verify the image was filed.

The Next Step is to proceed to the General Settings, see Configure General Settings on page 180.

NetWare NCP (NetWare Core Protocol)

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close].**

  The Configuration Report will print. Verify the NetWare settings configured under Network Setup.

  NetWare should read Enabled.

  For instructions on how to enable NetWare refer to the NetWare topic in the Protocol section of this guide.
- 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:

1. Open the web browser and enter the *IP address* 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.

7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, 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.
9. 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. In the **[Alt1 Repository Server]** field, enter the host name of the NetWare server.
   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 **[Document Path]** field.
   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
   i. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
   j. Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.
   k. Click on the **[Save]** button to accept the changes.

At the Device:

1. Press the **<All Services>** button.
2. Touch **[Workflow Scanning]** on the touch screen.
3. Touch the **[Workflow Scanning]** tab.
4. Select **[All Templates]** from the **[All Templates]** drop-down menu.
5. Select the **[Default Template]** and place a document in the document handler.
6. View template details on the monitor.
7. Press the **<Start>** button to scan the document.
8. Check the scan repository on your server to verify the image was filed.

The Next Step is to proceed to the General Settings, see Configure General Settings on page 180.

Server Message Block (SMB)

Information Checklist

Before starting the procedure, please ensure the following items are available or 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:

1. Open the web browser and enter the *IP address* 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, 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.

9. 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 the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the SMB location for **[Alt1 Repository Server]**.
   e. Type in the share name in **[Share Name]** field.
   f. Type in the path to the repository in **[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

h. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.

i. 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.

At the Device:

1. Touch the **[Workflow Scanning]** button on the touch screen.
2. Touch the **[Workflow Scanning]** tab.
3. Touch the **[Show]** button.
4. Select **[All Templates]** from the **[All Templates]** drop-down menu.
5. Select the **[Default]** template and place a document in the document handler.
6. View template details on the monitor.
7. Press the **<Start>** button to scan the document.
8. Check the scan folder on your file server to verify the image was filed.

The Next Step button is to proceed to the Configure the Default Template instructions.

HTTP/HTTPS

Information Checklist

Before starting the procedure, please ensure that the following items are available and/or the 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:

  a. Open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

  b. Click the **[Properties]** tab.

  c. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.

  d. Click on the **[Services]** link.

  e. Click on the **[Workflow Scanning]** link.

  f. Select on the **[File Repository Setup]** link.

  g. Click on the **[Add New]** button in the File Repository Setup area, or the **[Edit]** button (If the default File Repository has been set).

h. Select **[HTTP]** or **[HTTPS]** from the **[Protocol]** drop-down menu.
i. Click on the **[Get Example Scripts]** link under *Script Path and Filename:* to download an example script in **PHP**, **ASP** or **Perl** language:
j. Select an appropriate *Script Language* file which is supported by your HTTP Scan Repository server.
k. Right click on the required script and select **[Save Target As...]** to save the file to your HTTP Scan Repository server.
l. Save the **[.zip]** or **[.gz]** file to a location on the desktop and extract it.
m. 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:

1. Open the web browser and enter the *IP address* 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[File Repository Setup]** in the directory tree.
8. Click on the **[Add New]** button in the File Repository Setup area, 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.

9. 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 the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the HTTP or HTTPS server for **[Alt1 Repository Server]**.
   e. 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.
   f. Enter the script path and filename you downloaded and saved on your desktop earlier in the **[Script path and filename (from HTTP root)]** field.
   g. 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***.
   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
   i. Enter a **[Login Name]** and **[Password]**, if the system will be directly accessing the file server.
   j. Check the **[Select to Save New Password]** checkbox, if you need to change the password for an existing Login Name.
   k. Click on the **[Save]** button to accept the changes.

At the Device:

1. Touch the **[Workflow Scanning]** button on the touch screen.
2. Touch the **[Workflow Scanning]** tab.
3. Select **[All Templates]** from the **[All Templates]** drop-down menu.
4. Select the **[Default]** template and place a document in the document handler.
5. View template details on the monitor.
6. Press the **<Start>** button to scan the document.
7. Check the scan folder on your file server to verify the image was filed.

The Next Step button is to proceed to the Configure the Default Template instructions.

Configuring Validation Servers

The Validation Servers link within Internet Services enables you to configure a Validation Server that will verify metadata. Metadata is an 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 has 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, please ensure the following items are available or 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.

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 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 **[Workflow Scanning]** link.
7. 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.
8. 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.

9. 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 or Hostname of the Validation Server and the port number.

   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** screen.
10. To **Delete** a Validation Server from the list:
   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:

1. Open the web browser and enter the *IP address* or location 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Scanning Web Services]** in the directory tree.
8. 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 160.
   - **Scan Template Management** - displays the status of the Scan Template Management service. Click on the **[Settings]** button to enable or disable this HTTP Web Service.

- **Scan Extension** - displays the status of the Scan Extension service (enabled or disabled). Click **[Settings]** button to enable or disable this HTTP Web Service.

9. For **Scan Template Management** and **Scan Extension** click on the **[Settings]** button to display the **HTTP - Web Services** page.
   c. Check the **[Enable]** checkboxes for the individual services you want and/or uncheck to disable required service.
   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. Once 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.

1. At your Workstation, open the web browser and enter the *IP address* or location 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Default Template]** in the directory tree.
8. 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, 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 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.

1. To add an additional file destination or to edit an existing file destination, in the **File** area, click on the **[Add]** or **[Edit]** button, the **File Destination** page will display.

2. In the **File Destination** area:
   a. From the **[Filing Policy]** drop-down menu, select one of the following option to set the behavior when a file name conflict exists:
      - **Rename New File** - this adds an incrementing numeric value to the file name.
      - **Overwrite Existing File** - this deletes the previous file with the new one.
      - **Do Not Save** - the new file is not saved.
      - **Add Date to Name** - the current date and time are appended to the file name.
   b. The **File Destination** identifies the selected file repository by its descriptive name, form the drop-down menu select the repository name.

   Note: When in **Edit** mode, this is a display only field.

   c. **Protocol** identifies the protocol (**FTP**, **SMB**, **HTTP**, **HTTPS**) used to communicate with the file repository.
   d. **Host Name and Port** identifies the host of the repository.
   e. **Document Path** identifies the file path to the repository.
   f. In the **[Add (Optional)]** field, specify a subdirectory for all scanning through this template.
   g. **Login Name** displays the account name used to access the repository.
3. Click on the **[Apply]** button to return to the Default Template page.

Fax

In the **Default Template** page, 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 enables 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.

- 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 file from the list and click the **[Edit]** button. This brings up the **Add Document Management Field** page.
- To delete a field, highlight a Document Management file from the list and click on the **[Delete]** button.

The following fields are available:

1. In the **Document Management Fields** 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 a 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. The **[Default Value]** field is an optional requirement. The information entered defines the actual data that is to be assigned to that particular scan job. This field can be created blank or the user may edit this value at the device user interface screen.

   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 prevent 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 changes the Workflow Scanning settings, click on the **[Edit]** button, this will display the **Workflow Scanning** page.

1. In the **Workflow Scanning** area:
   a. For **[Output Color]**, select one of the following:
      - Auto Detect
      - Color
      - Black (Black and White)
      - Grayscale

   Note: If you select Black as the Output Color, the JPEG option is not available on the Filing Options page. You can only select Color as the Output Color if you have a color scanner attached to your printer.

   b. 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.
   c. The **Original 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.
      - **Map** - this is best for black and white or color line drawings and other printed materials of this type.
      - **Newspaper/Magazine -** this is best for scanning materials produced with an offset printer.
   d. For **[How Original was Produced]**, select one of the following media type used of the original document:
      - **Printed Original**
      - **Photocopied Original**

- **Photograph**
- **Inkjet Original**
- **Solid Ink Original**

e. **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. To changes the Advanced Settings, click on the **[Edit]** button, this will display the **Advanced Settings** page.
2. In the **Advanced Settings** area:

a. For the **Image Options**, adjust the following options:

- **Lighten / Darken -** use the controls (left and right arrow button) to adjust the overall brightness reproduction compared to the original.
- **Soften / Sharpen** - use the controls (left and right arrow button) to adjust how much edge sharpening is used.
- **Pastel / Vivid** - use the controls (left and right arrow button) to adjust how much color is reproduced compared to the original.

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 button) 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. For **Resolution**, select from the **[Resolution]** drop-down menu the settings from which the scan service shall output the scanned input image. Changing the resolution affects the amount of detailed 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 changes the Layout Adjustment settings, 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 option:
      - **Upright Images** - this instructs the printer that the original document pages are loaded with the top of the page at the top of the document feeder.
      - **Sideways Images** - this instructs the printer that the original document pages are loaded sideways (the top of the page rotated to the left).
      - **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:
      - **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 changes the Filing Options settings, 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.
      - **JPEG (.JPG)** - select this for Full Color or Grayscale documents. Creates a .JPG file name extension.
      - **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, 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, click on the **[Edit]** button in the **Workflow Scanning Image Settings** area.
2. In the **Fast Web Viewing Options** area, check the **[Optimized for Fast Web Viewing]** checkbox 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 defaults to 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 **[Enable]** 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 allows you to set compression type you want to be enabled by default on the device.

1. To change settings for Compression Capability, click on the **[Edit]** button in the **Compression Capability** area.
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. Allows for fast scan and viewing performance but creates larger file sizes
   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. 3-

Layer Compression is a less aggressive format. For that reason, 3-Layer Compression does not provide as much image enhancement and file size reduction as the Multi-Mask Compression format.
The MRC Compression settings enable 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 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 **[Enable]** checkbox to enable Image Compression.

3. In the **TIFF Setting** area:
   a. For **TIFF Color Compression**, select one of the following option:
      - **TIFF 6.0 (old JPEG)** - select this option utilizes the most universally compatible version of the JPEG compression format.
      - **TIFF 6.0 Supplement 2 (New JPEG)** - this is an update to the TIFF 6.0 specification and provides a more fault-free JPEG compression algorithm, but may not be compatible with older graphics software.
      - **LZW (Lempel-Ziv-Welch)** - this is a lossless compression method yielding very high compression efficiency. This works best for files containing lots of repetitive data, such as is the case with text and monochrome images. LZW has long been associated with TIFF and GIF images. This compression algorithm was widely used in Adobe Photoshop, until version 6, and Adobe Acrobat, until version 5.
4. 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.

Display Settings

This feature allows you to set a user's template to be displayed on the top position in the list of templates. Allows you to hide or show the default template in the template list and also allows you to set the feature to select the top position template automatically.

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 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 **[Workflow Scanning]** link.
7. Select **[Display Settings]** in the directory tree.
8. In the **Template Order** area:
   a. In the **Templates** list, select the template you want on 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.
9. In the **Default Template Display** area, select one of the following:
   - **Show Default Template in the Templates list**
   - **Hide 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.
10. In the **Template Selection** area, select one of the following:
    - **Automatically select the top position template** - with this option, the top positioned template will be highlighted automatically.
    - **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.
11. Click on the **[Apply]** button.

