Nuance®
EQUITRAC®

Embedded for Xerox
Extensible Interface Platform®
Setup Guide
Equitrac Embedded for Xerox Extensible Interface Platform® Setup Guide

Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Revision Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 15, 2016</td>
<td>• Updated for Equitrac Express and Equitrac Office release 5.6</td>
</tr>
<tr>
<td>June, 2015</td>
<td>• Updated for Equitrac Express and Equitrac Office release 5.5</td>
</tr>
<tr>
<td>March, 2014</td>
<td>• Updated for Equitrac Express and Equitrac Office release 5.3</td>
</tr>
<tr>
<td>April 16, 2013</td>
<td>• Updated for Equitrac Express and Equitrac Office release 5.0</td>
</tr>
<tr>
<td>November 9, 2012</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.2.5</td>
</tr>
<tr>
<td>December 16, 2011</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.2.3</td>
</tr>
<tr>
<td></td>
<td>• Added Copy Stop information for select Xerox 2.0 MFPs</td>
</tr>
<tr>
<td>July 11, 2011</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.2.2</td>
</tr>
<tr>
<td>July 16, 2010</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.2.0</td>
</tr>
<tr>
<td>June 23, 2009</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.1.1</td>
</tr>
<tr>
<td>October 30, 2008</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.1</td>
</tr>
<tr>
<td>September 25, 2007</td>
<td>• Updated for Equitrac Express and Equitrac Office version 4.0.3</td>
</tr>
<tr>
<td>February 16, 2007</td>
<td>• Initial release for Equitrac Express and Equitrac Office version 4.0.2</td>
</tr>
</tbody>
</table>

© 2016 Nuance Communications, Inc. All rights reserved.

All rights to this document, domestic and international, are reserved by Nuance Communications, Inc. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission of Nuance.

Trademarks

Equitrac®, Equitrac Express®, Equitrac Office®, Follow-You Printing®, and PageCounter® are registered trademarks of Nuance Communications, Inc. All other brands and their products are trademarks or registered trademarks of their respective holders, and should be noted as such.

Symbols Used In This Guide

The following symbols are used in the margins of this guide:

- **Note**
  The accompanying text provides cross-reference links, tips, or general information that can add to your understanding of the topic.

- **Caution**
  The accompanying text provides key information about a step or action that might produce unexpected results if not followed precisely.

- **Warning**
  Read the accompanying text carefully. This text can help you avoid making errors that might negatively affect program behavior.
# Contents

1 Introduction ........................................................................................................... 7  
   About User Authentication......................................................................................... 8  
   About Secure Document Release.............................................................................. 9  
   Installation and Configuration Requirements ......................................................... 10  
      Licensing, Server, and MFP Requirements............................................................... 10  
   Authentication Device Component Requirements ................................................. 11  
   System Requirements ............................................................................................. 11  
   Supported MFPs ....................................................................................................... 11  
   Supported Card Readers .......................................................................................... 12  
      Magstripe Device Reader ....................................................................................... 12  
      Proximity and Contactless Smart Cards ............................................................... 12  
   Additional Documentation ....................................................................................... 12  
   List of Terms ........................................................................................................... 13  

2 MFP Configuration .................................................................................................. 15  
   Configuring MFP Properties ................................................................................... 16  
   WorkCentre 3315 and 3325 Series ........................................................................ 17  
   WorkCentre 3615 and 6605 .................................................................................... 21  
   WorkCentre 4265 .................................................................................................... 25  
   WorkCentre 52xx, 7232/7242, 73xx, and 74xx Series .............................................. 31  
   WorkCentre 56xx Series .......................................................................................... 35  
      Locating Custom Services .................................................................................... 35  
      On the MFP Console ............................................................................................. 36  
      Via the Internet Services Interface ....................................................................... 36  
   WorkCentre 75xx Series .......................................................................................... 39  
      Locating Custom Services .................................................................................... 39  
      On the MFP Console ............................................................................................. 40  
      Via the Internet Services Interface ....................................................................... 41  
   WorkCentre 76xx Series .......................................................................................... 47  
      Locating Custom Services .................................................................................... 47  
      On the MFP Console ............................................................................................. 48  
      Via the Internet Services Interface ....................................................................... 48  
   WorkCentre 77xx Series and ColorQube 93xx, 92xx or 89xx Series .......................... 52  
      Locating Custom Services .................................................................................... 52  

## Contents

On the MFP Console. .......................................................... 53
Via the Internet Services Interface ...................................... 54

**WorkCentre Pro 2xx Series** ............................................. 59
Locating Custom Services .................................................. 59
On the MFP Console. .......................................................... 59
Via the Internet Services Interface ...................................... 60

**Phaser 3635** ................................................................. 61
Internet Services Interface Configuration .................................. 61
Phaser MFP Configuration .................................................... 61
Other settings ................................................................. 64

**Smart Card Configuration** .............................................. 65
On the MFP Console. .......................................................... 65
Via the Internet Services Interface ...................................... 66

### 3 Server-Side Configuration ............................................ 69

**Licensing Embedded Devices** ........................................ 70

**Configuring Authentication Prompts** .............................. 72
- Setting Xerox Secure Access Prompts ................................ 73
- Setting Xerox JBA Prompts ............................................. 74
- Enabling Release Key Prompt ........................................... 75

**Configuring Card Self-Registration** ................................ 75

**Configuring Billing Code Popup Behavior** ........................................ 76

**Configuring Embedded Devices** ...................................... 77

**Configuring Smart Card Authentication** ............................ 79

**Setting Up Authentication Devices** .................................... 81
- Set the Authentication Device IP Address ................................ 81
- Mount the Authentication Device ........................................ 84
- Connect the Hardware .................................................... 85

**Associating Authentication Devices with MFPs** ....................... 86

**Configuring Print Tracking** ............................................ 87
- Print Tracking Through Printer Ports .................................. 87
- Print Tracking Using Xerox Network Accounting .................... 88
- Color Tracking Using Xerox Tiered Billing ............................ 91
- Receiving Print Error Messages ....................................... 92

**Configuring SNMP Communication** .................................. 93

### 4 User Workflow ......................................................... 95

**Authenticating at a Card Reader** ..................................... 96
- Authenticating with a Magnetic Stripe Card .......................... 96
- Authenticating with a Proximity or Smart Card ..................... 96

**Card Reader Status Messages** ....................................... 97
Contents

Logging In to a User Session ................................................................. 98
  Smart Card Authentication .................................................................. 98
  Equitrac Server Authentication ....................................................... 98

Using Follow-You Printing ................................................................. 99

Resetting an Authentication Device .................................................. 102

5 Troubleshooting ............................................................................. 103
Introduction

Equitrac Embedded for Xerox Extensible Interface Platform® supports Secure Access Authentication Devices within an Equitrac Office or Equitrac Express environment. In a secure printing Equitrac Office/Express environment, users must authenticate at a Secure Access Device before they are allowed to access the supported Xerox® MFP controlled by the device.

In addition to authentication, users can select and release secure print documents directly from the MFP front panel. This guide provides instructions to configure the server-side requirements within an Equitrac Express or Office environment.
**About User Authentication**

Equitrac Embedded for Xerox Extensible Interface Platform® provides the ability to control access to the print, copy, and scan functions of Xerox® Multifunction peripheral (MFP) devices. When a user approaches an Equitrac-controlled device, they enter user credentials either by using a card, or manually entering data on the MFP front panel. The MFP front panel is unlocked only when the user's account information is authenticated by the accounting server.

Using a proprietary protocol (Convenience Authentication Protocol), the Authentication Device contacts the accounting server via an ethernet network connection to verify the user information gathered from the swipe or proximity card. If the accounting server verifies the user, the MFP device panel unlocks and is ready for use. If the user is not verified, the MFP remains locked and the user cannot perform any tasks at the device.

The Equitrac Device Control Engine (DCE) handles all communication with the MFP devices. When a user wants to use the copy, scan, or fax functionality on a MFP, they must first trigger the card reader. A swipe or proximity read initiates an access request. The Authentication Device forwards the login request to the DCE, which then contacts the Core Accounting Server (CAS) to verify the user account data associated with the card. This process is depicted below.

If the user wants to scan documents, the accounting server provides the network user ID to the compatible MFP; the MFP can then use the ID to implement Single Sign-on functionality and automatically authenticate for scanning.
Chapter 1: Introduction

About Secure Document Release

Secure document release (SDR) holds jobs in the print queue until a user releases them from the MFP panel. When CAS is configured to support SDR, users can view a Follow-You Printing screen on the MFP via the Release My Documents option. This screen displays queued print jobs for the current user. The user can select one or more jobs and release or delete them directly from the MFP front panel.

If you enable multi-server Follow-You Printing on the CAS, the user can view print jobs on other servers also. For additional information on multi-server Follow-You Printing, refer to the Advanced Printing Configuration chapter in the Equitrac Office and Express Administration Guide.

The following diagram illustrates the process flow that occurs after a user submits a print job to a controlled queue on a Xerox® MFP. After sending the print job, the user goes to a controlled MFP, authenticates via a Secure Access Authentication Device, then uses the Follow-You Printing screen on the front panel to access the Equitrac Embedded secure document release functions.

**NOTE:** When the Follow-You Printing extension is not configured, the Follow-You Printing screens are not available on the MFP panel and the user cannot select individual jobs for release. After the user authenticates, all jobs are released from the local or home server or workstation client.
Chapter 1: Introduction

Installation and Configuration Requirements

If you have already set up and configured your Equitrac Office/Express server, you do not need to install the basic Equitrac Embedded for Xerox Extensible Interface Platform® application; you only need to follow configuration procedures.

For instructions on installing and configuring Equitrac Office/Express, see the Equitrac Office and Express Installation Guide and the Equitrac Office and Express Administration Guide.

Before configuring Equitrac Embedded for Xerox Extensible Interface Platform®, you need the following:

- The IP address of the Device Control Engine (DCE) server. You need this address when configuring the MFP to communicate with the DCE server.
- Administrative access to Equitrac System Manager. For details, see Configuring Administrative Access in the Equitrac Office and Express Administration Guide.

Licensing, Server, and MFP Requirements

To enable the Equitrac Embedded solution, you must obtain the following:

- **Equitrac Office/Express Software**
  Equitrac Embedded for Xerox Extensible Interface Platform® requires configuration of the MFPs, Equitrac core accounting server (CAS), and the Secure Access Authentication Devices. This guide provides complete setup instructions for all of these components.

- **One Authentication Device per controlled Xerox® MFP**
  Each MFP is controlled by an Authentication Device, comprised of an authentication terminal and card reader. See Authentication Device Component Requirements on page 11 for details.

- **One Equitrac embedded license per Xerox® MFP**
  Each Secure Access Authentication Device requires an Equitrac embedded license applied in Equitrac's System Manager. For example, if you plan to control 20 Xerox® MFPs, you need to obtain 20 corresponding embedded licenses (enabled for Xerox®) from Equitrac. See Licensing Embedded Devices on page 70 for instructions on adding licenses to the CAS.

- **EIP-enabled Xerox® MFPs**
  If you are not certain whether your MFPs meet this requirement, contact Xerox® for further details. Visit http://www.nuance.com/for-business/by-product/equitrac/supported-devices/xerox/index.htm for a list of supported MFP models.

- **One Network Accounting Enablement Option per Xerox® MFP**
  Only required if you are tracking copy, scan, or fax usage.
  This licensable device option obtained from Xerox® enables the Xerox® MFP to automatically track print, scan, server fax and copy usage for each account.
Authentication Device Component Requirements

A Secure Access Authentication Device is comprised of an Authentication Terminal and an external card reader. When connected to an external card reader, the Authentication Terminal controls user access to the MFP. The user must swipe or pass a card through or near the card reader, and validate user credentials against the accounting server before the MFP is available for use.

Ensure that you have all the hardware provided with each Authentication Device:

- Power supply
- Power cable
- Bypass (Reset) key (metal key used to reset the device to defaults) See Resetting an Authentication Device on page 102.
- 10/100 Base-T Ethernet network cable
- Card Reader

System Requirements

To review the system requirements for the machine or machines hosting the Equitrac server components (Core Accounting Server and Device Control Engine), see the Equitrac Office and Express Installation Guide.

Supported MFPs


Supported MFP models must be EIP-enabled prior to installing the Equitrac Embedded for Xerox Extensible Interface Platform® solution. Please contact your local Xerox® Sales Representative for more information.
Supported Card Readers


All card readers are preconfigured from the manufacturer and require no further configuration.

Magstripe Device Reader

Equitrac Embedded for Xerox Extensible Interface Platform® supports external magnetic stripe reader devices. Users can enter validation data by swiping an encoded magnetic card through the card reader. The reader reads virtually any standard magnetic card medium on track 2, and accepts standard or custom encoded data.

Proximity and Contactless Smart Cards

Equitrac Embedded for Xerox Extensible Interface Platform® supports HID proximity cards, and Mifare and Legic contactless smart cards. Users can enter validation data by passing the card within about one inch of the card reader.

Additional Documentation

You may need to refer to one of the following documents when performing server-side configuration tasks. These documents are located on the Equitrac product CD, and are installed automatically with any server-side component in the Program Files\Equitrac\Office\Documentation or Express\Documentation folder.