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 **<All Services>** button.
2. Touch **[Workflow Scanning]** on the touch screen.
3. Touch the **[Advanced Settings]** tab.
4. Select **[Update Templates]** to display the Update Template screen.

   The following information will be displayed on the screen:

- **Last Updated** - this will display the date and time of the last update.
- **Status** - this will display the status of the last update.

5. Select **[Update Now]**.
6. Touch **[Confirm]**.

   Note: If you are not using a template pool repository, when selecting **[Update Now]** will display only a partial list of templates.

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:

1. Open the web browser and enter the *IP address* 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 **[Services]** link.
6. Click on the **[Workflow Scanning]** link.
7. Select **[Custom File Naming]** in the directory tree.
8. 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.
9. If **Auto** is selected:
   a. In the **Name** area, enter text that will be prefix of the automatic file name. The device will add numbers to the end of the text you enter to complete the file name.
10. 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 filed.
       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 filed.
    c. You can position the option you have selected in your own prioritized order, by using the up and down arrow in the **Position** area.

11. 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)	% m (month)
% T (time)	% d (day of month)
% Y (year)	% sn (device serial number)
% H (hour)	% ui (user id)
% M (minute)	% ji (job id)
% S (second	

    These variables can be in any order desired.
12. When complete, click on the **[Apply]** button.
13. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

Set up Remote Template Pool Repository

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 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 **[Workflow Scanning]** link.
7. Click on the **[Advanced]** link.
8. Select **[Template Pool Setup]** in the directory tree.

FTP Server

1. From the **Template Pool Setup** screen, 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 the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the FTP server in the **[Template Pool Server]** 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, if the system will be directly accessing the file server.

   Note: A Login (account) Name and (server) Password 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

1. From the **Template Pool Setup** screen, in the **Settings** area, select **[NetWare]** from the **Protocol** drop-down menu.
2. Enter details in the following fields:
   - **Template Pool Server** - 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, if the system will be directly accessing the file server.

   Note: A Login (account) Name and (server) Password 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** screen, in the **Settings** area, select **[SMB]** from the **Protocol** drop-down menu.
2. Select either the **[IPv4 Address]** or **[Host Name]**.
3. Enter the **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the SMB server in the **[Template Pool Server]** 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, if the system will be directly accessing the file server.

   Note: A Login (account) Name and (server) Password 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** screen, 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 **[IP Address]** and **[Port]** or **[Host Name]** and **[Port]** of the FTP server in the **[Template Pool Server]** field.
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 enables file transfers with the server. For example: ***/directory name/folder name)***.
   Click on the **[Get Example Scripts]** link to download a working example scripts.
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, if the system will be directly accessing the file server.

   Note: A Login (account) Name and (server) Password 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"**.

10

Scan to Home

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]** button on the Services screen of the user interface. The device queries LDAP to acquire the authenticated user’s home directory, or appends the authenticated user’s login name to a predefined network home path.

Information Checklist

Before starting the procedure, ensure the following items are available or 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 privileges.

Enable and Configure Scan to Home

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 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 **[Scan to Home]** link.
7. Select **[General]** in the directory tree to display the Scan to Home page.
8. In the **Setup** area:
   a. Check the **[Enabled]** checkbox for **Status**.
   b. If a friendly (descriptive) name has been assigned for the external server, enter the name in the **[Friendly Name]** filed, type in a name of up to 127 characters for the template that will appear in Template Details 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 can be created on the device by the Workflow Scanning, Scan to Mailbox and Scan to Home features with the same name.
9. 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.
10. 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.
11. 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 to 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.*

12. 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.
13. 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.
14. 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.

11

Scan to Mailbox

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, please ensure the following items are available or 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 **[Information Pages]**.
  d. Touch **[Configuration Report]**.
  e. Touch **[Print]**, then touch **[Close]**.

  Check under the **Services** heading to verify Workflow Scanning enablement.

Enable Scan to Mailbox

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 the **[Properties]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Scan to Mailbox]** link.
6. Select **[Enablement]** from the directory tree.
7. In the **Feature Enablement** area, check the following checkboxes:

- **Enable Scan to Mailbox** - to activate this feature on the device. Once 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.

8. Click on the **[Apply]** button.
9. 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 / disable encryption of user data on the **User Data Encryption** page, see User Data Encryption on page 149.

Create a New Mailbox

To create a new storage folder (mailbox) on the device's hard drive for receiving scanned images. When a registered user creates a folder, only that user (or a System Administrator) can view, edit or delete the folder's content.

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 213.

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 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. Click on the **[Create Folder]** link to display the **Create Folder** page to create a new folder.
5. In the **New Folder** area:
   f. 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.

   It is possible to have Scan to Mailbox folders with the same name as scan templates created with the Network Scanning and Scan to Home features. However, Scan to Mailbox templates display a '#' symbol on the device Network Scanning screen.

   g. 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.
   h. Enter the password again to confirm in the **[Confirm Folder Password]** field.
6. Click on the **[Apply]** button.

Personalize Settings or Modify Settings

This option allows you to change the attributes settings for your folder.

1. Click the **[Scan]** tab.
2. In the **Scan to Mailbox** area, select either the **[Default Public Folder]** or your personal folder.
   i. Enter the password for the folder in the **[Folder Password]** field.
   j. Click on the **[OK]** button.
   k. Click on the **[Personalize Settings]** button.

   If you select the Default Public Folder, click on the **[Modify 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 **[Output Color]**, select one of the following:
      - Auto Detect
      - Color
      - Black (Black and White)
      - Grayscale

      Note: If you select Black as the Output Color, the JPEG option is not available on the Filing Options page. You can only select Color as the Output Color if you have a color scanner attached to your printer.

   b. 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.
   c. The **Original 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.
      - **Map** - this is best for black and white or color line drawings and other printed materials of this type.
      - **Newspaper/Magazine -** this is best for scanning materials produced with an offset printer.
   d. For **[How Original was Produced]**, select one of the following media type used by that represents the original document:

- **Printed Original**
- **Photocopied Original**
- **Photograph**
- **Inkjet Original**
- **Solid Ink Original**

e. **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 **Personalized 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 button) to adjust the overall brightness reproduction compared to the original.
      - **Soften / Sharpen** - use the controls (left and right arrow button) to adjust how much edge sharpening is used.
      - **Pastel / Vivid** - use the controls (left and right arrow button) to adjust how much color is reproduced compared to the original.

   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 button) 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. For **Resolution**, select from the **[Resolution]** drop-down menu the settings from which the scan service shall output the scanned input image. Changing the resolution affects the amount of detailed 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 **Personalized 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 option:

      - **Upright Images** - this instructs the printer that the original document pages are loaded with the top of the page at the top of the document feeder.
      - **Sideways Images** - this instructs the printer that the original document pages are loaded sideways (the top of the page rotated to the left).
      - **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:

      - **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 **Personalized 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.
      - **JPEG (.JPG)** - select this for Full Color or Grayscale documents. Creates a .JPG file name extension.
      - **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 **Personalized 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 accept the changes, and return to the **Personalized 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, check the **[Optimized for Fast Web Viewing]** checkbox 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 defaults to 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 **[Enable]** to compress the resulting searchable files.
4. Click on the **[Apply]** button to accept the changes, and return to the **Personalized 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. Allows for fast scan and viewing performance but creates larger file sizes
   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. 3-Layer Compression is a less aggressive format. For that reason, 3-Layer Compression does not provide as much image enhancement and file size reduction as the Multi-Mask Compression format.
The MRC Compression settings enable 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. In the **TIFF Setting** area:
   a. For **TIFF Color Compression**, select one of the following option:
      - **TIFF 6.0 (old JPEG)** - select this option utilizes the most universally compatible version of the JPEG compression format.
      - **TIFF 6.0 Supplement 2 (New JPEG)** - this is an update to the TIFF 6.0 specification and provides a more fault-free JPEG compression algorithm, but may not be compatible with older graphics software.
      - **LZW (Lempel-Ziv-Welch)** - this is a loss less compression method yielding very high compression efficiency. This works best for files containing lots of repetitive data, such as is the case with text and monochrome images. LZW has long been associated with TIFF and GIF images. This compression algorithm was widely used in Adobe Photoshop, until version 6, and Adobe Acrobat, until version 5.
4. Click on the **[Apply]** button to accept the changes and return to the Personalized Settings page.

Configure Scan to Mailbox

Storage Capacity

To view the information on the amount of hard drive space being consumed by files in Mailboxes:

1. Click the **[Properties]** tab.

2. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**, and click on the **[Login]** button.
3. Click on the **[Services]** link.
4. Click on the **[Scan to Mailbox]** link.
5. Click on **[Capacity]** in the directory tree to display the **Capacity** page.
6. In the **Capacity** area, the following information are displayed:
   - **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 capacity available for document storage.
   - **Percentage Used:** The amount of storage capacity, 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**

1. From the **Scan to Mailbox** link, click on **[Files]** in the directory tree.

   The **Files** page allows administrators to delete files stored in Scan to Mailbox folders.
2. 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.
3. 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.

1. From the **Scan to Mailbox** link, click on **[Folders]** in the directory tree.
2. 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"**.
3. 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?"**.
4. 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.

1. From the **Scan to Mailbox** link, click on **[Scan Policies]** in the directory tree.
2. In the **Scan Policies** area, check the required checkboxes:
   - **Allow scanning to Default Public Folder** - enable 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 must 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.

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

   Note: To see individual Mailboxes, click the Scan tab of Internet Services. To scan to these mailboxes, refer to the directions in the **Interactive User Guide** delivered with your device.

Use Scan to Mailbox

At the Device:

1. Press the **<All Services>** button.
1. Touch the **[Workflow Scanning]** icon.
2. Touch your mailbox folder template in the **All Template** 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 to scan 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 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 **[Go]**.
   c. To delete the image select **[Delete]** from the drop-down menu and click **[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 **[Go]**.
8. To remove all files from your mailbox, click the **[Delete All]** button.
9. To change your mailbox folder password or to remove your mailbox folder, click **[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?"**.

12

E-mail

The E-mail feature enables 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 127 of this guide. Authentication can be configured after E-mail has been installed.

Information Checklist

Before starting ensure the following items are available or 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.
- Obtain the IP Address or Host Name of a functional SMTP mail server that accepts inbound mail traffic.
- 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

Print a Configuration Report:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

Check under Services on the Configuration Report to verify if E-mail is enabled.

To Verify or Configure your TCP/IP Domain Name (if necessary)

1. At your 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 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Verify or re-configure the Domain for this device in the **[Domain Name]** box, for example abc.xyz.company.com. Note that it is preferable for the mail server to reside in the same domain as that of the device.

   Note: If Dynamic Addressing has been set on the device (DHCP, DHCP/AutoNet, BootP or RARP) the Domain Name will not be accessible. If you need to change it, select **[Static]** from the **IP Address Resolution** drop-down menu.

9. Click on the **[Apply]** button to implement any changes. If required, click the **[Undo]** button to cancel any changes made and return to the previous values.

Configure an SMTP Server on the device

1. At your 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 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.

7. Select **[SMTP E-mail]** 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**
   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 **[ColorQube 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.
8. 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 when 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 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: System** - when selected, each user will need to enter the system credentials specified on the SMTP Server configuration screen.
9. Click on the **[Apply]** button to implement any changes.

Configure General E-mail Settings

1. At your 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 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 **[E-mail]** link, select **[Defaults]** in the directory tree.

General

7. In the **General** area, click on the **[Edit]** button.
   a. To change the e-mail **[From Address]**, enter a valid e-mail address.
   b. Optional Step: Enter a **[From Name]**.
   c. If LDAP is configured, 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 select to add the following details in the message:
      - User Name
      - E-mail Address
      - Number of Images attached to the e-mail
      - Attachment File Type (TIFF, JPEG)
      - Device Name (ColorQube)
      - Device Location
      - Serial Number
      - IP Address
      - MAC Address
   f. In the **[Signature]** entry box enter text that you want to appear as the default signature in every e-mail.
   g. 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.
      - **[On Errors Only]** - This setting will produce a Confirmation Sheet only when error detected.
   h. Check the **[Enable]** checkbox for **Auto Send to Self**, 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. The **Only Send to Self** feature, if selected, will automatically include the Authenticated user's e-mail address in the 'To:' field. Additionally, the New Recipient and Address Book buttons will be disabled, preventing the user from adding any additional recipients.

j. Click on the **[Save]** button to implement changes and return to the **Default** page.

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**, click on the **[Edit]** button in the **Scan to E-mail** area.
2. Select the required option for **[Output Color]**.

   Note: If you select Black as the Output Color, the JPEG option is not available on the Filing Options page. You can only select Color as the Output Color if you have a color scanner attached to your printer.

3. Select the required document scanning option for **[2-Sided Scanning]**.
4. Select the required method used to optimize the quality of your scanned output images based on the content in your original documents for **[Original Type]**.
5. Select the option that best describes the **[How Original was Produced]** of your e-mail documents.
6. Select the required option used to optimize scan settings to match the intended purpose of the scanned document for **[Scan Presets]**.
7. Click on the **[Apply]** button to accept the changes.

Advanced Settings

Advanced settings allows you to select options as follows:

- **Image Options** - allows you to lighten - darken, soften - sharpen, or pastel - vivid the image to be scanned.
- **Image Enhancement** - prevents 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 **E-mail > Default** screen, click on the **[Edit]** button in the **Advanced Settings** area.
2. Select the required options in the **[Advanced Settings]** area.
3. Click on the **[Apply]** button to implement changes and return to the **Default** page.

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 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 accept changes and return to the **Default** page.

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, JPEG, 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 **Default** page.

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 allow 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.
- **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 **Default** page.

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 email 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 email recipients.

The majority of word processing or spreadsheet packages will allow you to create a CSV file. A selection of email 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 device supports two types of address book:

- **Internal** - A global address book provided by LDAP (Lightweight Directory Access Protocol) services.
- **Public** - An address book created from a list of names and 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.

LDAP Addressing - Internal Address Book

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

For LDAP Addressing, see LDAP Addressing - Internal Address Book on page 229.

For Public Address book, see To Create a Public Address Book on page 233.

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 enables 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, see Authentication on page 127.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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:

1. Open your web browser and enter the *IP address* or *Host Name* 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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[LDAP]** in the directory tree.
8. In **Server Information** area:
   a. select either the **[IPv4 Address]**, **[IPv6 Address]** or **[Host Name]** radio button and enter the **IP Address** and **Port** or the **Host Name** and **Port** of the Primary and Alternate LDAP Server.
   b. Select the server type from the **[LDAP Server]** drop-down menu.
   c. Enter any further information, as required, in the **Optional Information** area.
      - **Search Directory Root** allows you to limit the LDAP search by entering the location on the server where the LDAP information is stored.
      - **Login Credentials to Access LDAP Server**: Select the **[None]** radio button if no login is required.
        If you select **[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.
        If **[System]** is 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.
      - **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.
      - **SSL**: If SSL is required, check the **[Enable]** checkbox.

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

      - If you want the device to verify that the server certificate is trusted, valid and has a fully qualified domain name (FQDN), check the **[Validate Repository SSL Certificate]** checkbox.

        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).
      - **Maximum Number of Search Results** (between 5 and 100). This is 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.
      - **Search Timeout:** There are two options. You can let the server use its timeout limit by selecting the [Wait LDAP Server Limit], or 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.

- **[LDAP Referrals]:** if the primary LDAP server is connected to additional servers, the search will continue on those servers as well.
- The **Perform Query on option** will help control the returns by allowing the LDAP query to be 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".

9. Click on the **[Apply]** button to implement the changes.

To Figure Contexts for LDAP

1. From the **LDAP** screen, click on the **[Contexts]** tab 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 information in the **[Default Login Context]** field.
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. The **Search** area lets you test the LDAP name search and field matching capability. Enter details in the **[Enter Name]** field and click on the **[Search]** button.
   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 **[Apply]** button.

At the Device:

1. Select the **[E-mail]** button, then touch **[OK]**.
2. Touch **[Address Book]**.
3. Enter a name using the keyboard touch screen, for example: lastname, firstname.

4. Touch **[Search]**. The Search Results Screen is shown.
5. Select the required name from the list (if there is more than one match).
6. Touch the **[To]:** button to select the name as a recipient for your e-mail.
7. Touch **[Close]**. 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.

Configuring the 'From' Address

For 'From' address configuration refer to the E-mail Settings screen within Internet Services. For instructions refer to the Configure General E-mail Settings on page 225.

You have completed the steps to configure a company address book via LDAP.

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:

1. Open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Common Tasks]** area, click on the **[Add New Name]** link.
6. In the Enter Name Address Area, enter details in the following fields:
   - **Friendly Name**
   - **E-mail Address**
   - **Internet Fax Address**

7. Click on one of the following:
   - **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 screen.

To Edit a Name

1. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **Public Address Book** area, ensure **[View All Names]** link is highlighted.
6. Click on the **[Edit]** link for the name you want to edit.
7. Edit the required fields, click on the **[Save & Close]** button when finished.

To Delete a Name

1. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **Public Address Book** area, ensure **[View All Names]** link is highlighted.
6. Click on the **[Delete]** link for the name you want to delete.
7. 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 address and then import to the device.

1. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Management]** area, click on the **[Download Sample]** link.
6. Click on the **[Save]** button.
7. 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 addresses with the following headings: name and address.
   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 once created.

To Import an Address Book

1. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Management]** area, click on the **[Import]** link.
6. In the **Import Your Address Book File** area, click on the **[Browse]** button.
7. Browse to the location of the Address Book File **(*.CSV)** and highlight the **CSV** file and click **[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.
8. Click on the **[Next]** button.
9. 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.
10. 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.

11. Click on the **[Import]** button to import the CSV file.
12. 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. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Management]** area, click on the **[Export]** link.
6. Click on the **[Save]** button.
7. 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. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Management]** area, click on the **[Delete All Names]** link.
6. When the pop-up window displays stating **"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. At your Workstation, open the web browser, enter the *IP address* or *Host Name* of the device in the Address bar, and press **[Enter]**.
2. Click on the **[Address Book]** tab.
3. If prompted, enter the Administrator User ID and Password. The default is **[admin]** and **[1111]**.
4. Click on the **[Login]** button.
5. In the **[Security]** area, click on the **[Access Rights]** link.

6. 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.
7. Click on the **[Save]** button.

To Send a E-mail Using the Address Book

1. At the Device, select the **[E-mail]** icon, then touch **[OK]**.
2. Touch **[Address Book]**.
3. Touch **[Public]** in the Address Books drop-down list.
4. Enter the name of the recipient of your e-mail.
5. Touch **[Search]**.
6. The public address book appears. Select the required name from the list.
7. Touch the **[To]:** button.
8. Touch **[Close]**.
9. Place a document to e-mail in the document handler and press the green start button.
10. Verify that the recipient received the scanned document in his/her e-mail inbox.

You have completed the steps to create a public address book.

13

Internet Fax

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. Once 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 127 of this guide. Authentication can be configured after Internet Fax has been installed.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 24.
- Obtain the IP Address (or Host Name) of a functional SMTP (Simple Mail Transport Protocol) mail server that accepts inbound mail traffic.
- 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

Check under Services on the Configuration Report to verify if Internet Fax is enabled.

Configure a Domain Name

Note: A domain name must be entered to enable configuration of the Internet Fax feature.

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[IP (Internet Protocol)]** in the directory tree.
8. Enter the domain name in the **[Domain Name]** field, (for example; abc.xyz.company.com).

   Note: If Dynamic Addressing has been set on the device (DHCP, DHCP/AutoNet, BootP or RARP) the Domain Name will not be accessible. If you need to change it, select **[Static]** from the IP Address Resolution menu list, and click on the **[Apply]** button.

9. Click on the **[Apply]** button to implement any changes.

   Note: It is only necessary to configure the DNS settings if Host Names are to be used.

Configure an SMTP 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 **[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 **[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 the **[IP Address]**and **[Port]**, or the **[Host Name]** and **[Port]**of the SMTP Server.
   c. Enter a valid E-mail address in the **[ColorQube 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.
8. 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** setting is set to a number greater than 1.
   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.
   f. Enter details for the SMTP server account in the **[Login Name]**, **[Password]** and **[Retype Password]** fields.
   g. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

h. 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: System** - when selected, each user will need to enter the system credentials specified on the SMTP Server configuration screen.

9. Click on the **[Apply]** button to implement any changes.

Configure POP3 Settings

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 **[Connectivity]** link.
6. Click on the **[Protocols]** link.
7. Select **[POP3 Setup]** in the directory tree.
8. In the **Server Information** area:
   a. Select either **[IPv4 Address]** or **[Host Name]** and enter the IP Address and Port number or Host Name and Port number in the **[POP3 Server]** field.
   b. Enter the **[Login Name]** and **[Password]** details.
   c. Check the **[Select to save new password]** checkbox to save the password.
9. 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.
10. Click on the **[Apply]** button to implement any changes.

Configure General Internet Fax Settings

1. At your 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 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 **[Internet Fax]** link, select **[Defaults]** in the directory tree to display the **Internet Fax > Defaults** screen.