<table>
<thead>
<tr>
<th>Guide</th>
<th>When to refer to this guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equitrac Office and Express Planning Guide</td>
<td>Before installing Equitrac Office or Express, use this guide to select the appropriate combination of product variables to support the needs of your institution or organization.</td>
</tr>
<tr>
<td>Equitrac Office and Express Installation Guide</td>
<td>Use this guide to perform an initial installation or upgrade.</td>
</tr>
<tr>
<td>Equitrac Office and Express Administration Guide</td>
<td>After installing Equitrac Office or Express, use this guide to configure advanced options for use on your campus or in your organization.</td>
</tr>
</tbody>
</table>
## List of Terms

The following unique terms are used within this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternate Primary PIN</td>
<td>A sequence of personal identification numbers that uniquely identifies a user who wants to release a print job. The alternate primary PIN can be data encoded on a magnetic swipe card or entered into an MFP keypad.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of entering a primary and optional secondary personal identification number to gain access to a controlled MFP. Users can authenticate via a card reader, or through the MFP control panel.</td>
</tr>
<tr>
<td>Core Accounting Server (CAS)</td>
<td>The Core Accounting Server is a core component of Equitrac Office/Express. This service controls the accounting database that stores all printer, user, department, transaction and balance information. The CAS also verifies users, calculates printing charges and assigns charges to an appropriate user or department.</td>
</tr>
<tr>
<td>Convenience Authentication</td>
<td>A protocol that enables communication between the Authentication Device and the Equitrac server to verify user information gathered from a swipe or proximity card.</td>
</tr>
<tr>
<td>Device Control Engine (DCE)</td>
<td>A core component of Equitrac Office/Express, the DCE communicates with terminals that control access to MFPs.</td>
</tr>
<tr>
<td>Device Routing Engine (DRE)</td>
<td>A core component of Equitrac Office/Express, the DRE enables document flow from workstations to output devices. When a job is released, the DRE captures the job characteristics and communicates the characteristics to the CAS.</td>
</tr>
<tr>
<td>Follow-You Printing</td>
<td>A secure printing feature that holds print jobs in a virtual print queue until the user “pulls” the print job to a selected device. A user can select a particular printer when they submit a print request, then walk to an entirely different compatible MFP and pull the job to that device.</td>
</tr>
<tr>
<td>Follow-You Printing screen</td>
<td>An additional screens that appears as a custom service on the MFP when the Follow-You Printing extension is configured. Users can select one or more jobs from different print servers.</td>
</tr>
<tr>
<td>Multi-server Follow-You</td>
<td>A secure printing feature that extends the Equitrac Follow-You functionality to allow users to view and release secure print jobs from different print servers.</td>
</tr>
<tr>
<td>Network Accounting</td>
<td>A feature of the Xerox® MFP which automatically tracks print, scan, server fax and copy usage for each user. Network accounting is run over a network and the accounting transactions are performed remotely by Equitrac Office/Express server software.</td>
</tr>
<tr>
<td>Print Tracking</td>
<td>The ability to track the attributes of a released network print job. For example, number of pages, page size, color, etc. You can configure Equitrac Embedded for Xerox Extensible Interface Platform® to track printing through the embedded device or through a printer port.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary PIN</td>
<td>A sequence of numbers that act as a user ID to uniquely identify a user who wants to release a print job. The primary PIN can be entered on the MFP keypad.</td>
</tr>
<tr>
<td>Secondary PIN</td>
<td>A sequence of numbers that act as a password when used in conjunction with a Primary PIN. After entering the Primary PIN, the user must enter the Secondary PIN code on a MFP keypad before the print job is released to a device. Secondary PINs are an optional configuration.</td>
</tr>
<tr>
<td>Secure Document Release (SDR)</td>
<td>An Equitrac Office/Express feature that holds network print jobs in a secure virtual print queue. Users must authenticate at an MFP to release jobs from the secure queue. The goal of secure printing is to ensure that proprietary information does not sit at an output device for public consumption.</td>
</tr>
</tbody>
</table>
MFP Configuration

Topics

- Configuring MFP Properties
- WorkCentre 3315 and 3325 Series
- WorkCentre 3615 and 6605
- WorkCentre 4265
- WorkCentre 52xx, 7232/7242, 73xx, and 74xx Series
- WorkCentre 56xx Series
- WorkCentre 75xx Series
- WorkCentre 76xx Series
- WorkCentre 77xx Series and ColorQube 93xx, 92xx or 89xx Series
- WorkCentre Pro 2xx Series
- Phaser 3635

To enable Equitrac Embedded for Xerox Extensible Interface Platform®, you must configure the MFPs. Follow the steps for each MFP series in the order they are presented to ensure a successful install.
Configuring MFP Properties

The following are the main steps when configuring Xerox® MFPs:

1. Ensure that the time zone on the MFP is correct. If the time zone is not correct, Equitrac Embedded transaction times are incorrectly reported.

2. Confirm that the date and time setting on the MFP is within 24 hours of the date and time configured on the server that hosts the Equitrac DCE component. If the settings are more than 24 hours apart, the Equitrac Embedded application on the MFP will not connect to the server.

3. Configure the MFP to use Secure Access Authentication and to communicate with the DCE Server.

4. Ensure that the SNMP settings on the device are correct. The device can be configured for SNMPv2 or SNMPv3 communication. See Configuring SNMP Communication on page 93 for SNMP options.

5. Ensure SSL is enabled on the Xerox® MFP. If it is not enabled, generate a self-signed certificate and then enable SSL communication.

6. Verify the firmware version on the Xerox® MFP. MFPs running Xerox Extensible Interface Platform® firmware versions 1.5 and 2.0 require that the Embedded Manual Override is Enabled in order for the attached Equitrac card reader to operate normally. Contact your local Xerox® representative for information on the appropriate firmware for your MFPs. Refer to WorkCentre 75xx Series on page 39 for details on enabling this option.
WorkCentre 3315 and 3325 Series

Configuration of WorkCentre 33xx MFPs is performed via the Internet Services interface, and through System Manager. No configuration at the MFP console is required. This process assumes that you have created a self-signed certificate as discussed in the Equitrac Office/Express Administration Guide, and have enabled https communications for the device.

**NOTE:** The WorkCentre 3315 and 3325 devices do not support the Xerox Extensible Interface Platform® framework. These devices are included here for their ability to use Convenience Authentication.

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **Authentication** folder, and then **Authentication**.
4. In the right pane, select **Xerox Secure Access**, then click **Apply**.
5 In the left pane, select the **Network Security** folder, then the **External Authentication Server** subfolder, and finally **Xerox Secure Access**.

![Network Security Setting](image)

6 Select Xerox Secure Access options:

   a. Under **Feature Coverage**, select **All Features** to force users to log in before using any device features such as copying or email. Select **Scanning Features Only** to allow the use of device features other than scanning without logging in.

   b. Under **Login Initiation**, select the **Enable** check box to allow users to login manually from the device. This provides an alternate login option.

   **NOTE**: Do not modify the Server Communication settings. These are set automatically upon device registration.

7 Click **Apply**.
8 In System Manager, navigate to Configuration > Devices > Embedded Devices. The Embedded Devices dialog opens:

![Embedded Devices dialog](image)

9 Ensure Xerox Secure Access is selected in the Device type drop down list.

10 Configure the Device Prompts:
   a In the Title field, enter text that will display on the device panel as a title.
   b In the Login Prompt field, enter text that will display to instruct the user how to log in.
   c Select the Enable release all jobs prompt check box to prompt the user to confirm printing rather than automatically releasing waiting print jobs upon login.

11 Click OK.

12 In System Manager, navigate to Configuration > Devices > Embedded Devices. The Embedded Devices dialog opens:

![Embedded Devices dialog](image)

13 Select Xerox/Fuji Xerox JBA from the Device Type drop-down list.

14 Ensure Tracked activities is showing there are <no jobs> selected.
15 Ensure Enable authentication upload is deselected.
16 Ensure Automatic Job release of all print jobs upon validation is selected.
17 Click OK.
18 In System Manager, select Devices from the left pane to display a list of available devices.
19 Locate the device in the list, and find its associated embedded device. Double click the embedded device link to display the options for the embedded device.
20 Click the Initialize button to display the Initialize Xerox EIP, JBA device screen:

![Initialize Xerox EIP, JBA device screen]

21 Ensure the Enable Follow-You Printing applet check box is deselected. Leave all other values as default.
22 Click Initialize.
**WorkCentre 3615 and 6605**

Use System Manager and the browser-based Internet Services interface to configure the WorkCentres 3615 and 6605 MFPs. No configuration at the MFP console is required. This process assumes that you have created a self-signed certificate as discussed in the Equitrac Office/Express Administration Guide, and have enabled https communications for the device.

**NOTE:** The WorkCentre 3615 and 6605 devices do not support the EIP framework. These devices are included here for their ability to use Convenience Authentication.

Do the following:

1. Open a Web browser and enter `http://<MFP IP address>` in the URL bar.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **Security** folder, and then **SSL**. The SSL settings display.
4. In the **Enable SSL** option, ensure the check box is **selected**, then click **Save Changes**.
5 In the left pane, select the Security folder, and then Secure Settings. The Secure Settings screen displays:

6 Under **Network Authentication**, ensure the **Network Authentication** option check box is **selected**. Scroll down and click **Save**.
7 In the left pane, select the **Security > Authentication System**. The **Authentication System** screen displays:

![Authentication System screen](image)

8 From the Authentication System Settings drop-down list, select **Xerox Secure Access**. Then click **Save Changes**.
9 In the left pane, select Security > Xerox Secure Access Settings. The Xerox Secure Access Settings screen displays:

In the Optional Information section, ensure the Alternate Login check box is selected. This allows users to use Alternate Login from the device.

NOTE: Do not modify the Server Communication settings. These are set automatically upon device registration.
WorkCentre 4265

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with User ID and Password if prompted. The Extensible Service Setup screen displays:

3. In the left tab, click the General Setup > Extensible Service Setup.
4 Click the **Edit** button in the **Extensible Service Registration** row. The **Web Services** options display:

![Web Services Configuration](image)

5 Click **Enable all** at the top of the screen. Both the **Authentication & Accounting Configuration** and **Job Limits** options are enabled by default. Ensure this is the case; if these services are not enabled, errors occur when initializing the Xerox embedded device in System Manager, causing the Copy Stop feature to not work.

**NOTE:** The Authentication & Accounting Configuration and Job Limits services must be enabled via the Internet Services interface.
6. In the left pane, click the **Login/Permissions/Accounting** folder, then the Login Methods subfolder. Select **Convenience**. Select **User can login at device if card is not available** option if desired.

7. Click **Edit** icon for **Convenience Authorization Setup**.

8. In the **Accounting Information** section, select **Automatically apply Account Codes from the server**. The Server communication information will be filled out by the initialization process. Click **Save**.
9. In the left pane, click the **Login/Permissions/Accounting** folder, then the **Login Methods** subfolder. Click the **Edit** icon for **Card Reader Policy**. Select option for the Card reader policy and click **Save**.

10. In the left pane select **Login/Permissions/Accounting**. Select **User Permissions**.
11 Click **Edit** icon under **Non-Logged-In (Guest) User Role**. Select **Not Allowed** for services to be locked and click **Save**.
12 In the left pane select **Login/Permissions/Accounting** and then **Accounting**. Select **Network Accounting**.

13 Click **Edit** beside **Accounting Workflow**. Select **Capture Usage**. Click **Save**.
WorkCentre 52xx, 7232/7242, 73xx, and 74xx Series

All configuration of the WorkCentre 52xx, 7232/7242, and 73xx MFPs is performed via the Internet Services interface. No configuration at the MFP console is required.

**NOTE:** If prompted to reboot during this process, reboot and resume configuration at the next step.

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the **Services** folder, then the **Custom Services** subfolder, and then **Custom Services**.

4. In the right pane, ensure that **Custom Services** is set to **Enabled**, then click **Apply**. The Custom Services button should now be present on the MFP user interface when All Services is selected.

5. In the left pane, select the **Accounting** folder, then the **Accounting Configuration** subfolder.
6 In the **Authentication Configuration > Step 1 of 2** page, set the following options:
   a Select **Network Accounting** from the **Accounting Type** drop-down list.
   b Enable the services you want to track on this MFP: **Copy, Fax, Scan, and Print**.
   c Select **Yes** from the **Verify User Details** drop-down list.
   d Select **No** from the **Verify User Details for Printer Jobs** drop-down list. (Jobs will not print if set to Yes.)

   **NOTE:** For models 72x2 with older firmware, it may be necessary to set the **Verify User Details** option to **No** in order to avoid transactions being recorded against “Unidentified user”.

   e Select **Display User ID & Account ID Prompts** from the **Customize User Prompts** drop-down list. Failure to set this option causes transactions to be recorded against “Unidentified user”.

7 Click **Apply** to save these settings.

8 Click **Reboot Machine**, if prompted.

   **CAUTION:** While the MFP is rebooting, do NOT click anywhere on the web page, as an error message indicating that services are unavailable will appear. If this occurs, once the device is back online, you will need to login again to the web page and navigate to the applicable menu before continuing.