General

1. From the **Internet Fax > Defaults** screen, click on the **[Edit]** button in the **General** area.
   a. In the **Activity Report** section, 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 the **[Print Activity Report]** button.
   b. In the **Delivery Confirmation Timeout** section, 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. In the **Subject** section, enter details of what you want to appear as the default subject in every mail.
   d. 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 select to add the following details in the message:
      - User Name
      - E-mail Address
      - Number of Images
      - Attachment File Type (TIFF, JPEG)
      - Device Name (ColorQube)
      - Device Location
      - Serial Number
      - IP Address
      - MAC Address
   e. In the **Signature** entry field enter text that you want to appear as the default signature in every mail.
   f. 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.
      - **[On Errors Only]** - This setting will produce a Confirmation Sheet only when error detected.
2. 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**, click on the **[Edit]** button in the **Internet Fax** area.
2. Select the required option for **[Output Color]**.
3. Select the required document scanning option for **[2-Sided Scanning]**.
4. Select the required method used to optimize the quality of your scanned output images based on the content in your original documents for **[Original Type]**.
   Select the option that best describes the **[How Original was Produced]** of your e-mail documents.
5. 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 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, click on the **[Edit]** button in the **Advanced Settings** area.
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.

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.

1. From the **Internet Fax > Default** screen, click on the **[Edit]** button in the **Layout Adjustment** area.
2. Select the required options.
3. Click on the **[Apply]** button to accept changes and return to the **Internet Fax > Default** screen

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 or PDF/A.
- **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, 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 **Internet Fax > Default** screen.

Filename Extension

Filename Extension option allows you to set the filing name extension to one of the following:

- **Lower Case (.pdf, .xps, .jpg, .tif)**

- **Upper Case (.PDF, .XPS, .JPG, .TIF)**

1. From the **Internet Fax > Default** screen, click on the **[Edit]** button in the **Filename Extension** area.
2. Select the preferred options.
3. Click on the **[Save]** button to save changes and return to the **Internet Fax > Default** screen.

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, click on the **[Edit]** button in the **Internet Fax Image Settings** area.
2. Select the required options.
3. Click on the **[Apply]** button to implement changes and return to the **Internet Fax > Default** screen.

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.

1. Click on the **[Internet Receive Settings]** link in the directory tree.
2. In the **Filter Options** area, check the **[Accept E-mail with no attachment]** checkbox, to filter out attachments, or check the individual checkboxes for **[Accept the following attachments:]** to select the file types that will be allowable as e-mail attachments.
3. In the **Finishing Options** area, select the required options 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.

4. In the **Receipt Options** area, check the following checkboxes to:
   - **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.
5. Click on the **[Apply]** button to save the changes.
6. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

7. Select **[Logout]** in the upper right corner of your screen if you are still logged in as Administrator, and click on the **[Logout]** button.

At the Device:

1. Press the **<Services>** button, touch the **[Internet Fax]** icon.
2. Touch **[New Recipient]** button.
3. Enter an internet fax recipient address.
4. Touch the **[Add]** button, then touch **[Close]**. The e-mail address will appear in the Address List.
5. Place a document to fax in the document handler and press the **<Start>** button.
6. Verify the recipient receives the document at the internet fax address.

The 'From' Address

The Internet Fax 'From' address is the e-mail Address entered for the device when the POP3 address details were configured and is not an editable field.

Receipt of Internet Fax Messages

Verify the device can also receive Internet Fax messages.

At the Device:

1. Press the **<Services>** button, touch the **[Internet Fax]** icon.
2. Touch the **[New Recipient]** button.
3. Enter the e-mail address configured for the device.
4. Touch the **[Add]** button then the **[Close]** button.
5. Place a document in the document handler and press the green start button.
   The document should be received and printed as an Internet Fax job.

Internet Fax Public Address Book

Once configured, an internal and a public address book can be accessed when using the Internet Fax feature at the device. Lightweight Directory Access Protocol (LDAP) provides access to the internal (corporate) address book.

A public address book can be created from a list of names and addresses saved in a .CSV file (Comma Separated Values) file. Both address book types can be configured for use on the device at the same time.

To configure a Public Address Book, refer to Configuring Public and Internal Address Books (LDAP) on page 228.

14

Embedded Fax

Embedded Fax enables 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.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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.
- Locate the 2 Line Fax Kit if this has been purchased.

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, fit the kit following the instructions contained with the kit. Once fitted, 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 (or Install) screen should appear. If it does, touch **[Set up Now]** if it does not, see Deferred Fax Setup on page 247.

   Note: If you do not wish to run through the fax configuration, touch the **[Set up Later]** button. Embedded Fax will be unavailable until the fax configuration screens are completed from within the administrator tools screens. See Deferred Fax Setup on page 247, for instructions.
2. Select the required (or nearest) country location by touching an entry in the **[Country Setup]** list.
3. Touch **[Next]**.
4. Touch **[Line 1]** or **[Line 2]** if applicable.
5. The Line Configuration screen appears. 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.
6. Enter the fax telephone number for the device by touching the **[Fax Phone Number]** button and pressing the buttons on the keypad. At least two digits must be entered here.
7. Optional step: To define a name for this line, touch the keyboard icon next to **Line Name**, enter a name by using the on-screen keyboard. A maximum of 30 characters may be entered.
8. Touch **[Save]**.
9. Touch **[Next]**.
10. The **[Line Settings]** window appears. Select the required option for the line by touching one of the buttons as follows:
    - **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.
11. Touch **[Next]**.
12. Touch **[Save]** to exit the Line Setup Complete screen.
13. Touch **[Save]** to save the Fax Install Complete screen.

    The device will reboot with the new settings.
14. Test the fax connection by sending a fax document. Press the **<Services>** button.
15. Touch the **[Fax]** icon button.
16. Enter the number of a nearby fax device using the keypad and touch the **[Add]** button.
17. Place your documents in the document handler and press the **<Start>** button.
18. Verify that your documents are received at the other fax device.

You have completed the embedded fax setup.

Configure 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:

1. Press the **<Log In / Out>** button to enter the Tools pathway.

2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]**.
6. Touch **[Line 1 Setup]** or **[Line 2 Setup]**.
7. The Line 1 (or 2) Setup screen appears.
8. Select the required **[Dial Type]**. 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.
9. Touch **[Fax Number]** and enter the device's fax number by using the keypad.

   Note: Customers in the Czech Republic are advised to contact their Xerox Service Representative to perform this function.
10. Optional step: To define a name for this line, touch the keyboard icon next to **Line Name**, enter a name by using the on-screen keyboard. A maximum of 30 characters may be entered.
11. Select the required option for the line by touching one of the buttons as follows under **[Options]**:
    - **[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.
12. Touch **[Save]** to exit the Line Setup screen.
13. Touch **[Log In / Out]** to exit the Tools pathway and the device will reboot with the new settings.

You have completed the steps. For detailed information about other embedded fax features, refer to the Training and Information CD2 delivered with your device.

Deferred Fax Setup

This procedure is only necessary if you pressed the Setup Later button when the Fax Setup screens appeared and you now wish to configure Embedded Fax settings using the Fax Setup Screens.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]**.
6. Touch the **[Fax Country Setting]**
7. Select the required (or nearest) country location by touching an entry in the **[Country Selection]** list.
8. Touch **[Save]**.
9. Touch **[Line 1]** or **[Line 2]** Setup.
10. The Line 1 Setup screen appears.

11. Select the required Dial Type. 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.

12. Enter the fax telephone number for the device by touching the **[Fax Number]** button and pressing the buttons on the keypad. At least two digits must be entered here.

    Note: Customers in the Czech Republic are advised to contact their Xerox Service Representative to perform this task.

13. Optional step: To define a name for this line, touch the keyboard icon next to **Line Name**, enter a name using the on-screen keyboard. A maximum of 30 characters may be entered.
14. Select the required option for sending and receiving fax for **[Options]**:
    - **[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.
15. Touch **[Save]** to exit the Line Setup screen.
16. Touch **[Log In / Out]** to exit the Tools pathway and the device will reboot with the new settings.
17. Test the fax connection by sending a fax document. Press the **<Services>** button.
18. Touch the **[Fax]** icon.
19. Enter the number of a nearby fax device using the keypad.
20. Place your documents in the document handler and press the **<Start>** button.
21. 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.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. Touch the **[Feature Defaults]** to display the **Fax Service - Setting** screen.

Fax

1. From the **Fax Service - Setting** screen, select the **Fax** tab.
2. Touch the **[Cover Sheet]** icon, the Cover Sheet screen will display.

3. To assign a cover Sheet to the fax job, touch **[On]**.

   Note: To use the Cover Sheet assigned to the recipients selected from the Address Book, touch **[Off]**.

4. Touch the **[To...]** field, enter description for the "To Field" using the on-screen keyboard and touch **[Save]**.
5. Repeat for the **[From...]** field.
6. For **Comment...**, upto six different comments can be added, select a comment field and touch **[Edit]**.
7. Enter comment using the on-screen keyboard, and touch **[Save]**.
8. To delete a comment, select comment and touch **[Clear]**.
9. Touch **[Save]** to return to the **Fax** tab.
10. 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.
11. 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.
12. 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 is best 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.
3. For **Lighten/Darken** option, move the slider **up** to lighten and **down** to darken the output of the original fax job.
4. For **Sharpness** option, move the slider **up** to sharpen and **down** to soften the output of the original fax job.
5. Touch **[Save]** to return to the **Fax Service - Setting** screen.

Layout Adjustment

1. From the **Fax Service - Setting** screen, select the **Layout Adjustment** tab.

2. Touch the **[Original Size]** icon.
   a. Select one of the following method for the device to determine the size of the original fax documents:
      - **Auto Detect** - this method enables 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/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. Select one of the following method to determine how the receiving device will handle images that are to 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.

Fax Options

1. From the **Fax Service - Setting** screen, select the **Fax Options** tab.
2. Touch the **[Starting Rate]** icon.
   c. 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)**
   d. Touch **[Save]** to return to the **Fax Options** tab.
   e. Touch **[Send Header Text]** icon.
   f. Select **[On]** to allow the header text set by the System Administrator.
   g. Touch **[Save]** to return to the **Fax Options** tab.

Select the Fax Country Setting

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. Touch the **[Fax Country Setting],** to display the **Country Setup** screen.

7. Select the relevant country from the list.
8. Touch **[Save]** to return to the Embedded Fax Settings screen.

Configuring Embedded Fax Settings

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
1. Select **[Line 1 Setup]** or **[Line 2 Setup]** to display the **Line Setup** screen.
2. Touch **[Fax Number]** then enter the fax number using the touchscreen keypad.
3. Touch **[Save].**
4. Touch **[Line Name]** then enter the Line Name using the touchscreen keypad, maximum of 30 character can be entered.
5. Touch **[Save].**
6. Select the required option for sending and receiving fax for **[Options]**:
   - **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.
7. Touch **[Save]** to return to Embedded Fax Settings screen.

Incoming Fax Defaults

Use this feature to configure settings for incoming faxes.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. From the Embedded Fax Settings screen, select **[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]**.
2. Enter a delay time from 0 to 15 seconds using the left and right arrow.

3. Touch **[Save]**, to return to the **Incoming Default Settings** screen.

Junk Fax Prevention

This feature prevent the receipt of unwanted 'junk' fax documents. When enabled, the device allow the receipt of faxes from numbers held in the Dial Directory.

1. From the **Incoming Default Settings** screen, touch **[Junk Fax Prevention]**.
2. Select **[Enabled]**.
3. Touch **[Save]**, to return to the **Incoming Default Settings** screen.

Paper Settings

This feature allows you to select whether a received Embedded 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 **[Paper Settings]**.
2. 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 enables the user to hear an audible ringing sound when an Embedded Fax is received.

1. From the **Incoming Default Settings** screen, touch **[Ring Volume]**.
2. Select **[Enabled]**.
3. Select the required level of audible volume.
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]**.
2. Select **[Enabled]**.
3. Touch the passcode field, and enter a four digit passcode using the on-screen keypad, and touch **[Save]**.
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]**.
2. Select **[Enabled]** for the following options:

- **Staple** - this option if the device has a finisher, and you want documents stapled.
- **2-Sided** - this option allows the faxes to be printed on both sides of the pages.

3. Touch **[Save]**, to return to the **Incoming Default Settings** screen.

Transmission Defaults

This feature allows you to set the outgoing fax settings.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. From the Embedded Fax Settings screen, use the up and down buttons and select **[Transmission Defaults]** to display the **Transmission Defaults** screen.

Automatic Redial Setup

Automatic Radial Setup allows you to specify the time interval before the devices radials 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 **Transmission Defaults** screen, touch **[Automatic Radial Setup]**.
2. There are two options:
   - **Redial Time Interval** (in minutes, the range is from1 to 25)
   - **Automatic Redial Attempts** (the range is from 0 to 10)
3. Use the up and down arrow to select the required amount.
4. Touch **[Save]** to return to the **Transmission Defaults** screen.

Automatic Resend

The Automatic Resend automatically resends part or all of a failed fax transmission. You can set the number of automatically resend attempt.

1. From the **Transmission Defaults** screen, touch **[Automatic Resend]**.
2. For **Set Number of Resends**, use the up and down arrow to select the required amount, the range is 0 to 5.
3. Select one of the following option to 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 out 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 **Transmission Defaults** screen, touch **[Audio Line Manager]**.
2. Select **[Enable]**.
3. For **Select Line Monitor Volume**, select one of the following:
   - **High**
   - **Medium**
   - **Low**
4. For **Select Line Monitor Duration**, use the up and down arrow to select the required amount, the range is from 1 to 25.
5. Touch **[Save]** to return to the **Transmission Defaults** screen.

Send Header Text

Transmission Header Text feature enables you to specify a text string to be transmitted as part of the transmission header.

1. From the **Transmission Defaults** screen, touch **[Send Header Text]**.
2. Use the on-screen keyboard to type the text string (upto 30 characters can be entered).
3. Touch **[Save]** to return to the **Transmission Defaults** screen.

Batch Send

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 **Transmission Defaults** screen, touch **[Batch Send]**.
2. Select **[Enable]**.
3. Touch **[Save]** to return to the **Transmission Defaults** screen.

Mailbox & Polling Policies

This feature allows you to configure how you will like to keep the document received or stored.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.

6. From the Embedded Fax Settings screen, use the up and down buttons and select **[Mailbox & Polling Policies]** to display the **Mailbox & Polling Policies** screen.
   h. To set option for Received Documents, select **[Received Document]** and 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 up/down arrow to set time scale from 1 - 72 hours.
      - **Keep Forever** - select this option to save the document forever.
   i. To set option for Stored Documents, select **[Stored Document]** and select one of the following:
      - **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 up/down arrow to set time scale from 1 - 72 hours.
      - **Keep Forever** - select this option to save the document forever.
   j. Touch **[Save]** to return to **Embedded Fax Settings** screen.

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.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. From the Embedded Fax Settings screen, use the up and down buttons and select **[Mailbox Setup]** to display the **Mailbox Setup** screen.

To Edit a Mailbox

1. From the **Mailbox Setup** screen, touch a mailbox from the **Mailbox List** and touch **[Edit]**.
2. To assign a name for the mailbox:
   a. Touch **[Mailbox Name]**.
   b. Touch **[Delete Text]** to clear the text. Type a name for the mailbox using the on-screen keyboard.
   c. Touch **[Save]**.
3. To assign a passcode for the mailbox:
   a. Touch **[Mailbox Passcode]**.
   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]**.
4. To receive fax notification, ensure the **Mailbox Notification** option is set to **[Enable]**.
5. Touch **[Save]** to return to the **Mailbox Setup** screen.

To Delete a Mailbox

1. From the **Mailbox Setup** screen, touch a 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
- Confirmation Report
- Broadcast and Multipoll Report

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. From the Embedded Fax Settings screen, use the up and down buttons and select **[Setup Fax Reports]** to display the **Setup Fax Reports** screen.

Activity Reports

An Activity report shows the result of the incoming and outgoing fax jobs.

1. From the **Setup Fax Reports** screen, touch **[Activity Report]**.
2. Touch one of the following options:
   - **Auto Print** - to automatically print an activity report.
   - **Off** - to disable the option.
3. Touch **[Save]** to return to the **Setup Fax Reports** screen.

Confirmation Report

Allows you to choose whether or not a confirmation report is printed following a fax transmission.

1. From the **Setup Fax Reports** screen, touch **[Confirmation Report]**.
2. For **Report Option**, touch one of the following options:
   - **Always Print** - to automatically print a confirmation report informing you whether the fax transmission was transmitted successfully or not.
   - **Off** - to disable the option.
   - **Print On Error** - to print a report if the fax transmission failed.
3. For **Print Options**, touch 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.
4. Touch **[Save]** to return to the **Setup Fax Reports** screen.

Broadcast & Multipoll Report

This option when configured, shows the result of transmissions and polling requests to multiple machines.

1. From the **Setup Fax Reports** screen, touch **[Broadcast/Multipoll Report]**.
2. Touch one of the following options:
   - **Always Print** - to automatically print a confirmation report.
   - **Off** - to disable the option.
   - **Print On Error** - to print a report when fax transmission error occurs.
3. Touch **[Save]** to return to the **Setup Fax Reports** screen.
4. Touch **[Close]** to return to the **Embedded Fax Settings** screen.

Print Fax Reports

The following reports can also be printed for the Embedded Fax feature:

- **Activity Report** - this shows the result of the incoming and outgoing fax jobs.
- **Protocol Report** - this contains the protocol information about the last fax transmission whether it was a send or receive job.
- **Dial Directory Report** - this shows the list of individual directory number of the sent faxes.
- **Group Directory Report** - this report shows the list of group directory number of the sent faxes.
- **Options Report** - this shows the device configuration, the firmware level and options.
- **Pending Jobs Report** - this shows the list of jobs in the memory waiting to be printed.

At the Device:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then touch the **[Tools]** tab.
4. Touch **[Service Settings]**.

5. Touch the **[Embedded Fax Settings]** to display the Embedded Fax Settings screen.
6. From the Embedded Fax Settings screen, use the up and down buttons and select **[Print Fax Reports]** to display the **Print Fax Reports** screen.
7. Touch the required report from the list, and touch **[Print Now]**.
8. Touch **[Close]** to return to the **Embedded Fax Settings** screen.

15

Server Fax

Server Fax is a standard feature that can be enabled on your device. If enabled, it can be accessed by selecting the **Services Home** button then the **Server Fax** option. *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.

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 toAuthentication on page 127. Authentication can be configured after Server Fax has been installed.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 24.
- 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

Check under Services on the Configuration Report to verify if Server Fax is enabled.

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, please ensure the following items are available or 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

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 **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. 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 the IP Address and Port or Host Name and Port of the **Repository Server**.
   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]** and **[Password]** entry fields.
   f. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
9. Click on the **[Apply]** button to accept the changes.
10. Configure the Defaults settings, refer to Configure Default Settings on page 265.

Configure a Fax Repository using NetWare

Information Checklist

Before starting the procedure, please ensure the following items are available or 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

Check under Connectivity Protocols on the Configuration Report to verify if Netware protocol is enabled.

Enter the Fax Repository Details via 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. 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 **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. In the **Settings** area:
   a. Select **NetWare** from the **[Protocol]** drop-down menu.
   b. Enter the host name or the NetWare server in the **[Repository Server]** 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]** and **[Password]** entry fields.
   h. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
9. Click on the **[Apply]** button to accept the changes.
10. Configure the Defaults settings, refer to Configure Default Settings on page 265.

Configure a Fax Repository using SMB

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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 **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. In the **Settings** area:
   a. Select **SMB** from the **[Protocol]** drop-down menu.
   b. Select either **[IPv4 Address]** or **[Host Name]**.
   c. Enter the IP Address and Port or Host Name and Port of the server in the **Repository Server** field.
   d. Enter details of the Share name in the **[Share Name]** 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]** and **[Password]** entry fields.
   g. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.
9. Click on the **[Apply]** button to accept the changes.
10. Configure the Defaults settings, refer to Configure Default Settings on page 265.

Configure a Fax Repository using HTTP/HTTPS

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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 **[Services]** link.
6. Click on the **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. 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 the IP Address and Port or Host Name and Port of the server in the **Repository Server** 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, 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]** and **[Password]** entry fields.

i. Check the **[Select to save new password]** checkbox, if you want to change the password for an existing Login Name.

9. Click on the **[Apply]** button to accept the changes.
10. Configure the Defaults settings, refer to Configure Default Settings on page 265.

Configure a Fax Repository using SMTP

Information Checklist

Before starting the procedure, please ensure the following item is available or has been performed.

- Obtain the domain name of your SMTP mail server.

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 **[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 **[Server Fax]** link.
7. Select **[Fax Repository Setup]** in the directory tree.
8. Select **[SMTP]** from the **Protocol** drop-down menu.
9. Enter details in the **[Domain]** field.
10. Click on the **[Apply]** button to accept the changes.

Configure Default Settings

1. At your 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 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 **[Server Fax]** link, select **[Defaults]** in the directory tree.

General

1. In the **General** area, click on the **[Edit]** button:
   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 **Server Fax** - **Default** screen.

Server Fax

1. From the **Server Fax > Default** screen, click on the **[Edit]** button in the **Server Fax** area.
   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 **[Original Type]**.
   c. Specify the resolution from the **[Resolution]** drop-down menu. The resolution affects the amount of detailed 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 **Server Fax** - **Default** screen.

Image Quality

1. From the **Server Fax > Default** screen, click on the **[Edit]** button in the **Image Quality** area.
   a. For **Image Quality**, select either the **[Lighten]** or **[Darken]** button 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. Click on the **[Apply]** button to return to the **Server Fax** - **Default** screen.

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.

1. From the **Internet Fax > Default** screen, click on the **[Edit]** button in the **Layout Adjustment** area.
2. Select the required options.
3. Click on the **[Apply]** button to accept changes and return to the **Server Fax** - **Default** screen.

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 **Server Fax > Default** screen, click on the **[Edit]** button in the **Filing Options** area.
2. 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 **Server Fax** - **Default** screen.