9 In the left pane, select the **Security** folder, then the **Authentication Configuration** subfolder.

10 In the **Authentication Configuration > Step 1 of 2** page, set the following options:
   a Select **Xerox Secure Access** from the **Login Type** drop-down list.
   b Select **Off** from the **Guest User** drop-down list.
   c Leave all other options unchanged.

11 Click **Apply** to save the settings.

12 Reboot the machine when prompted. Do NOT click anywhere on the web page until the reboot is complete.

13 Click **Next** to continue to the **Authentication Configuration > Step 2 of 2** page.
14 To lock the front panel of the MFP, click the **Configure** button beside the **Device Access** option.

![Authentication Configuration > Step 2 of 2](image)

15 Set the **All Services Pathway** to **Locked**, and then click **Apply**.

![Authentication Configuration > Device Access](image)

16 Reboot the machine when prompted. Do NOT click anywhere on the Web page until the reboot is complete.

17 To lock some, but not all, of the Services, click the **Configure** button located beside the **Service Access** option.

![Authentication Configuration > Step 2 of 2](image)
18 On the Service Access page, select the services you want to control access to, then click **Save**.

- **Locked (Show Icon)** - the service appears on the MPF control panel, but cannot be accessed without authentication.
- **Unlocked** - the service appears on the control panel and is accessible without authentication.

19 Click the **Apply** button to save all of the Configuration Authentication settings.

20 In the left pane, select the **Security** folder, then the **Remote Authentication Servers** subfolder, and then **XeroxSecureAccess Settings**.

21 In the Xerox Secure Access Settings page in the right pane, set the following options:

   a Set **Local Login** to **Enabled** (checked) if you want to make the keyboard access button visible.

      **NOTE:** Although the Local Login setting is optional, ensure that you check this option at first configuration. After first initialization, this option can only be enabled if the device is cleared from all settings (back to the factory defaults).

   b Set **Get Accounting Code** to **Enabled** (checked). You must select this option to enable authentication.

   c Set the **Connection Time-Out** value to at least **15** seconds, or a larger value to avoid timeout messages on the MFP.

22 Click **Apply** to save these settings and to complete the configuration of this MFP.

23 Click **Reboot Machine**, then close the web browser.
WorkCentre 56xx Series

You must configure the WorkCentre 56xx series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the General Setup folder, then select the Custom Services Setup subfolder.
   - If it says Configured beside Custom Service Registration the option is enabled.
   - If it says Not Configured, click the Configure button and click the Custom Services Registration option. Click the Save button.
4. In the Enable Custom Services section, select the Display Custom Services Section button at the local user interface option.
5. In the Browser Settings section, select the Enable the Custom Services Browser option. If you do not enable this option, nothing will happen when you press the button.

   **CAUTION:** If the services are not installed, contact Xerox regarding custom services installation.

6. In the right pane, ensure that Custom Services is set to Enabled, then click Apply. The Custom Services button should now be present on the MFP user interface when All Services is selected.
On the MFP Console

1. Log into the Tools menu with your Administrator user ID and password.
2. Touch All Services. Ensure that you can see the Custom Services button. If not, power off/on the MFP and wait until the MFP is ready.
3. Touch Access and Accounting.
4. Touch Authentication Mode.
5. Under Network Accounting, touch the On option to enable Network Accounting. Ensure that all other authentication options are disabled. Touch Save.
6. Return to the Access and Accounting menu, then touch Network Accounting Setup.
7. Touch Network Accounting Authentication.
8. If you are print tracking via an printer port or the Direct IP Printing Client (DRC), touch Disable under Network Accounting Authentication Setup, then touch Save. If this setting is not disabled, no jobs will print.
9. Exit the Tools screen, and return to copy mode. Configuration on the MFP console is now complete.

Via the Internet Services Interface

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the Security folder, then select Authentication Configuration.
4 In the **Where is the information located** section, select **Xerox Secure Access** from the **Device User Interface Authentication** drop-down list, and then click **Next**.

**NOTE:** If the MFP device is in Sleep mode, click the **Exit Sleep Mode** button to wake the device.

5 Click the **Edit** button beside the **Access Setup Wizard** option.

6 In the **Pathway Services** section, select the services you want to control access to, then click **Save**.

7 In the **Installed Services Pathway Access** section, select **Locked** under Services Pathway and click the **Next** button to lock everything on the device. To lock only certain features, leave **Services Pathway** set to **Unlocked** and click the **Next** button. Select the services you want to control access to, then click **Save**.

   - **Unlocked** - the service appears on the control panel and is accessible without authentication.
   - **Locked** - the service appears on the MFP control panel, but cannot be accessed without authentication.
   - **Hidden** - the service does not appear on the control panel.

8 Still on the Authentication Configuration page, click the **Edit** button beside the **Device User Interface Authentication** option.
9 Click the **Manual Override Settings** button at the bottom of the page

![Manual Override Settings](image)

10 Under **Device Log In Methods**, select the preferred method:
   - Xerox Secure Access Device Only – if you do not want people to use the alternate key board login button to enter their user ID
   - Xerox Secure Access Device + alternate on-screen authentication method – if you want people to also be able to use the alternate key board login button to enter their user ID

11 Under **Accounting Information (Requires Network Accounting)**, select Automatically apply Accounting Codes from the server. This prevents additional unnecessary authentication prompts.

12 Click the **Save** button.

13 Logout of the MFP’s configuration utility and close the web browser.
Chapter 2: MFP Configuration

WorkCentre 75xx Series

The WorkCentre 75xx series MFPs utilize the Job Limits functionality to support Copy Stop enforcement. The MFP scans the copy job, collects the job information in a JBA (Job-based Accounting) style record and sends it to the server for approval. The server approves or rejects the job depending upon the funds available, color quotas, and copy/print rules. The user balance is updated as each job is copied. The Copy Stop is enforced at the start or during the session.

You must configure the WorkCentre 75xx series MFPs from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

Xerox Extensible Interface Platform® cannot be configured unless Custom Service is installed on the MFP. To determine if custom services is installed on a WC75xx series, perform these steps:

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the General Setup folder, then select Extensible Service Setup.
4. Click the Edit button beside the Extensible Service Registration option.
5 Click on **Enable All**, then click **Save**. The Custom Services button should now be present on the MFP user interface when All Services is selected.

If you cannot access or locate these options, contact Xerox® regarding correct installation of Custom Services.

**On the MFP Console**

1 Log into the **Tools** menu with your Administrator user ID and password.

2 Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.

3 Enter the user name and password.

4 On the Machine Status screen, touch the **Tools** tab.

5 Touch **Accounting Settings > Accounting Mode**.

6 On the Accounting Mode screen, touch **Network Accounting**, then touch **Customize Prompts**.

7 On the Customize User Prompts screen, touch **Display Prompt 1 and 2**, then touch **Save**. Failure to set this option causes transactions to be recorded against “Unidentified user”.

8 Set **Code Entry Validation** to **Disabled**.

9 Touch the **Save** button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.
1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the Properties tab, and login with your User ID and Password when prompted.
3. In the left pane, click the General Setup folder, then select Extensible Service Setup.
4. Click the Edit button beside the HTTP (SSL) option.
5. Set the Secure HTTP (SSL) option to Enabled, then click Save.
6 Click the **Edit** button beside the **Extensible Service Registration** option.
7 Click **Enable All**, then click **Save**.

### HTTP

<table>
<thead>
<tr>
<th>Device Discovery</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-Discovery</td>
<td>Enabled</td>
</tr>
<tr>
<td>WS-Discovery Multicast</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote System Management</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensible Service Registration</td>
<td>Enabled</td>
</tr>
<tr>
<td>XEIP Proxy Configuration</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Interface Configuration</td>
<td>Enabled</td>
</tr>
<tr>
<td>Device Configuration</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Print Services</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-Print</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scan Services</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Template Management</td>
<td>Enabled</td>
</tr>
<tr>
<td>Scan Extension</td>
<td>Enabled</td>
</tr>
<tr>
<td>WS-Scan</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication &amp; Accounting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox Secure Access</td>
<td>Enabled</td>
</tr>
<tr>
<td>Authentication &amp; Accounting Configuration</td>
<td>Enabled</td>
</tr>
<tr>
<td>Session Data</td>
<td>Enabled</td>
</tr>
<tr>
<td>Job Limits</td>
<td>Enabled</td>
</tr>
<tr>
<td>Digital Certificate Management</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Ensure that both **Authentication & Accounting Configuration** and **Job Limits** are enabled. They are enabled by default. These services must be enabled via the Internet Services interface—not through the physical device.

If these services are not enabled, errors occur when initializing the Xerox® embedded device in System Manager, causing the Copy Stop feature to not work.

**NOTE:** Job Limits is not supported on all Xerox® devices.
8 In the **Browser Settings** section on the Extensible Service Setup page, select the **Enable the Extensible Services Browser** checkbox and click **Apply**.

<table>
<thead>
<tr>
<th>Enable the Extensible Services Browser</th>
<th>Browser Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>checked</td>
<td>2.1.10.12030002.02</td>
</tr>
</tbody>
</table>

9 In the left pane, click the **Security** folder, then the **Authentication** subfolder, and then **Setup**.

10 On the **Xerox Access Setup** page, click the **Edit** button to change the Authentication method.

![Xerox Access Setup](image)

**NOTE:** If the copier has not been previously configured, you may need to click the **Next** button (instead of **Edit**) and then work through a wizard to configure the copier.
11 On the Authentication, Authorization and Personalization page, do the following:

- Select Xerox Secure Access Unified ID System from the Authentication method on the machine's touch interface drop-down list.
- Select User Name/Password Validated Locally on the Xerox Machine from the Authentication method on the machine's web user interface drop-down list.
- Select Locally on the Xerox Machine from the Authorization information is stored drop-down list.
- Click Save to apply the changes.

12 On the Xerox Access Setup page, click the Edit button beside the Xerox Secure Access Setup option under Configuration Setting.

13 On the Xerox Secure Access Setup page, click the Manually Override Settings button.
On the Manual Override page, set the following:

- In the **Server Communication** section, set the **Embedded** option to **Enabled**.

  **NOTE:** The **Embedded** option must be **Enabled** on Xerox® MFPs running Xerox Extensible Interface Platform® firmware version 1.5 or 2.0 in order for the attached Equitrac card reader to operate normally.

- In the **Device Log In Methods** section, select the preferred method.

- In the **Accounting Information** section, select **Automatically apply Account Codes from the server**.

15 Click **Save** to apply the changes, then click **Close**.

16 Click **Close** again on the Xerox Secure Access Setup page to return to the main Authentication Configuration page.

17 Click the **Edit** button beside the **Service Registration** option.

18 Select the services you want users to access, then click **Save**.

Select the services you want to display as the machine’s touch interface.
19 In the left pane, click the **Security** folder, then the **Authentication** subfolder, and then **Tools & Feature Access**.

![Tools & Feature Access](image)

20 In the **Presets** section, select the **Custom Access** option to select the services you want to control access to.

- **Unlocked** - the service appears on the control panel and is accessible without authentication.
- **Locked** - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
- **Hidden** - the service does not appear on the control panel.

21 Click **Apply** to complete the configuration of this MFP.

22 Logout of the MFP’s configuration utility and close the web browser.
WorkCentre 76xx Series

You must configure the WorkCentre 76xx series from both the MFP Console and the Internet Services interface. Before starting the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the General Setup folder, then select Extensible Service Setup.
4. Click the Settings button for the Extensible Service Registration setup option.

5. Click Enable All, then click Save. The Custom Services button should now be present on the MFP user interface when All Services is selected.

If you cannot access or locate these options, contact Xerox® regarding correct installation of Custom Services.
On the MFP Console

1. Log into the Tools menu with your Administrator user ID and password.
2. Touch All Services. Ensure that you can see the Custom Services button. If not, power off/on the MFP and wait until the MFP is ready.
3. Enter the user name and password.
5. Touch Accounting > Accounting Enablement > Accounting Mode.
6. On the Accounting Mode screen, touch Network Accounting, then touch Customize Prompts.
7. On the Customize User Prompts screen, touch Display Prompt 1 and 2, then touch Save to save the changes. Failure to set this option causes transactions to be recorded against “Unidentified user”.
8. Touch the Save button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.

Via the Internet Services Interface

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the Security folder, then select Authentication Configuration.
4. On the Authentication Configuration page, click Edit Methods to change the Authentication method.

NOTE: If the copier has not been previously configured, you may need to click the Next button (instead of Edit Methods) and then work through a wizard to configure the copier.

6. Click Save to apply the changes.

7. On the Authentication Configuration page, click the Edit button beside the Xerox Secure Access option.
8 Ensure that all services listed are enabled, and then click save.

9 On the Authentication Configuration page, click the Edit button beside the Device User Interface Authentication option.

10 On the Xerox Secure Access Setup page, click the Manually Override Settings button.

11 Click Manual Override Setting at the bottom of the page.

12 On the Manual Override page, set the following:
   a In the Device Log In Methods section, select the preferred method.
      • Xerox Secure Access Device Only – if you do not want people to use the alternate key board login button to enter their user ID
      • Xerox Secure Access Device + alternate on-screen authentication method – if you want people to also be able to use the alternate key board login button to enter their user ID
Chapter 2: MFP Configuration

b In the Accounting Information section, select Automatically apply Account Codes from the server.