To send a Fax

At the Device:

1. Press the **<All Services>** button.
2. Select the **[Server Fax]** button from the touch screen.
3. Enter a valid fax number. Press **[Add]**.
4. Load a document in the document handler and press the green start button.
5. Verify that your fax is received at the specified fax device.

16

LAN Fax

LAN (Local Area Network) Fax enables users to send documents to fax devices directly from their computers. Once 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 the Embedded Fax on page 245 before continuing with this procedure.

Before starting the procedure, please ensure the following items are available or 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 ColorQube 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. Enter the IP Address of your printer, if necessary.
6. Ensure **Bi-directional Communication** is set to **[Automatic]**, or click on **[Manual]** and enter the Device Name or IP Address. Click on **[OK]**.
7. Click on the **[Installable Options]** button.
8. Ensure that LAN Fax shows a status of **[Installed]**.

9. Click on **[OK]**.

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]** menu.
3. Click on **[Installed]**.
4. Click on **[OK]**.
5. Click on **[OK]** to close the print driver Properties.

Using LAN Fax

Windows: At your Workstation

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.

Mac OS Users

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 **[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 will display, 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**
   - **Email 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. In the **Cover Sheet Image Editor** screen will display, 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 option:
      - **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, and 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 **[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**, 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.

17

Reprint Saved Jobs

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 enables 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 and e-mail these files.

You can enable/disable encryption of user data, refer to User Data Encryption on page 149.

Information Checklist

Before starting the procedure, please ensure the following items are available or 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

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 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 **[Reprint Saved Jobs]** link.
7. Select **[Enablement].**
8. In the **Enablement** area:
   a. Select **[Enabled]** to enable Saved Jobs for Reprint.
   b. Select **[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.

9. 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 / disable encryption of user data on the **User Data Encryption** page, refer to User Data Encryption on page 149.

Enable Reprint Saved Jobs in your Print Driver

Windows 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 ColorQube 9201/9202/9203 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.

Mac Operating Systems

1. At your Mac Workstation, open the **[Printer Setup Utility]**.
2. Select the Xerox printer and click 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.

Back-up Jobs

The Back-up Jobs feature allows you to configure a server to save jobs stored on the device.

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 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 **[Reprint Saved Jobs]** link.
7. Select **[Backup Jobs]** in the directory tree.
8. 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 the IP Address and Port or Host Name and Port 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 onto the end of 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.
9. 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:

1. Open the web browser and enter the *IP address* 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 **[Services]** link.
6. Click on the **[Reprint Saved Jobs]** link.
7. Select **[Restore Jobs]** in the directory tree.
8. 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 the IP Address and Port or Host Name and Port 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 to restore in the **[File Name]** field. This name will be appended onto the end of 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.
9. 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 the Internet Services.

1. To create a new folder, access Internet Services. Open your web browser on your PC and enter the IP address of the ColorQube 9201/9202/9203 into the *Address (URL)* field.
2. Press **[Enter]**.
   The Internet Services options for your device are displayed.

   Note: To find out the IP address of your device, print a Configuration Report. Refer to Configuration Report on page 28.
3. Select the **[Jobs]** options.
4. Select the **[Saved Jobs]** tab to access the folder options.
5. Select **[Create New Folder]**.
6. Input the name for the folder in the **[Name]** field.
   As a normal user you are only able to create **Public** folders. These are the other kind of folders you may see.
   - The **Public** folder has been created by a user. It can be used by any user and has no access authority limitations. Any user can access and modify the documents in this folder.
   - The **Read Only** folder is created by the System Administrator or a user as a **Read Only Public** folder. Any user can print from the folder but documents cannot be deleted or modified by non System Administrator users.
   - The **Private** folder is created by a user only when the device is in **Authentication** mode. The user marks the folder as **Private** and the folder is only visible to the Owner and the System Administrator.
7. 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. To modify a folder, access Internet Services. At your workstation, open the web browser and enter the *IP address* of the device in the Address bar, and press **[Enter]**.

2. The Internet Services options for your device are displayed.

   Note: To find out the IP address of your device, print a Configuration Report. Refer to Configuration Page on page 28.

3. Select the **[Jobs]** option.
4. Select **[Saved Jobs]** tab to access the folder options.
5. Select **[Manage Folders]**.
   The window displays all the **Public** folders and any **Private** folders belonging to you.
6. Check the checkbox next to the folder you want to modify.
7. 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 278 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 ColorQube 9201/9202/9203 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. Program 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.
6. Program the print features required for the saved job.

   Note: The **Help** option provides an explanation of all the options.

7. Select **[OK]** to save the print settings.
8. 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]**.

   Note: Click on the **[Services]** link.To find out the IP address of your device, print a Configuration Report.
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. Select 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.
   - **Job Name** is used to enter a name for the job.
   - **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.
   - **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.
   - Program the **Paper**, **2 Sided Printing**, **Output Colour**, **Collate**, **Orientation**, **Staple** and **Output Destination** as required.
5. Select **[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.

18

Custom Services

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

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 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 **[Custom Services]** link.
7. Select **[Validation Options]** in the directory tree.
8. To have the user name sent with the validation request if the user is authenticated at the device user interface, click the **[Include User Name with validation request]** checkbox.
9. Click the **[Apply]** button.
10. 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, please ensure the following items are available or have been performed.

- Ensure the device is fully functioning on the network.
- Ensure SSL is enabled on the device. For further information refer to Machine Digital Certificate Management on page 157.

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 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 **[General Setup]**.
6. Click on **[Extensible Service Setup]** in the directory tree.
7. In the **Setup (Required)** area, for **Extensible 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:
      - **Extensible 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 option available to restrict access to printer services and features.
      - **Authentication & Authorization Configuration** - this feature allows you to remotely configure user access to the device's services.
      - **Session Data** - this feature allows an EIP application to access user session information.
   d. Click on the **[Save]** button to return to the **Extensible Service Setup** screen.
   e. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.
8. In the **Enable Extensible Services** area:
   a. Check the **[Export password to Extensible Services]** checkbox to send passwords to Extensible services.
   b. In the **Browser Settings** area, check the following checkboxes:
      - **Enable the Extensible 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"**.
9. Click on **[Services]**.
10. Click on **[Service Registration]** in the directory tree.
11. In the **Service Registration** area:
    a. After you have installed and registered the EIP application to the device. You should check in the **Service Registration** area to verify the EIP application is enabled, if the application is disabled, check the **Extensible Service** checkbox to enable the application.
    b. Click on the **[Apply]** button.
    c. Click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

At the Device:

1. Press the **<Services>** button.
2. Touch the **EIP Application** icon that you registered. Your XEIP workflow is accessible from the new icon.

20

WSD (Web Services for Devices)

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).

Once 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 (can be accessed by selecting **Properties > Connectivity > Protocols > HTTP > Web Services** tab).

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 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 **[WSD (Web Services for Devices]** in the directory tree.
7. In the **WSD Services** area, check the **[Enabled]** checkbox to enable the services.
8. In the **WSD Services Selection** area:
   a. Check the following individual services checkbox you want to enable or uncheck the services checkbox to disable a services:
      - **WS-Discovery** - supports the discovery of services in an ad-hoc network with a minimum of networking services, for example, no DNS, UDDI or other directory services. It does this by announcing or advertising the existence of the printer and its services on the network when it becomes available, and announcing its departure when unavailable.

When disabled, WSD does not respond to WS-Discovery requests.
The default port number is **3702**.

Note: This does not disable or prevent access to Internet Services.

- **WS-Discovery Multicast** - allows the printer to use the Multicast protocol to respond and announce. Multicast Discovery communicates the service URLs provided by the printer to client computers on the network. WS-Discovery must be enabled to make this feature available for selection.
  When disabled, WS-Discovery Multicast is unavailable on the printer. WS-Discovery Multicast should be disabled if your network utilizes a discovery proxy to handle multicast group communication and reduce overall WS-Discovery traffic.
  The assigned port number is identical to that of WS-Discovery.
- **WS-Print** - this allows the printer's print capabilities to be announced through WS-Discovery.
  When disabled, WS-Print service is unavailable on the printer. When disabled, print capabilities will not be discoverable by any network client and no printing is possible through the WSD port.
  The default port number is **53303**.
- **WS-Transfer** - lets you specify an alternate communication port number used for metadata exchange with WSD clients. WS-Transfer defines how to invoke a simple set of familiar verbs, such as Get, Post, Put, and Delete, using SOAP.
  This service is always available when WSD Services is enabled.
  The default port number is **53202**.

b. Each active WSD service must be assigned a unique port number. An assigned port number can be changed if your network's WSD implementation mandates it. Under normal conditions, these default assignments should not be changed.

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

21

Xerox Standard Accounting

When enabled, XSA tracks the numbers of Copy, Print, Workflow Scanning, E-mail, Server Fax, Internet Fax and Embedded Fax 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 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 is mutually exclusive from any other accounting feature. If XSA is enabled at the device, you cannot enable Foreign Device Interface, Auditron or Network Accounting.

Each device supports 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, please ensure the following items are available or 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

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]**, and click on the **[Login]** button.
4. Click on the **[Accounting]** link.
5. Click on the **[Xerox Standard Accounting]** link.
6. Select **[Manage Accounting]** in the directory tree.
7. In the **Enablement** area, click on the **[Enable Accounting]** button, click on the **[OK]** button when you see the message **"Properties have been successfully modified"**.

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.

1. Select **[Group Account]** in the directory tree to create a new group account.
2. 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, 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.
3. To add a user to this account group, click the **[Manage]** link in the **General Accounts** list.
   d. In the **[Account]** area, make any relevant changes.
   e. In the **[User Access]** area, check the checkboxes for the users you want the Account to have.
   f. Click on the **[Save Changes]** button to return to the **Group Accounts** screen.

To Create a User Account and Set Usage Limits

Note: A group account must be created before you create user accounts.

1. Select **[Manage Accounting]** in the directory tree.
2. In the **Users** area:
   a. Click on the **[Add New User]** button.
   b. In the **User** area, enter an ID for the user in the **[User ID]** field. The user ID can contain alphanumeric characters to a maximum of 32 alphanumeric characters (for example: A10). User ID's must be unique.
   c. Enter the descriptive user name (for example Jane Smith) in the **[User Name]** field. The user name can contain a maximum of alphanumeric characters. User names must be unique.

d. In the **Usage Limits** area, specify the usage limits for this account in the **[User Limits]** fields. The maximum value for each limit is 16,000,000. Usage limits can be specified for:
   - **Black or Color Printed Impressions** - the maximum number of documents that can be printed by a user, from their workstation via the print driver.
   - **Black or Color Copied Impressions** - the maximum number of copies that can be produced by a user via the Copy feature on the device.
   - **Network Images Sent** - the maximum number of documents that can be sent over the network by the user.
     This applies to the following features when enabled on the device: Workflow Scanning, E-mail, Server Fax and/or Internet Fax.