13 Click Save to apply the changes, then click Close.
14 On the Authentication Configuration page, scroll down and click the Edit button beside the Access Setup Wizard option.
15 In the Device Access page, if you want to lock the front panel of the MFP, set the Services Pathway to Locked and then click Save, otherwise click the Next to continue.
16 To lock only certain features, leave Services Pathway set to Unlocked and click Next. Select the services you want to control access to, then click Next.
   - Unlocked - the service appears on the control panel and is accessible without authentication.
   - Locked - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
   - Hidden - the service does not appear on the control panel.

17 Click Finished on the Feature Access page to complete the configuration of this MFP. The WorkCentre 76xx series device is now configured.
18 Logout of the MFP's configuration utility and close the web browser.
WorkCentre 77xx Series and ColorQube 93xx, 92xx or 89xx Series

You must configure the WorkCentre 77xx series MFP and the ColorQube 93xx, 92xx or 89xx Series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

NOTE: This document assumes that any 89xx devices are running upgraded firmware that allows the device to function as a "ConnectKey" device. Devices with older firmware do not follow these instructions. For information about identifying which firmware version your device is running, see the Xerox® support web site.

Locating Custom Services

Xerox Extensible Interface Platform® cannot be configured unless Custom Service is installed on the MFP. To determine if custom services is installed on a WC77xx series and ColorQube 93xx, 92xx or 89xx Series, perform these steps:

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the General Setup folder, then select Extensible Service Setup.
4. Click the Edit button beside the Extensible Service Registration option.
Click on **Enable All**, then click **Save**. The Custom Services button should now be present on the MFP user interface when All Services is selected.

If you cannot access or locate these options, contact Xerox® regarding correct installation of Custom Services.

**On the MFP Console**

1. Log into the **Tools** menu with your Administrator user ID and password.
2. Touch **All Services**. Ensure that you can see the **Custom Services** button. If not, power off/on the MFP and wait until the MFP is ready.
3. Enter the user name and password.
4. On the Machine Status screen, touch the **Tools** tab.
5. Touch **Accounting Settings > Accounting Mode**.
6. On the Accounting Mode screen, touch **Network Accounting**, then touch **Customize Prompts**.
7. On the Customize User Prompts screen, touch **Display Prompt 1 and 2**, then touch **Save**. Failure to set this option causes transactions to be recorded against "Unidentified user".
8. Set **Code Entry Validation** to **Disabled**.
9. Touch the **Save** button again to save all changes, then log off the MFP Console. Configuration at the console itself is now complete. You now need to complete the rest of the configuration via the web interface.
Chapter 2: MFP Configuration

Via the Internet Services Interface

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your User ID and Password when prompted.
3. In the left pane, click the **General Setup** folder, then select **Extensible Service Setup**.

- **Extensible Service Setup**
  - **HTTP (SSL)**
  - **Extensible Service Registration**

4. Click the **Edit** button beside the **HTTP (SSL)** option.
5. Set the **Secure HTTP (SSL)** option to **Enabled**, then click **Save**.
6 Click the **Edit** button beside the **Extensible Service Registration** option.

7 Click **Enable All**, then click **Save**.

8 In the **Browser Settings** section on the Extensible Service Setup page, select the **Enable the Extensible Services Browser** checkbox, and click **Apply**.
9. In the left pane, click the **Security** folder, then the **Access Rights** subfolder, and then **Setup**.

10. In the right pane, click **Edit Methods** to change the Authentication method.

   ![Authentication Configuration](image)

   **NOTE:** If the copier has not been previously configured, you may need to click the **Next** button (instead of **Edit Methods** and then work through a wizard to configure the copier.

11. Select **Xerox Secure Access** from the **Device User Interface Authentication** drop-down list. Leave both **Web User Interface Authentication** and **Authorization** options set to **Locally on the Device**.

12. Click **Save** to apply the changes.

13. On the Authentication Configuration page, click the **Edit** button beside the **Device User Interface Authentication** option.

14. On the Xerox Secure Access Setup page, click the **Manually Override Settings** button.
On the Manual Override page, set the following:

a. In the **Server Communication** section, set the **Embedded** option to **Enabled**.

b. In the **Device Log In Methods** section, select the preferred method.

c. In the **Accounting Information** section, select **Automatically apply Account Codes from the server**.

16. Click **Save** to apply the changes, then click **Close**.

17. Click **Close** again on the Xerox Secure Access Setup page to return to the main Authentication Configuration page.

18. Click the **View** button beside the **Service Registration** option.

19. Select the services you want users to access, then click **Save**.
20 In the left pane, click the **Security** folder, then the **Access Rights** subfolder, and then **Tools & Feature Access**.

![Tools & Feature Access](image)

21 In the **Presets** section, select the **Custom Access** option to select the services you want to control access to.

- **Unlocked** - the service appears on the control panel and is accessible without authentication.
- **Locked** - the service appears on the MPF control panel, but cannot be accessed until the user authenticates.
- **Hidden** - the service does not appear on the control panel.

22 Click **Apply** to complete the configuration of this MFP.

23 Logout of the MFP’s configuration utility and close the web browser.
WorkCentre Pro 2xx Series

You must configure the WorkCentre Pro 2xx series MFP from both the MFP Console and via the Internet Services interface. Before you perform the configuration, ensure that Custom Services is installed on the MFP.

Locating Custom Services

1. Open a Web browser and enter the URL http://<MFP IP address> in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. Select the Services folder in the left navigation pane, then select the Custom Services subfolder. If there is another sub-option in this folder called Custom Services, then the service is installed and you can proceed.

   NOTE: If the services are not installed, contact Xerox® regarding correct installation of these services.

4. In the right pane, ensure that Custom Services is set to Enabled, then click Apply. The Custom Services button should now be present on the MFP user interface when All Services is selected.

On the MFP Console

1. Log into the Tools menu with your Administrator user ID and password.
2. Touch All Services. Ensure that you can see the Custom Services button. If not, power off/on the MFP and wait until the MFP is ready.
3. Touch Access and Accounting.
4. Touch Authentication Mode.
5. Under Network Accounting, touch the On option to enable Network Accounting. Ensure that all other authentication options are disabled. Touch Save.
6. Return to the Access and Accounting menu, then touch Network Accounting Setup.
7. Touch Network Accounting Authentication.
8. If tracking printing via an printer port or the Direct IP Printing Client (DRC), under Network Accounting Authentication Setup, touch Disable, then touch Save.
9. Exit the Tools screen, and return to copy mode. Configuration on the MFP is now complete.
Via the Internet Services Interface

1. Open a web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the **Properties** tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the **Security** folder, then the **Authentication Server** subfolder, and the **General**.
   
   ![Authentication Server Screenshot]

4. In the right pane, set the following options:
   
   a. In the **General** section, set the **Authentication Type** to **Xerox Secure Access**.
   b. In **Feature Coverage**, select **All Features**.
   c. In **Account Codes Access**, enable the **Accounting Codes Provided by Server** option.
   d. In **Login Initiation**, enable the **Allow Local User Interface Initiation** option to make the keyboard access button visible. This is optional.
   e. In **Server Communication**, leave the fields blank. The Equitrac server will complete this information when you initialize this MFP later on in the workflow.

5. Click **Apply** to complete the configuration of this MFP.
6. Logout of the MFP’s configuration utility and close the web browser.
Phaser 3635

Configuration of Phaser 36xx MFPs is performed in two steps: First, via the Internet Services interface, and then at the MFP to select Xerox® ECSP as the default application.

**CAUTION:** In order to enable Network Authentication, a default "From" address must be configured. If you have not yet done so, designate an email address by navigating to Services > E-mail Settings > Defaults. Under the General section, click the Edit button, and type a default From email address in the From address field, then click Apply.

**Internet Services Interface Configuration**

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, select the Services > Custom Services. The Custom Services screen displays:

![Custom Services](image)

4. Ensure that Custom Services is set to Enabled, then click Apply. The Custom Services button should now be present on the MFP user interface when All Services is selected.

**NOTE:** Select this option only if you want to enable keyboard access to the device for login purposes. With this option deselected, only card swipe login is possible.

f. The settings in the Server Communication section are populated from settings determined when the embedded device was set up.
g. Provide a Default Title and Default Prompt the user sees when starting to use the device.
h. The Logoff Reminder is selected by default, and cannot be altered.
5. Click Apply.

**Phaser MFP Configuration**

Phaser MFPs require that you set the device default application manually. By setting this, the device uses the Xerox® ECSP by default.

For each Phaser MFP using Xerox® ECSP, go to the device, and do the following:

1. Press the Machine Status hard key to the left of the display.
2. Touch the Guest button at the top right of the display, then select Log In from the drop-down menu.
3 Touch the Keyboard icon in the center of the screen, and using the soft keyboard, provide your administrator password to log in to the device. The System Administration screen displays:

4 Select the Tools tab, then select User Interface, and General. The User Interface General settings options display.

5 From the list of features, select Screen Defaults.

   a Select Entry Screen Default

   b Select Features
c  Select Save

d  Select Default Feature and Priority Order

6 Set the Highest Priority service:

a  From the list of priorities, touch the Custom Services... button to select it.

   NOTE: If the Custom Services... option is absent from the list, return to the Entry Screen Default list, deselect Features and then reselect Features. This resets the Highest Priority list.

b  Use the arrow buttons to the right of the list to move the Custom Services... button to the top of the list.

   NOTE: The Highest Priority list can only display 4 options. If your option is not listed, move one of the listed options to the bottom of the list.

7 From the EIP app list, touch Xerox ECSP to select it.

8 Touch Save.

9 Touch Close.

10 Touch the Admin button at the top right of the display, then select Log Out.

   CAUTION: If a device is initialized to point to a different DWS server after initial setup, the default Highest Priority service must be manually reset to prevent ECSP from inappropriately displaying the login screen. To reset the Highest Priority service follow steps 6 through 8 above, selecting Custom Services from EIP app list, and then follow these steps a second time, reselecting Xerox ECSP as the Highest Priority service.
Other settings

1. In the left pane, select the **Security > Authentication > Authentication**. The **Authentication** screen displays:

   ![Authentication Screen](image)

   - Ensure in the **Guest Access** section, **Allow Guest Access** is **deselected**.
   - Ensure in the **Feature Coverage** section, **All Features** is **selected**.
   - Ensure **Accounting Code Access** is **Enabled**.
   - In the **Login Initiation** section, deselect **Allow Local User Interface Initiation**.
Smart Card Configuration

The Xerox® Smart Card solution provides a two-factor identification requirement. Users must insert their access card and enter a unique PIN at the device. Once validated, a user is logged into the Xerox® device for all features. The Smart Card solution requires a Smart Card Enablement Kit and a Feature Enable Key, provided by Xerox®. Before installing the Xerox® Smart Card solution, the software needs to be enabled on both the MFP Console and via the Internet Services interface.

On the MFP Console

1. Log into the Tools menu with your Administrator user ID and password.
2. Touch More to access additional Tools options.
3. Touch Optional Services. If necessary, use More to navigate to the option.
4. Touch Smart Card. If necessary, use More to navigate to the option.
5. When prompted, touch the Option Kit Number entry field and enter the unique Feature Enable Key provided with the Smart Card Enablement kit.
7. Reboot the device. The device may automatically reboot.

Once the reboot is complete, the Smart Card function is ready to be configured using the Internet Services interface.

NOTE: No services on the device will be restricted until Smart Card has been configured using Internet Services. Via the Internet Services Interface
Via the Internet Services Interface

To enable and configure the Smart Card, do the following:

1. Open a Web browser and enter the URL `http://<MFP IP address>` in the Address field.
2. Select the Properties tab, and login with your Administrator user ID and password when prompted.
3. In the left pane, click the Security folder, then the Authentication subfolder, and then Setup.
4. On the Xerox Access Setup page, click the Edit button to change the Authentication method.
5. On the Authentication, Authorization and Personalization page, do the following:

   a. Select SmartCards from the Authentication method on the machine's touch interface drop-down list.

   b. Select User Name/Password Validated Remotely on the Network from the Alternate authentication method on the machine's touch interface (Touch UI) drop-down list.

   c. Select User Name/Password Validated Locally on the Xerox Machine from the Authentication method on the machine's web user interface (Web UI) drop-down list.

   d. Select Locally on the Xerox Machine (Internal Database) from the Authorization information is stored drop-down list.

   e. Click Save to apply the changes.

A list of configuration settings appears at the bottom of the Xerox Access Setup page. Click Edit to configure any settings that are marked in red text as Required; Not Configured.
Configuring Domain Controller Settings

1. In the Configuration Settings table on the Xerox Access Setup page, click Edit on the Domain Controller(s) row. The domain certificate on a user's Smart Card must be validated on the domain controller server before they can access the MFP.

2. Click Add Domain Controller.

3. Under Domain Controller Type, select Windows Based Domain Controller.

4. Select the IPv4 option and enter the domain controller server IP Address and Port number.

5. Enter the Domain name.

6. Click Save to apply the new settings and return to the Domain Controller page.

**NOTE:** If you have more than one domain controller server, you can click Change Domain Priority and use the Up and Down arrows to change the search priority of the server.
7 Click Edit beside Network Time Protocol (NTP).