Note: If the device is set to print Scan Confirmation reports and/or Internet Fax Acknowledgement reports, then these reports printed are also counted towards the user's limit.

   - **Fax Images Sent** - if Embedded Fax is enabled on your device, you will see this option in Internet Services.
     Fax Images Sent sets the maximum number of documents that can be faxed by a user with the Fax feature (Embedded Fax).
     The device calculates the number of faxed documents by multiplying the number of images faxed (this includes cover sheets), by the number of destinations.
   - **Black Faxed Impressions -** if Embedded Fax is enabled on your device, you will see this option. This sets the maximum number of fax documents that a user can send.

For example, to restrict the maximum number of prints this user can make, to *1000* prints, enter 1000 in the **[Black or Color Copied Impressions]** field. Cover sheets and banner sheets are counted as part of the job and will add to the number of impressions.

3. Click on the **[Apply]** button when you have finished setting the usage limits.
4. The **Limits & Access** page is displayed, in the **Usage Limits** area the following information and settings are available:
   - **Users Limit -** this column indicates the limit of page (impressions and sent fax images). This field can be modified. The maximum limit is 16,000,000.
   - **Used** - this column indicates the number of pages processed by this user.
   - **Remaining** - this column indicates the remaining limit for the user.

   a. Click on the **[Reset]** button to zero-out the **Used** page count to match the corresponding user limit and refresh the page.
      Click on the **[Reset All]** button to reset the remaining counts of all usage metrics.
5. In the **Access Rights** area at the bottom of the page. The two options are:
   - **Group Account Access -** click on the **[Edit]** button to open the **Group Account Access** page. This will let you add and/or change the group accounts to which the user will have access
   - **General Account Access -** click on the **[Edit]** button to open the **Group Account Access** page. This will let you add and/or change the general accounts to which the user will have access.
6. Click on the **[Edit]** button for **Group Account Access**.

   a. In the **Group Accounts** area, lists the group accounts assigned to this user, and which one is assigned as the default for this user.
      To grant the user access to a group account, check the corresponding checkbox under **[Access]**.
      You can click on the **[Select All]** button to grant access to all accounts. To withdraw access to a group account, uncheck the corresponding checkbox.

   b. Select **[Default]** to allow the Group Account to be a default user.
   c. Click on the **[Save Changes]** button to return to the **Limits & Access** page.
7. Click on the **[Edit]** button for **General Account Access**.
   a. In the **General Accounts** area, lists the group accounts assigned to this user, and which one is assigned as the default for this user.
   b. To grant the user access to a group account, check the corresponding checkbox. Click Select All to grant access to all accounts. To withdraw access to a group account, uncheck the corresponding checkbox.
   c. Click on the **[Save Changes]** button to return to the **Limits & Access** page.

Maximum Usage Limits

The first time a user logs in to the device after they have reached their maximum usage limit, a message displays on the user interface. The message notifies the user that they have reached their limit for the feature. Users will not be able to use the feature until their limit is reset. If the user performs a copy, scan or fax job at the device, and mid way through the job their limit is exceeded, the job will continue. The device will track the number of sheets that were printed over the limit and subtract them from the user's new allocation, when it is updated by the administrator.

If the user's limit is reached before a print job is completed, an error report will print at the device to notify the user that their limit has been reached. The job will be deleted from the print queue. The job may run over due to sheets committed to the paper path.

The System Administrator has unlimited access to the device.

User limits can be reset on the Internet Services Report and Reset screen.

Using XSA at the device

When you enable XSA, users must enter a valid user name at the device to access the features.

At the Device:

1. Press the **<Services>** button.
2. The **Accounting - User ID** screen displays. Enter the User ID using the on-screen keyboard of one of the users that you created in the Manage Accounting area of Internet Services.
3. Touch the **[Enter]** button.
4. The Validation in Progress screen will show.

   If the user is a member of more than one Group Account or General Account, they will be asked to select the account that they wish to log in to.

   When the user is logged in, the Services screen will show. The user can now select the feature that they want to use.

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.

1. At your Workstation, open your web browser and enter the *IP address* 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 **[Accounting]** link.
6. Click on the **[Xerox Standard Accounting]** link.
7. Select **[General Accounts]** in the directory tree to create a new general account.
8. In the **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, 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.
   d. To add a user to this account group, click 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 you want the Account Group to have.
   g. Click on the **[Save Changes]** button. The user appears as a member of the Group and General Accounts.

Generate Report and Reset User Limits

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 **[Accounting]** link.
6. Click on the **[Xerox Standard Accounting]** link.
7. Select **[Report and Reset]** in the directory tree.
8. To generate a Report:
   h. In the **Generate Report** area, click on the **[Generate Report]** button. This will generate a report in .CSV format.
   i. When the page refreshes, to save the report, right-click on the **[Right-click to download]** link, select **[Save Target As....]**.
   j. Select where on the workstation you want to save the file, and click **[Save]**.
9. To reset the usage data to zero:
   a. In the **Reset Usage Data** area, 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.
10. Click on the **[OK]** button to confirm when the **"All current usage data will be rest to zero and lost"** dialog box appears.

WARNING: The following step will delete all the XSA accounts set up for your device!

11. To delete all user, group and general accounts:
    a. In the **Reset to Default** area, 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.
8. You may also select the **[Mask User ID]** and **[Mask Account ID]** checkboxes to show asterisks (******) when ID's are entered.
9. Select the **[Save Accounting Codes]** to save selection.
10. Otherwise select **[Use Default Accounting Codes]** and enter the default user ID and the default Account Type.
11. Enter the default Account ID.
12. Click **[OK]**.
13. Click **[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 enables 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

1. At a networked workstation, open the web browser and enter the *IP address* of the device that you want to clone to 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 **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. From the display of available check boxes, verify that Accounting is among them.
8. Click again on the **[General Setup]** link, then select **[Configuration]** in the directory tree, and verify that both devices have the same System Software Version.

To make a Back-up file

1. At your workstation, open the web browser and enter the *IP address* of the device with the settings that you want to copy, 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 **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. 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.
8. Right-click on the **[.dlm]** link that appears and select **[Save Target As]**.

9. A dialog box will prompt you to specify and name and location for the cloned file. Ensure the extension reads **.dlm**.
10. 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 will be unavailable over the network for several minutes.

1. Open your web browser and enter the *IP address* of the device that you wish to restore or clone the settings to. 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 **[General Setup]** link.
6. Select **[Cloning]** in the directory tree.
7. In the **[Install Clone File]** area, click on the **[Browse]** button.
8. Locate the **[.dlm]** clone file.
9. Click on the **[Install]** button.

   The device will be unavailable over the network for several minutes. Once rebooted a Configuration Report will print, if enabled.
10. 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.

22

Network Accounting

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, please ensure the following items are available or 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.
- 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

When you purchased the Network Accounting Kit, you received the information and SIM required to install this feature. Following the supplied instructions for full details, with the device powered on, the SIM is inserted into an orange slot on the device's backplane. An Options Assist screen pops up to help with installation.

To Enable the Network Accounting Feature at the Device

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Accounting Settings]**.
5. Touch **[Accounting Mode]**.
6. Touch **[Network Accounting]** and touch **[Save]**.

To Configure Network Accounting

1. Press the **<Log In/Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press the **<Machine Status>** button, then the **[Tools]** tab.
4. Touch **[Accounting Settings]**.
5. Touch **[Accounting Mode]**.
6. Touch the **[Network Accounting]** button to enable it, a **Network Accounting Configuration** menu will display on the right hand side of the touch screen.
   a. Touch the **[Customize Prompt]**, select the required option from the **[Display Prompt 1 Only]** drop-down menu.
   b. Touch **[Prompt 1 Label]**, and enter an ID between 1 and 32 characters and touch **[Save]**.
   c. Touch **[Prompt 2 Default Value]**, and enter an ID between 1 and 32 characters and touch **[Save]**.
   d. Touch the **[Mask Entries]** box to place a tick, and touch **[Save]** to return to the **Accounting Mode** screen.
   e. Touch **[Code Entry Validation]**.
   f. Touch the **[Enabled]** button to enable authentication or **[Disabled]** to disable authentication.
      - **Authentication Enabled**
        If you want to track copy, print and scan usage by both User ID, Account ID and amount of resources each user account uses (for example, types and sizes of paper stock, duplex or simplex, stapled or not stapled) ensure that Authentication is Enabled. Users will then be required to enter a valid User ID and an Account ID for any job. The User ID and Account ID are alphanumeric strings between 1 and 32 characters in length.
      - **Authentication Disabled**
        Disabling Authentication allows the device to accept both valid and invalid User and Account ID's. Authentication Disabled is useful if conducting an analysis for the resources used on a particular device before Authentication controls are instituted. Users will still be required to enter at least one character into the User and Account ID fields.
   g. Touch the **[Save]** button to retain the settings.
7. Touch the **[Save]** button.
8. Touch the **[Log In / Out]** button, and touch **[Logout]** to log out.
9. To verify Accounting is enabled, press the **<Services>** button on the front panel.

10. 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.
11. 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

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 **[OK]**.
   d. Click **[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 **[OK]**.

d. Click **[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 **[OK]**. Ensure the *Accounting* preset is selected in the **Presets** menu each time you print.

   f. Click **[Print]**.

   g. Enter your Network Accounting information.

   h. Click **[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 **[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.

23

Xerox Secure Access

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 the **Network Accounting** or **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, please ensure the following items are available or 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 **Local User Information Database** must be configured. For instructions, refer to the Local User Information Database section within this guide. There must be a mapping between the accounts created on the Authentication Server and the Local 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 the LDAP section within this guide. 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

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 **[Security]** link.
6. Click on the **[Access Rights]** link.
7. Select **[Setup]** in the directory tree to access **Authentication Configuration** screen.
8. In Current Configuration area, click on the **[Edit Methods]** for **Authentication**.
9. In **Where is the information located?** area:
   a. Select **[Xerox Secure Access]** from the **Device User Interface Authentication** drop-down menu.
   b. Select your required option from the **Web User Interface Authentication** 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 **[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 2000/2003), SMB (Windows NT4/2000) or LDAP is supported.
   c. Select the Authorization method in 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 networked databases such as LDAP server to determine levels of authorization.
   d. For **Personalization**, check the **[Automatically retrieve the following information for the authenticated user from LDAP: Home directory for the 'Scan to Home' service. E-mail address for the 'E-mail' and 'Internet Fax' services.]** checkbox if required.
   e. Click on the **[Save]** button to return to the **Authentication Configuration** screen.

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]/ [Edit]** button for **Device User Interface Authentication** Xerox Secure Access.
   b. The device will automatically configure itself to work with the XSA remote server. If the Authentication Solution has been configured correctly the address information should be populated with the address of the Authentication Solution server.In the **Manual Override** area, click on the **[Manually Override Settings]** button if the XSA remote server does not configure automatically.
   c. In the **Server Communication** area, select either **[IPv4 Address]** or **[Hostname],** and enter the **IP Address** and **Port** or **Host Name** and **Port** details.
   d. Enter the network path to the Authentication server in the **Path** field.