8 Enable NTP to ensure time synchronization between the domain controller and the MFP.

9 Click Close to return to the Xerox Access Setup page.

**Setting the Inactive Time Limit**

1 In the Configuration Settings table on the Xerox Access Setup page, click Edit on the Smart Card Inactivity Timer row.

2 Specify the maximum amount of Smart Card inactivity time (in minutes) before a user is automatically logged out.

3 Click Save to apply the new settings and return to the Authentication Setup page.

The Smart Card settings are now configured. Please refer to the Xerox® Smart Card Installation Guide to install the Smart Card hardware.
To enable Equitrac Embedded for Xerox Extensible Interface Platform®, you must configure the Authentication Devices, MFPs, and the core accounting server (CAS). Follow the steps below in the order they are presented to ensure a successful install.
Chapter 3: Server-Side Configuration

Licensing Embedded Devices

Each MFP requires a single Equitrac Embedded license configured for Xerox. You must obtain these licenses before configuring the CAS or adding embedded devices. You can buy a single license or a license pack as needed.

Licensing requires a combination of a serial number and an activation code to enable each Equitrac Embedded device. Although the serial numbers are supplied with the software, you must also enter an activation code. You can enter this code automatically through an online registration form, or manually by requesting the code by telephone or via the Equitrac website. Regardless of the method used, follow the instructions below to apply licenses and activate components.

1. Start System Manager by selecting Start > Programs > Equitrac Office/Express > System Manager.
2. In the Select Accounting server window, choose the CAS with which System Manager is associated, then click Connect.
3. Click the System Manager > Licensing in the left menu pane.
4. Under Current tasks, click Add license.
5. When the activation window opens, click Next to start the activation process.
6. Enter the serial numbers for the components you want to activate. These serial numbers were supplied with your software. After you enter each complete serial number, click Add to add it to the list, then enter additional serial numbers as required.
7. When all numbers are entered, click Next.
8. Select Automatic online activation or Manual activation, and click Next.

NOTE: If you do not have a connection to both the Internet and CAS, choose Manual activation.

9. For Manual activation, do the following:
   a. Contact Equitrac at www.nuance.com/for-business/by-product/equitrac/index.htm or by telephone to obtain the corresponding activation codes.
   b. After receiving the required activation codes, click Finish to continue.
   c. On the Add licensing Information dialog box, enter the Activation code, and click Add.

The activated software license appears in System Manager.

10. For Automatic online activation, do the following:
    a. In the Embedded device licensing screen, select Xerox from the Manufacturer list, then click Next.
    b. Follow the Activation wizard prompts to provide contact information. If you have already registered one or more Equitrac components, the Activation wizard fills the form with previously-collected data.
    c. The Activation wizard displays a Collecting information... message while retrieving system data. If you want to omit technical details about your system, click the Show technical details button and select the information you do not want to transmit. You must transmit the following:
        • Accounting server serial number
        • Domain-qualified print server name
        • Organization name as registered in Windows
        • Fully-qualified server DNS name
When the Activation wizard is ready to transmit the information, review the collected data. Choose whether to send optional data with your activation request.

**NOTE:** The Activation wizard transmits the data using an HTTP connection to the Equitrac activation server. If the connection fails, the Activation wizard prompts to confirm that you have configured the default gateway correctly, and that the Internet is accessible from this machine. You can retry or cancel the activation request at this point. If you cancel, the Activation wizard prompts you to use manual activation instead.

Once the Activation wizard sends the activation data and Equitrac returns the activation code, the Wizard automatically records the license activation in System Manager, and displays a summary of the activation results:

- Activation code
- Description
- Serial number
- Status (either **Success**, **Invalid**: the serial number and activation code is an invalid combination, or **Denied**: the serial number was valid but not accepted).

If the License is Invalid

If the status is **Invalid**, ensure that you entered all serial numbers and activation codes precisely. Each component requires a separate license—unless you purchased a suite license. If the problem persists, contact the Equitrac Customer Support Center to resolve this problem.

If the Serial Number is Denied

If the status is **Denied**, the serial number may already be registered to a different system ID. Contact the Equitrac Customer Support Center to resolve this problem. Contact the Equitrac Customer Support Center to resolve this problem. Switch to the Assignment View in System Manager, to see the number of licenses purchased and the number of licenses used.
Configuring Authentication Prompts

The user authentication prompts on the MFP login screen are determined by your Equitrac Office/Express configuration.

1. In System Manager, navigate to Configuration > Security and authentication > User authentication.

2. Select one of the following Authentication options from the Input type drop-down list:
   - Card swipe only – Users authenticate with a swipe card.
   - Card swipe or keypad entry – Users authenticate with a swipe card or at the MFP front panel.
   - Keypad only – Users authenticate at the MFP front panel

3. Select one of the following options from the Secondary prompt drop-down list:
   - Always – User must enter a secondary PIN via the keyboard after they swipe their card.
   - If PIN2 available – User must enter a secondary PIN if they have a PIN 2 value associated with their user account.
   - If PIN2 available or keyboard login – User must enter a secondary PIN if they have a PIN 2 value associated with their user account, or if they entered their primary PIN via the keyboard.
   - Never – Secondary PIN is not required.
   - Only with keyboard login – User must enter a secondary PIN if they entered their primary PIN via the keyboard (rather than with a swipe card). This option prevents users from typing in someone else's primary PIN while still allowing valid users to login without a card.
NOTE: If a change is made to the Secondary prompt option, then you must re-initialize the device in order to enable the new selection.

4 In the Card setup area, enter the data start and stop positions in the Use data from position. For details on entering HID decoding parameters, refer to the Using PageCounters chapter in the Equitrac Office and Express Administration Guide.

5 Select Auto-register primary PINs if you want users to register an unrecognized swipe card for future use. An External authority must be selected to allow card self-registration. See Configuring Card Self-Registration on page 75 for details.

6 Click OK to save the change.

For more detailed user authentication options see Accounts System Configuration in the Equitrac Office and Express Administration Guide.

Setting Xerox Secure Access Prompts

The following settings must be set before creating Xerox embedded devices.

1 In System Manager, navigate to Configuration > Embedded Devices.

2 Select Xerox Secure Access from the Device type drop-down list.

3 Click on the link beside Tracked activities to open the Embedded device configuration dialog box and select the activities you want to track. If you do not wish to track any activity, uncheck all of the options.

NOTE: Only select Print if you intend to use the popup feature of the Xerox print driver to prompt for User and Account IDs. See Configuring MFP Properties on page 16 if you intend to use Xerox Secure Access as the authentication method.

4 Enter a Title and Login prompt to display on the login screen of the embedded device.

NOTE: If you modify the Title or Login prompt after a device has been initialized by the Equitrac server, you will have to re-initialize the device again. See Configuring Embedded Devices on page 77 for instructions.

5 Select Enable release all jobs prompt if you are not using the Follow-You Printing application and want to prompt for batch release of all jobs.

6 Select Force logout on swipe to allow the user to logout by swiping their card a second time.

7 Click OK to save the changes.
Setting Xerox JBA Prompts

These settings are only required if using the user and account ID popups provided in the Xerox print driver. These settings determine which activities to track and the fields of information that the user must complete in the Xerox driver's popup dialog box when they submit a print job.

1. In System Manager, navigate to Configuration > Embedded Devices.

2. Select Xerox/Fuji Xerox JBA from the Device type drop-down list.

3. Click on the link beside Tracked activities to open the Embedded device configuration dialog box and select the activities you want to track. If you do not wish to track any activity, uncheck all of the options.

   **NOTE:** Only select Print if you intend to use the popup feature of the Xerox print driver to prompt for User and Account IDs. See Configuring MFP Properties on page 16 if you intend to use Xerox Secure Access as the authentication method.

4. Select Enable authentication upload if you intend to use local (on-box) validation.

   **NOTE:** Local validation will not work with Follow-You Printing. For uploading to occur, select Xerox EIP, JBA as the authentication method when initializing the device. See Configuring Embedded Devices on page 77.

5. Select the method that specifies which account data to map to the Xerox print driver's user ID and account ID fields.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Enter at User ID Prompt:</th>
<th>Enter at Account ID Prompt:</th>
<th>Equitrac Account Charged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary and Secondary PIN</td>
<td>Primary PIN</td>
<td>Secondary PIN</td>
<td>User, Billing Code, or Department</td>
</tr>
<tr>
<td>Primary PIN and Billing Code</td>
<td>Primary PIN</td>
<td>Billing Code</td>
<td>Billing Code</td>
</tr>
<tr>
<td>User Only</td>
<td>Network Logon</td>
<td>Network Logon</td>
<td>User</td>
</tr>
</tbody>
</table>

6. Click OK to save the changes.
Chapter 3: Server-Side Configuration

Enabling Release Key Prompt

Release key is an Equitrac Express feature that lets users assign a key value to their documents when they submit print requests. Users can also assign a release key to a print job allowing other users to walk up to any embedded device, and print any jobs in the queue that were submitted using that release key. The job is tracked and charged to the user releasing the job, not the user who assigned the release key.

When prompted for a release key at an embedded device, users are required to enter the same alpha-numeric key value used at print time to release a job from the secure print queue.

To enable release key prompts on the embedded device, do the following:

1. Open System Manager, and navigate to Configuration > User interaction > Session flow.
2. Select Prompt for release key in the Other prompts section to enable release keys, and click OK.

Configuring Card Self-Registration

If you want users to self-register their swipe cards, you must enable this option in System Manager. When a user swipes an unregistered card, they are required to login to the MFP with valid User ID and Password. The User ID must already exist in CAS, or in the External authority defined to allow self-registration. The Password comes from one of the defined external authorities. The information the user must enter depends upon the authentication options that are set in System Manager. Two-level authentication is required to register new cards, and the user must manually enter both primary and secondary login credentials.

1. Open System Manager and navigate to Configuration > Security and authentication > User authentication.
2. In the Authentication options section, do the following:
   a. Set Secondary Prompt to either If PIN2 available or keyboard login or Only on keyboard login to ensure that the password is prompted during card registration.
   b. Select the Auto-register primary PINs checkbox. Optionally, you can select Register as alternate PIN to record the PIN as the Alternate PIN instead of the Primary PIN.
3. Select one or more Authentication mechanisms:
   - Equitrac Office/Express PINs – Select to connect an Equitrac print account with login information.
   - External user ID and password – Select to verify all user information outside of Equitrac.
   - Equitrac Office/Express PIN with external password – Select if users swipe their cards for identification, and must also enter their domain user account password. Equitrac cross-checks the database for the corresponding Equitrac account name, then verifies the credentials against the selected external authority for network logon.
4. Click OK to save the changes and close the User authentication dialog box.
5. Navigate to Configuration > Security and authentication > External authentication and select an External authority – Windows, NetWare or LDAP. Refer to External User Authentication in the Equitrac Office and Express Administration Guide for more details on setting up an external user authentication method.

Once the user registers their card, their account information is automatically associated with that card. The next time the user swipes their card, they can login automatically without manually entering their password. However, if Secondary prompt is set to Always in System Manager, the user must enter a secondary PIN, or an external authority password after they swipe their card.
Configuring Billing Code Popup Behavior

Client Billing prompts users at the workstation for a billing code each time they attempt to print a document. These prompts are referred to as "popups". You can configure the behavior of the billing code popup on workstations, PageCounter terminals and, where supported, on embedded devices.

To configure billing codes for Xerox devices, do the following:

1. In System Manager, navigate to Configuration > User interaction > Session flow.

2. Select Prompt for billing code after user authentication (at copiers) if you want the user to enter a billing code before they can access the MFP functions. If the user has only one associated billing code, then the prompt is suppressed, and the billing code is automatically applied to the job.

   **NOTE:** If a user logs on to a Xerox Smart Card configured device to copy, scan or fax, then the Billing code prompt is not available since user authentication is performed through the Smart Card solution, not through Equitrac.

3. Select Prompt for billing code at job release (at copiers) if you want the user to enter a billing code before they can release a print job. If the user has only one associated billing code, then the prompt is suppressed, and the billing code is automatically applied to the job.

   **NOTE:** Billing codes assigned via the workstation popup, or prompted for at job release (at the device) will not be recorded when tracking print jobs through Xerox Network Accounting. See Print Tracking Using Xerox Network Accounting on page 88 for details.

4. Select the Billing code prompt details you want to display at the MFPs.
   - **Required field** – The user must enter a billing code.
     Users with only one billing code are not prompted for a billing code even if the Required field option is selected. Instead, the embedded device acts as if the user has entered one.
     If this option is not selected, and the user does not have an associated billing code, they can enter a "blank" billing code to continue.

   **NOTE:** DCE must be restarted any time you enable or disable the Required field prompt.

   - **Search** – Adds a Search function where users can search for billing codes.
   - **Security mode** – Displays the Billing code in asterisk characters.
   - **Show most recently used** – Does not apply to Xerox embedded devices.
   - **Default to the previous billing code** – Does not apply to Xerox embedded devices.

5. Enter a name for the Billing code label on the MFP panel (e.g. Billing Code).

6. The Billable options (Prompt for billable and Billable label) does not apply to Xerox Extensible Interface Platform® embedded devices.

7. Validate billing codes against CAS when it is available and/or unavailable (at workstations only) in their respective fields.