   Note: Enter the HTTP path of **[public/dce/xeroxvalidation/convauth]** and port number of **[1824]** to facilitate communication.

   e. In the **Device Log In Method** area, select one of the following:
      - **Xerox Secure Access Device Only (e.g., Swipe Cards)**
        The XSA Device (swipe card or badge, for example) is required to be authenticated on the device.
      - **Xerox Secure Access Device + an alternative on-screen authentication method**
        Select to allow users to authenticate using the device's control panel in addition to the XSA feature.
        When enabled, a button labeled **"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 pages on the printer's control panel. The remote server is still responsible for authenticating the user. All other XSA options are supported with this setting.
   f. If you are using the Network Accounting feature, the Xerox device can be set to automatically obtain accounting data for the user from the Authentication server when the user authenticates. This reduces the number of screens that the user is presented with when they login at the device. To implement this feature, select **[Automatically apply Accounting Codes from the server]** or If you want the user to provide accounting data manually at the user interface, select **[User must manually enter accounting codes at the device]**.

   Note: Ensure Network Accounting is enabled and the server supports this.

   g. If you select **[Xerox Secure Access Device + alternate on-screen authentication method]** for **Device Log In Method**, in the **Device Instructional Blocking Window** area, enter text in the **[Window Title (Reference 1)]** field to define a title that will display on the Xerox device screen.

h. Enter text in the **[Instructional Text (reference2)]** field to define a prompt that will show on the Xerox device screen to tell the user what they need to do to be authenticated at the device.

Note: If the Title and Prompt have been configured on the Xerox Partner authentication server, then this information will override the Default Title and Prompt text entered within Internet Services.

i. Click **[Save]** to return to **Xerox Secure Access Setup** screen, and click the **[Close]** button to return to **Authentication Configuration** screen.

2. Click the **[Configure]/ [View]** button next to **Web User Interface Authentication**.
3. If you have selected **[Remotely on the Network]** for **Web User Interface Authentication**:
   a. follow the instructions to select the required **Authentication Type**.
      - See Authentication Configuration for Kerberos (Solaris) on page 129.
      - See Authentication Configuration for Kerberos (Windows 2000/2003) on page 130.
      - See Authentication Configuration for NDS (Novell) on page 132.
      - See Authentication Configuration for SMB (Windows NT4) and SMB (Windows 2000/2003) on page 133.
      - See Authentication Configuration for LDAP/LDAPS on page 134.
   b. When you have configured the required Authentication Type, click on the **[Save]** button to return to the **Authentication Configuration** page.
4. If you selected **[Locally on the Device]** for **Web User Interface Authentication**, the **Local User Information Database** will display.
   a. Click on the **[Add New User]** button, in the **User Identification** area, enter details of the new user in the following fields:
      - **User Name**
      - **Friendly Name**
      - **Password**
      - **Retype Password**
   b. In the **User Role** area, select one of the following option:
      - **System Administrator** - this will appear in the 'Role' column as **"SA"**, and will have access to all pathways, services and features on the device.
      - **Accounting Administrator** - this will appear in the 'Role' column as **"AA"**, the Accounting Administrator will have access to all the pathways, services and features on the device as well as the accounting tools and any non-secured tools features, but will not be able to modify or create any new user for the device.
      - **User** - this will appear in the 'Role' column as **"USER"**, and will have access only to the pathway, service or features they are assigned to.
   c. Click on the **[Add New User]** button to add the user, then click on the **[Close]** button to return to the **Authentication Configuration** screen.

   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.

   d. Click on the **[Close]** button to return to **Authentication Configuration** screen.

5. If you selected **Locally on the Device** for the **Authorization**, click **[View]** next to **Local User Information Database**, to display the **Local User Information Database** screen.
   a. Click on the **[Add New User]** button, in the **User Identification** area, enter details of the new user in the following fields:
      - **User Name**
      - **Friendly Name**
      - **Password**
      - **Retype Password**
   b. In the **User Role** area, select one of the following option:
      - **System Administrator** - this will appear in the 'Role' column as **"SA"**, and will have access to all pathways, services and features on the device.
      - **Accounting Administrator** - this will appear in the 'Role' column as **"AA"**, the Accounting Administrator will have access to all the pathways, services and features on the device as well as the accounting tools and any non-secured tools features, but will not be able to modify or create any new user for the device.
      - **User** - this will appear in the 'Role' column as **"USER"**, and will have access only to the pathway, service or features they are assigned to.
   c. Click on the **[Add New User]** button to add the user, then click on the **[Close]** button to return to the **Authentication Configuration** screen.

   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.

6. If you selected **Remotely on the Network** for the method of **Authorization**, click on the **[Configure]/[Edit]** button for **LDAP - Server** and verify the information is correctly configured. At the LDAP screen, click **[Authorization Access]** and enter the group names from your LDAP server that you want to grant access to. For more information, refer to Authentication Configuration for LDAP/LDAPS on page 134.
7. Click on **[Close]** to return to the **Authentication Configuration** screen.
8. If you checked **[Automatically retrieve the following information for the authenticated user from LDAP: Home directory for the 'Scan to Home' service. E-mail address for the 'E-mail' and 'Internet Fax' services]** checkbox under **Personalization**, click **[Configure]** next to LDAP Server and verify the information is correctly configured. For more information, refer to Authentication Configuration for LDAP/LDAPS on page 134.

   Note: If you have already checked the LDAP server information, this step is optional.

9. To set Authentication to control access to individual Services:
   a. In the **Current Configuration** area, click on the **[View]** button for **Service Registration**.
   b. On the **Service Registration** screen, check the checkboxes to select the services you want to display on the machine touch interface.
   c. Click on the **[Save]** button and return to the **Authentication Configuration** screen.
10. To set Authentication to control access to individual Features:
   a. Select **[Tools & Feature Access]** in the directory tree under **Access Right**.
   b. In the **Tools & Feature Access** page, under **Presets**, select one of the following:

- **Standard Access - Only Lock Tools**
- **Open Access - Unlock All Tools and Features**
- **Custom Access**

c. If you select **[Custom Access]**, for each Pathways and services within the pathway you can select either **[Unlocked]** or **[Locked]** from the drop-down menu. For certain **Services** within the **Service Pathway** you can also select **[Hidden]**.

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

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

11. 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.

24

Software Upgrade

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 two methods for upgrading the software on the device:

- Over a network connection using Internet Services via a web browser.
- Auto upgrade.

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.

To determine whether your device has a network connection, print a Configuration Report as follows:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**

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, please ensure the following items is available or 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. View the **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:

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 **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Click on the **[Upgrades]** in the directory tree.
8. In the **Upgrades** area:
   a. Check the **[Enabled]** checkbox.
   b. Click on the **[Apply]** button.
9. Click on the **[Manual Upgrade]** in the directory tree.

10. 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.
11. Once 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, please ensure the following items are available or 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:

1. 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 **[General Setup]** link.
6. Click on the **[Machine Software]** link.
7. Click on the **[Upgrades]** in the directory tree.

8. In the **Upgrades** area:
   a. Check to **[Enabled]** checkbox.
   b. Click on the **[Apply]** button.
9. Click on the **[Auto Upgrade]** in the directory tree to set the Auto Upgrade time.
10. 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 IP Address and Port or the Host Name and 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. Once 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. Once 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.

25

Troubleshooting

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>** 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 179.

> Note: If you have enabled Workflow Scanning, but the icon is grayed out or unavailable, at the device press the **<Log In / Out>** button. Enter the Administrator's User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Workflow Scanning, set the service to Enable, and touch Save. Reboot 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 labeled Power On/Off Button.

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.

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]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Select **[General]** in the directory tree
7. Select **[On]** from the **Confirmation Sheet** drop-down menu and click on the **[Apply]** button.
8. 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:

1. 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]**, and click on the **[Login]** button.
4. Click on the **[Services]** link.
5. Click on the **[Workflow Scanning]** link.
6. Select **[File Repository Setup]** in the directory tree
7. Click on the **[Edit]** box and check the details configured for your Scan Filing Repository.
8. 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 **[Exit]** to 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 186.

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>** button.

Enable E-mail before proceeding. For instructions refer to E-mail on page 223.

> Note: If you have enabled E-mail but the icon is grayed out or unavailable, at the device press the **<Log In/Out>** button. Enter the Administrator's User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then E-mail, set the service to Enable, and touch Save. Reboot 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 labeled Power On/Off Button.

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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

View the Network Setup details. 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 223.

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>** button.

Install Internet Fax before proceeding. For instructions, refer to Internet Fax on page 237.

> Note: If you have enabled Internet Fax but the icon is grayed out or unavailable, at the device press the **<Log In/Out>** button. Enter the Administrator’s User Name (default is **[1111]**), touch **[Next]**, enter Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Internet Fax, set the service to Enable, and touch Save. Reboot 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 labeled Power On/Off Button.

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 **[Information Pages]**.
4. Touch **[Configuration Report]**.

5. Touch **[Print]**, then touch **[Close]**.

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 237.

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>** button.

Is the Fax Button Available on the Device?

Install Server Fax before proceeding. For instructions, refer to Server Fax on page 259.

> Note: If you have enabled Server Fax, but the icon is grayed out or the service is unavailable, at the device press the **<Log In / Out>** button. Enter the Administrator User Name (default is **[1111]**), touch **[Next]**, enter the Password (default is **[1111]**), touch **[Enter]**, touch the Tools tab, and touch User Interface Settings. Touch Service Enablements, then Server Fax, set the service to Enable, and touch Save. Reboot 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.

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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

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 259.

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:

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Embedded Fax Settings]**.
6. This should read **[Enable]**. If this is not Enabled or the Fax Install screen appears, refer to the instructions to configure Embedded Fax in this guide.

Ensure the Fax Settings are Correctly Configured

Ensure the device has been configured with the correct fax (telephone) number.

At the Device

1. Press the **<Log In / Out>** button to enter the Tools pathway.
2. Enter the Administrator's User Name **[admin]**, touch **[Next]**, enter Password **[1111]**, touch **[Enter]**.
3. Press **<Machine Status>**, then the **[Tools]** tab.
4. Touch **[Service Settings]**.
5. Touch **[Fax Service Settings]**.

Verify that all Fax Setting configuration steps have been performed. Refer to Embedded Fax on page 245.

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>** 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 verify that Network Accounting is installed, print a Configuration Report and look under Installed Options to see the status of Network Accounting.

To Print a Configuration Report

At the Device:

1. Press the **<Machine Status>** button.
2. Touch the **[Machine Information]** tab.
3. Touch **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then touch **[Close]**.

For instructions to both install and enable the Network Accounting feature, refer to Network Accounting on page 297. 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 **[Information Pages]**.
4. Touch **[Configuration Report]**.
5. Touch **[Print]**, then 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 right front of the device. Press the button to the On (I) position 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 circuit breaker must be set to the On (I) position. 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

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X