8. Click OK to save the settings.
Configuring Embedded Devices

Embedded devices are manufacturer-specific software bridges that handle the transfer of user authentication and transaction details between these devices and your accounting server database. Supported devices prompt users for valid user and account ID information for all print release, walk-up copy, scan, and fax jobs.

You must create an embedded interface for each Xerox MFP that will be controlled by Equitrac Office/Express. Equitrac’s System Manager component provides the tools to create these interfaces.

1. Open System Manager and select Devices in the left pane.
2. Right-click on a Xerox MFP in the right pane, then select Add embedded device from the menu.

3. Enter a Name and Description to identify the embedded device.
4. Select the Server hosting the DCE associated with the embedded device from the drop-down list.

   **NOTE:** If you change the server associated with an embedded device that has already been initialized by the Equitrac server, you must re-initialize the device.

5. Select Xerox EIP, JBA from the Type drop-down list.
6. Select the Card Reader HID decoding from the drop-down list.

   For details on HID decoding, see the Equitrac Office and Express Administration Guide.

7. Click Pricing to configure pricing at the embedded device level.

   For pricing details, see Configuring Price Lists in the Equitrac Office and Express Administration Guide.

   **NOTE:** To configure the embedded device to use the price list for that device, select the default price list. If you select an alternate price list for the embedded device, the embedded device price list overrides the default price.

8. Enter an Admin ID and Password to set up secure administrator access to the device. This password and ID must be identical to those used with the eqxeroseipregistration.exe utility.
Chapter 3: Server-Side Configuration

9 Click the **Initialize** button to open the Initialize device dialog box.

10 Select the **Server-based authentication** option, and choose a method from the drop-down list.
   - **Fuji Xerox authentication (EPA)** – to track printing through Xerox Network Accounting. See Print Tracking Using Xerox Network Accounting on page 88.
   - **Xerox off-box JBA** – to validate prior to processing print activity.
   - **Xerox Secure Access** – to track printing through printer ports or the Direct IP Printing Client (DRC). See Print Tracking Through Printer Ports on page 87.

11 From the **Prompt for billing code** drop-down list, select the billing code behavior at the device:
   - **Default** – uses the billing code prompt behavior configured in User interaction > Session flow.
   - **Prompt** – overrides the Default setting on supported devices.

12 Click **Initialize** to configure communication between this device and the Equitrac server, and return to the Embedded device dialog box.

   **CAUTION:** Clicking **Initialize** changes the configuration on the device itself and requires some MFPs to reboot. Ensure that the MFP is not in use before you click Initialize. You must manually reboot WorkCentre 52xx, 7232/7242, 73xx, and 74xx models for these settings to take effect. Click the Reboot button on the MFP's web configuration page to accomplish the reboot remotely.

13 Click **OK** to save the embedded device details and close the dialog box. The new embedded device appears in the Devices list beneath the Physical device it is associated with.

14 Repeat these steps to create an embedded device on each supported Xerox MFP in the Devices list.

   **NOTE:** If initialization fails, and the Xerox device does not appear in System Manager, go back to Configuring Authentication Prompts on page 72 and confirm that the MFP is properly configured.

After Initialization, log into a Xerox MFP configuration page as the Administrator to verify that the Admin ID and Password entered in System Manager are configured properly. When login is successful, a web page opens displaying the Xerox MFP model name and its settings.

   **NOTE:** If the MFP is running EIP firmware version 1.5 or 2.0, the Embedded Manual Override option must be Enabled through the MFP Internet Services Interface in order for the attached Equitrac card reader to operate normally. See WorkCentre 75xx Series on page 39 for setup details.
Configuring Smart Card Authentication

Embedded devices configured with Smart Card authentication require users to log in using the physical Smart Card and entering a valid userID at the device for all print, copy, scan, and fax jobs.

To configure Smart Card authentication, do the following:

1. Open System Manager and select Devices in the left pane.
2. Right-click on a Xerox MFP in the right pane, then select Add embedded device from the menu.
3. Enter a Name and Description to identify the embedded device.
4. Select the Server hosting the DCE associated with the embedded device from the drop-down list.
5. Select Xerox EIP, JBA from the Type drop-down list.
6. Select the Card Reader HID decoding from the drop-down list. For details on HID decoding, see the Equitrac Office and Express Administration Guide.
7. Click Pricing to configure pricing at the embedded device level. For pricing details, see Configuring Price Lists in the Equitrac Office and Express Administration Guide.
8. Enter an Admin ID and Password to set up secure administrator access to the device. This password and ID must be identical to those used with the eqxeroxeipregistration.exe utility.
9. Click the Initialize button to open the Initialize device dialog box.
10. Select the Local authentication option, and choose Xerox Native SmartCard from the drop-down list.
CAUTION: Xerox Print Admin Suite relies upon existing SmartCard functionality to allow authentication for embedded functions. Authentication through SmartCard is dependent upon a pre-existing operational native smart card setup per device. Ensure your setup includes smart card authentication before installing the embedded solution.

11 Select the **Enable Follow-You Printing applet** checkbox to enable Follow-You Printing on the device.

12 Click **Initialize** to configure communication between this device and the Equitrac server, and return to the Embedded device dialog box.

13 Click **OK** to save the embedded device details and close the dialog box.
Setting Up Authentication Devices

Using a proprietary protocol called Convenience Authentication, the Authentication Device contacts the accounting server via an Ethernet network connection to verify the user information gathered from the swipe or proximity card. If the accounting server verifies the user, the MFP device panel unlocks and is ready for use. If the user is not verified, the MFP remains locked and the user cannot perform any tasks at the device. The user can access the Equitrac Embedded functions only when they are authenticated and the front panel is unlocked.

Setup of each Authentication Device requires a three-step process, outlined below. Before proceeding, ensure that you have all required Authentication Device components. See Authentication Device Component Requirements on page 11.

1. Set the IP Address for each Authentication Device and indicate the DCE IP Address that will communicate with this Authentication Device. Follow Set the Authentication Device IP Address on page 81.

2. Mount the Authentication Device hardware on or near the MFP. Follow Mount the Authentication Device on page 84.

3. Plug in the power, serial, expansion, and card reader connections. Follow Connect the Hardware on page 85.

Set the Authentication Device IP Address

Xerox Authentication Devices are configured for DHCP communication by default. You need to assign an IP Address to each Authentication Device, and set the server IP Address of the DCE component. There are two methods to assign the IP Address:

- Using a DHCP server to assign addresses ensures that the IP Address assignments are handled by the DHCP server when you connect the Authentication Device to the network. However, you need to configure the DHCP server to locate the Authentication Devices. Follow Configure the DHCP Server to Locate the Authentication Devices on page 82.
• If you are not using a DHCP server, or if you prefer not to set option 230 on your DHCP server, you need to use the Authentication Device Web Admin application to set the addresses manually. Follow **Manually Assign the IP Address** on page 82.

**Configure the DHCP Server to Locate the Authentication Devices**

1. In Windows Administrative Tools, open the DHCP windows management console.
2. Select the DHCP server root node.
3. From the **Action** menu, select **Set Predefined Options**.
4. From the **Option Class** drop-down list, select **DHCP Standard Options**.
5. In the **Option Name** section, click **Add**.
   a. In the **Name** field, enter Xerox Secure Access. This field is used for identification purposes only.
   b. From the **Datatype** drop-down list, select **String**.
   c. In the **Code** field, enter 230.
   d. In the **Description** field, type: Secure Access.
   e. Click **OK**.
6. In the **String Value** section, enter `EQ;A;<DCE Server IP Address>` in the **String** field, where `<DCE Server IP Address>` is the IP Address of your DCE server. For example:
   
   `EQ;A; 192.168.100.137`
7. Expand the **Scope** node and select **Scope Options**.
8. From the **Action** menu, select **Configure Options**.
10. Click **OK** to save the changes.

**Manually Assign the IP Address**

**CAUTION:** Follow these instructions only if you are not using a DHCP server to set the IP Address of the Authentication Device OR if you are using a DHCP server, but prefer to use static IP Addresses rather than using option 230.

When first powered up, the Authentication Device looks for a DHCP server to secure an IP Address. If no DHCP server is found, the device switches to static communication and defaults to a static IP Address of 192.168.2.1. You can use a standard Ethernet cable to connect a system (for example, a laptop) to the Downlink port on each Authentication Device, then use the Web Admin tool to change the IP Address, and enter the DCE Server IP Address. Print out the Tear sheet found on page 107 before you start. Use this sheet to record the IP Addresses you assign to each Authentication Device.
Configure the Admin Laptop

The system running the Web Admin tool must recognize the static IP Address before you can access the Web Admin tool.

1. On the system (laptop) that will run the Web Admin tool, select **Network Connections > Local Area Connection > Properties**.
2. Double-click **Internet Properties (TCP/IP)**, then click **Advanced**.
3. In the IP Addresses section, click **Add**.
4. Enter the following:
   - IP Address: 192.168.2.x (where x is an unassigned IP)
   - Subnet Mask: 255.255.255.0
5. Click **Add** to save the changes.

Use the Web Admin Tool to Set IP Addresses:

Perform the following procedure on each Authentication Device.

1. Use a regular Ethernet cable to connect a laptop to the Downlink port on the Authentication Terminal.
2. To power up the Authentication Terminal, attach one end of the AC power cable to the Authentication Terminal, then plug the other end into an available outlet.
3. Open a web browser, and enter **192.168.2.1** in the Address field.
   - This is the factory default IP Address assigned to the Authentication Device.
4. Select the **Configure** link at the top of the page.
5. Enter the following to login:
   - User name: deviceadmin
   - Password: pc_passwd
6. Change the password used to access the Web Admin tool. You can reset the password at any time, but ensure that you change the password from the default setting before the Authentication Device is up and running.
7. In the **Configure Authentication Device** section, choose Static IP from the **Addressing mode** drop-down list.
   - **Configure Authentication Device**
     | Addressing mode | Static IP (x) |
     |-----------------|--------------|
     | IP Address      | 192.168.0.001|
     | Network mask    | 255.255.0.009|
   - **Configure server**
     | Server IP Address | 192.168.0.031|
8. Enter a static IP Address in the **IP Address** field to set the address of this Authentication Device.
9. In the **Configure Server** section, enter the DCE Server's IP Address in the Server IP Address field.
Chapter 3: Server-Side Configuration

10 Click the **Update Configuration** button located below the Configure Server fields.
11 Click the **Restart** link at the top of the page, then click “Click here to confirm restart” to restart the terminal.
12 Repeat these instructions for each Authentication Device that you are deploying.

**NOTE:** Remember to reconfigure the laptop Internet Properties when you are done.

**Mount the Authentication Device**

Print out the Configuration Tear Sheet found on page 107. As you work, complete the Authentication Device’s IP Address and MAC Address columns on this sheet. You need this information when you configure communication between devices within System Manager.

1 Lay the Authentication Device on the floor, behind and on the input side of the MFP. The device should be placed in an unobtrusive location, but ensure that the device is placed within 6 feet of the card reader (serial cable length is 6 feet).
2 Mount the Card Reader on the shelf on the left side of the MFP front panel using the supplied Velcro strip. If you have the Convenience Stapler option, place the Card Reader to the right of the stapler so the Card Reader is between the stapler and MFP. Ensure the Document Handler top cover can be opened without being obstructed by the Card Reader before attaching the Velcro strip.
3 Use the Tear Sheet (see page 107) to record the IP and MAC Address of the MFP that this Authentication Device will control.
Connect the Hardware

Using the labeled graphic below for reference, connect the components. Note that the Authentication Device provides a serial port and a copy control port that is not used in this configuration.

1. Use the Tear sheet to record the MAC address of the Authentication Device. Enter this address in the same row as the MFP it will control.

2. Plug the Card Reader serial cable into the Card Reader connector on the Authentication Device.

3. Connect one end of the Ethernet cable into the network drop and the other end into the Uplink port on the Authentication Device.

4. Connect the MFPs ethernet cable to the Downlink port on the Authentication Device.

   **NOTE:** When the Authentication Device is powered off, there is no Ethernet connectivity available from the Downlink port. Alternatively, you can plug the MFP Ethernet cable directly into another Ethernet port. The Downlink port is provided on the Authentication Device for situations when another Ethernet port is not available.

5. Connect the power supply to the Authentication Device, then plug the other end into the nearby receptacle.

The physical hardware setup of the Authentication Device is now complete. Repeat these instructions for each Authentication Device.

   **NOTE:** The Authentication Device does not control access to an MFP until you perform an association in System Manager, described below.
**Associating Authentication Devices with MFPs**

When you initially power on an Authentication Device connected to the network, the DCE registers the device. The DCE then forwards the configuration details to the accounting server, and the Devices list in System Manager updates accordingly.

Unassigned Authentication Devices appear in the Devices list under the `<Unassigned control terminals>` section (using the Standard view in the Devices window).

<table>
<thead>
<tr>
<th>Name</th>
<th>Server</th>
<th>Description</th>
<th>ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox WorkCentre Pro 575</td>
<td>192.168.96.254</td>
<td>Xerox</td>
<td>192.168.96.254</td>
<td>Physical device</td>
</tr>
<tr>
<td>Xerox WorkCentre Pro 575</td>
<td>192.168.96.254</td>
<td>Xerox</td>
<td>192.168.96.254</td>
<td>Physical device</td>
</tr>
<tr>
<td>Unassigned control terminals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each Authentication Device is labeled as "Auto-generated device", but can be differentiated by MAC Address. Use your Tear sheet to determine which Authentication Device MAC Address maps to the corresponding MFP IP Address.

1. Open System Manager and select **Devices** in the left pane.
2. To associate an Authentication Device with a Physical Device (MFP), simply drag and drop the terminal to the Physical Device. The Authentication Device will then appear below the Physical device.

<table>
<thead>
<tr>
<th>Name</th>
<th>Server</th>
<th>Description</th>
<th>ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox WorkCentre Pro 575</td>
<td>192.168.96.254</td>
<td>Xerox</td>
<td>192.168.96.254</td>
<td>Physical device</td>
</tr>
<tr>
<td>Xerox WorkCentre Pro 575</td>
<td>192.168.96.254</td>
<td>Xerox</td>
<td>192.168.96.254</td>
<td>Physical device</td>
</tr>
<tr>
<td>Auto-generated device</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Unassigned control terminals&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Users must now authenticate to use the MFP. See **User Workflow** on page 95 for instructions that you can provide to end-users.
Configuring Print Tracking

There are two methods to track printing—through printer ports or through the Xerox client driver popup (also called Xerox JBA or Job-based Accounting). Read the descriptions below to determine the appropriate print tracking setup for your environment.

Print Tracking Through Printer Ports

When DRE is set to track printing, it gathers details when the user submits a print job. When a job is released, DRE forwards these details to CAS based on the job characteristics determined by the port monitor.

The job details are gathered by the port monitor when the user releases the print job at a device. If the user decides to cancel the print job mid-way through printing, or if the user originally selected color printing but the final output device cannot print in color, the precise page details are not captured at the time of output and therefore tracking may not be fully accurate.

Enable tracking from the physical device

1. Open System Manager and select Devices in the left pane.
2. Select the physical device to open the Physical device summary dialog box.

![Physical device summary dialog box]

3. In the Settings area, ensure Track and record print transactions on this device is selected from the Tracking Behavior drop-down list. This is the default setting.
4. Click OK to save the changes.
Chapter 3: Server-Side Configuration

5 Navigate to Configuration > Devices > Embedded devices.
6 Select Xerox/Fuji Xerox JBA from the Device Type drop-down list.
7 Click on the link beside Tracked activities to open the Embedded device configuration dialog box.
8 Ensure that Print is NOT selected, then click OK.

Print Tracking Using Xerox Network Accounting

When tracking print jobs through a Xerox embedded device, configure the device and its print drivers to accept only authenticated print jobs. Users are prompted to enter user and account credentials prior to printing. The user authentication data is checked by the Xerox device when it receives the print job. The embedded device tracks printing and captures appropriate accounting information.

Use this method when you require precise job accounting. When the user releases a print job, the precise output details are gathered and held at the device after the job is completed. If the user cancels mid-way through a job, or if the device is not capable of producing output as the user intended (i.e. duplex was selected, but the device is not capable of duplexing and produces single-sided output only), the device calculates the precise output details only after the job is fully processed.

The DCE obtains the transaction details from the output device and forwards them to the CAS at a later interval.

This method requires additional configuration steps and your Xerox devices must meet the following prerequisites:

- JBA-supported Xerox device with the Network Accounting module installed and enabled and Authentication (Network Accounting option) enabled.
- TCP/IP enabled and configured on the devices.
- A static IP Address or reserved DHCP IP Address (recommended).
- TCP/IP port 443 communication enabled on the network between the Equitrac Office/Express server and the devices.
- Depending on the Xerox device and server operating system, you may require Xerox Advanced Services Management before you can enable the Accounting option on the printer driver. See the Xerox device documentation for details.
- Off-printer (also called off-box) validation must be configured on the Equitrac Office/Express server. This option forces the device to send a request to Equitrac to validate the data input by the user.
- For Xerox devices to accept authenticated print jobs and the embedded device to track print jobs correctly, the Xerox device and Xerox print drivers must be configured as described in the following table.

<table>
<thead>
<tr>
<th>Device and Print Driver Configuration</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Network Accounting</strong> module must be installed and enabled on each Xerox device.</td>
<td>Equitrac does not support the Internal Auditron authentication method. When you set the authentication mode on the device, ensure you select the <strong>Network Accounting</strong> option.</td>
</tr>
<tr>
<td>The <strong>Network Accounting Configuration &gt; Authentication</strong> option must be enabled.</td>
<td>Depending on the Xerox device Authentication configuration, job information can be accurately tracked by the Xerox device regardless of whether or not the user and account information exists on that device. See the Xerox device documentation for details on configuring options for the physical device.</td>
</tr>
</tbody>
</table>
| Installed Xerox print drivers must have the **Accounting** option enabled for each printer to prompt users for user and account ID prior to printing. | The location of the Accounting option in the Xerox print driver dialogs may not be the same for all printer connections you create. The option may be located on the **Properties > Document Details** or the **Printer Preferences** dialogs. You may find that the location of the Accounting option varies by Windows platform, driver language type (Postscript or PCL), driver version, or device model. The Xerox device deletes print jobs to prevent anonymous (un-billable) printing when any of the following situations apply:  
  • The Xerox print driver does not have authentication features.  
  • The **Accounting** option for the print driver is disabled. |
| Configure the embedded device to perform print tracking. | By default, both the printer port and the embedded device track the print job. You must disable the tracking on the physical device and allow the embedded device to perform the tracking instead. See **Disable tracking from the physical device** on page 90 |

Once the prerequisites and configuration steps are complete, you must disable tracking on the physical device.
Chapter 3: Server-Side Configuration

Disable tracking from the physical device

1. Open System Manager and select Devices in the left pane.
2. Select the physical device to open the Physical device summary dialog box.
3. In the Settings area, select Do not track or record print transactions on this device is selected from the Tracking Behavior drop-down list. This is the default setting.
4. Click OK to save the changes.
5. Navigate to Configuration > Devices > Embedded devices.
6. Select Xerox/Fuji Xerox JBA from the Device Type drop-down list.
7. Click on the link beside Tracked activities to open the Embedded device configuration dialog box.
8. Ensure that Print is selected, then click OK.
9. Click OK again to save the change to the global options set in the Embedded devices dialog box.

**NOTE:** When print tracking from the device you must set the Tracking behavior to Do not track and record printing on this device on the Physical device summary screen, and select the Print checkbox on the Embedded device configuration dialog box. Failure to set these options results in double tracking or no tracking.
Color Tracking Using Xerox Tiered Billing

Tiered billing refers to a pricing scheme for color copies and prints based on the amount of actual color printed on the page, as opposed to a flat rate regardless of coverage. This coverage is categorized by two tiers (Xerox T1 and T2+) or three tiers (Xerox T1, T2, and T3), depending on the support provided by the Xerox device. Each tier denotes a percentage of color coverage area on the page.

Tiered billing requires additional configuration steps and must meet the following requirements:

- A Xerox color device enabled for tiered billing (e.g. Xerox ColorQube 9200 series)
- JBA-supported Xerox device with the Network Accounting module installed and enabled, and Authentication (Network Accounting option) enabled.
- Costing using the Equitrac Office/Express Advanced price list with the prices set to reflect the tiered billing options.
- JBA print tracking must be used instead of the port monitor.
- Follow-You Printing requires that the tracking behavior in System Manager must be set to **Track and do not record print transactions on this device**. If the tracking behavior is not set to this option, then the job is recorded twice—one by JBA, and once by the port monitor.
- Validation of JBA data must be disabled on the Xerox device to prevent it from discarding the print job.

**NOTE:** The cost of the job displayed in the Follow-You Printing screen on the Xerox device does not reflect the tiered billing price. However, once the job is released from the print queue, the tiered pricing information from the JBA log is recorded into the CAS database.

To set tiered billing for the Xerox device, do the following:

1. Open System Manager and select **Price lists** in the left pane.
2. Click **Add advanced price list** from the **Current tasks** section. An Advanced price list dialog box opens.
3 Enter a Name and Description for the price list.

4 Set the Job attributes, such as base price, finishing operations, and subcharges.

5 In the Page detail pricing section, specify a combination of page attributes.
   - Click Add from the Type column to create a new pricing rule.
   - Click the attribute fields (Type, Size, Color, Duplex, Tray, and Media) to select an option from the corresponding drop-down list.
   - Click the Col-type field to select the appropriate Xerox billing tier.
   - Enter a Price for the page detail pricing rule.

6 Click OK to save your Xerox tiered price list.

See the Equitrac Office and Express Administration Guide for more details on configuring advanced price lists.

**Receiving Print Error Messages**

On specific end-points, if you try to release a print job that costs more than the funds available in the account, a message displays indicating that there are insufficient funds to release the document. If a transaction with multiple documents fails due to insufficient funds, then a message displays indicating the first job that failed to print. The message does not list all the failed print jobs.
Configuring SNMP Communication

Xerox devices can use either SNMP v2 or SNMP v3 communication to manage networked devices. SNMP v2 uses community names to authenticate requests, and SNMP v3 uses a combination of authentication and privacy keys and protocols to send and receive information from devices on the network.

Both SNMP v2 and SNMP v3 require a SNMP configuration set. The Default configuration set can be used if all devices match the SNMP configuration, otherwise a custom configuration set must be defined. Although some devices support both SNMP v2 and SNMP v3 simultaneously, the physical device set in System Manager can only be configured for one or the other.

To create the SNMP configuration set, do the following:

1. In System Manager, navigate to Configuration > Network environment > SNMP configuration. The SNMP configuration dialog box opens.

2. Enter a Polling interval value for SNMP status changes (in minutes). Choose a polling interval value that is not too low so that network traffic is properly accounted for.

3. Click <Default> to open the default SNMP configuration dialog box.
4  Enable SNMP version 2 or SNMP version 3.
   • If Enable SNMP v1/2c is selected, set the Get (Read-only) and Set (Read and Write) community names to public and private respectively. All characters must be entered in lower case.
   —Or—
   • If Enable SNMP v3 is selected, provide the following information:
     • Security Name: User name is Xadmin.
     • Context Name: Not required for Fuji Xerox devices.
     • Authentication Key: The pass-phrase set at the device (at least 8 characters in length).
     • Authentication Protocol: Select MD5 from the drop-down list.
     • Privacy Key: The pass-phrase set at the device (at least 8 characters in length).
     • Privacy Protocol: Select DES from the drop-down list.
   Authentication Keys and Privacy Keys are generated from user-configurable pass phrases. An Authentication key value is required in order to enter a Privacy key value.

5  Click OK to save the settings.

If desired, click <Add> and follow the previous steps to create additional SNMP configurations.

**NOTE:** If you change the default names in System Manager, you must also change them on all of your physical devices to match, in order for SNMP communication to work. Consult your Xerox documentation for information on changing these settings.
User Workflow

Topics

- Authenticating at a Card Reader
- Card Reader Status Messages
- Using Follow-You Printing
- Resetting an Authentication Device

This section provides end-user instructions for authenticating and using the Equitrac Embedded functions at the Xerox MFP.
Authenticating at a Card Reader

When Equitrac Embedded for Xerox Extensible Interface Platform® controls an MFP, users must authenticate with a magnetic stripe card, proximity card, or smart card before they are able to use the device functions.

Authenticating with a Magnetic Stripe Card

1. Insert the card into the guide track with the magnetic stripe facing the indicated direction. Ensure the card is pressed firmly against the guide.
2. Pull the card down through the guide track and remove the card.

   **NOTE:** Do not run the card through at an angle or the terminal will not accept the data.
3. If the terminal cannot read the entry, the LED flashes red. Reinsert the card into the guide track and run the card through the reader again.
4. If **Secondary prompt** is enabled in System Manager, and a secondary PIN has been assigned in the database, the user must enter their ‘password’ on the MFP front panel when prompted. If the user has not been assigned a secondary PIN in the database, they can leave the field blank to proceed.

Authenticating with a Proximity or Smart Card

To enter data using a proximity card or smart card, pass the card within 1 inch or 2.5 cm of the proximity symbol located on the top of the card reader device. To locate the proximity card reader on the data reader module, look for this symbol:

If the swipe is invalid, the LED flashes red.

If secondary PINs are enabled, the user must enter their ‘password’ on the MFP front panel when prompted. If secondary PINs are enabled, but the user has not been assigned a secondary PIN, the user can leave the field blank to proceed.
### Card Reader Status Messages

Equitrac Office/Express displays its authentication messages through an LED light on the card reader module.

The following signals may be displayed on the card reader:

<table>
<thead>
<tr>
<th>LED Behavior</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid red</td>
<td>MFP is in Idle mode; it is ready but there is no active session.</td>
</tr>
<tr>
<td>Solid green</td>
<td>MFP is in Ready mode and a session is active.</td>
</tr>
<tr>
<td>Slow flashing green</td>
<td>Data received from card reader, awaiting authentication for active session. The light continues to flash green until the user enters their secondary PIN at the front panel. If the time-out expires and the user does not enter their PIN, the LED changes back to solid red and the device remains locked.</td>
</tr>
<tr>
<td>Slow flashing red</td>
<td>No communication between card reader and MFP.</td>
</tr>
</tbody>
</table>

The MFP has two functional modes, Idle mode or Ready mode.

### Idle Mode

An MFP that is ready for use is in Idle mode. When a user passes a key fob or swipes a magstripe card, the device changes to Ready mode.

The MFP returns to Idle mode when:

- A user completes a transaction
- After a specified period of inactivity in Ready mode (Sleep Mode Timer, as configured on the device)
- The user logs out

When the device is in Idle mode, the LED light on the card reader is solid red.

### Ready Mode

When the device is in Ready mode, the LED light on the card reader is solid green and the user can begin using the controlled device to perform a transaction.
Logging In to a User Session

A user session begins when the user logs in with valid credentials through the MFP device interface. Once their login credentials have been authenticated, the user can manage and release documents via Follow-You Printing, or they can access any of the other device features, such as copying, scanning and faxing.

There are two authentication methods available to validate users at a Xerox MFP:

- **Local authentication** - users are authenticated at the Xerox device. For example, the Xerox Smart Card solution uses local authentication. See Configuring Smart Card Authentication on page 79.
- **Server-based authentication** - users are authenticated by CAS. See Configuring Embedded Devices on page 77 for details.

Smart Card Authentication

To authenticate through Xerox Smart Card, do the following:

1. The user inserts their Smart Card into the Xerox supported card reader to open the MFP Login screen.
2. On the Login screen, the user enters their user PIN.
3. If configured in System Manager to prompt for a release key on the device, the Release Key screen opens. The user enters the key code and clicks **OK** to continue. Release Key is an Equitrac Express feature, and does not apply to Equitrac Office users.
4. On the All Services screen, the user can access any of the native device features (e.g. copy, scan or fax), or they can touch **Custom Services** to access Follow-You Printing. See Using Follow-You Printing on page 99.

Equitrac Server Authentication

To authenticate through Equitrac, do the following:

1. On the Login screen, the user enters their User ID or swipes their card. If System Manager is configured to prompt for Secondary PIN, the user may also need to enter a password.

   Depending on how System Manager is configured, one of the following occurs after user authentication:

   - The MFP All Services screen opens, and the user can proceed to the Follow-You Printing application to release their documents.
   - A Billing Code prompt opens, and the user must enter a billing code before proceeding to Follow-You Printing. If the user has only one associated billing code, then the prompt is suppressed, and the billing code is automatically applied to the job.
2 If prompted for a Billing Code, the user must enter the code on the MFP front panel, or perform a search for the correct Billing Code:

![Billing Code Search](image)

3 Billing codes found through search populate in the field when selected. If billing codes are not a required field, the user can leave the Billing Code field empty and touch OK to continue.

4 If configured in System Manager to prompt for a release key on the device, the Release Key screen opens. The user enters the key code and clicks OK to continue. Release Key is an Equitrac Express feature, and does not apply to Equitrac Office users.

5 On the All Services screen, the user can access any of the native device features (e.g. copy, scan or fax), or they can touch Custom Services to access Follow-You Printing. See Using Follow-You Printing on page 99.

### Using Follow-You Printing

Users can use Follow-You Printing to release documents held in the print queue associated with the user’s account from any device within a predefined pull group, which is connected to the particular print server. Multi-Server Follow-You Printing allows users to select any remote print server accessible to the device within a predefined pull group, and pull documents for printing.

1 On the MFP Login screen, the user enters their user credentials or swipes their card. See Smart Card Authentication on page 98 or Equitrac Server Authentication on page 98 for login options.

2 On the All Services screen, the user touches Custom Services.
3 On the Custom Services screen, the user touches **Follow-You Printing** (or **Release Documents** on some devices). The Follow-You Printing screen opens.

![Follow-You Printing Screen](image)

4 On the Follow-You Printing screen, the user can perform the following functions at the device:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print</td>
<td>Touch one or more documents in the list, then touch <strong>Print</strong> to print the documents and delete the jobs from the list.</td>
</tr>
<tr>
<td>Print &amp; Save</td>
<td>Touch one or more documents in the list, then touch <strong>Print &amp; Save</strong> to print the documents but keep the jobs in the list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Touch one or more documents in the list, then touch <strong>Delete</strong> to remove the jobs from the queue without printing them.</td>
</tr>
<tr>
<td>Select All</td>
<td>Selects all jobs in the list, after which you can touch <strong>Print</strong>, <strong>Print &amp; Save</strong>, or <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Server</td>
<td>If multiserver Follow-You Printing is enabled on the Equitrac server, touch <strong>Server</strong> to display a list of authorized network print servers. If you select another server from the list, the Follow-You Printing screen refreshes to show any print jobs waiting on the other server. If multiserver Follow-You is not enabled, you will only see the local server listed. For multiserver Follow-You Printing configuration information, see the &quot;Advanced Printing Configuration&quot; chapter in the <em>Equitrac Office and Express Administration Guide</em>.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Contacts the DCE server to determine if any new pending jobs are available for the current user. If any print jobs are found, they are added to the bottom of the document list.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns to the MFP Service screen.</td>
</tr>
<tr>
<td>Force Monochrome</td>
<td>Allows a user to force a color job to print in black &amp; white.</td>
</tr>
</tbody>
</table>
If configured in System Manager to prompt for a billing code at job release, the user must enter the billing code and touch **OK** to release the print job(s).

The user touches **Exit** to end the user session and return to the Custom Services screen.

### Logging Out of a User Session

While in the Follow-You Printing screen, the user must first touch **Exit** to return to the Custom Services screen, then touches **Close** to return to the main screen on the MFP.

To fully log out of an active session, the user touches the **Clear All** button beside the panel keyboard, then chooses **Log out** in the confirmation dialog box.

If using the Smart Card solution, the user can simply remove their Smart Card to end the user session and completely log out of the device.
Chapter 4: User Workflow

Resetting an Authentication Device

Use the metal bypass key to reset the Authentication Device to the default settings. This key was provided with the device and should be stored in a safe place.

1. Ensure the Authentication Device is powered on.
2. Insert the bypass key into the key slot.

3. Holding the device as shown above, turn the key a quarter turn TOWARD you.
4. After 5 seconds, turn the key back to the original position.
5. Ensure the key is fully back in its original position, then remove the key.

NOTE: The device will beep every 10 seconds if the key is not turned back to its original position before you remove the key.
Before contacting Technical Support for assistance, refer to the following table for symptoms that match the problem you are experiencing. Instructions for possible solutions are also provided.

### Symptoms and Solutions

If you experience a problem with your Equitrac Embedded for Xerox Extensible Interface Platform® application at a device, refer to the table below for symptoms and solutions that match your problem before contacting Equitrac Technical Support for help.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The indicator light on the card reader is off</td>
<td>When the light is not lit, this indicates a loss of power to the reader. Check the cable connection to the Authentication Device and ensure that it is firmly seated. If the light remains unlit, check the power to the Authentication Device. If the Authentication Device does not have power, neither does the card reader.</td>
</tr>
<tr>
<td>The Authentication device does not have power</td>
<td>To determine if the unit has power, check the back (connector side) of the unit. A yellow indicator light next to the jack marked &quot;Ethernet&quot; should be lit. If this light is not lit, ensure that the power supply cable is firmly seated in the Authentication Device, and that the power cord is plugged into the power supply brick and into the A/C wall jack. If the light is still not lit, verify that the wall jack has power.</td>
</tr>
<tr>
<td>The card reader indicator light is flashing red slowly</td>
<td>The Card Reader is working correctly; however, the Authentication device has failed to connect to the Equitrac Office/Express server. Ensure that the Ethernet cable is connected to both the Ethernet port on the Authentication Device and to the wall Ethernet jack. If the Ethernet link light on the Authentication Device flashes green when you first swipe your card, the Ethernet is active, and the problem is likely server-side. Ensure that the Authentication Device has been assigned to the correct MFP. See <a href="#">Associating Authentication Devices with MFPs</a> on page 86 for instructions.</td>
</tr>
<tr>
<td>The card reader indicator light rapidly flashes red upon swipe</td>
<td>The swipe was invalid at the card reader. The Equitrac Office/Express server has determined that the card ID does not correspond to a valid user on the network. Test the reader with another card for a user whose card is known to work at other readers. If the cards are not being read correctly at any reader, server configuration may be the cause. Read <a href="#">Configuring Authentication Prompts</a> on page 72 to ensure the card data positions are set correctly.</td>
</tr>
</tbody>
</table>
### Chapter 5: Troubleshooting

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The card reader indicator light stays red upon swipe</td>
<td>If the indicator light does not change color when you swipe, the reader has not detected the card. Verify that the swipe was performed correctly. A magnetic card may have been encoded with a different standard or swiped upside down or facing the wrong direction; a proximity card or contactless smart card may not have been placed close enough to the reader, or may not be a supported card type. If the same card works at other readers at the same site, the reader module may be at fault. If the card does not work at other readers, verify the card technology with the card vendor and reference <strong>Supported Card Readers</strong> on page 12.</td>
</tr>
<tr>
<td>The Ethernet link light on the Authentication Device is off</td>
<td>There is no Ethernet connection. Verify the Ethernet patch cable and verify that the Ethernet wall jack is active.</td>
</tr>
<tr>
<td>The Ethernet link light on the Authentication Device is solid green (as opposed to flashing)</td>
<td>There is Ethernet connectivity, but no activity. Ensure that the Ethernet wall jack is connected to the correct hub or switch.</td>
</tr>
<tr>
<td>The Authentication Device is not listed in System Manager &gt; Devices</td>
<td>Authentication Devices appear in the Devices list by MAC Address. Check the list of &lt;Unassigned control terminals&gt; to check for the IP Address of the Authentication Device in question. If you cannot locate the correct MAC Address, the DCE Server has not located the device on the Ethernet. If you manually configured the Authentication Device (without DHCP) ensure that you entered the correct DCE IP Address in the Web Admin utility. If you allowed DHCP to assign an IP Address, ensure the Authentication Device is connected to the Ethernet and powered on. You may need to wait approximately 60 seconds for the DCE to contact the device and communicate with the Core Accounting Server before it can populate the Devices list. Also check to ensure that the DHCP server sets value 230 to the DCE Server's IP Address. Ensure the Authentication Device is powered on.</td>
</tr>
<tr>
<td>Cannot connect to the Authentication Device's web page</td>
<td>If you set the IP Address manually, check the Tear sheet to ensure you are entering the correct IP Address. If the address looks correct, either the device is not connected correctly, it cannot communicate, or the IP Address was recorded incorrectly. To check the device connection, use an Ethernet cable to connect the Downlink Port on the Authentication Device directly to a PC. If the connection is established, verify the network settings and IP Addresses set for both the Authentication Device itself and the DCE Server. If you cannot connect to the device using an Ethernet cable, reset the Authentication device. See <strong>Resetting an Authentication Device</strong> on page 102 for instructions. Perform the Authentication Device setup and configuration again. If the web page is still unreachable, the Authentication terminal may be defective.</td>
</tr>
<tr>
<td>The Authentication Device beeps at a frequent interval</td>
<td>The bypass key was not returned to its correct position before the key was removed. See <strong>Resetting an Authentication Device</strong> on page 102 for instructions on correctly resetting the device.</td>
</tr>
</tbody>
</table>
After the user authenticates at the MFP, an error message appears stating “access to copy job denied”.

A copy rule has been applied to the user and device. The user is not authorized to use the copy function on this device. The user can touch Yes or Exit to logout.

For more information on copy rules, refer to the Routing Rules chapter in the Equitrac Office and Express Administration Guide.

Device initialization failed

A common cause of device initialization failure is due to incorrect DNS configurations. To determine where the error has occurred, run the EQXeroXEIPRegistration.exe file located in the Equitrac Tools folder. This program will produce a verbose error description that will help you diagnose the problem. If DNS configuration is the problem, this file allows you to change DNS addresses into IP Address registrations.

Run the executable from a command prompt, followed by /h to view a list of options.

What trace logging settings are required by Support?

In case of failure to initialize Xerox devices, failure to initialize Xerox Secure Access Authentication devices, undesirable authentication behavior, or undesirable network accounting behavior, enable all XeroxDC items within the CAS and DCE logs.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the user authenticates at the MFP, an error message appears stating “access to copy job denied”</td>
<td>A copy rule has been applied to the user and device. The user is not authorized to use the copy function on this device. The user can touch Yes or Exit to logout. For more information on copy rules, refer to the Routing Rules chapter in the Equitrac Office and Express Administration Guide.</td>
</tr>
<tr>
<td>Device initialization failed</td>
<td>A common cause of device initialization failure is due to incorrect DNS configurations. To determine where the error has occurred, run the EQXeroXEIPRegistration.exe file located in the Equitrac Tools folder. This program will produce a verbose error description that will help you diagnose the problem. If DNS configuration is the problem, this file allows you to change DNS addresses into IP Address registrations. Run the executable from a command prompt, followed by /h to view a list of options.</td>
</tr>
<tr>
<td>What trace logging settings are required by Support?</td>
<td>In case of failure to initialize Xerox devices, failure to initialize Xerox Secure Access Authentication devices, undesirable authentication behavior, or undesirable network accounting behavior, enable all XeroxDC items within the CAS and DCE logs.</td>
</tr>
</tbody>
</table>